WHITE PAPER

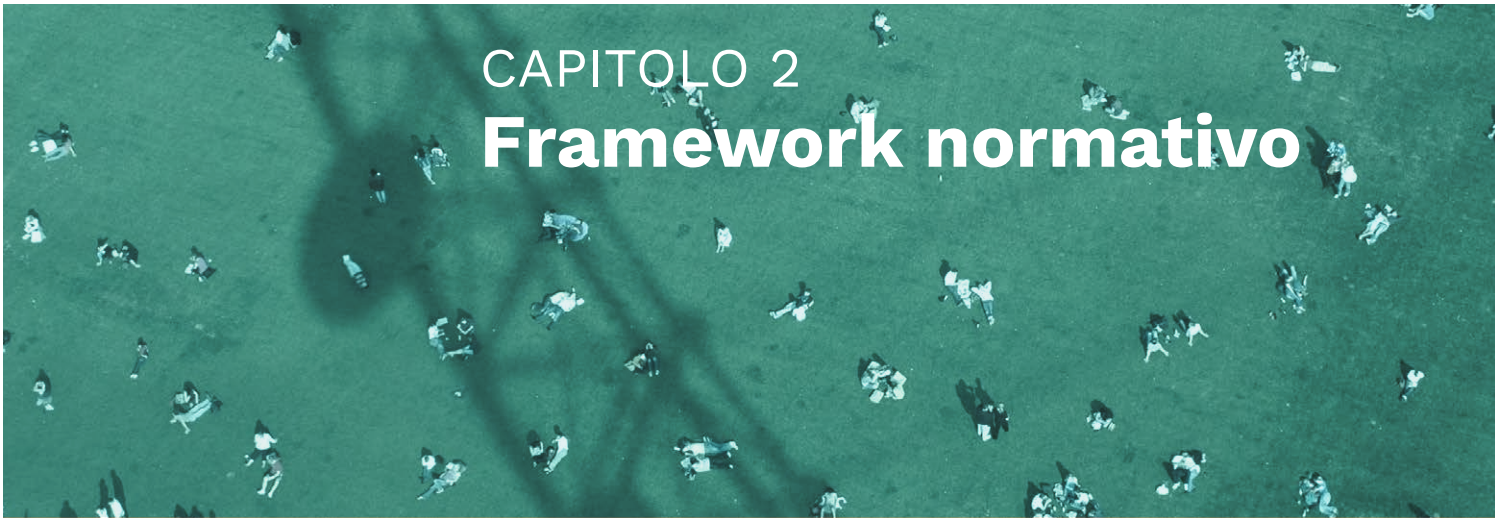
La Funzione Compliance

lab4compliance

CAPITOLO 1

Aspetti generali

La Funzione Compliance



CAPITOLO 2

Framework normativo

CAPITOLO 3

Aspetti di processo

Indice

Premessa

Il presente White Paper della Funzione Compliance vuole rivolgersi a tutti gli attori giuridici, economici e sociali ed ha lo scopo di:

- **Fornire un riferimento per la definizione del concetto di Compliance e della Funzione Compliance**, attraverso un excursus della normativa più rilevante e che ha maggiormente inciso nella trasformazione della disciplina e nell'affermazione del ruolo della medesima Funzione[1].
- **Indagare** e, poi, **esplicitare** in modo chiaro e semplificato il **ruolo della Compliance all'interno dell'impresa**, individuando **responsabilità ed attribuzioni** della Funzione Compliance, del cd. "Compliance Officer" e degli altri soggetti coinvolti nelle attività inerenti al campo di applicazione in oggetto;
- **Individuare** gli **obiettivi dell'attività di compliance**, definendo il **perimetro di azione** (valutazione e gestione dei rischi, implementazione di una struttura di controllo, supporto strategico per il business ecc..) e le rilevanti attività di competenza del Compliance Officer, al fine di comprenderne al meglio la rilevanza;
- Sottolineare **l'essenzialità del ruolo della Compliance** per le imprese sia nella veste di attore del sistema di controllo interno e gestione dei rischi, sia nella veste di partner strategico per le funzioni che gestiscono attività di business;
- **Indirizzare e guidare gli operatori economici** - di natura pubblica o privata, di grandi, medie e piccole dimensioni - nella **creazione e nella conduzione di una struttura di compliance efficiente** nella gestione dei rischi di impresa.
- **Orientare Autorità di riferimento, magistrati ed accademici** sulla opportunità di indirizzare il proprio operato tenendo in considerazione l'attuale contesto imprenditoriale ed organizzativo.

1. Giova citare in questa sede il riferimento allo Standard ISO 37301 "Compliance management system – Requirements with guidance for use" che presenta un valido schema di impostazione della Funzione, preso in considerazione quale fonte per la stesura del presente documento.

CAPITOLO 1

Aspetti generali

In un contesto sociale, economico e giuridico in costante evoluzione è fondamentale che l'istituzione economica organizzata sia in grado di adattarsi al cambiamento e sapersi rinnovare attraverso l'adozione di nuove strategie, nuovi meccanismi di funzionamento ed interazione con il contesto economico e sociale esterno, nuovi processi e strumenti tecnologici.

Negli ultimi anni il quadro normativo regolamentare che ha disciplinato il funzionamento dei mercati ha reso, per le aziende, la dinamica dell'adeguamento e della conformità (da adesso anche "Compliance") questione di complessità crescente e spesso di difficile interpretazione applicativa. A ragione di ciò, è progressivamente emersa la necessità di adottare, all'interno delle organizzazioni economiche, aree di competenza e ruoli dedicati ad assicurare che la direzione di impresa fosse allineata e conforme alle norme di legge applicabili e, così, scongiurare il rischio di fuoriuscita dal perimetro regolatorio. Di fatto, si è delineata una progressiva affermazione della capacità di gestire il rischio di non compliance quale elemento cardine della buona gestione di impresa. Per rischio di non compliance si vuole intendere «***il rischio di incorrere in sanzioni giudiziarie o amministrative, perdite finanziarie, impatti alla reputazione d'azienda e alla sua capacità di attrarre clienti, investitori e nuove opportunità di sviluppo degli affari in conseguenza di violazioni di norme imperative (di legge o di regolamenti) ovvero di autoregolamentazione (es. statuti, codici di condotta, codici di autodisciplina, procedure ecc.)***».

In tale contesto di sovraproduzione normativa e data l'esigenza delle imprese di comprendere e rispettare i dettami del legislatore è diventata cruciale la presenza di una funzione dedicata, la cd. "Compliance" - nello specifico attribuita al ruolo del cd. Compliance Officer - che opera con il mandato di contenere l'esposizione al rischio di non conformità e mantenere salde le fondamenta dell'organizzazione aziendale.

Come meglio si dirà in seguito, la Funzione Compliance nell'assicurare la conformità alle norme di legge obbligatorie, (anche definite come norme di etero regolamentazione) e di autoregolamentazione interne alle aziende, si adopera per assistere l'organizzazione nell'espletamento di attività, quali - a titolo esemplificativo - la stipulazione di accordi di collaborazione commerciale tra imprese, l'assistenza all'esecuzione di operazioni societarie straordinarie, l'introduzione di nuove aree di operatività e di nuove tipologie di business anche con l'obiettivo di perseguire la crescita dell'impresa e di conseguire vantaggi a livello reputazionale.

