LA GESTIONE DEI RISCHI DI NON CONFORMITÀ CONNESSI AL FENOMENO CORRUTTIVO

Alessandro Biagioli, Carlo Regoliosi

ISSN 2611-9633
Working Papers (Dipartimento di Economia Aziendale)
[online]

Working Paper Numero 15, 2021
Collana del Dipartimento di Economia Aziendale

I Working Paper del Dipartimento di Economia Aziendale svolgono la funzione di divulgare tempestivamente, in forma definitiva o provvisoria, i risultati di ricerche scientifiche originali.
La loro pubblicazione è soggetta all'approvazione del Comitato Scientifico.
Per ciascuna pubblicazione vengono soddisfatti gli obblighi previsti dall'art. l del D.L.L. 31 agosto 1945 n. 660 e successive modifiche.
Copie della presente pubblicazione possono essere richieste alla Redazione.
Esemplare fuori commercio ai sensi della Legge 14 aprile 2004 n. 106.

SOMMARIO: 1. Il rischio di non conformità e le funzioni di compliance – 1.1. L'identificazione del rischio di non conformità – 1.2. La valutazione dei rischi di non conformità – 1.3. Il rapporto di interdipendenza tra le funzioni di compliance – 2. Modelli di gestione delle non conformità – 2.1. Introduzione ai modelli – 2.2. L'Enterprise Risk Management applicato ai rischi di non conformità – 2.3. Compliance programs e principali standard internazionali di riferimento – 2.4. Il rischio di non conformità connesso al fenomeno corruttivo – 2.5. Modelli orientati a riconoscere e gestire il fenomeno corruttivo all'interno dell'organizzazione – 3. Il ruolo del compliance manager – 3.1. Il ruolo di coordinamento del Responsabile della Prevenzione della Corruzione e della Trasparenza (RPCT) – 3.2. Il repertorio dei validi comportamenti nella ricerca di un nuovo equilibrio di poteri

ABSTRACT

Nel corso degli ultimi anni, molti eventi su larga scala un tempo considerati improbabili, distanti o isolati – quali la crisi economica, i cambiamenti climatici, la necessità di nuove fonti di approvvigionamento energetico, l'evoluzione tecnologica e la crisi pandemica – hanno cambiato il corso del *business* di molte organizzazioni ed il modo di approcciarsi alla gestione dei rischi emergenti.

Nel corso dell'ultimo ventennio, in particolare, orizzonte d'analisi fissato nel suo *dies a quo* dalla pubblicazione del d.lg. n. 231/2001, l'evoluzione del *compliance risk management* si è caratterizzata per il mutato approccio al rischio di non conformità non più calibrato esclusivamente su azioni volte ad evitare la finalizzazione di sanzioni e/o conseguenze reputazionali, ma anche sulle proprie caratteristiche preventive e difensive delle proprie operatività.

Ci si è resi conto, in definitiva, che l'esplorazione dei rischi emergenti è importante tanto quanto la gestione di quelli conosciuti.

La vera sfida che il *management* è chiamato ad affrontare, infatti, non concerne esclusivamente la sistematica eliminazione del rischio, in ogni sua forma, ma attiene al riconoscimento, alla valutazione e alla gestione differenziata delle sue manifestazioni per evitare conseguenze che potrebbero minare la sopravvivenza dell'organizzazione o determinare una significativa compromissione nel medio termine delle sue principali opportunità.

Dando per assodato e compreso che la mutevolezza dei fenomeni è, per sua stessa natura, portatrice di rischio, ci pare altrettanto chiaro che più un'organizzazione è complessa, più l'alea del rischio si presenta rilevante.

In tale contesto, assume particolare valore la prevenzione del fenomeno corruttivo. Sapersi approcciare a quest'ultimo attraverso strategie flessibili e dinamiche, che tengano conto di un contesto economico, normativo e sociale in continua evoluzione, diviene per tutto quanto detto strumento indispensabile per garantire il raggiungimento degli obiettivi dell'organizzazione.

Saper riconoscere e qualificare il rischio corruttivo all'interno del contesto organizzativo di riferimento richiede un'importante esperienza sul campo, parimenti esigita dalla conseguente assunzione di responsabilità che il giudizio professionale sotteso alla valutazione effettuata dalle strutture dedicate comporta.

In questo senso, la qualificazione del rischio, essendo attività intrinsecamente soggettiva, rappresenta già di per sé un momento critico di cui tener conto per valutare la tenuta dell'intero sistema.

Per ridurre tale soggettività, è necessario affidarsi a modelli comuni di prevenzione e gestione dei rischi di non conformità orientati alla riduzione di fenomeni dannosi per l'organizzazione e per la collettività, tra i quali quello corruttivo si pone come *primus inter pares*.

Tale affidamento, in particolare, evolve l'approccio dell'organizzazione alla prevenzione del fenomeno corruttivo, attraverso l'implementazione di un modello strutturato e dinamico,

costruito per garantire una valutazione del rischio non difforme per medesime situazioni e un'attività di monitoraggio costante sul lungo periodo.

Per tale ragione «il tema della *compliance* diventa oggi, ancora più che in passato, una sfida per qualsiasi organizzazione in quanto non è più confinato al rispetto delle norme ma ha assunto una valenza di natura strategica ed è sempre più legato al sistema di valori dell'impresa»[1], nonché al necessario investimento di risorse finanziarie, organizzative, formative e manageriali volta a far propria la cultura del rischio.

L'implementazione di un valido *compliance program*, idoneo a prevenire le conseguenze delle non conformità o della poca aderenza dei processi organizzativi alle disposizioni di legge, ai regolamenti, alle previsioni di autoregolamentazione ed alle fonti di *soft law*, dovrebbe partire dall'indagine del livello di maturità dei presidi esistenti e del livello di conoscenza, comprensione e consapevolezza delle tematiche di *compliance* all'interno dell'organizzazione, evitando che l'azione di conformità sia percepita come mera azione di natura burocratica legata all'astratto concetto del "dover fare".

Come confermato recentemente dall'ANAC, un mero approccio burocratico all'attività di costruzione della mappa dei processi interni, che miri alla realizzazione dell'adempimento piuttosto che all'analisi del fenomeno, andrebbe ad eludere – anche involontariamente – lo scopo della norma, che è quello di disporre di uno strumento utile, chiaro e comprensibile per la definizione degli obiettivi strategici in materia di prevenzione della corruzione, all'interno del documento di programmazione strategica legato all'organizzazione.

In tale contesto, si evidenzia il superamento della logica meramente repressiva del fenomeno corruttivo, in favore di un modello di prevenzione innestato all'interno del processo decisionale e strategico dell'organizzazione, in un rapporto di interconnessione con la *mission*, la *vision* ed i valori fondamentali della stessa.

È chiaro che un sistema così concepito, per produrre effetti positivi per la collettività, dovrà risultare non solo accettabile e proporzionato, ma anche e soprattutto sostenibile per l'organizzazione, attraverso l'individuazione di obiettivi sfidanti, sebbene non impossibili.

In questa prospettiva, il RPCT ha un ruolo fondamentale, che non si sostanzia nella sola attività di controllo di secondo livello derivante dalla necessità di poter garantire la conformità, l'uniformità e l'integrità dei buoni comportamenti, ma attiene anche alla diffusione di una coscienza collettiva, che dovrà essere percepita come unitaria dai dipendenti e da tutti i portatori di interesse che orbitano attorno all'organizzazione.

È anche per questo motivo che l'indagine sul livello di maturità di un *compliance program* non può prescindere dall'analisi sul repertorio dei comportamenti che dovrebbero far parte del corretto stile di *leadership* di un *compliance manager*.

È l'approccio condiviso alla prevenzione, alla gestione ed al monitoraggio delle esternalizzazioni negative il vero obiettivo a cui tendere per garantire l'idoneità del sistema di controllo interno.

---

[1] G. FIORI, *La compliance effettiva nelle imprese e nei gruppi aziendali*, in *La gestione della compliance*, cit., p. 9. L'autore evidenzia come la gestione dei rischi sia articolata non solo su un approccio scientifico che guida la definizione di metodologie e tecnicalità ma, anche, su un principio di buonsenso comune nel compimento delle attività, nel raggiungimento degli obiettivi, nella prevenzione e limitazione dei rischi e nella riduzione degli ostacoli.

Se non si muta l'approccio culturale alla materia, infatti, e non si cerca di diffondere una logica *win-win*[2], evitando comportamenti devianti che si pongono come fonti di esternalità negative, sarà sempre più difficile programmare, implementare e gestire un *compliance program* orientato alla creazione ed alla conservazione del valore all'interno dell'organizzazione.

[2] Come risulta dal contenuto *win-win situation* della rassegna del Sole24ore (reperibile in *argomenti.ilsole24ore.com/parolechiave/win-win-situation.html*), si tratta di un'espressione inglese (traducibile come vincente-vincente, oppure io vinco-tu vinci) che indica la presenza di soli vincitori in una data situazione. Per estensione si considera *win-win* una qualsiasi cosa che non scontenti o danneggi alcuno dei soggetti coinvolti. In economia è una negoziazione alla fine della quale entrambe le parti soddisfano i propri interessi.

1. IL RISCHIO DI NON CONFORMITÀ E LE FUNZIONI DI *COMPLIANCE*

1.1. *L'identificazione del rischio di non conformità*

All'interno del più complesso sistema di gestione dei rischi aziendali, la prevenzione del rischio normativo rappresenta un momento irrinunciabile nella conformazione dell'agire collettivo in direzione della legalità[3].

L'analisi giuridica di conformità rispetto ai *silos* di *compliance*, riconducibili ai differenti ambiti normativi di riferimento, è oggi parte integrante del processo decisionale e strategico del *top management* che, sin dalla fase di progettazione della strategia di impresa, deve adeguare lo stile ed i comportamenti dell'organizzazione alle pretese dell'ordinamento.

In tal modo è possibile attivare un circolo virtuoso, in un'ottica di *continuous monitoring*, volto ad assicurare l'implementazione di un «sistema automatico di riscontro utilizzato dal *management* per monitorare che le attività e i controlli operino secondo il disegno predefinito e le transazioni e i processi si svolgano secondo le procedure esistenti»[4].

Tra i diversi livelli di presidio del sistema di controllo interno, quelli cosiddetti di secondo, che tipicamente vengono affidati alle funzioni *lato sensu* di *compliance*, hanno l'obiettivo di assicurare la corretta identificazione e valutazione del rischio di conformità rispetto a leggi, regolamenti e previsioni di auto-regolamentazione.

Il principale scopo di tale livello di controllo è quello di presidiare il processo di individuazione, valutazione, gestione e controllo dei rischi di non conformità normativa, derivanti dall'operatività e dalla gestione dei processi dedicati al monitoraggio delle principali normative indagate.

Per tale ragione, i controlli di secondo livello si differenziano, sia dai controlli di linea (controlli di primo livello) – ovvero le verifiche svolte da chi pone in essere attività legate ad uno specifico processo –, sia dai controlli di terzo livello, che comunemente sono di competenza dell'*internal auditing*, al quale è tipicamente affidata l'attività di *assurance* complessiva dell'intero sistema di controllo interno.

L'attività di *compliance*, tuttavia, non ha ad oggetto solo la mera indagine sulla conformità dell'azione posta in essere dall'organizzazione rispetto alle leggi ma, in un'accezione più ampia, deve riguardare la fase di raccolta delle informazioni, le interviste effettuate agli *owners* interessati dal processo[5], l'analisi delle disposizioni contrattuali, il controllo degli

---

[3] In tema di prevenzione del rischio-reato C. PIERGALLINI, *Paradigmatica dell'autocontrollo penale (dalla funzione alla struttura del "MODELLO ORGANIZZATIVO" ex d.lgs. 231/2001)*, in *Le tipologie di colpa penale tra teoria e prassi* (incontro di studi organizzato dal CSM, Roma, 28 – 30 marzo 2011), p. 8.

[4] cfr. Associazione Italiana Internal Auditors, *Continuos auditing & continuous monitoring. Nuove opportunità da affiancare all'attività di Internal Auditing* (Workshop per i professionisti del settore manifatturiero), Roma, 15 aprile 2014.

[5] La *compliance* è definita anche come *«Investigations should comply with applicable laws and rules regarding gathering information and interviewing witnesses»* (cfr. The Istitute of Internal Auditors – The American Istitute of Certified Public Accountants – Association of Certified Fraud Examiners, *Managing the business Risk of Fraud: A Pratical Guide*, reperibile in www.acfe.com., p. 41).

standard professionali utilizzati, le politiche organizzative, le linee di indirizzo e le questioni etiche[6].

I recenti avvenimenti hanno dimostrato come il presidio sugli ambiti di conformità alle leggi, regolamenti e previsioni di autoregolamentazione, sia messo continuamente in discussione dalla mutevolezza dell'assetto normativo in molteplici ambiti.

In tale ottica, dunque, l'esplorazione dei rischi emergenti diviene fondamentale, così come la gestione dei rischi conosciuti.

Identificare e monitorare un rischio di non conformità quando l'evento si è già verificato, infatti, potrebbe non consentire all'organizzazione di intervenire tempestivamente per azzerare le esternalizzazioni negative determinate dall'evento.

1.2. *La valutazione dei rischi di non conformità*

Venendo all'analisi delle attività tipiche della funzione, è opportuno prendere le mosse da quella di *assessment*.

Questa attività consente di indagare la maturità dei presidi di *compliance* esistenti e di esaminare il livello di consapevolezza delle strutture in merito ai rischi collegati al mancato rispetto degli adempimenti applicabili al contesto di riferimento, valorizzandoli attraverso un'attività di *legal inventory* e di *alert* normativo[7].

Tale processo è parte integrante di una logica valutativa di tipo *risk based*, in cui lo specifico risultato dell'analisi dei presidi adottati sarà determinato: in termini di rischio inerente, dalle sanzioni applicabili in caso di accertata violazione e dagli eventuali danni derivanti dal mancato adempimento; in termini di rischio residuo, dall'analisi degli strumenti di controllo adottati per ridurre il verificarsi di tali eventi, in ragione dell'impatto e della probabilità.

Applicando una logica di valutazione orientata al rischio e metodologie comuni d'implementazione dei diversi standard di controllo, è possibile sviluppare un programma di *compliance* che miri fattivamente a ridurre l'esposizione della società alle discipline sanzionatorie domestiche e le conseguenze reputazionali nel mercato di riferimento, mediante l'adozione di linee di indirizzo e procedure interne sinergicamente strutturate per rendere i comportamenti aziendali conformi alle normative esistenti[8].

In un'accezione ormai condivisa, il rischio viene definito come «l'effetto dell'incertezza sugli obiettivi»[9].

---

[6] Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA), *Compliance Risk Management: Applying the COSO ERM Framework*, 2020, p. 5.

[7] Attività che tipicamente garantisce l'aggiornamento, l'analisi, il monitoraggio e le segnalazioni della normativa rilevante per gli ambiti di interesse. Questa attività consente, al contempo, di valutare la maturità dei presidi di *compliance* esistenti all'interno dell'organizzazione.

[8] Più in generale, in considerazione della necessità di adeguarsi a normative similari su ambiti analoghi o contigui, potrebbe essere opportuno definire dei *compliance programs* che consentano di ottemperare, in maniera efficace, a normative differenti (cfr. Confindustria, *Linee guida per la costruzione dei modelli di organizzazione, gestione e controllo*, 2004, p. 79).

[9] cfr. ISO 31000:2009 *Risk management – Principles and guidelines.*

Il raggiungimento degli obiettivi di *business* tipici dell'organizzazione è messo a repentaglio dall'effetto negativo che un singolo evento non adeguatamente gestito potrebbe generare.

In particolare, è possibile cogliere una duplice accezione del rischio: in primo luogo, come l'insieme degli effetti positivi (*upside risk*) che costituiscono un'opportunità di miglioramento dell'organizzazione interna e della *performance* aziendale, in termini di efficacia ed efficienza dei processi; in secondo luogo, come l'insieme di effetti negativi (*downside risk*) che vanno ad incidere direttamente sul *business* aziendale, determinando una riduzione dei profitti, variazioni significative nei mercati, impatti reputazionali non governabili e, nel peggiore dei casi, la mancata sopravvivenza dell'organizzazione nel mercato di riferimento[10].

Di conseguenza, la valutazione delle conformità, pur non annoverandosi all'interno della categoria "dell'obbligo giuridico", inserendosi invece nel più ampio ambito dei modelli volontaristici per la gestione degli adempimenti normativi, contribuisce in modo significativo alla salvaguardia degli obiettivi dell'organizzazione[11].

È indubbio che l'adozione di adeguati sistemi di valutazione delle non conformità stia assumendo una sempre maggiore centralità per le organizzazioni aziendali, anche e soprattutto per l'attenzione posta al tema dal legislatore e dalle Autorità di controllo.

In relazione alle possibili conseguenze di mancata conformità previste dalla normativa vigente nei diversi ambiti, l'analisi giuridica va declinata operativamente all'interno del funzionigramma delle specifiche unità chiamate a svolgere un'attività, al fine di garantire un efficace coordinamento, anche in materia di *risk assessment*[12].

In tal modo, l'organizzazione si apre alla prevenzione del rischio di non conformità del processo decisionale e produttivo, ponendo le basi per la creazione di un'infrastruttura etica[13].

Chi è posto in posizione apicale ha il compito di assicurare un'adeguata gestione del rischio – anche mediante l'adozione di modelli di prevenzione del rischio, non solo in ottica cautelativa, ma anche e soprattutto come strumenti di autoregolamentazione – allo scopo di: «1) mappare le aree esposte al rischio-reato e individuare i soggetti più esposti al rischio (soggetti apicali, middle management, dipendenti, ecc.); 2) forgiare regole cautelari

---

[10] S. BOZZOLAN e S. COSTANZO, *La compliance effettiva nelle imprese e nei gruppi aziendali Corporate Governance, sistemi di risk management e rischi di compliance* in *La gestione della compliance. Sistemi normativi e controllo dei rischi*, a cura di A. ADOTTI e S. BOZZOLAN, Roma, 2020, p. 15. Sul punto è chiarito che «adottando una differente prospettiva si può sostenere che l'attenzione verso il *downside risk* è nella prospettiva di "preservare il valore" mentre l'attenzione verso il *upside risk* è nella prospettiva di creare valore».

[11] Il risparmio di spese derivante dall'omessa adozione di un modello di organizzazione e gestione idoneo a prevenire il reato non integra il requisito dell'interesse o del vantaggio per l'ascrizione di responsabilità all'ente, non essendo obbligatoria l'adozione del *compliance program* da parte della società stessa. Cfr. Trib. di Tolmezzo, 23 gennaio 2012.

[12] È stato evidenziato come «le tematiche di *compliance* siano per loro natura "trasversali", esse si fondano infatti su aspetti normativi, talvolta settoriali e estremamente specifici, i quali identificano e definiscono l'oggetto e talvolta anche il campo d'azione, tuttavia la dimensione normativa resta a un livello speculativo se manca di una declinazione operativa in merito a come attuare una serie di presidi affinché le imprese possano efficacemente identificare, valutare, gestire (e quindi ridurre o annullare) il rischio di non essere *compliant* rispetto a normative, regolamenti e regole di autoregolamentazione», in A. ADOTTI e S. BOZZOLAN, *La gestione della compliance,* op. cit., p. 13.

[13] Molti economisti e giuseconomisti del '900 hanno analizzato gli impatti delle esternalità negative sul contesto sociale e l'importanza di valutare, nell'analisi costi benefici, gli impatti per la collettività. Su tutti cfr. R. H. COASE, *The problem of social coast*, *University of Virginia,* in *The Journal of LAW & ECONOMICS*, 1960, III.

orientate a ridurre il rischio-reato; 3) predisporre adeguati meccanismi di controllo sulla funzionalità del modello e sulla necessità di adeguamenti; 4) prevedere un sistema disciplinare rivolto a sanzionare i comportamenti devianti, implementato da meccanismi di scoperta/chiarimento degli illeciti»[14].

Un buon sistema di controllo interno permette, infatti, di supportare il processo di creazione e distribuzione di valore, con ciò tutelando l'interesse di tutte le parti sociali coinvolte nel processo.

Un sistema compartecipato che stimoli la condivisione, sia nella fase di definizione degli obiettivi, sia nella successiva e più delicata fase di valutazione dei risultati, contribuisce attivamente alla tutela del *business* e tende alla sistematica eliminazione dei rischi di non conformità. Un tale approccio richiede un forte *commitment* da parte del *management* aziendale a far propria una cultura di approccio al rischio come parte integrante della strategia dell'organizzazione.

Non a caso può essere individuato, come ulteriore corollario di un efficace sistema di *compliance*, il principio di adeguatezza degli assetti organizzativi interni che, sia nell'ordinamento interno, sia in quello europeo[15], permea l'azione degli organi di vertice delle società[16].

Considerata «(i) la mancanza di riferimenti normativi specifici, (ii) la molteplicità dei criteri/parametri che possono essere utilizzati e (iii) la necessità di calarsi di volta in volta nelle diverse realtà a cui tale concetto è riferibile»[17], non è possibile addivenire ad una nozione univoca e condivisa di "adeguatezza".

Ciononostante, la giurisprudenza prevalente ha chiarito che «un *compliance program* è adeguato nella misura in cui esso è ritagliato sulla specificità dell'impresa nel quale esso è adottato e, pertanto, qualora esso contempli procedure generiche, o addirittura lacunose, non potrà soddisfare le condizioni richieste dalla normativa[18]».

---

[14] C. PIERGALLINI, *op. loc. cit.*

[15] L'art. 24 del Regolamento (UE) 2016/679 (*General Data Protection Regulation* o GDPR) obbliga i titolari del trattamento ad effettuare l'analisi dei rischi ed a valutare l'adozione di misure di sicurezza tecniche e organizzative "adeguate". In particolare, il primo comma della norma sancisce che: «tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario».

[16] L'art. 2381, comma 3, cod. civ., in particolare, obbliga il Consiglio di amministrazione alla valutazione di adeguatezza dell'intero assetto organizzativo, amministrativo e contabile della società, nonché del generico andamento della gestione. Il medesimo onere, inoltre, è rimesso dall'art. 2403 cod. civ. al Collegio sindacale che, oltre a vigilare sull'osservanza delle leggi e dello statuto rispetto ai principi di corretta amministrazione, è tenuto proprio ad una valutazione di adeguatezza dell'assetto organizzativo.

[17] cfr. P. VERNERO, B. PARENA, M. F. ARTUSI, *Risk management, compliance program ed evoluzioni normative: l'organizzazione aziendale come strumento di prevenzione degli illeciti*, p. 5, 2018. Detti Autori, richiamando l'opera di V. BUONOCORE (*Adeguatezza, precauzione, gestione, responsabilità: chiose sull'art. 2381, commi terzo e quinto, del codice civile*, in Giur. comm., fasc.1, 2006, p. 5) rilevano che, dal punto di vista letterale, il termine "adeguatezza" ha diversi significati quali "commisurare", "comparare", "ragguagliare", ma non appare mai pienamente autosufficiente. Il termine necessita, infatti, di essere citato in rapporto con un altro elemento (categorie, grandezza, valori) che può essere rappresentato dalla "natura" e dalle "dimensioni" dell'impresa.

[18] A. BERNASCONI, *Razionalità e irrazionalità della Cassazione in tema di idoneità dei modelli organizzativi*, nota a Cass. pen., Sez. V, 30 gennaio 2014, n. 4677, in *Diritto penale e processo*, 2014, XIV, p. 1431.