Tuttavia, nonostante la rilevanza dell'operato della Compliance abbia assunto un'importanza crescente negli anni nell'ambito delle compagini aziendali, l'univoca definizione del suo mandato e del suo perimetro di copertura restano, talvolta, oggetti non ben chiariti e possono destare dubbi tanto sulla qualificazione dell'ambito di attività quanto sulla delineazione di perimetri e confini rispetto ad ambiti attigui al mandato di altre funzioni aziendali chiamate ad operare in campo legale e nel campo della gestione dei rischi e del controllo interno.

La Compliance viene in rilievo, a valle della determinazione normativa, per **preventivare le azioni che l'impresa dovrà intraprendere in ottica di conformità al fine di costruire un sistema di controlli interni adeguato, efficiente e strategico per operare correttamente sul mercato**. Assume un ruolo di importanza strategica all'interno dell'organizzazione, poiché:

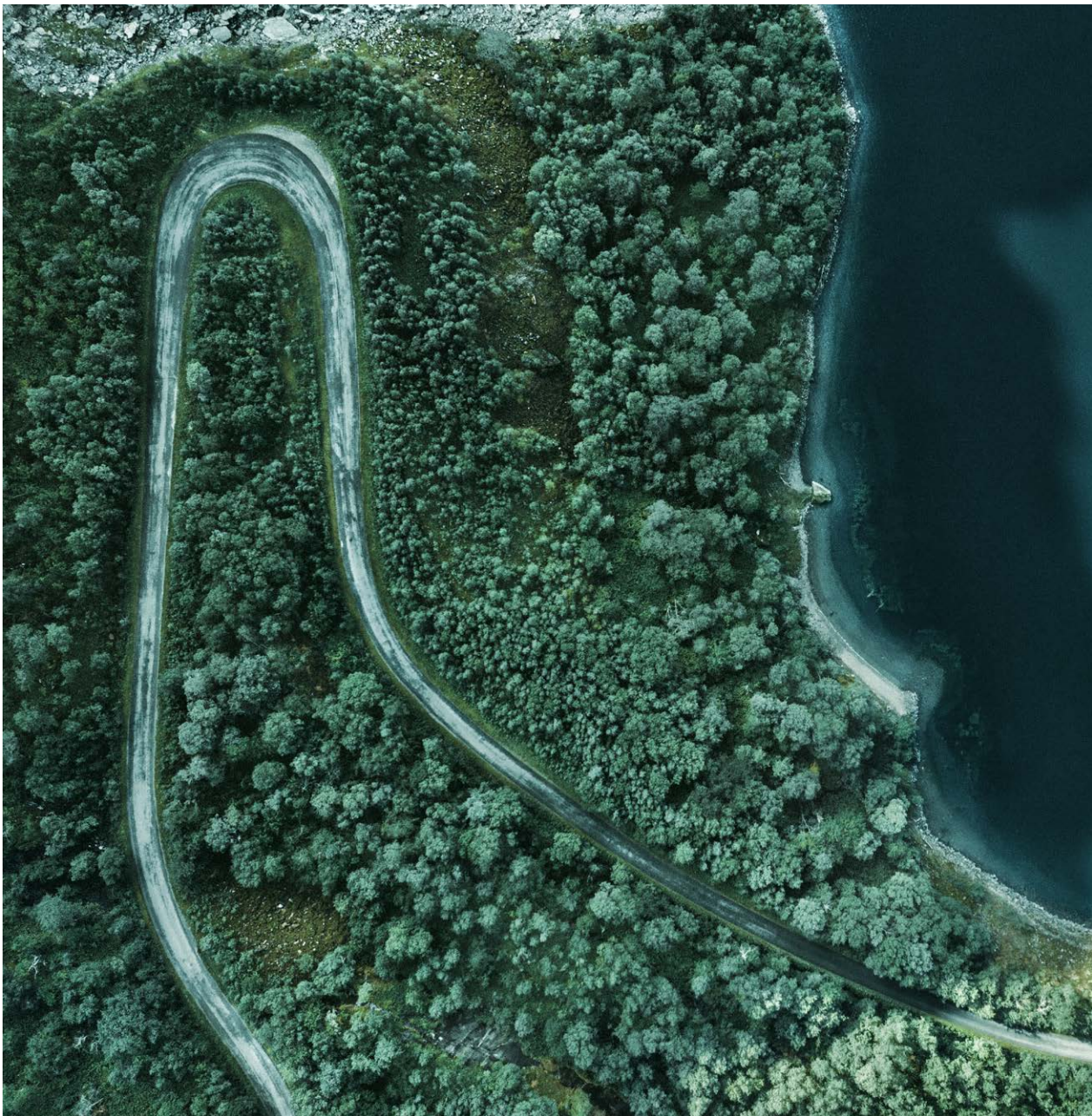
- è uno strumento operativo della corporate governance ossia del consiglio di amministrazione che ne definisce competenze e responsabilità;
- in considerazione degli aspetti connessi alla gestione dei rischi di compliance, è parte degli assetti organizzativi "adeguati" e allo stesso tempo, concorre, insieme agli altri organi del sistema di controllo interno, alla verifica di adeguatezza degli altri assetti organizzativi, amministrativi e contabili.

Giova precisare, in questa sede, che l'adeguatezza degli assetti organizzativi non è fonte dell'obbligo dei consiglieri di amministrazione, ma la misura dell'adempimento dei loro doveri ex art. 2381 cc.; pertanto è possibile affermare come la Compliance sia il presupposto

La Compliance viene in rilievo, a valle della determinazione normativa, per preventivare le azioni che l'impresa dovrà intraprendere in ottica di conformità al fine di costruire un sistema di controlli interni adeguato, efficiente e strategico per operare correttamente sul mercato.

della responsabilità degli organi societari in quanto rappresenta un dovere individuale dei singoli amministratori, ad adempimento collettivo. La Compliance non è quindi solo la base per un operare d'impresa conforme alle regole cogenti, ma anche un'opportunità per costruire un'organizzazione di successo e sostenibile.
Tanto premesso, è possibile **sintetizzare il ruolo della Compliance**, attraverso i seguenti concetti:

- Applicazione delle regole obbligatorie (cd. etero regolamentazione);
- Adozione di norme volontarie (cd. autoregolamentazione);
- Valutazione e riduzione dei rischi d'impresa;
- Predisposizione di un sistema di controllo interno;
- Adozione di misure strategiche per lo sviluppo del business.



Cos'è il cd. *Sistema di controllo interno* e a cosa serve?

La previsione di un impianto di controlli interno, o meglio, del cd. **Sistema di controlli interno (SCI)** - costituito dal complesso di regole, strutture, risorse, funzioni, procedure, politiche di gestione delle operazioni aziendali - è diventato un elemento imprescindibile nel sistema di governo dell'impresa, data la sua funzione di assicurare che l'attività dell'ente sia posta in essere in maniera conforme ai requisiti normativi di etero regolamentazione e di autoregolamentazione, in maniera coerente con le politiche interne e funzionale con le strategie e gli obiettivi del business.
Il compito affidato al sistema dei controlli è l'individuazione, valutazione, monitoraggio, misurazione e mitigazione/gestione di tutti i rischi d'impresa.

Nel contesto socioeconomico contemporaneo, gli enti riconoscono oramai l'importanza di tale sistema di controlli interno, definito, altresì, quale **strumento di gestione integrata del rischio d'impresa associato ai processi di risk assesment e di risk management**, poiché è lo strumento che permette di assicurare:

- rispetto/supporto delle strategie aziendali o governance operativa;
- salvaguardia del valore aziendale dalle perdite;
- affidabilità/integrità del sistema informativo;
- conformità a leggi, normative di vigilanza, piani, regolamento e procedure;
- funzionalità della struttura/processi;
- regolarità della gestione.