1.3. *Il rapporto di interdipendenza tra le funzioni di compliance*

Per sua natura il rischio di *compliance*[19] presenta alcune caratteristiche tipiche: «è trasversale a tutta l'organizzazione aziendale, in quanto intimamente collegato alla natura e alle caratteristiche operativo-gestionali dell'attività di *business*; ha implicazioni strategiche, traducendosi nell'effettuazione di determinate scelte "di risposta" da parte del management; ha per l'impresa conseguenze economiche sia dirette, in termini di possibili sanzioni applicate, sia indirette, in termini di danno reputazionale e di immagine»[20].

In ragione di tali caratteristiche, l'implementazione del *compliance program* non può prescindere da un'adeguata collocazione delle strutture di *compliance* all'interno dell'organigramma aziendale che ne assicuri capacità di manovra, trasversalità e l'interdipendenza.

L'evidente rapporto di interdipendenza tra la funzione di controllo di secondo livello, gli organi preposti alla *governance* societaria (es. il Consiglio di Amministrazione, l'Organismo di Vigilanza ex d.lg. n. 231/2001 e il Collegio Sindacale) e le altre strutture del sistema di controllo interno (Internal auditing, direzione legale, direzione appalti, risorse umane etc.), facilita la diffusione della cultura aziendale per la prevenzione dei rischi di non conformità.

Rendere nota ai dipendenti l'esistenza di sinergie operative tra le diverse strutture che, nel loro operare combinato, costituiscono il sistema di controllo interno, permette ai dipendenti di comprendere, attraverso la diffusione della cultura del rischio con i tipici canali informativi dell'organizzazione (organigramma, funzionigramma, comunicazioni organizzative, ordini di servizio etc.), l'importanza del sistema di gestione delle non conformità e l'impegno del *management* nel garantire la gestione delle stesse.

Alla suddetta analisi segue, inevitabilmente, la necessità di dimensionare quantitativamente e qualitativamente l'organico della struttura di *compliance*, al fine di garantire il presidio delle attività, la distinzione chiara e funzionale delle responsabilità ed una ponderata distribuzione dei compiti.

Il livello di competenza e professionalità del personale allocato nelle strutture preposte al controllo interno contribuisce in modo cruciale alla validità del modello che, per sua stessa natura, interviene su molteplici aree di conoscenza, di esperienza e di capacità (*privacy*, *antitrust*, *cyber security*, tutela del risparmio e disciplina dei mercati finanziari, anticorruzione e trasparenza, antifrode e antiriciclaggio etc.).

Possedere una formazione trasversale consente di operare attivamente sul sistema implementato, garantendo immediatezza nell'inserimento di interventi correttivi e maggiore capacità di "anticipazione" delle possibili azioni di mitigazione che necessitano di essere inserite. Le competenze differenziate e complementari del personale assegnato alla

---

[19] A. QUARANTA (*Che cosa si intende per "rischio compliance" e cosa fa il "compliance manager"?*, in *Ambiente & sviluppo,* 2020, XI, p. 916), ad esempio, chiarisce che «per "rischio *compliance*" si intende il rischio di incorrere in sanzioni giudiziarie o amministrative, perdite finanziarie rilevanti o danni di reputazione in conseguenza di violazioni di norme imperative o *mandatory* (di legge o di regolamenti); di norme autoregolamentazione o *voluntary* (es. statuti, codici di condotta, codici di autodisciplina, norme di settore); di comportamenti scorretti (*social and human behavioral*)».

[20] F. ACCARDI, *La compliance effettiva nelle imprese e nei gruppi aziendali*, in *La gestione della compliance*, cit., pp. 39 e 40. L'Autore aggiunge altresì che, sebbene attinenti a tematiche diverse i rischi di non conformità, presentano «interconnessioni tali per cui nella maggior parte dei casi i rischi si presentano non da soli, bensì in forma associata e con complesse relazioni reciproche».

struttura di *compliance* consentono, inoltre, di affrontare la "schizofrenia legislativa" tipica del nostro ordinamento.

In prospettiva, al fine di poter garantire la multidisciplinarietà in un contesto in continua evoluzione tecnologica, è sempre più evidente la necessità di dover affiancare, ai professionisti del mondo giuridico amministrativo, tecnici in grado – lì dove possibile, ragionevole ed efficiente – di "tradurre" le previsioni normative della legislazione vigente in un linguaggio informatico[21].

[21] In merito, si segnala il 5° *working paper* della collana scientifica dell'Autorità Nazionale Anticorruzione (ANAC), *Data analysis e costruzione di indicatori di rischio corruzione per la Banca Dati Nazionale dei Contratti Pubblici*, a cura di M. TROÌA, che propone la costruzione dei c.d. *"corruption indicator score"* per l'intercettazione e l'analisi dei rischi corruttivi in materia di appalti pubblici, attraverso l'implementazione di algoritmi basati su variabili quantitativo/qualitative (es: numero di partecipanti, tipologia di scelta del contraente, modalità di aggiudicazione) e variabili legate al tempo (per analizzare i tempi che effettivamente intercorrono tra la pubblicazione di un bando e la data di effettiva aggiudicazione, prendendo in considerazione alcuni elementi: data di pubblicazione, data di scadenza, data di aggiudicazione definitiva, data di stipula del contratto, data di inizio definitiva, data del termine contrattuale e data di ultimazione lavori). A valle del lavoro, inoltre, l'utilizzo dei *corruption indicator score* viene suggerito sia in considerazione della semplicità con cui possono essere valorizzati, sia per la possibilità di estendere alle variabili proposte le specificità dell'organizzazione.

2. MODELLI DI GESTIONE DELLE NON CONFORMITÀ

2.1. *Introduzione ai modelli*

La logica dei *framework* nasce dall'esigenza di poter gestire il rischio attraverso metodologie comuni di controllo[22].

L'utilizzo di tali programmi fa parte di quel processo evolutivo che individua nella gestione dei rischi una fonte di opportunità per le aziende. Il paradigma storico dell'esistenza dei modelli è l'esperienza americana dei *compliance programs* introdotti al fine di promuovere la conformità e l'etica[23].

Lo sviluppo dei modelli c.d. *business oriented* si basa sull'analisi dei possibili fattori di crisi del mercato di riferimento, in un'ottica di valutazione trasversale di tipo *risk based*, che riguarda l'organizzazione nel suo insieme ed i singoli processi.

La gestione integrata dei rischi diviene un tema di primaria rilevanza nelle strategie dell'organizzazione, poiché consente a quest'ultima di orientare gli assetti organizzativi interni alle effettive esigenze del momento, di ridefinire l'immagine aziendale all'occorrenza e di competere nel mercato di riferimento sul lungo periodo.

L'utilizzo dei *framework* e dei sistemi *multicompliance* proietta l'analisi oltre il tradizionale approccio di *risk management*[24], favorendo l'adozione di sistemi "comuni", ed al contempo "customizzabili", volti ad ottimizzare gli assetti di *governance* interni e la salvaguardia degli obiettivi di *business* sul lungo periodo.

Nel contesto moderno una buona *governance* non può prescindere da un sistema di controllo interno composto da regole, procedure e modelli che consentano di individuare, misurare e gestire i principali rischi di non conformità.

Nell'ottica di un comune approccio metodologico, possono essere individuati sistemi di controllo strutturati su matrici integrate ed implementate, che tengano conto sia degli obiettivi perseguiti dall'organizzazione, sia delle esigenze legislative a cui le stesse sono chiamate a conformarsi.

Punto di forza di tali modelli è la loro applicabilità – pur con i necessari momenti di customizzazione – ad ogni tipologia di organizzazione, in considerazione della natura, della dimensione, della complessità organizzativa e del contesto di mercato in cui la stessa opera.

---

[22] Come indicato dall'Associazione Italiana Internal Auditors (www.aiiaweb.it), gli Standard definiscono il controllo come «qualsiasi azione intrapresa dal management, dal board o da altri soggetti per gestire i rischi ed aumentare le possibilità di conseguimento degli obiettivi e dei traguardi stabiliti. Il management pianifica, organizza e dirige l'esecuzione di iniziative in grado di fornire una ragionevole sicurezza sul raggiungimento di obiettivi e traguardi».

[23] Per ulteriori approfondimenti, cfr. United States Sentencing Commission, *Federal Sentencing Guidelines for Organizations*, 1991, reperibile in https://www.ussc.gov/guidelines e successive linee guida organizzative.

[24] Il *risk management*, come evidenziato da P. VERNERO, B. PARENA, M. F. ARTUSI (*op. cit.*, p. 2), può essere definito come un approccio metodologico finalizzato a «individuare e valutare tutte le fonti di rischio legate all'attività dello stesso, per poi trattarle e gestirle attraverso gli strumenti più consoni, personalizzandoli a seconda delle esigenze e delle necessità aziendali, nel rispetto degli obiettivi e delle strategie dell'impresa».

La logica dei *compliance programs*, in realtà, ha per lungo tempo interessato le organizzazioni in ragione della possibilità di dimostrare la propria estraneità rispetto alla commissione di fatti illeciti, in un'ottica di prevenzione del "rischio-reato".

L'introduzione nel nostro ordinamento del d.lg. 8 giugno 2001 n. 231, emanato in conformità a quanto previsto dalla normativa comunitaria, «ha generato una vera e propria rivoluzione copernicana nell'ordinamento giuridico italiano segnando un passaggio culturale di fondamentale importanza per le imprese, promuovendone "l'organizzazione" come strumento per garantire la trasparenza e la legalità dell'agire imprenditoriale»[25].

Tale provvedimento ha posto, di fatto, le fondamenta per una modalità di organizzazione, gestione e controllo «per un verso semplice, organica ed autoregolamentata e, per altro verso, idonea a garantire una conduzione aziendale efficace e trasparente in un contesto di continuità di medio e lungo termine e coerentemente con gli obiettivi strategici che ciascuna realtà persegue»[26].

Proprio il concetto di organizzazione come "strumento" ha portato all'evoluzione dei modelli comuni di gestione dei rischi in diversi ambiti.

Non a caso, la mancata o l'inefficace adozione del Modello di Organizzazione e Gestione, previsto dal d.lg. n. 231/2001, permette «di rilevare il significato dell'esercizio generale del potere di organizzazione in rapporto al reato, sia dal punto di vista del difetto (oggettivo) di organizzazione, e quindi dal punto di vista del comportamento dell'ente, sia da quello dell'atteggiamento complessivo di quest'ultimo, in un'ottica propriamente soggettivizzante, alla quale non è improprio riportare anche un concetto di "volontà", sia pure adattato alle caratteristiche e peculiarità dell'ente»[27].

Tale disciplina ha sollevato diverse criticità sulla configurabilità della responsabilità dell'ente da reato come *tertium genus*[28] che «coniuga i tratti essenziali del sistema penale e di quello amministrativo nel tentativo di contemperare le ragioni dell'efficacia preventiva con quelle, ancor più ineludibili, della massima garanzia» riconosciuta all'organizzazione, nel caso in cui l'adozione del modello risulti corrispondente ai requisiti previsti dalla legge[29].

Le esigenze di corrispondenza così delineate e tipiche di un approccio *audit society* – dove la ricerca di una mera corrispondenza della "lettera" rispetto al dettato normativo ci restituisce una sensazione di sfiducia riguardo ai contenuti riportati ed alla loro esaustività – rischiano,

---

[25] M. ASCIONE, *La responsabilità amministrativa degli enti ex d.lgs. 231/01 e l'atteso ingresso dei reati tributari*, in *La Nuova Procedura Civile*, 2019, IV, par. I.

[26] E. LUNGARO, C. PAPA e C. REGOLIOSI, *Il sistema dei controlli delineato dalla "231" - Le opportunità della correlazione tra l'Organismo di Vigilanza e la Funzione di compliance … verso una compliance 2.0*, 2019, p. 1.

[27] A. FIORELLA e N. SELVAGGI, *Compliance programs e dominabilità "aggregata" del fatto. Verso una responsabilità da reato dell'ente compiutamente personale*, Relazione al Congresso italo-spagnolo, Università degli Studi di Milano, 29 – 30 maggio 2014, pubblicata in *Dir. pen. cont.*, 2014, III-IV, p. 112.

[28] L'apparato normativo introdotto nell'ordinamento con il d.lg. 231/2001, prevede, di fatto, un sistema sanzionatorio che «al di là della terminologia (responsabilità amministrativa) utilizzata dal Legislatore, è di natura essenzialmente penale perché comuni sono gli intenti (tutela di elevati valori di interesse pubblico) e comune è il meccanismo procedimentale e sanzionatorio, pur dovendo quest'ultimo necessariamente considerare le specificità proprie di soggetti diversi dalle persone fisiche (per la loro connotazione appunto di "entità non fisiche") che non ne rende possibile la completa assimilazione quanto ai caratteri effettuali». E. LUNGARO, C. PAPA e C. REGOLIOSI, *op.cit.*, p. 2.

[29] cfr. Relazione ministeriale al d.lg. n. 231/2001.

tuttavia, di determinare in concreto l'applicazione *tout court* delle norme senza una profonda analisi delle reali esigenze dell'organizzazione.

La possibile preminenza della forma rispetto alla sostanza, inoltre, rende difficile immaginare meccanismi di *accountability* il cui funzionamento non dipenda dall'esclusiva analisi di adeguatezza organizzativa dell'ente rispetto al disposto normativo, riducendo la valutazione sull'inidoneità o meno del modello di organizzazione, gestione e controllo al realizzarsi o meno di una delle fattispecie di reato previste nell'ampio catalogo dei reati presupposto identificati nel d.lg. 8 giugno 2001 n. 231.

Occorre dare atto al legislatore del 2001, di aver inserito all'interno dell'ordinamento un modello comune di prevenzione del "rischio-reato"[30], con l'obiettivo dichiarato di implementare l'adozione di regole di comportamento, volte ad orientare l'agire comune verso un sistema di prevenzione e non di mera repressione, realizzando «la dissociazione tra la responsabilità (la colpevolezza) della persona fisica e quella dell'ente collettivo nel cui interesse la prima ha agito»[31].

2.2. *L'Enterprise risk management applicato ai rischi di non conformità*

Il più significativo modello internazionale per la valutazione del sistema di controllo interno è l'*Enterprise Risk Management (ERM)*, un «processo posto in essere dal Consiglio di Amministrazione, dal management e da altri operatori della struttura aziendale; utilizzato per la formulazione delle strategie in tutta l'organizzazione; progettato per individuare eventi potenziali che possono influire sull'attività aziendale, per gestire il rischio entro i limiti del rischio accettabile e per fornire una ragionevole sicurezza sul conseguimento degli obiettivi aziendali»[32].

Con l'ERM si passa dal "modello di gestione dei rischi" ad un effettivo "processo orientato al rischio"[33]. In principio, con il "COSO I"[34], poi aggiornato nel 2013, è stato elaborato un primo *internal control framework* di riferimento per i vertici aziendali, seguito nel decennio

---

[30] Tra le attività che sono state sviluppate dal Gruppo di lavoro *Anti-corruption Task Force*, con l'obiettivo di individuare strumenti di prevenzione nel mondo degli affari con riferimento ai fenomeni corruttivi nei paesi appartenenti al *G20 - Anti-Corruption Working Group (ACWG)*, l'esito dell'indagine condotta da Confindustria nell'aprile 2017, contenuta nel report *Indagine modelli organizzativi 231 e anticorruzione,* a cura di Confindustria Affari Legislativi e TIM Direzione Compliance – Compliance 231 e Chief Pricing Office – Quality, ha evidenziato che l'87% delle imprese partecipanti conosce la disciplina contenuta nel d.lg. 231/2001. Tra dette imprese, che rappresentano la quasi totalità delle imprese di più grandi dimensioni (con oltre 250 dipendenti o con fatturato superiore a 250 milioni di euro), soltanto 16 su 45 (il 36%) ha dichiarato di aver adottato il modello organizzativo, mentre, la maggior parte delle restanti imprese (22 su 29), ha dichiarato di volerlo adottare. Cfr. Confindustria, *Indagine modelli organizzativi 231 e anticorruzione*, 2017, p. 6.

[31] C. PIERGALLINI, *op. loc. cit.*

[32] Definizione del *Committee of Sponsoring Organizations (COSO) della Treadway Commission*, reperibile in www.aiiaweb.it.

[33] Obiettivo di un buon sistema di *risk management* non è l'eliminazione totale del rischio, resa impossibile dalla mutevolezza dei contesti di riferimento (es: economico, ambientale, sociale, normativo etc.), quanto, piuttosto, una coerente e sistematica gestione degli stessi. L'ERM rappresenta lo «strumento con cui il management analizza gli eventi aziendali ed identifica, tra questi, quelli potenzialmente negativi, valutandone l'impatto sul raggiungimento degli obiettivi prefissati», S. BOZZOLAN e S. COSTANZO, *op. cit.*, p. 28.

[34] Il COSO Framework del 1992 ha inglobato, in un'ottica progredita, il controllo interno sulle attività operative, sulle informazioni e sulle conformità a leggi, regolamenti e previsioni di autoregolamentazione (azioni di *compliance*) (v. *infra* nota 32).

successivo da altri importanti atti, come il *Sarbanes - Oxley Act*[35] (SOA) ed il c.d. *internal control framework - ERM COSO II* del 2004[36].

Nel modello ERM COSO II, alle tre categorie di obiettivi (*operations*, *reporting* e *compliance*) già previste[37], è stata aggiunta la categoria degli "obiettivi strategici" che devono essere considerati nella trattazione e nella gestione dei rischi aziendali ed è stata ampliata la componente riguardante il *risk assessment* all'interno del processo di controllo, alla quale sono state aggiunte: l'identificazione degli obiettivi, l'identificazione degli eventi, la valutazione dei rischi e la risposta ai rischi[38].

Con l'obiettivo di massimizzare il valore all'interno dell'organizzazione, con il COSO ERM II l'attenzione si sposta da un procedimento sequenziale di controllo del rischio all'introduzione di un approccio orientato all'identificazione ed alla gestione dei rischi – che possono potenzialmente pregiudicare il raggiungimento degli obiettivi di *business* – disancorato da mere logiche di processo e dalla sola analisi *ex post* di fattori esogeni non prevedibili. Con l'implementazione di detto modello, la gestione dei rischi in termini di accettabilità e tollerabilità diviene strumento strategico per il *management* al pari delle altre categorie di obiettivi di *operations*, *reporting* e *compliance*[39].

---

[35] Come risulta dall'Enciclopedia Italiana Treccani (Dizionario di Economia e Finanza, 2012), si tratta della «legge emanata il 30 luglio 2002 dal governo degli Stati Uniti in risposta agli scandali contabili della Enron, della Tyco e di altre società, con lo scopo di ristabilire la fiducia della nazione e del mondo, particolarmente degli investitori nel settore societario, fissando nuovi codici di autoregolamentazione e obblighi di legge. Tali obblighi riguardano: la certificazione di tutte le informazioni finanziarie; la trasparenza delle scritture contabili; la predisposizione di controlli interni per la regolarità e la tracciabilità delle informazioni finanziarie; la responsabilità personale e oggettiva del CEO (Chief Executive Officer) e del CFO (Chief Financial Officer) per l'informativa di bilancio; l'aumento delle pene per il falso in bilancio e altri illeciti fiscali; la costituzione del Public Company Accounting Oversight Board, ossia un consiglio di vigilanza sui bilanci delle aziende quotate».

[36] Al cubo sono state aggiunte ulteriori componenti. È stata inserita la dimensione degli *objective setting*, la sezione dedicata al risk assessment è stata suddivisa nelle tre componenti che descrivono le fasi in cui si articola tipicamente un'attività di *risk management* (*event identification; risk assessment; risk response*) ed è stata estesa l'attività di analisi all'intera organizzazione (*legal entities, divisioni, business units e subsidiaries*).

[37] Nella sua versione originale il cubo tridimensionale illustrava sulla prima "faccia" il collegamento tra tre categorie di obiettivi (*operations*, *reporting* e *compliance*) e le 5 componenti del processo di *risk management* della seconda "faccia" (*Control environment, Risk assessment, Control Activities, Information & Communication, Monitoring Activities*). Sulla terza "faccia", invece, erano rappresentati gli ambiti di intervento tipici dell'organizzazione interna aziendale (*entity level, division, operation unit e function*).

[38] Tali quattro fasi di analisi del rischio si possono sintetizzare come di seguito rappresentato: l'identificazione degli obiettivi che l'organizzazione intende perseguire (*objective setting*); l'identificazione degli eventi che possono interferire con il perseguimento degli obiettivi e la loro definizione in termini di opportunità e rischio (*Event Identification*); l'attività di valutazione dei rischi (*Risk Assessment*). La valutazione dovrà essere effettuata sia in termini di probabilità e impatto, sia indagando distintamente l'alea del rischio inerente (rischio in assenza di qualsiasi intervento di riduzione) e del rischio residuo (il livello di rischio dopo aver attuato interventi di riduzione); l'attività di risposta ai rischi emersi a seguito del *risk assessment* (*Risk Response*) che, principalmente, verrà effettuata mediante la definizione di azioni di azzeramento, mitigazione dei rischi ed in termini di costi benefici oggetto di specifica valutazione da parte del *management*.

[39] Ad ogni buon conto va detto che l'integrazione del Modello 231 con gli altri sistemi di gestione introdotti dall'organizzazione, come evidenziato da P. Vernero, B. Parena, M. F. Artusi (op. cit., p. 14 e ss.), rappresentando una tecnica di controllo della criminalità di impresa del tutto nuova che affida all'organo giudicante una valutazione sull'adeguatezza organizzativa dell'ente, tutti connessi ad un più lato concetto di compliance, potrebbe «quindi rappresentare il valore aggiunto che trasforma il sistema di valutazione dei rischi, sin qui considerato come risultato dell'integrazione gestionale, in un vero e proprio strumento strategico, inserito in un sistema di governance: i protocolli in esso descritti si basano infatti su una serie di componenti di un sistema di controllo preventivo che dovranno essere attuate per garantire l'efficacia del Modello stesso».

L'ERM COSO II è stato a sua volta rinnovato nel 2017[40]. Il nuovo *framework* denominato *Enterprise Risk Management – Aligning Risk with Strategy and Performance*, anche mediante una diversa rappresentazione grafica a spirale, stressa alcuni concetti, ponendo in risalto il legame tra strategia e *performance*.

L'aggiornamento del 2017, inoltre, ha sostituito il significato di controllo interno – in questo allineando anche il glossario ai nuovi contenuti – in favore di un più ampio concetto di gestione del rischio quale perimetro più ampio, strettamente legato alla gestione ed ai suoi obiettivi.

Più precisamente, il nuovo *framework* evidenzia l'importanza di considerare il rischio, sia nel processo di definizione della strategia, sia nella guida delle prestazioni, migliorando l'allineamento tra queste ultime e l'ERM.

In questa nuova accezione, l'ERM non deve essere considerato come una funzione, un dipartimento o un processo, bensì come «la cultura, le capacità e gli strumenti, integrati con la strategia e l'operatività, su cui le organizzazioni fanno affidamento per gestire i rischi nel processo di creazione, mantenimento e realizzazione del valore»[41].

La mutazione del focus del *framework*, immediatamente percepibile dal passaggio grafico da un cubo a tre dimensioni ad un diagramma a nastri elicoidali, che intrecciano cinque elementi nel corso del ciclo di vita di un'organizzazione (*governance & culture, strategy & objective setting, performance, review & revision, information communication and reporting*)[42], vuole evidenziare la sinergia tra la gestione del rischio e le strategie aziendali, al fine di massimizzare la *performance* nel mercato di riferimento in coerenza con la *mission* e la *vision* aziendale[43].

In altre parole, dove non c'è rischio non c'è impresa, da cui consegue che la logica del minimizzare non può essere l'unica soluzione, l'unico modo di fronteggiare eventi dall'esito soggetto a non perfetta prevedibilità. Il cuore della vicenda si sposta quindi dal controllo volto a minimizzare, alla puntuale definizione degli obiettivi e delle quote di rischio accettabili in funzione di detti obiettivi, da un lato, e dei *requirement* normativi, dall'altro.