Dunque, la predisposizione di tale sistema di controlli consiste nella predisposizione di codici di condotta, regole di governo, politiche e procedure necessarie a guidare le attività di impresa, garantendo che queste siano poste in essere con le giuste modalità in risposta alla necessità di prevenire specifici rischi e a conseguire gli obiettivi di business.

Il sistema di controllo interno si sviluppa su tre livelli, secondo il modello delle "tre linee di difesa" identificato dall'Institute of Internal Auditors nel 2013[1]:

1. The Three Lines of Defense in Effective Risk Management and Control, IIA 2013

- **Controllo di primo livello**: garantisce maggiormente l'organizzazione dalla concretizzazione dei rischi potenziali, in quanto i controlli sono di competenza dei soggetti e delle funzioni operative che prendono parte all'attività di riferimento che lavorano quotidianamente in prima linea ed espongono l'organizzazione a fattori di rischi esterni, le strutture operative sono le prime responsabili del processo di gestione dei rischi: nel corso dell'operatività giornaliera tali strutture devono identificare, misurare o valutare, monitorare, attenuare e riportare i rischi derivanti dall'ordinaria attività aziendale in conformità con il processo di gestione dei rischi ove tali attività non siano assegnate ad una funzione di controllo di secondo livello (come di norma avviene nei principali settori industriali);
- **Controllo di secondo livello: attribuito agli attori/funzioni del sistema di gestione del rischio e della conformità dell'operatività aziendale alle norme controllo interno chiamati ad effettuare una supervisione sul corretto disegno dei controlli applicati al primo livello e sulla loro corretta applicazione. La Funzione Compliance è la rappresentazione calzante, nella tipica architettura del sistema, di attore di secondo livello.**
- **Controlli di terzo livello**: il terzo livello di controllo garantisce una review indipendente sull'efficacia dei controlli, effettuando prevalentemente test sui controlli effettuati al primo livello (test di efficacia) ovvero sui controlli di secondo livello (test di review). Il terzo livello di controllo è tipicamente oggetto del mandato dell'Internal Audit.

Come può essere articolato un sistema di controllo interno costituito da sistemi di gestione e modelli di compliance?

I sistemi di gestione ed i modelli di compliance rappresentano l'architettura complessiva del sistema di controllo interno teso a definire **i controlli organizzativi e operativi atti a intercettare o evitare condotte non conformi o comportamenti anomali, in violazione delle regole del contesto nel quale l'organizzazione si trova ad operare**, garantendo una **piena e continua conformità alla normativa vigente ed applicabile**. Parimenti, i sistemi di gestione ed i modelli di compliance identificano la struttura dei ruoli e delle responsabilità di definizione ed applicazione dei controlli su soggetti e transazioni, siano essi interni o esterni all'organizzazione secondo quanto rilevato nella fase di identificazione dei rischi, le policy e procedure ad indirizzo dei comporta-

menti, i requisiti infrastrutturali ed informatici necessari a garantire la gestione delle transazioni in conformità ai requisiti identificati, le modalità di formazione ed informazione al personale interessato, le modalità di verifica di efficacia del sistema, la valutazione della performance del sistema ed i meccanismi di aggiornamento e miglioramento continuo, i sistemi di incentivazione, disincentivazione e sanzione, i meccanismi di reporting interno ed esterno all'organizzazione.

La Funzione Compliance è responsabile, dunque, dell'identificazione delle procedure e dei controlli di conformità o della modifica di quelli già in essere nell'organizzazione e che la stessa ha messo in atto per prevenire, rilevare e gestire i fenomeni che rientrano nell'alveo degli scenari di rischio di compliance così come prospettati nell'ambito dell'attività di identificazione e valutazione dei rischi di compliance. Fra le componenti del sistema di controllo all'interno di un sistema di gestione o modello di compliance, meritano un approfondimento specifico le policies e procedure in quanto ne rappresentano la struttura portante.

Cosa sono i codici di condotta e di comportamento e che ruolo giocano all'interno dei sistemi di gestione e dei modelli di compliance?

I codici di condotta, comportamento e/o codici etici sono documenti che prescrivono quel complesso di **principi etici, comportamentali e di condotta generali** ai quali i soggetti interni all'organizzazione ed i soggetti che con la stessa interagiscano devono conformarsi. Tali codici, che possono essere anche considerati come la Costituzione dell'Organizzazione, stabiliscono e dichiarano **i valori ed i propositi** a cui si ispira l'organizzazione nei campi del buon governo, dell'integrazione con l'ecosistema degli stakeholder, delle politiche ambientali e sociali, dell'applicazione di comportamenti improntati alla legalità, alla trasparenza e all'equità. La Funzione Compliance deve farsi promotrice della formalizzazione di tali codici e della verifica di coerenza rispetto alla missione, ai valori fondanti ed alle strategie dell'organizzazione.

Cosa sono le policies e che ruolo giocano all'interno dei sistemi di gestione e modelli di compliance?

Le aziende **sono organizzate per processi** funzionali allo svolgimento dell'attività di impresa e che si distinguono in (i) **primari** ovvero quelli che creano valore immediatamente riconoscibile all'esterno, ad esempio i processi relativi alla produzione e alla commercializzazione dei beni e (ii) **secondari** o di supporto al miglioramento del prodotto o del servizio.

La precisa descrizione di ogni processo aziendale e delle sue interdipendenze con gli altri pone le condizioni per il corretto ed efficiente perseguimento degli obiettivi aziendali e per tale proposito è necessario e opportuno che i processi vengano formalizzati mediante policies e procedure, o anche attraverso ulteriori strumenti quali ordini di servizio, flowchart e ogni atto di natura normativa o regolamentare, finalizzato a stabilire ruoli e responsabilità in relazione ad una determinata attività aziendale.

Le **policies** rispondono alla necessità di **formalizzare e regolamentare un particolare processo aziendale nel suo complesso** e indirizzare i comportamenti dei soggetti appartenenti all'organizzazione e di quelli che con la stessa intrattengono rapporti o entrano in contatto nell'ambito di una specifica attività. Parimenti, funzione delle policies è quella di evidenziare e governare le interdipendenze e le interconnessioni tra processi.
Ai fini della **redazione della policy** è necessario:

- individuare la situazione così com'è "*as-is*", ovvero la prassi operativa in quel momento adottata per quel determinato processo;
- analizzare tutte le fasi e le sottofasi che compongono il processo con un approccio basato sul rischio;
- individuare le responsabilità e le attività delle funzioni coinvolte in ottica di una loro segregazione;
- valutare eventuali necessità di miglioramento in termini di efficienza, di conformità, di mitigazione dei rischi; e, infine
- formalizzare tutto il processo (la formalizzazione può variare in relazione alla rilevanza, alla natura del processo).

La **formalizzazione del processo** mira a garantire, *ex post*, la verificabilità della funzionalità e dell'efficienza del processo stesso. Infatti, con il tracciamento di tutte le attività che costituiscono il processo è possibile, in ottica di un controllo, ripercorrere tutte le fasi, tutti gli step autorizzativi alla base delle decisioni tale che si possa individuare l'eventuale inadeguatezza o adeguatezza del processo rispetto ai rischi correlati e con lo stesso presidiati. Talvolta, risulta molto importante la previsione di un **adeguato sistema di flussi informativi** finalizzato a consentire il monitoraggio da parte degli organi a ciò preposti circa il corretto funzionamento del processo disciplinato nella policy, al fine di determinarsi rispetto alle azioni da porre in essere.