I cinque componenti del nuovo *framework* sono supportati da una serie di principi che, partendo dall'analisi della *governance*, valorizzano la strategia aziendale e le attività di monitoraggio.

Tali principi descrivono pratiche che possono essere variamente applicate ad organizzazioni diverse, prescindendo dalle dimensioni e dal settore di riferimento; l'adesione agli stessi può

---

[40] *Enterprise Risk Management – Integrating with Strategy and Performance*, settembre 2017, che riflette l'evoluzione del rischio di impresa integrando i principi introdotti nella versione precedente.

[41] Definizione del *Committee of Sponsoring Organizations (COSO) della Treadway Commission*, in *Enterprise risk management: un profondo cambiamento nella gestione del rischio d'impresa*, a cura di F. D. ATTISANO, ottobre 2019, reperibile in www.riskcompliance.it.

[42] F. D. ATTISANO, *op. cit.*

[43] L'Enciclopedia Italiana Treccani (Dizionario di Economia e Finanza, 2012) definisce il termine "*mission*" come quello «che esprime l'identità e gli obiettivi dell'azienda o dell'organizzazione, al fine di comunicarne l'orientamento strategico di fondo e la sua connessione con la visione e i valori di riferimento. Nella m. vengono spiegate la ragion d'essere dell'organizzazione e la giustificazione stessa della sua esistenza: l'attività svolta, i mercati o i clienti serviti, le risorse e le competenze distintive, i fattori che la contraddistinguono dalle altre. L'esplicitazione della m. supporta il processo di formulazione della strategia e indica in modo più preciso gli scopi che l'organizzazione si prefigge, favorendo comportamenti coerenti nel tempo che, secondo alcuni tra i più autorevoli studiosi di strategia (G. Hamel e C.K. Prahalad), portano a risultati superiori». Nel linguaggio gestionale la *vision* è la proiezione degli ideali, dei valori e delle aspirazioni della azienda nel futuro.

fornire al *management* ed al Consiglio di Amministrazione una ragionevole aspettativa che l'organizzazione comprenda e si impegni a gestire i rischi associati al proprio *business*[44].

Fonte: *Coso Enterprise Risk management: integration with strategy and Performance*, USA, 2017.

Con l'implementazione dell'ERM[45], il *management* «massimizza il valore quando formula strategie e obiettivi al fine di conseguire un equilibrio ottimale tra *target* di crescita e di redditività e rischi conseguenti, e quando impiega in modo efficiente ed efficace le risorse nel perseguire gli obiettivi aziendali»[46] tra cui, inevitabilmente, vanno considerati anche gli obiettivi di conformità a leggi, regolamenti e previsioni di autoregolamentazione.

[44] cfr. *Enterprise Risk Management Integrating with Strategy and Performance. Executive summary,* giugno 2017, p. 7.

[45] Come osservato in *La gestione del rischio aziendale. ERM – Enterprise Risk Management: modello di riferimento e alcune tecniche applicative,* edizione italiana a cura della Associazione Italiana Internal Auditors (AIIA) e PricewaterhouseCoopers, edita da Il Sole 24ore, 2006, p. 5, l'ERM, in questo contesto, «non è concepito come un mero procedimento strettamente sequenziale, nel quale un componente influisce solo sul successivo. Si tratta, invece, di un processo interattivo e multidirezionale in cui ogni componente può influire o influisce su un altro componente, indipendentemente dalla sequenza del processo».

[46] Come osservato in *La gestione del rischio aziendale. ERM – Enterprise Risk Management: modello di riferimento e alcune tecniche applicative,* edizione italiana a cura della Associazione Italiana Internal Auditors (AIIA) e PricewaterhouseCoopers, edita da Il Sole 24ore, 2006, p. 5, l'ERM, in questo contesto, «non è concepito come un mero procedimento strettamente sequenziale, nel quale un componente influisce solo sul successivo. Si tratta, invece, di un processo interattivo e multidirezionale in cui ogni componente può influire o influisce su un altro componente, indipendentemente dalla sequenza del processo».

2.3. *Compliance program e principali standard internazionali di riferimento*

L'esigenza di prevenire rischi di non conformità ha ampliato il ruolo dei modelli organizzativi e dei *compliance programs* all'interno delle organizzazioni, quali strumenti di *corporate social responsibility*[47].

La loro adozione consente di sviluppare all'interno dell'organizzazione, attività di *law enforcement* per evitare di subire le conseguenze delle violazioni di conformità e per limitare l'impatto derivante dalle possibili esternalizzazioni degli effetti negativi dell'evento sulla collettività.

È evidente come l'implementazione dei *compliance programs* consenta alle organizzazioni d'inserire misure ragionevoli per garantire sia il presidio del sistema, sia la valutazione periodica di efficacia del programma di conformità ed etica incidendo, al contempo, sulla strategia aziendale con un approccio *by design* e *by default*, che introduce criteri di prevenzione dei rischi di non conformità, dalla fase di avvio delle progettazioni, alle successive fasi di valutazione[48].

Come già evidenziato nella trattazione, il rischio di conformità generalmente attiene a violazioni di leggi, regolamenti e previsioni di autoregolamentazione, ma può anche riguardare disposizioni contrattuali, standard professionali, politiche organizzative e questioni etiche, a seconda del settore a cui appartiene l'organizzazione.

Una pedissequa applicazione di tali previsioni, tuttavia, non è sufficiente, occorrendo altresì una continua azione di rinnovamento che tenga conto della mutevolezza dei contesti. Applicare una regola interna nella mera convinzione che questa sia ancora conforme al precetto previsto dall'ordinamento potrebbe, infatti, determinare un susseguirsi di comportamenti illegittimi ed esporre l'organizzazione ad inefficienze e, nel peggiore dei casi, a ulteriori rischi.

Allargando il ragionamento all'utilizzo diffuso dei modelli di gestione, si può osservare che l'obiettivo di un buon sistema di controllo interno non è tanto quello di rilevare difetti e prevedere azioni di mitigazione, quanto, piuttosto, quello di contribuire al processo di creazione e distribuzione di valore, riconducendo i processi e le attività ad un livello di rischio accettabile[49].

Ciò posto, è logico pensare che tale aspettativa, se ragionata all'interno di un sistema di ERM applicato alla *compliance*, possa risultare facilmente compromessa dalla mancata applicazione delle disposizioni vigenti per singolo ambito di indagine e dai repentini mutamenti della norma.

Va rilevato, in realtà, che le linee guida riconducibili a programmi di *compliance & ethics* sono spesso circoscritte ad aree legislative che indagano specifici ambiti su cui

---

[47] R. H. COASE, *op. cit.*

[48] Questo tipico approccio già adottato in ambito *privacy* (la 32° conferenza mondiale dei garanti in materia di *privacy* aveva adottato tale definizione coniata da Ann Cavoukian, *Privacy Commissioner* dell'Ontario) è riscontrabile nelle logiche di prevenzione di un *compliance program*.

[49] Secondo la UNI ISO 31000:2018, standard internazionale, disegnato dall'*International Organization for Standardization (ISO)* allo scopo di supportare le aziende nella definizione e implementazione di programmi di *Risk Management* adeguati ed efficienti, attraverso la formulazione di un set di principi e linee guida per l'analisi, la valutazione ed il monitoraggio dei rischi.

l'ordinamento, per ragioni diverse, anche legate al momento storico ed a particolari eventi, pone specifica attenzione (es: *antitrust*, anticorruzione[50], ambiente, *privacy*[51], etc.).

Pertanto, mentre in passato l'attività di *compliance* è stata indagata all'interno del più ampio sistema dei controlli interni: più precisamente, nella dimensione dedicata al processo di *risk management*, l'applicazione dell'ERM agli specifici rischi di non conformità sembra emancipare l'attività della funzione e valorizzare la gestione di questi particolari rischi con modelli "vestiti" sulle attività tipiche di quest'ultima.

Tuttavia, in assenza di una definizione universalmente accettata riguardante lo scopo di un valido *Compliance & Ethics Program*, la gestione dell'attività può presentare peculiarità tipiche dell'organizzazione e necessitare di interventi "customizzati".

Di conseguenza, preso atto che l'analisi delle non conformità in alcuni ambiti può essere svolta sotto la supervisione di strutture organizzative non tipicamente riconducibili alle funzioni preposte al controllo interno delle società (es. direzione legale, direzione risorse umane, direzione appalti, etc.), va chiarito che la funzione di *compliance* dovrà comunque assicurare un'attività sinergica di prevenzione delle non conformità o almeno assistere le strutture preposte nella gestione dei relativi rischi in caso di manifesta necessità[52].

È evidente, a questo punto, come il sistema di controllo interno per il monitoraggio delle non conformità, debba favorire l'utilizzo di strumenti comuni accelerando la cooperazione tra le funzioni preposte tramite un approccio *multicompliance*.

L'evoluzione dei *framework* ben si addice alla gestione di tali tematiche poiché, nella logica di gestione dei rischi, i principali standard internazionali hanno sviluppato metodologie comuni di controllo per fornire alle organizzazioni, in un'ottica integrata, idonei strumenti per l'identificazione, la valutazione e la gestione di tali rischi.

La norma internazionale ISO 19600:2014 (oggi ritirata) e l'attuale ISO 37301:2021[53], sviluppate dall'Organizzazione internazionale per la standardizzazione (ISO), hanno

---

[50] Le linee guida contenute nel *Bribery Act*, emanato nel 2010 dal Ministero della Giustizia del Regno Unito, sono strettamente collegate alle *U.S. Federal Sentencing Guidelines* per la previsione di procedure basate sui seguenti principi comuni: *top-level commitment; risk assessment; due diligence; communication (including training); monitoring and review*. Anche l'Organizzazione internazionale per la standardizzazione ha pubblicato lo standard "ISO 37001:2016, *Anti-bribery management systems*", sui sistemi di gestione anticorruzione. Questo include una più ampia previsione di attività programmatiche per la prevenzione del fenomeno corruttivo: *performance of a bribery risk assessment; leadership and commitment to the anti-bribery; management system; establishment of an anti-bribery compliance function; sufficient resources provided for the anti-bribery management system; competence of employees; awareness and training on anti-bribery policies; due diligence in connection with third-party business associates and employees; establishment and implementation of anti-bribery controls; internal audit of the anti-bribery management system; periodic reviews of the anti-bribery management system by the governing body*.

[51] Le leggi sulla protezione dei dati e sulla *privacy* generalmente differiscono da un paese all'altro, ma spesso hanno effetti diretti o indiretti sui programmi C&E, come rilevato in *Compliance risk management: applying the COSO ERM framework*, cit., p. 3.

[52] I rischi relativi alle risorse umane e al diritto del lavoro possono essere gestiti interamente all'interno della funzione dedicata, ovvero dalla funzione di *compliance* preposta al monitoraggio dei rischi (cfr. *Compliance risk management: applying the COSO ERM framework*, cit., p. 5).

[53] La norma internazionale "ISO 37301:2021, *Compliance management systems — Requirements with guidance for use"*, pubblicata ad aprile 2021, elaborata dal Comitato Tecnico ISO / TC 309 Governance delle organizzazioni, si propone come valido strumento operativo adattabile a tutti i contesti organizzativi a prescindere dalle dimensioni, dalla natura, dal livello di maturità dei presidi e dal livello di complessità delle attività. Rispetto alla precedente ISO 19600:2014, la ISO 37301:2001 rappresenta un'evoluzione. Riportando requisiti prescrittivi, infatti, si presenta anche come possibile standard di riferimento per una certificazione.

introdotto nel sistema dei controlli matrici comuni per stabilire, sviluppare, attuare, valutare, mantenere e migliorare un sistema di gestione della *compliance* efficace e reattivo nell'ambito dell'organizzazione.

Con riferimento a tali norme, la conformità – ovviamente ivi intesa in senso ristretto, quale "obbedienza" a norme cogenti – è l'esito a cui l'organizzazione deve tendere in risposta agli obblighi normativi imposti dalla legge. Tale attività, in particolare, è resa "sostenibile" all'interno del contesto organizzativo, grazie allo sviluppo di azioni di coordinamento e alla diffusione della cultura della *compliance* e di comportamenti condivisi.

Un valido sistema per la gestione delle conformità deve prevedere una duplice attività prodromica all'implementazione del modello: la prima, necessaria a perimetrare il campo di applicazione dei punti norma attraverso l'analisi dei fattori interni ed esterni che incidono sull'attività dell'organizzazione di riferimento; la seconda, incentrata sullo studio della *governance* interna e delle politiche di *compliance* già adottate dall'organizzazione e sull'analisi del corretto "posizionamento" della struttura di *compliance* all'interno dell'organigramma aziendale a cui, secondo le linee guida sul *Compliance risk management: applying the COSO ERM framework*[54], dev'essere garantita l'indipendenza funzionale[55].

Un ulteriore elemento di valutazione dell'idoneità del modello riguarda l'adeguatezza delle politiche di conformità e delle linee di indirizzo diffuse dal *management*[56].

La scelta di idonei strumenti di comunicazione e diffusione della cultura aziendale del rischio applicato alla *compliance* consente alla popolazione aziendale di percepire un forte *commitment* da parte del *board* e di partecipare attivamente, anche se in parte inconsapevolmente[57], alla gestione della non conformità attraverso l'applicazione delle procedure e delle prassi aziendali.

Venendo, invece, alla fase di implementazione del modello, la norma ISO 37301:2021 prevede quattro fasi di miglioramento (*Plan*, *Do*, *Check* e *Act*)[58], nonché una serie di ulteriori

---

[54] cfr. *Compliance risk management: applying the COSO ERM framework*, cit., p. 3.

[55] Sebbene mantenga la sua indipendenza, è preferibile che la gestione della *compliance* sia integrata con i processi di rischio in diversi ambiti (cfr. ISO 19600:2014).

[56] Un *compliance program* deve assicurare che le linee di indirizzo di politica interna non contengano un mero messaggio volto ad inibire o azzerare condotte non tollerate. Le procedure interne, inoltre, dovranno garantire: l'assegnazione delle responsabilità, programmi di formazione, sistemi di incentivazione, sanzioni disciplinari e l'integrazione del programma di conformità nei processi aziendali (cfr. *U.S. Department of Justice Criminal Division. Evaluation of Corporate Compliance Programs*, giugno, 2020, p. 1).

[57] L'applicazione sistemica delle procedure da parte del personale genera un circolo virtuoso che vede coinvolta l'intera popolazione aziendale nella gestione dei rischi di non conformità, favorendo lo sviluppo del modello e la gestione delle attività in un'ottica di *continuous monitoring*.

[58] Le tipiche attività di sviluppo del modello dovrebbero riguardare la pianificazione delle azioni di risposta ai rischi emersi a seguito dell'*assessment* e l'individuazione degli obiettivi e delle modalità per integrare i processi esistenti e la loro efficacia. A tale attività dovrebbe poi far seguito l'attuazione dei controlli sulle azioni di risposta (es. politiche operative, la previsione di un impianto sanzionatorio, la *segregation of duty*, l'attività di audit sui processi, l'attività di reporting tra le strutture di *compliance*, il *management* ed il *board*, un'attività di *due diligence* su terze parti in caso di affidamenti all'esterno), l'attività di monitoraggio (es: metodologie, periodicità, analisi dei risultati, flussi per l'invio di informazioni di ritorno da parte di tutti gli *stakeholders* e la loro classificazione etc.), l'attuazione dei controlli sulle azioni di risposta (es. politiche operative, la previsione di un impianto sanzionatorio, la *segregation of duty*, l'attività di audit sui processi, l'attività di reporting tra le strutture di *compliance*, il *management* ed il *board*, un'attività di *due diligence* su terze parti in caso di affidamenti all'esterno) e l'individuazione di azioni correttive appropriate agli effetti prodotti dalle non conformità e la previsione delle necessarie azioni di *escalation* successive al verificarsi dell'evento.

requisiti che permeano l'intera attività e che riguardano la *leadership*, il rapporto con le altre funzioni e la responsabilità.

Tale lavoro sembra porsi in linea con lo standard internazionale *Compliance risk management: applying the COSO ERM framework* del *Committee of Sponsoring Organizations of the Treadway Commission (COSO),* che mira a fornire una guida sull'applicazione del framework COSO ERM per l'identificazione, valutazione e gestione dei rischi di conformità.

Quest'ultimo *framework*, a sua volta, ripercorre taluni obiettivi di conformità e prevenzione degli atti illeciti che, già dai primissimi anni '90, hanno caratterizzato i programmi di conformità ed etica (C&E).

La struttura di tali programmi si caratterizza, infatti, per sette elementi descritti nelle *U.S. Federal Sentencing Guidelines* (USSG)[59]: 1) *standards and procedures*; 2) *governance*, *oversight, and authority*; 3) *due diligence in delegation of authority*; 4) *communication and training*; 5) *monitoring*, *auditing*, *and reporting systems*; 6) *incentives and enforcement*; 7) *response to wrongdoing*[60].

La valutazione di questi elementi si pone come base per la comprensione del *Compliance risk management: applying the COSO ERM framework* che, come già evidenziato (cfr. *supra* par. 2.2), nell'ottica di allineare detti modelli di gestione dei rischi di conformità, enfatizza l'importanza di effettuare una corretta analisi del contesto interno ed esterno all'organizzazione prima di proseguire nella valutazione del rischio.

Il modello prevede un ruolo sinergico dell'autorità di governo dell'organizzazione che, oltre a dover fornire le linee di indirizzo per l'implementazione del programma e conoscere il contenuto, dovrà esercitare una supervisione ragionevole riguardo all'implementazione dello stesso ed individuare il personale di più alto livello cui assegnare le responsabilità operative, provvedendo al corretto dimensionamento della struttura con risorse adeguate.

2.4. *Il rischio di non conformità connesso al fenomeno corruttivo*

Nel più ampio sistema di monitoraggio dei rischi di non conformità, rientra anche l'attività volta alla valutazione e gestione del fenomeno corruttivo all'interno dell'organizzazione[61].

Nonostante non sia possibile addivenire ad una definizione univoca del fenomeno, questo è da intendersi comprensivo di tutti quei comportamenti soggettivi impropri che un soggetto pone in essere al fine di curare un interesse personale o un interesse particolare di terzi deviando, in cambio di un vantaggio, dai propri doveri e dalla cura imparziale dell'interesse collettivo[62].

---

[59] Le linee guida federali sulle condanne degli Stati Uniti costituiscono un impianto di regole per l'applicazione di una politica sanzionatoria uniforme, con particolare enfasi sullo sviluppo della politica di condanna organizzativa relativa a programmi di compliance ed etica efficaci.

[60] Per approfondire, cfr. *Compliance risk management: applying the COSO ERM framework*, cit.

[61] Con delibera n. 206 del 2019, l'ANAC, modificando l'art. 8, comma 4, della delibera n. 1196 del 2016, ha promosso l'analisi dei dati concernenti le cause e i fattori della corruzione, mediante l'elaborazione di specifici indicatori di misura ed attraverso la valutazione sistematica della BDNCP e delle altre banche dati gestite dall'Autorità.

[62] v. delibera n. 1064 del 2019 (PNA 2019).

Con il passare del tempo il fenomeno ha acquisito i connotati di un processo sistemico caratterizzato da un *quid pluris* variamente rappresentato dalla presenza, tra soggetto corrotto e soggetto corruttore, di un vantaggio concorrenziale, di una riconoscenza e disponibilità reciproca, di un arricchimento economico diretto o indiretto o addirittura di favori politici.

Per quel che interessa la presente trattazione, in particolare, la riduzione del fenomeno corruttivo così inteso, si pone tra i principali obiettivi di un valido *compliance program*.

Con l'entrata in vigore della legge del 6 novembre 2012, n. 190, nota come "legge Severino", è cambiato l'approccio alla disciplina dei fenomeni corruttivi che, originariamente incentrata su interventi per lo più sanzionatori, introduce ora anche strumenti di tipo organizzativo, mediante la regolazione e la procedimentalizzazione di specifiche attività, al fine di ridurre l'assunzione di decisioni devianti dalla cura dell'interesse generale a causa del condizionamento improprio da parte di interessi particolari.

Con l'approvazione nel 2013 del primo Piano Nazionale Anticorruzione, infatti, vengono emanati gli obiettivi strategici governativi per lo sviluppo delle strategie di prevenzione a livello centrale, nonché le linee di indirizzo cui le pubbliche amministrazioni ed alcuni soggetti privati espressamente individuati saranno tenuti per la gestione del rischio corruzione e per la stesura dei relativi Piani Triennali di Prevenzione, delineati su processi di *risk assessment*.

È evidente come un sistema così disegnato sia rivolto alla prevenzione del fenomeno ed alla sua mitigazione, piuttosto che alla ricerca puntuale dell'illecito, attraverso l'adozione di valide politiche di contrasto finalizzate all'introduzione di presidi, la cui adeguatezza deve essere misurata in base all'entità, alla dimensione territoriale e alle specificità del contesto organizzativo di riferimento.

In tale ottica, la dinamica di valutazione dei rischi adottata dall'organizzazione per la riduzione del fenomeno corruttivo e delle sue esternazioni negative, dovrebbe restare quella tipica dei modelli basati sull'analisi preliminare del rischio inerente e residuo[63].

A tal riguardo, si evidenzia la possibilità di riscontrare nella prassi l'utilizzo di metodologie per la valutazione del rischio inerente, indagato quindi in assenza delle misure di contrasto, cosiddette di *Control & Risk Self-Assessment*[64], eventualmente già adottate dall'organizzazione. Il metodo consente l'adozione di un approccio misto alla valutazione del rischio, di natura quantitativa e qualitativa, scelto dagli stessi soggetti che hanno proceduto all'identificazione degli eventi rischiosi attraverso un percorso di auto analisi senza la necessità di dover utilizzare metodi predefiniti[65].

---

[63] Sul punto preme rilevare che l'ANAC, all'allegato 1 del Piano Nazionale Anticorruzione del 2019, rubricato *indicazioni metodologiche per la gestione dei rischi corruttivi*, fornisce indicazioni metodologiche per la progettazione, la realizzazione ed il miglioramento continuo del sistema di gestione del rischio corruttivo. Come i tipici modelli internazionali di riferimento, la logica del *framework* individua nel processo di gestione tre fasi principali: l'analisi del contesto interno ed esterno all'organizzazione, la valutazione del rischio (riconducibile alle attività volte all'identificazione, analisi e ponderazione del rischio) ed il trattamento.

[64] Come indicato dall'Associazione Italiana Internal Auditors (www.aiiaweb.it), il *Control Risk Self-Assessment* si pone l'obiettivo di fornire al *management* uno strumento in grado di effettuare analisi qualitative per la gestione del rischio.

[65] Questo tipico approccio alla valutazione del rischio legato al fenomeno corruttivo è riscontrabile nella delibera ANAC n. 452 del 2020. Con specifica nota, in particolare, l'ente pubblico di ricerca rappresentava all'Autorità il completamento del processo di programmazione delle misure di

Tuttavia, le organizzazioni continuano ad adottare un approccio alla repressione del fenomeno corruttivo ancorato a logiche meramente difensive calate dall'alto (di tipo *top-down*), limitandosi per lo più all'applicazione delle misure di contrasto e repressione previste dall'ordinamento[66].

Un'evoluzione di tale approccio, che si concretizzi nello sviluppo di presidi basati invece sul modello *bottom-up*, consentirebbe la partecipazione dell'intera struttura aziendale nell'attività di individuazione dei fenomeni corruttivi all'interno dei singoli processi, nonché l'accesso alle informazioni detenute dall'organizzazione.