Il sistema improntato con la procedura ed il rispetto delle prescrizioni in essa contenute possono funzionare solo se, al di là di un sistema di controlli in senso stretto, sia predisposto un **sistema sanzionatorio finalizzato a colpire quei comportamenti in violazione delle policy e dei processi aziendali**. Il controllo sull'effettiva attuazione delle policy rientra nel perimetro di valutazione adeguatezza del sistema di controllo interno la cui responsabilità è dell'organo di gestione.

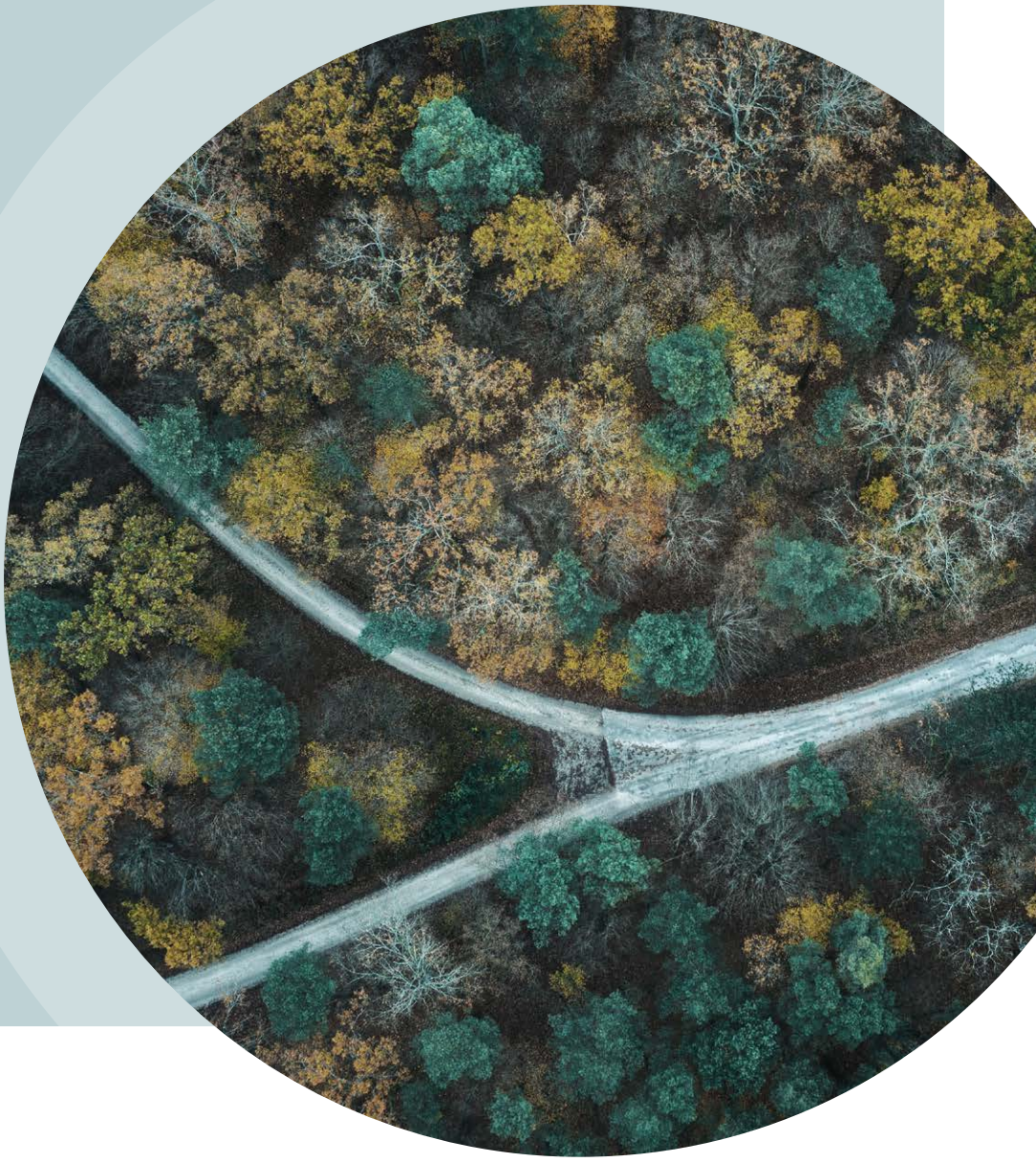
Cosa sono le procedure e che ruolo giocano all'interno dei sistemi di gestione e modelli di compliance?

Le **procedure** sono, quindi, **la descrizione dettagliata di come un processo aziendale deve essere eseguito**, o meglio, di una fase specifica del singolo processo e sono spesso riferite a singole funzioni e consistono in un insieme di attività ripetitive, sequenziali e finalizzate al raggiungimento di un determinato risultato. Tali procedure:

- descrivono puntualmente le modalità con cui le attività devono essere espletate;
- individuano i compiti e le responsabilità in capo alle risorse coinvolte in ciascun processo;
- stabiliscono i controlli su ciascuna attività costituente il processo;
- coordinano i vari organi aziendali coinvolti, definendo nel dettaglio i passaggi tra una funzione aziendale e un'altra;
- individuano dei flussi di comunicazione (work flow) tra le funzioni coinvolte nel processo e necessari all'efficienza dello stesso.

È ampiamente condiviso che per essere funzionali, adeguate ed efficaci le regole interne, i principi di comportamento, i protocolli operativi, i regolamenti interni, le policies e le procedure aziendali, devono essere:

- **formalizzate**, in modo chiaro ed esaustivo, in apposita documentazione che deve essere conservata successivamente in appositi archivi (cartacei/informatici) per un determinato periodo di tempo, al fine di una costante consultazione;
- **comunicate** in maniera efficace e con cadenza periodica - mediante apposite clausole contrattuali, circolari operative interne, incontri e sessioni formative organizzate - a tutta la compagine aziendale e, in particolare, nei confronti di quei soggetti che in relazione all'oggetto sono tenuti ad applicarle. La **conoscenza** di tali regole dovrà necessariamente essere **verificata** per mezzo di **test periodici** sottoposti per compilazione a tutto il personale.



La Funzione Compliance

Ciò premesso, si nota che la Funzione Compliance è, dunque, la **funzione di controllo di secondo livello** il cui compito consiste nel **presidiare i rischi di non conformità** alle norme per prevenire **i conseguenti impatti della non conformità** in termini di perdite finanziarie, di reputazione d'azienda e alla sua capacità di attrarre clienti, investitori e nuove opportunità di sviluppo degli affari, nonché intervenire a seguito di non conformità per abilitare le attività di risposta al rischio.

La funzione compliance svolge un ruolo cruciale nelle organizzazioni, assicurando il rispetto di norme, leggi e regolamenti. La sua attività si sostanzia principalmente nell'individuazione dei rischi di non conformità ed i relativi i controlli posti a presidio di tali ultimi rischi, nel supporto alla corretta definizione, diffusione, nonché corretta attuazione delle policies e delle procedure tese ad indirizzare i comportamenti del Management e dell'organizzazione nel suo complesso.

Tuttavia, il ruolo della compliance va oltre il mero controllo, infatti, è fondamentale evidenziare il ruolo della Funzione Compliance quale partner strategico per le funzioni che gestiscono attività di business e di supporto all'operatività aziendale. La funzione compliance può contribuire a creare un vantaggio competitivo sostenibile nel tempo, integrando la gestione del rischio di compliance nelle attività quotidiane e nella pianificazione strategica.