L'adozione di tale modello alimenterebbe poi la stessa percezione dell'esistenza e dell'efficacia di un presidio anticorruzione da parte di tutta la popolazione aziendale, il cui ruolo quindi diviene centrale all'interno dell'organizzazione, mediante comportamenti condivisi improntati all'adozione di condotte lecite.

L'ANAC, inoltre, ha evidenziato la necessità di un approccio metodologico alla costruzione del Piano Triennale per la Prevenzione della Corruzione e della Trasparenza fondato sull'analisi del contesto e sulla mappatura dei processi che, orientata all'individuazione dei rischi corruttivi, tenga conto della peculiarità dell'assetto organizzativo e della *mission* istituzionale dell'organizzazione, senza limitarsi al mero adempimento di natura programmatica previsto dall'art. 1, comma 8, della legge n. 190/2012[67].

In ragione di ciò, l'implementazione del Piano dovrebbe prevedere l'introduzione di riferimenti specifici all'analisi di contesto (interno ed esterno), alla mappatura dei processi con l'individuazione delle relative misure, all'indicazione del responsabile, alle tempistiche di attuazione, agli indicatori di monitoraggio e alle misure di prevenzione volte a presidiare l'area di rischio degli enti partecipati, in relazione alle specifiche criticità accertate all'esito delle verifiche.

Un mero approccio burocratico all'attività di costruzione della mappa dei processi interni, che miri alla realizzazione dell'adempimento piuttosto che all'analisi del fenomeno, andrebbe ad eludere lo scopo della norma che è quello di disporre di un Piano utile, chiaro e comprensibile per la definizione degli obiettivi strategici in materia di prevenzione della corruzione, come contenuti necessari di tale documento di programmazione strategica legato all'organizzazione[68].

---

prevenzione della corruzione per il triennio 2020-2022, mediante un'attività di ponderazione del rischio basata sia sui criteri del PTPCT, sia sulla logica che combina l'approccio decisionale accentrato con l'acquisizione delle informazioni trasmesse dalle strutture. Nel caso di specie, l'attività di *Control Risk Self-Assessment* è stata caratterizzata da un approccio misto. In particolare, è stato utilizzato un "approccio quantitativo" per la determinazione del rischio inerente, poiché basato sull'impiego di criteri aritmetici (es. la media) ed un "approccio qualitativo" per la valutazione del rischio residuo, che è dipesa dalle scelte strategiche effettuate dal RPCT sulla scorta degli indicatori analizzati e delle informazioni ottenute dalle strutture interessate.

[66] Tra le misure difensive introdotte dal legislatore possono essere richiamate: le misure di trasparenza, il FOIA e l'accesso civico, i codici di comportamento, la rotazione del personale, l'incompatibilità e l'inconferibilità di incarichi, l'analisi di possibili conflitti d'interesse, l'istituto del *revolving doors* o del *pantouflage* ed il *whisteblowing*.

[67] Come evidenziato nella delibera ANAC n. 769 del 2020, la Corte dei Conti, sezione regionale di controllo per l'Abruzzo, aveva informato l'Autorità della Deliberazione adottata nei confronti di un Comune Abruzzese all'esito delle verifiche sul funzionamento del sistema integrato dei controlli interni con riguardo agli esercizi 2017 e 2018, che aveva evidenziato carenze nella realizzazione del PTPCT per la parte relativa all'analisi del contesto ed alla mappatura dei processi.

[68] L'ANAC, con delibera n. 7 del 2021, ha recentemente sanzionato «il comportamento dell'Amministratore Unico della Società, per non aver tenuto in debito conto la rilevanza dell'attività

Gli aspetti organizzativi riportati nel Piano, in particolare, dovranno consentire l'emersione sia del livello di complessità strutturale dell'organizzazione, sia del sistema delle responsabilità.

2.5. *Modelli orientati a riconoscere e gestire il fenomeno corruttivo all'interno dell'organizzazione*

Un approccio *risk based* all'individuazione delle non conformità in ambito anticorruzione, come fin qui evidenziato, promuove l'analisi del contesto interno ed esterno a necessario corollario dell'azione di prevenzione delle condotte illecite all'interno dell'organizzazione.

Tale analisi, seppur non orientata all'individuazione degli specifici reati o delle condotte proprie dei singoli ordinamenti, consente di introdurre uno strumento di rilevazione, gestione e monitoraggio del fenomeno all'interno del contesto di riferimento. Ciò permette una riduzione dell'esposizione dell'organizzazione al rischio corruzione, che si pone in linea con gli altri modelli di gestione volti alla direzione e all'implementazione del sistema di controllo interno delle amministrazioni.

Tali aspetti svolgono un ruolo fondamentale per il contrasto alla corruzione incidendo, da un lato sulla maturità dei presidi preposti e, dall'altro, sulla loro adeguatezza.

In tale ottica, il sistema di gestione anti-corruzione, definito dallo standard internazionale ISO 37001 nel 2016 e implementato dall'*International Organization for Standardization*, si pone l'obiettivo di prevenire, rilevare ed affrontare il fenomeno corruttivo, mediante l'adozione di un modello di gestione disegnato per ridurre la possibilità che l'evento si verifichi, e di limitare l'impatto dello stesso per l'organizzazione[69].

Lo standard riflette l'attuazione delle politiche interne, delle procedure e dei controlli tipici dell'organizzazione con riguardo ai rischi corruttivi rilevati e, in un'ottica *risk based*, consente di: testare il livello di maturità dei presidi esistenti; indagare il livello di rischiosità residuale del fenomeno corruttivo rispetto alla soglia di tolleranza individuata dall'organizzazione; implementare azioni di rimedio e mitigazione ove necessarie all'azzeramento o alla riduzione dell'evento rischioso, in considerazione delle peculiarità tipiche dell'amministrazione di riferimento[70].

A tal fine, diviene di fondamentale importanza anche la messa a sistema dei dati in possesso dell'organizzazione.

---

di prevenzione della corruzione; l'elemento psicologico che caratterizza la censurata condotta dei soggetti su citati è dunque da rinvenirsi nella colpa, potendosi escludere che il loro comportamento omissivo, seppur caratterizzato da inosservanza degli ordinari doveri di diligenza, fosse il fine ultimo della loro azione».

[69] La norma internazionale ISO 37001, basata sul *British Standard BS 10500/2011 (Specification for anti-brybery management system – "ABMS")*, connesso alla legge britannica *UK Bribery Act del 2010* di contrasto al fenomeno corruttivo, è stata elaborata dal Comitato Tecnico ISO/PC 278 "Anti-bribery management system" ed è stata approvata il 13 dicembre 2016.

[70] Ci si riferisce, in particolare, al punto norma numero 9 della ISO 37001/2016. Le attività riguardano principalmente: l'attività di monitoraggio; la misurazione; l'analisi e la valutazione di alcuni elementi (es. il processo, i responsabili, le metodologie applicate, le modalità di analisi delle informazioni acquisite, i flussi informativi di ritorno, etc.); l'attività di audit interno e l'attività di riesame da parte del *management*.

La selezione delle informazioni rilevanti per la corretta individuazione dell'articolazione organizzativa dell'amministrazione a livello centrale e periferico, tenendo conto delle peculiarità della stessa, favorisce lo svolgimento di indagini mirate al riconoscimento di profili di rischio correlati all'effettiva attività svolta dalle singole strutture[71].

Intervenire sui modelli organizzativi di gestione e controllo esistenti, garantendo la chiara distinzione di compiti e responsabilità dei soggetti interni, consente di assicurare: il coinvolgimento degli organi di indirizzo e dei vertici dell'organizzazione, il presidio delle strutture di controllo e la centralità del Responsabile per la Prevenzione della Corruzione e della Trasparenza, garantendone autonomia e indipendenza rispetto all'organo di indirizzo ed effettivi poteri di interlocuzione e controllo.

Tra i modelli di contrasto alla corruzione, deve essere annoverato anche il sistema di gestione delle segnalazioni.

In attesa del recepimento della direttiva UE 1937 del 23 ottobre 2019, nell'ordinamento domestico[72], nel 2018, il Comitato tecnico ISO/TC 309 – che opera nel campo della standardizzazione dei modelli di *governance* relativamente agli aspetti di direzione, controllo e responsabilità delle organizzazioni – è stato incaricato dalla *International Organization for Standardization* di redigere una linea guida in materia di *whistleblowing*.

Tale istituto, entrato nell'ordinamento italiano ad opera dell'art. 1, comma 51, della legge n. 190/2012, tutela l'autore di segnalazioni di illeciti o irregolarità, di cui è venuto a conoscenza nel corso del rapporto di lavoro[73].

Il nuovo standard ISO 37002, attualmente in bozza, è prossimo all'approvazione del Comitato e dovrebbe essere validato e pubblicato entro il terzo trimestre dell'anno in corso. Questo si pone l'obiettivo di fornire indicazioni pratiche per stabilire, attuare, mantenere e migliorare il sistema di gestione delle segnalazioni all'interno dei contesti organizzativi del settore pubblico e privato.

In conformità con quanto previsto dal combinato disposto dell'articolo 8, comma 5, e dell'articolo 9, comma 1, della direttiva UE 1937 del 23 ottobre 2019[74], il modello ruoterà attorno a tre principi cardine posti a tutela del segnalante: riservatezza dell'identità della persona segnalante, massimo livello di protezione degli eventuali terzi citati nella segnalazione che potrebbero subire ritorsioni e la designazione di una persona o di un servizio imparziale competente per dare seguito alle segnalazioni e garantire il mantenimento dei livelli di presidio interni all'organizzazione.

---

[71] v. delibera ANAC n. 954 del 2020.

[72] La Direttiva UE 1937 del 23 ottobre 2019 ha richiesto agli Stati membri di rafforzare l'applicazione del diritto e delle politiche dell'Unione in specifici settori, mediante norme minime comuni volte a garantire un elevato livello di protezione dei soggetti che segnalino violazioni. Con la pubblicazione in Gazzetta Ufficiale n. 97 del 23 aprile 2021, della Legge n. 53 del 22 aprile 2021, recante *Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea - Legge di delegazione europea 2019-2020*, all'art. 23, si chiede al Governo di osservare, nell'esercizio della delega, i principi e criteri direttivi specifici per l'attuazione della direttiva (UE) 2019/1937.

[73] Il legislatore con l'art. 1, comma 51, della Legge n. 190/2012, ha inserito l'art. 54 *bis* all'interno del d.lg. n. 165/2001, con l'obiettivo di tutelare il dipendente pubblico che segnala illeciti di cui è venuto a conoscenza durante il proprio rapporto di lavoro. Successivamente, con l'articolo 2 della Legge n. 179/2017, la tutela prevista inizialmente dalla suddetta normativa è stata estesa anche al settore privato.

[74] Direttiva in materia di protezione delle persone che segnalano violazioni del diritto dell'Unione Europea.

3. IL RUOLO DEL COMPLIANCE MANAGER

3.1. *Il ruolo di coordinamento del Responsabile della Prevenzione della Corruzione e della Trasparenza (RPCT)*

L'analisi del sistema di controllo interno di secondo livello non può prescindere da un'indagine sulla c.d. dimensione immateriale e, più in particolare, sul corretto stile di *leadership* a cui dovrebbe tendere il *compliance manager*, in considerazione del fatto che «laddove manchi il supporto del *top management* nella gestione del rischio e nel rispetto delle regole, anche attraverso una comunicazione chiara e diffusa, l'efficacia di qualsiasi previsione interna sarebbe minata alle fondamenta»[75].

All'interno di un *compliance program*, infatti, il ruolo del *management* si riflette, sia sulla capacità di quest'ultimo di trasmettere un mutato approccio al rischio di non conformità rispetto agli obiettivi di *business* come parte integrante della strategia d'impresa, sia sul livello di esposizione al rischio che l'organizzazione è disposta a tollerare[76].

Con particolare riguardo alla prevenzione del rischio derivante dalla corruzione, il Responsabile della Prevenzione della Corruzione e della Trasparenza (RPCT), viene chiamato a ricoprire un importante ruolo di coordinamento del processo di gestione del fenomeno, sia perché chiamato alla predisposizione del Piano Triennale di prevenzione, sia in quanto tenuto all'attività di monitoraggio tipica delle funzioni coinvolte nel sistema di controllo interno dell'organizzazione.

Il ruolo di coordinamento del RPCT «non deve in nessun caso essere interpretato dagli attori organizzativi come un pretesto per deresponsabilizzarsi in merito allo svolgimento del processo di gestione del rischio.

Al contrario, l'efficacia del sistema di prevenzione dei rischi corruttivi è strettamente connessa al contributo attivo di altri attori all'interno dell'organizzazione»[77].

Non diversamente, gli altri organi direttivi interni all'organizzazione devono manifestare la propria *leadership* ed il proprio impegno nell'implementazione dei modelli di gestione dei rischi fin dalla fase di condivisione delle strategie, approvando politiche di prevenzione e sottoponendo a riesame le informazioni di ritorno riscontrabili dalle attività di controllo interno effettuate ed esercitando un'attività di sorveglianza "ragionevole".

---

[75] L. BASSI e M. MORELLI, *Paese che vai responsabilità che trovi: il "sistema 231" italiano e la corporate compliance estera*, in *Giurisprudenza penale*, 2020, X, p. 10.

[76] S. BOZZOLAN e S. COSTANZO, *op. cit.*, p. 26, chiariscono che la soglia di *risk appetite* deve intendersi come il livello e la tipologia di rischio che una società è disposta ad accettare ai fini del raggiungimento degli obiettivi prefissati. Sul punto, è chiarito che «la declinazione del rischio per ciascuna categoria alle quali la società è esposta, quali il rischio strategico e operativo, di *compliance* ovvero finanziario, consente al management di determinare il grado di accettabilità del rischio o *risk tolerance*, intesa come il livello di rischio massimo che la società è disposta ad assumere». L'individuazione del rischio che si ritiene di voler accettare e del rischio che si è disposti a tollerare consente l'identificazione del *risk target*, ovvero il livello di rischio che l'azienda intende assumere ai fini del raggiungimento degli obiettivi di business.

[77] cfr. Autorità Nazionale Anticorruzione, allegato 1 del PNA 2019, *Indicazioni metodologiche per la gestione dei rischi corruttivi*, p. 7.

Chi si occupa di *compliance* deve «saper ragionare "per sistemi complessi", e non per singolo ambito normativo o singolo processo; deve possedere, attraverso la formazione specifica e l'aggiornamento continuo, competenze multidisciplinari che lo rendano in grado di dialogare e collaborare con i diversi ruoli e livelli dell'organizzazione»[78].

Ciò premesso, è chiaro che in ogni contesto aziendale il repertorio di comportamenti tenuti da ogni *manager* e l'ampiezza degli stili su cui può fare affidamento, determinano la sua efficacia all'interno del contesto organizzativo di riferimento. Non può ritenersi sufficiente, infatti, lo sviluppo di uno stile di *leadership* meramente affine alle naturali predisposizioni del soggetto che ricopre un ruolo di responsabilità e ciò è particolarmente vero per quanto riguarda il ruolo di responsabile della funzione di *compliance*.

È necessario, infatti, che il *manager* sviluppi ed accresca nel lungo periodo competenze personali e professionali che possano consentirgli di mutare il proprio stile, in base alle variabili situazionali che incidono sul contesto interno ed esterno dell'organizzazione (es. attitudini dei collaboratori, esperienza, momento storico, etc.)[79].

È soprattutto in questa prospettiva che il RPCT all'interno del contesto organizzativo si trova a ricoprire un ruolo dirimente, che non si sostanzia nella sola attività di controllo di secondo livello derivante dalla necessità di poter garantire la conformità, l'uniformità e l'integrità dei buoni comportamenti, ma che attiene alla diffusione di una coscienza collettiva, che dovrà essere percepita come unitaria dai dipendenti e da tutti i portatori di interesse che orbitano attorno all'organizzazione.

Il repertorio dei comportamenti ritenuti fondamentali dall'organizzazione per la diffusione di un approccio al rischio orientato a prevenire, gestire e monitorare le non conformità legate al fenomeno corruttivo (cfr. *ultra* par. 3.2), deve riflettersi nei documenti societari che contengono gli aspetti maggiormente "valoriali" dell'organizzazione, articolandosi in legittime aspettative sui buoni comportamenti (es. codice di condotta o di etica, carta dei valori, politiche di indirizzo e *framework* in ambito anticorruzione, etc.).

Tale repertorio, inoltre, deve poter trovare un riscontro anche all'interno delle procedure aziendali e dei processi organizzativi esistenti, stimolandone altresì la revisione (es. valutazione della *performance*, sistema delle remunerazioni e delle incentivazioni, rotazione del personale[80], etc.)[81].

Non a caso i modelli internazionali per la valutazione dei rischi, anche applicati alla *compliance*, prevedono la necessaria adozione di flussi di comunicazione (*reporting*) tra le

---

[78] A. QUARANTA, *op. loc. cit*. Il *compliance* manager è un "direttore d'orchestra" che, attraverso l'utilizzo di specifiche metodologie, deve tradurre ogni aspetto aziendale oggetto di *compliance* in un tutt'uno armonico, la cui "somma" costituisce la *compliance* aziendale.

[79] Per approfondire, cfr. P. HARSEY e K.H. BLANCHARD, *Leadership situazionale: come valutare e migliorare le capacità di gestione e degli uomini***,** edito Sperling e Kupfer, Economia & Manangement, 1984.

[80] Come riportato nell'allegato 2 del Piano Nazionale Anticorruzione 2019, pubblicato dall'ANAC, l'art. 1, comma 5, lett. b) della l. 190/2012, prevede che le pubbliche amministrazioni devono definire e trasmettere ad ANAC «procedure appropriate per selezionare e formare, in collaborazione con la Scuola superiore della pubblica amministrazione, i dipendenti chiamati ad operare in settori particolarmente esposti alla corruzione, prevedendo, negli stessi settori, la rotazione di dirigenti e funzionari». Inoltre, ai sensi dell'art. 1, co. 10, lett. b) della, il RPCT deve verificare, d'intesa con il dirigente competente, «l'effettiva rotazione degli incarichi negli uffici preposti allo svolgimento delle attività nel cui ambito è più elevato il rischio che siano commessi reati di corruzione».

[81] cfr. *Compliance risk management: applying the COSO ERM framework*, cit., p. 8.

funzioni di *compliance*[82], il *management* ed il Consiglio di Amministrazione che, se effettuati con cadenza periodica, consentono alle funzioni preposte di ricevere informazioni di ritorno per lo svolgimento delle attività di *continuous monitoring*.

Affinché le decisioni prese dal *management* siano sempre orientate ad una corretta gestione del rischio, infatti, è necessario prevedere frequenti occasioni di incontro tra il *top management* e le funzioni di *compliance*.

3.2. *Il repertorio dei validi comportamenti nella ricerca di un nuovo equilibrio di poteri*

Come cennato in precedenza, le strutture di *compliance* all'interno dell'organizzazione hanno da sempre esercitato il proprio ruolo e, di conseguenza, il proprio stile di *leadership*, anteponendo le tipiche funzioni di comando e controllo alle necessità dell'organizzazione rispetto alla sua natura, al suo sistema di valori e convinzioni ed alle strategie per la tutela del *core business*.

Chi si occupa di *leadership* nell'ambito dei sistemi di gestione dei controlli interni, sta ripensando al ruolo del *compliance manager* ponendo attenzione all'intero sistema dei poteri che fino ad oggi ha interessato la materia[83].

Se prima era sufficiente parametrare l'analisi delle non conformità partendo dallo studio della *governance*, dalla valutazione delle interazioni tra processi e dal mero controllo formale dell'adempimento della disposizione legislativa, oggi è necessario parametrare il ragionamento su diversi e più maturi elementi che consentano di gestire le attività di *compliance* ponendo l'attenzione su questioni che tipicamente non rappresentano un'analisi di conformità ma, piuttosto, un'analisi di contesto con impatti gestionali[84] e risvolti giuridici.

Se, ad esempio, si allarga il ragionamento in considerazione dei recenti mutamenti che, per diverse ragioni, hanno interessato il rapporto di lavoro, è evidente come lo *smart working* (o lavoro agile) rappresenti oggi una valida, quanto necessaria, alternativa alla modalità "ordinaria" di espletamento dell'attività lavorativa[85].

In tale contesto, venendo meno il tipico assetto orientato alla definizione della prestazione lavorativa anche in virtù di un tempo contrattualizzato da trascorrere sul luogo di lavoro, si accentua la necessità di un mutato stile di comportamento che tenga conto dell'impossibilità

---

[82] Come osservato da L. BASSI e M. MORELLI, *op. loc. cit.*, le funzioni di *compliance* dovranno essere adeguate alle strutture in cui operano in termini di professionalità, integrità e autonomia finanziaria.

[83] Come chiarito da T. FOX, *Innovation in Compliance Leadership. Prescription for an evolving Complinace Program*, marzo 2020 (reperibile in corporatecomplianceinsights.com.), i risultati dell'azione collettiva, in termini di valori e convinzioni, generano "circuiti di feedback" che conferiscono alle persone un "nuovo potere".

[84] Per approfondire, cfr. J. HEIMANS e H. TIMMS, *Understanding New Power. The crowd is challenging traditional leadership. Here's how to harness its energy,* in *Harvard Business Review*, dicembre, 2014, reperibile in hbr.org/2014/12/understanding-new-power.

[85] Come definito dalla normativa vigente, il lavoro agile (o *smart working*) è una modalità di esecuzione del rapporto di lavoro subordinato che si caratterizza per l'assenza vincoli orari o spaziali, per un'organizzazione del lavoro basata su fasi, cicli e obiettivi e per l'utilizzo di strumentazioni informatiche che consentano lo svolgimento dell'attività fuori dai locali aziendali. Tale modalità di svolgimento della prestazione lavorativa nasce dall'esigenza di voler conciliare i tempi di vita e lavoro favorendo, al contempo, la crescita della produttività. L'istituto del lavoro agile è attualmente disciplinato dalla legge 22 maggio 2017, n. 81, Capo II.

di poter garantire le tipiche attività di *compliance* che, per loro natura, restano facilitate dalla presenza del personale sul luogo di lavoro e dall'utilizzo di strumenti aziendali che, per ovvie ragioni, potrebbero non risultare accessibili ai lavoratori che prestano la propria attività fuori dai locali aziendali[86].

Nell'era dell'economia digitale, un buon *manager* non può prescindere dallo sviluppo di competenze, capacità personali e professionali che facilitino la gestione delle risorse ed il raggiungimento di obiettivi condivisi attraverso nuovi approcci che tengano conto dei mutati assetti riguardanti il mondo del lavoro.

In questa prospettiva, è indispensabile lo sviluppo di un'intelligenza collettiva[87] e soprattutto di una *leadership* emotiva[88] orientata alla gestione delle risorse.

Tale competenza, assicurando una maggiore consapevolezza per il controllo dei propri stati emozionali e lo sviluppo della capacità di poter incidere su quelli altrui, favorisce nuovi comportamenti orientati alla collaborazione, alla condivisione ed alla definizione di obiettivi comuni.

[86] «Il "lavoro agile" si configura in misura sempre crescente come un punto di svolta nella cultura delle imprese e dei processi organizzativi», A. TIRALONGO, *Il lavoro agile richiede un nuovo stile di leadership*, in *Forbes*, marzo, 2020.

[87] Attingere all'intelligenza collettiva dell'azienda, sollecitando i pensieri del consiglio di amministrazione, della direzione e dei dipendenti, consente di guardare oltre i muri dell'organizzazione per comprendere gli sviluppi del settore e le reazioni dei concorrenti alla conformità aziendale. Cfr. F. ACCARDI, *op. cit.*, p. 43.

[88] Per approfondire cfr. D. GOLEMAN, *Leadership emotiva. Una nuova intelligenza per guardarci oltre la crisi*, traduzione a cura di F. PERI, 2013.