In un contesto in cui le organizzazioni devono affrontare sfide sempre più complesse e nuove, la funzione compliance può svolgere un ruolo proattivo e strategico, anticipando i rischi e lavorando a

stretto contatto con le diverse funzioni aziendali per assicurare che le decisioni di business siano prese tenendo conto dei requisiti normativi e delle possibili implicazioni per la reputazione dell'organizzazione. Collaborando con le funzioni di business, la funzione compliance può contribuire a identificare opportunità di miglioramento, ottimizzare i processi e garantire che l'organizzazione operi in modo efficiente ed etico. Allo stesso tempo, la compliance si dimostra un alleato strategico in grado di guidare l'organizzazione attraverso le incertezze e i cambiamenti degli scenari economici, politici e normativi, grazie alla sua conoscenza approfondita delle normative e delle leggi in vigore, e alla sua capacità di analizzare e prevedere l'impatto di tali disposizioni sulle attività aziendali, supportando così la crescita sostenibile e l'innovazione responsabile.

Nell'operatività questo si traduce:

- nell'identificazione della normativa rilevante per l'organizzazione monitorando eventuali modifiche legislative;
- nel costante supporto al top management nella definizione degli standard attesi rispetto all'etica, all'integrità ed al rispetto di norme, leggi e regolamenti;
- nella rilevazione e valutazione dei rischi di non conformità, di violazione degli standard etici e di integrità definiti;
- nella formulazione di proposte relative a standard comportamentali e controlli di processo a mitigazione dei rischi;
- nell'esecuzione di verifiche sull'efficace attuazione dei controlli e dei comportamenti attesi;
- nella predisposizione di adeguato reporting al top management, agli organi aziendali preposti e/o alle eventuali Autorità o altri soggetti esterni;
- nel coinvolgimento nella valutazione ex ante della conformità alla regolamentazione applicabile di tutti i progetti innovativi (inclusa l'operatività in nuovi prodotti o servizi nell'ambito del relativo processo di approvazione);
- nell'attività di supporto e consulenza agli organi aziendali e agli altri uffici interni in tutte le materie in cui assume rilievo il rischio di non conformità;
- nella progettazione e realizzazione di interventi formativi e nella diffusione della cultura dell'etica, dell'integrità e della conformità.

1.1

Requisiti, competenze, struttura, attività

Autonomia e indipendenza

Art. 1

La Funzione Compliance deve garantire un livello appropriato di integrità, autonomia e indipendenza nello svolgimento delle proprie attività, compatibilmente ed in coerenza con gli obiettivi strategici dell'organizzazione. Per tale ragione è consigliata la collocazione organizzativa a diretto riporto gerarchico al Chief Executive Officer, garantendo un flusso di comunicazione nei confronti del Consiglio di Amministrazione - anche per mezzo di un riporto funzionale - o all'Amministratore Delegato, senza responsabilità diretta di aree operative sottoposte a controllo e senza subordinazione gerarchica ai responsabili di tali aree. Si potrà, così, essere ragionevolmente certi che la Funzione Compliance si trovi in una posizione che non determini conflitti di interesse rispetto a Funzioni o unità interne preposte alla gestione del business (es. Commercial) o operazioni di produzione di beni e servizi (i.e. Operations) esposte ad uno dei rischi di compliance identificati.

È possibile, nei limiti di quanto consentito da eventuali normative di settore, altresì, ricorrere a soluzioni esternalizzate all'interno del gruppo societario (Funzione Compliance di Gruppo) o all'esterno con il supporto di professionisti specializzati, attraverso la modalità dell'out-sourcing o del co-sourcing. Il responsabile della Funzione Compliance può anche essere membro del Consiglio di Amministrazione della società a cui appartiene o delle società del gruppo societario, purché sia destinatario di specifiche deleghe in materia di controlli e non sia destinatario di altre deleghe e/o linee di riporto gerarchico e/o funzionale che ne pregiudichino l'autonomia.

Art. 2

La Funzione Compliance deve operare secondo un mandato formalizzato dall'Organo Delegato o dal Consiglio di Amministrazione, nel quale siano adeguatamente rappresentati gli aspetti di collocazione organizzativa e riporto gerarchico e/o funzionale, obiettivi, poteri e compiti, mezzi e risorse assegnate. Annualmente l'organizzazione deve valutare l'adeguato assetto della Funzione, delle risorse ad essa assegnate e la sostenibilità degli obiettivi definiti.

Art. 3

La Funzione Compliance viene istituita tenendo in considerazione l'organizzazione, il contesto in cui essa opera, il suo business model, il contesto economico, normativo e regolamentare esterno, la struttura dei processi interni e l'infrastruttura di controllo esistente, nonché gli aspetti connessi alla cultura della conformità.

Focus

Come si garantisce l'autonomia delle Funzione Compliance?

Per assicurare l'autonomia della Funzione Compliance l'organo di gestione o il Consiglio di Amministrazione deve assegnare alla stessa poteri e risorse sufficienti e su base continuativa senza alcun tipo di interferenza o condizionamento da parte dell'organizzazione. La Funzione Compliance dovrebbe avere accesso a tutti i dati aziendali necessari per svolgere in modo appropriato i propri compiti. La Funzione dovrà essere autonoma ed indipendente rispetto alle altre aree operative aziendali tale che il suo giudizio e la sua condotta non siano condizionati da elementi che impediscano o ostacolino la libertà di azione ed il raggiungimento degli obiettivi di conformità.

Come si garantisce l'indipendenza della Funzione Compliance?

Il più ampio livello di indipendenza viene garantito attraverso il posizionamento organizzativo della Funzione Compliance a diretto riporto del Consiglio di Amministrazione, realizzando, in tal modo, uno svincolo da funzioni e ruoli di gestione esecutiva. Ove questo non fosse possibile sono da preferire soluzioni che prevedano il diretto riporto all'Amministratore Delegato. Diversamente, soluzioni organizzative alternative possono essere adottate salvaguardando, in ogni caso, l'indipendenza e la segregazione della funzione da quelle aree aziendali che - in ragione di fattori specifici di rischio

connaturati con il contesto, il mercato, la regolamentazione di settore e l'articolazione del business - sono esposte in forma diretta ai rischi che l'azienda è chiamata ad affrontare e che afferiscono l'ambito di trattazione tipico della compliance. In tali ipotesi, sarà fondamentale assicurare costanti flussi informativi dalla Funzione Compliance verso il Consiglio di Amministrazione, per il tramite di relazioni periodiche che consentano di fornire aggiornamenti in merito alle attività svolte e alle risultanze emerse. Un proficuo confronto tra il Consiglio di Amministrazione e la Funzione Compliance è indispensabile al fine di garantire un costante miglioramento dei presidi di controllo interni e il consolidamento di una cultura aziendale improntata al rischio-reato, che prenda le mosse dall'organo di vertice.

È, inoltre, necessario che la Funzione, nel raggiungimento dei propri obiettivi annuali o di lungo periodo, non sia influenzata ovvero incentivata da obiettivi commerciali, economici o di altro tipo che possano compromettere la sua indipendenza di giudizio nel suggerire o promuovere azioni in linea con gli obiettivi della conformità.

Al fine di assicurare l'indipendenza ma anche l'autonomia è indispensabile, come anticipato, che la Funzione disponga di adeguati mezzi e risorse che possono sostanziarsi in dotazioni organizzative, di risorse umane, tecnologiche o un budget di spesa per l'acquisizione esterna delle stesse

Quali caratteristiche, a garanzia di autonomia e indipendenza, deve avere il mandato della Funzione?

Al fine di garantire autonomia e indipendenza della Funzione, il Consiglio di Amministrazione dovrà definire un mandato alla Funzione formalizzato, attraverso la precisa indicazione di compiti, responsabilità, risultati attesi. Sarà importante, altresì, che l'organizzazione preveda adeguati strumenti e presidi tesi alla prevenzione e alla gestione di eventuali conflitti di interesse, esistenti all'atto del conferimento del mandato o che dovessero insorgere nel corso dello svolgimento dello stesso.

La Funzione dovrà essere connotata, da una parte, da un adeguato livello di autonomia e indipendenza rispetto alle aree di business/operative e, dall'altra, dalla presenza di collegamenti funzionali e di tipo gerarchico in grado di assicurare, in ogni momento, all'Organo di gestione, all'Amministratore Delegato o all'Organo di controllo la conoscenza del livello di rischio assunto dalla società e le modalità di gestione dello stesso.

Competenze

Art. 4

La Funzione Compliance deve essere costituita da risorse umane qualitativamente e quantitativamente adeguate rispetto ai compiti da espletare e che presentino specifiche competenze tecniche e professionali, ricorrendo ove necessario a programmi ed interventi di formazione specialistica.

Art. 5

Ove le condizioni organizzative, la dimensione e le risorse disponibili lo permettano, sono da ricercarsi configurazioni interne della Funzione Compliance di tipo multidisciplinare, in grado di integrare competenze di tipo giuridico ed economico e, ove possibile, capacità di utilizzare gli strumenti informatici, oltre ad un'approfondita conoscenza del settore e del business della Società. Tale principio è da ricercarsi nella coesistenza nell'ambito della Funzione di profili professionali eterogenei, caratterizzati dalla sussistenza di molteplici attributi tecnici in capo a singoli soggetti, ad effetto di percorsi di formazione didattica, scientifica o esperienze sul campo.

Focus

Quali sono le caratteristiche di un team di compliance adeguato alla mission?

Un team di compliance idoneo al perseguimento della mission dovrebbe essere composto da **professionalità adeguate** ad effettuare attività di:

- analisi dei processi di business e delle problematiche connaturate allo svolgimento delle transazioni tipiche dell'azienda, mediante l'utilizzo degli strumenti informatici messi a disposizione dall'azienda;
- analisi del perimetro legale applicabile all'universo di leggi, norme e regolamenti riferiti al settore e all'azienda, ovvero capacità di acquisire ed interpretare nozioni giuridiche in oggetto;
- analisi di aspetti amministrativi ed organizzativi;
- public speaking e formazione in aula;
- instaurare un dialogo concreto con tutti i dipartimenti dell'organizzazione finalizzato ad un virtuoso processo di generazione del valore per le attività di Compliance attraverso interazione con soggetti che gestiscono in prima persona le attività potenzialmente esposte a rischio.

Struttura

Art. 6

La Funzione Compliance viene dimensionata e adattata tenendo conto delle caratteristiche e delle specificità di ciascuna organizzazione tale che disponga delle strutture e delle risorse ad esse proporzionate.

Art. 7

Il modello di governo, l'articolazione interna dei suoi uffici ed il sistema delle interazioni con le altre funzioni ed unità organizzative ed operative dell'organizzazione devono essere improntate a principi di efficacia ed efficienza, avuto riguardo al sovraordinato obiettivo della Funzione, identificato nella preservazione della conformità dell'operato aziendale alle norme, ai regolamenti, alle procedure e ai codici di condotta vigenti, suggerendo - ove si riscontrino disallineamenti - le più opportune soluzioni.

Quale struttura può presentare la Funzione Compliance?

Il ruolo di Responsabile della Funzione Compliance – cd. **Chief Compliance Officer** – può essere ricoperto da un organo unipersonale o da un organo collegiale nell'ambito del quale venga individuato il soggetto che la rappresenta in qualità di Responsabile della compliance. Ragioni di efficienza e di efficacia portano a preferire, nella prassi, per l'assegnazione del ruolo ad organo unipersonale.
Dunque, considerato il raggio di operatività della Funzione è necessario prevedere ed implementare dei modelli di governance efficienti e funzionali. Nella determinazione dell'assetto della struttura della compliance e della scelta del modello organizzativo più aderente alla loro realtà, le imprese tengono conto dei vincoli normativi prescritti dal legislatore, della peculiarità del business, delle caratteristiche dimensionali dell'organizzazione.

Sono **tre le principali tipologie di modelli** che possono essere adottati:

- **Modello centralizzato**: tipico dei settori regolamentati o delle grosse corporation multinazionali, caratterizzato da un forte accentramento delle attività di indirizzo, pianificazione, decisione, e controllo realizzate nell'ambito dell'organizzazione in relazione al tema della compliance, con l'individuazione di un Chief Compliance Officer.
- **Modello decentralizzato**: l'esercizio di attività riconducibili al mandato tipico della Funzione Compliance è distribuito nell'ambito di operatività di più Funzioni, quali ad esempio Legale, Health Safety & Environment, Qualità.
- **Modello intermedio**: prevede strutture specializzate mantenute a livello centrale e strutture più operative articolate a livello decentrato, all'interno di società strutture di business e/o strutture territoriali per tipologia di rischi di compliance.

Spesso la scelta dell'impresa ricade sull'implementazione di un **modello organizzativo *flessibile***, connotato da un grado di accentramento delle attività più elevato nelle fasi intense di recepimento di nuove normative, capace poi di decentrare le attività di gestione quotidiana e operativa della compliance d'azienda.

Obiettivi e attività

Art. 8

La Funzione Compliance opera secondo obiettivi definiti dall'organo amministrativo dell'azienda. Competono, inoltre, all'organo amministrativo valutazioni e decisioni inerenti al profilo di rischio, l'assetto organizzativo, i meccanismi di incentivazione e disincentivazione dei comportamenti considerati conformi.
La Funzione Compliance opera secondo principi e regole di funzionamento definite e formalizzate nella cd. "compliance policy" approvata dall'organo amministrativo e messa a disposizione dell'intera compagine societaria ai fini di conoscenza e di effettivo rispetto della stessa.
Nella determinazione delle caratteristiche di struttura, del perimetro di operatività e degli obiettivi della Funzione, la policy di compliance deve tener conto ed allinearsi agli scopi, alle strategie e ai valori dell'organizzazione.

Art. 9

La Funzione Compliance svolge, secondo un approccio risk based, attività dirette a garantire la conformità dell'operato dell'ente alle norme di etero regolamentazione e di autoregolamentazione, promuovendo tutte le attività necessarie e propedeutiche all'individuazione del perimetro normativo applicabile, all'identificazione e alla valutazione dei rischi di conformità, alla predisposizione dei sistemi di gestione e dei modelli di compliance, alla predisposizione ed attuazione dei piani di monitoraggio, alla consulenza alle funzioni aziendali ed al top management, al reporting, alla formazione e comunicazione, nonché alla diffusione della cultura di compliance.

Art. 10

La Funzione Compliance opera come promotore della cultura dell'etica, dell'integrità e della conformità all'interno e all'esterno dell'azienda. Pertanto, ancorché il mandato sia stato chiaramente definito, la Funzione può essere chiamata a partecipare come attore principale o come coadiuvatore di specifiche progettualità o iniziative esterne al proprio mandato, allorquando tali progettualità o iniziative abbiano attinenza, inerenza o incidenza anche parziale con gli ambiti tipici del proprio mandato.

Quali attività svolge la Funzione Compliance?

Dal punto di vista strettamente operativo, le **attività della Funzione Compliance** possono essere sinteticamente rappresentate come segue:

- Individuazione e monitoraggio del perimetro normativo applicabile;
- Identificazione e valutazione dei rischi di non conformità;
- Predisposizione dei sistemi di gestione e modelli di compliance adeguati ed aggiornamento degli stessi a ragione di eventuali riorganizzazioni o mutamenti;
- Predisposizione ed attuazione di piani di monitoraggio;
- Formazione al personale e implementazione di un sistema di comunicazione e segnalazione efficiente;
- Reporting (periodico e ad evento);
- Consulenza alle funzioni aziendali ed al top management, sia in fase di progettazione organizzativa, di nuovi prodotti, di nuovi servizi, che in occasione della realizzazione di azioni specifiche sul sistema di controllo interno e conformità;
- Nell'ambito delle **interazioni della Funzione Compliance con le altre funzioni interne e con gli attori esterni**, come si dirà di seguito, è possibile annoverare attività di:
  - Consulenza interna sulla materia della compliance;
  - Diffusione della cultura di compliance.

Interazioni, ruolo consulenziale e diffusione della cultura di compliance

Art. 11

La Funzione Compliance opera sotto la costante supervisione della Funzione, dell'Organo o del soggetto sovraordinato gerarchicamente, in coordinamento e relazione costante con la Funzione, l'Organo o soggetto cui è determinato un eventuale riporto di tipo funzionale. La Funzione Compliance deve poter garantire una pronta interazione con tutte le Funzioni o unità interne, deve poter attivare un celere canale di informazione ed interazione con gli Amministratori, l'organo di controllo e gli altri attori del sistema di controllo interno e gestione dei rischi e dovrebbe poter avere accesso a tutte le attività dell'azienda, centrali e periferiche, e a qualsiasi informazione a tal fine rilevante, anche attraverso il colloquio diretto con il personale coerentemente con il proprio mandato.

Art. 12

La Funzione Compliance deve ricercare sinergia di metodo ed azione con gli altri attori del sistema di controllo interno e gestione dei rischi promuovendo, ove possibile e compatibilmente con i propri obiettivi ed il proprio mandato, l'integrazione dei sistemi di gestione e dei modelli organizzativi.

Focus

La Funzione Compliance può essere ritenuta anche un consulente interno sulla materia?

La Funzione Compliance fornisce supporto **all'Organo di gestione** sull'osservanza delle norme legislative, regolamentari e amministrative, **assiste costantemente il Top management** nella modellizzazione dei processi e nella stabilizzazione degli obiettivi interni ed esterni, in conformità con la normativa ed, infine, **supporta l'operatività aziendale e il business al fine di creare un vantaggio competitivo** sostenibile nel tempo, integrando la gestione del rischio di compliance nelle attività quotidiane e nella pianificazione strategica.
Tale attività di supporto, assistenza e consulenza determina un sempre più assiduo e tempestivo coinvolgimento della Funzione Compliance, in **qualità di advisor**, più che nel ruolo di funzione di controllo e rappresenta un utilissimo, quasi indispensabile strumento, ai fini

di prevenzione dei rischi di compliance e di gestione degli stessi. Tale coinvolgimento rappresenta l'unico strumento adeguato a far fronte al cambiamento delle variabili esogene, quali, l'attività del legislatore nazionale ed internazionale, l'atteggiamento dei consumatori, l'evoluzione giurisprudenziale. Dunque, diventa imprescindibile l'adeguata implementazione di una solida struttura di compliance che svolga un ruolo fondamentale di consulente autorevole nei confronti del Top Management, di tutte le aree operative e di business, e talvolta, perfino nel design di cambiamenti strategici, organizzativi, distributivi, operativi ed informatici dell'impresa.
I compiti consultivi della funzione Compliance non implicano, tuttavia, che essa assuma poteri decisionali o che le venga trasferita alcuna responsabilità derivante dalle azioni o omissioni dell'Organo di gestione dell'alta direzione o delle posizioni dell'organizzazione dotati di procure e deleghe.

Qual è il ruolo della Funzione Compliance nella diffusione della cd. *cultura di compliance*?

La Funzione Compliance ha il compito di contribuire alla diffusione ed al consolidamento di una consapevolezza e una cultura d'impresa in materia di compliance, così come la trasparenza e la responsabilità di tutta l'organizzazione.

- Risulta, infatti, fondamentale sensibilizzare l'impresa ed aumentare la consapevolezza del personale dell'organizzazione di tutti i rischi di non di conformità. Iniziative mirate a diffondere la cultura della compliance possono essere a titolo esemplificativo: la messa a disposizione del personale interno e delle terze parti all'uopo identificate di Codici Etici, Codici di condotta o testi equivalenti che enuncino e sanciscano i valori e gli standard di comportamento attesi dall'organizzazione; la messa a disposizione del personale interno e delle terze parti all'uopo identificate di Sistemi di gestione e Modelli di compliance definiti allo scopo di indirizzare comportamenti e modalità di esecuzione delle operazioni aziendali in conformità con norme, leggi e regolamenti ovvero con standard volontariamente adottati dalla Società;
- la promozione di attività di formazione, comunicazione e discussione interna ed esterna sul contenuto dei summenzionati documenti onde facilitare una migliore e più efficace diffusione dei loro contenuti ed una adeguata comprensione di essi da parte dei destinatari; l'instaurazione di un canale di dialogo e di supporto con tutto il personale interno e, compatibilmente e coerentemente con le regole di comunicazione esterna, con soggetti esterni all'organizzazione, al fine di fornire prontamente gli elementi utili alla migliore comprensione di Codici, Policy e Procedure di Compliance e, in generale, di prestare supporto per favorire l'adozione di condotte allineate alle politiche di gestione della compliance adottate.

CAPITOLO 2

Framework Normativo

La presenza di una Funzione Compliance, obbligatoria in taluni settori di attività, nasce dalle riflessioni condotte a livello internazionale, anche a fronte di scandali e fallimenti che hanno coinvolto istituzioni economiche di rilievo.
A tal proposito, divengono casi emblematici quelli di alcuni colossi economici coinvolti in fatti di bancarotta fraudolenta, aggiotaggio e corruzione internazionale che hanno reso sempre più evidente la debolezza dei modelli di corporate governance, adottati ed applicati dalle organizzazioni economiche e, soprattutto, l'esigenza di rafforzare i presidi organizzativi interni, volti ad assicurare la piena osservanza delle normative di autoregolamentazione e di etero regolamentazione e a tutelare le relazioni con il mercato.

Da tale ultima esigenza si muovono i legislatori nazionali ed internazionali per l'avvio di una importante produzione normativa che detta disposizioni che si fanno normalmente rientrare nelle attribuzioni della compliance, richiedendo il contributo della omonima Funzione affinché le organizzazioni operino in maniera conforme a quanto prescritto dalle stesse.

Di seguito si riporta, a titolo meramente esemplificativo e non esaustivo, il perimetro regolatorio rilevante per l'operatività della Funzione Compliance, distinto in:

- **normative internazionali**: tra le quali, trattati internazionali, patti e convenzioni che rientrano nel novero delle norme di diritto internazionale generalmente riconosciute di cui all'art. 10 della Costituzione Italiana;
- **normative nazionali**: tra le quali il D.lgs. 231/2001 in materia di responsabilità amministrativa delle persone giuridiche, il GDPR, normativa in materia di concorrenza ed altre;
- **normative di settore**: che disciplinano gli aspetti di conformità dei settori regolamentati.

2.1

Le principali normative internazionali

Global compact

Per **Global Compact** si intende il **Patto Globale stipulato tra i leader dell'economia mondiale** - proposto nel 1999 da Kofi Annan l'allora Segretario delle Nazioni Unite in occasione del World Economic Forum - nell'ottica di promuovere la **cultura della responsabilità sociale d'impresa** e di supportare e dare realizzazione ai **10 principi universali nell'ambito dei diritti umani, del lavoro, della tutela dell'ambiente e della lotta alla corruzione** per creare finalmente una **economia globale il più possibile sostenibile e inclusiva.**

A partire **dal 2000** il Global Compact inizia ad essere sviluppato nell'obiettivo di diventare progressivamente la sede globale del confronto tra le potenze mondiali circa i temi più delicati, critici ed importanti per la società contemporanea. Tale accordo ha origine dall'assunto che le imprese hanno una visione strategica di lungo periodo orientata alla responsabilità sociale, all'innovazione e all'accountability che permette loro di contribuire ad una nuova globalizzazione caratterizzata da sostenibilità, cooperazione internazionale e partnership multi-stakeholder ed azioni collettive nel perseguimento di obiettivi comuni o condivisi. In concreto, le attività si sostanziano nell'approfondimento, nel costante dialogo culturale ed istituzionale, nella predisposizione di progetti e iniziative che hanno quale centro di attenzione la sostenibilità e la responsabilità d'impresa verso i temi più rilevanti e così enunciati nei principi universali.

Per quanto riguarda l'**Italia**, il cd. "**Global Compact Network Italia**" si costituisce nel **2002** con la mira di dare un importante contributo al "Patto Globale" con l'accrescimento della credibilità e della serietà nell'impegno a favore della responsabilità sociale da parte delle imprese aderenti all'iniziativa. Nel **2013** viene a costituirsi in fondazione - **Fondazione Global Compact Network Italia** – ai fini di promozione nel territorio nazionale dei dieci principi del Global Compact e nell'avanzamento degli "Obiettivi globali di Sviluppo Sostenibile" (SDGs) per lo sradicamento della povertà estrema, la diffusione della pace e la promozione della prosperità e dello sviluppo umano entro il 2030.

Convenzione OCSE sulla lotta alla corruzione dei pubblici ufficiali stranieri nelle transazioni commerciali internazionali

La **Convenzione dell'Organizzazione per la Cooperazione e lo Sviluppo Economico (OCSE) sulla lotta alla corruzione dei pubblici ufficiali stranieri nelle transazioni commerciali internazionali** - redatta a Parigi nel 1997 ed è entrata in vigore il 15 dicembre del 1999 - dà il via ad una serie di interventi estremamente rilevanti nell'ambito della normativa nazionale circa la lotta ed il contrasto alla corruzione.

In prima istanza e più nel dettaglio, la Convenzione OCSE ha condotto all'introduzione della fattispecie di cui all'**art. 322-bis c.p.,** disciplinante la **corruzione dei pubblici ufficiali di altri Stati esteri o organizzazioni pubbliche internazionali nelle operazioni economiche internazionali**.

In seconda istanza, la Convenzione ha **condotto ad una svolta sensazionale nell'ambito della disciplina della responsabilità delle persone giuridiche per i fatti di corruzione in esse concretizzatisi**, ponendo in capo agli Stati aderenti e alle imprese in questi operanti **l'obbligo di perseguire** non solo la persona fisica autrice della fattispecie corruttiva, ma anche **le organizzazioni economiche eventualmente coinvolte nel fatto illecito**. La Convenzione arrivava, addirittura e per la prima volta, a riconoscere l'opportunità per gli Stati aderenti di prevedere una **responsabilità di natura penale in capo alle persone giuridiche** purché strumento efficace in termini di deterrenza.

Tuttavia, come noto, l'ordinamento nazionale italiano non prevedeva l'ascrivibilità di una responsabilità di natura penale, civile o amministrativa in capo alle persone giuridiche – data la pregnanza dell'assunto *"societas delinquere non potest"* – per eventuali fatti corruttivi avvenuti in costanza del perseguimento degli obiettivi di business e dell'espletamento delle attività d'impresa.

Ciò posto, è evidente che la Convenzione e la relativa necessità di recepimento della medesima abbia condotto il legislatore nazionale a consacrare per la prima volta una **responsabilità di natura amministrativa derivante dalla realizzazione di un fatto penalmente rilevante** – quale ad esempio la corruzione sia interna che internazionale - **delle persone giuridiche** con l'introduzione del summenzionato **decreto legislativo 231 del 2001**.
Orbene, l'introduzione della Convenzione OCSE nell'ordinamento na-

zionale ha condotto, dunque, all'imposizione di importanti vincoli giuridici alle organizzazioni economiche attive nei mercati nazionali ed internazionali volti a garantire non solo l'integrità delle amministrazioni pubbliche, ma anche e soprattutto la correttezza e lealtà della concorrenza internazionale.

Regolamento UE 2021/821, *Export Control*

Il regolamento in argomento stabilisce le norme valide in tutta l'Unione Europea per il controllo delle esportazioni, dell'intermediazione (negoziazione o l'organizzazione di operazioni tra paesi terzi ai fini della vendita o dell'acquisto di prodotti a duplice uso), dell'assistenza tecnica, del transito e del trasferimento di prodotti a duplice uso (quei prodotti, inclusi software e tecnologie, che possono avere un utilizzo sia civile che militare).
La disciplina in materia di esportazioni è oggi posta, dunque, dal **Regolamento UE 2021/821** che mira a:

- sostenere l'implementazione di un sistema di controlli in materia più armonizzato ed efficace;
- adeguare il sistema dei controlli alle nuove minacce associate al progresso tecnologico;
- fornire elevata protezione dei diritti umani mediante un fermo sostegno di un commercio più sostenibile e responsabile.

Da tali iniziative si evince la rilevanza del tema del controllo della **corretta gestione delle esportazioni**, oggi più che mai rilevante, dato il contesto socioeconomico contemporaneo caratterizzato da sistemi di comunicazione e scambio sempre più celeri e complessi.
Si riscontra, dunque, la necessità che le organizzazioni attive sui mercati internazionali adottino i cd. **Export Compliance Administration Program**, che contemplano:

- una **preliminare valutazione del rischio dell'operazione di esportazione** da realizzare, osservando se le caratteristiche tecniche dei prodotti da esportare determinino la richiesta di autorizzazioni particolari, come quelle per i beni a duplice uso (cd. *Dual Use*: prodotti e tecnologie destinati ad usi civili ma utilizzabili anche nello sviluppo di armamenti, di programmi nucleari di tipo bellico o di armi di distruzione di massa) e se le merci debbano essere esportate in Paesi soggetti a sanzioni o misure restrittive da parte di Organismi Internazionali o dell'Unione Europea;

- **l'adozione di specifiche politiche, procedure o istruzioni interne** volte a disciplinare le attività attinenti alle esportazioni cosicché siano svolte in ottemperanza alla normativa di settore.

L'attuale perimetro normativo in materia di Export Control trova origine nella necessità di contrastare il pericolo che i beni a duplice uso venissero esportati con il fine di impiegarli per scopi illeciti. Tuttavia, gli scopi della normativa si sono di tanto ampliati essendo emersi ulteriori rischi da fronteggiare relativi alla violazione dei regimi sanzionatori, embarghi e altre misure restrittive applicati ai paesi considerati più a rischio da un punto di vista geopolitico o della concorrenza, nei confronti di organizzazioni ed anche delle persone fisiche.

Focus

Qual è il ruolo della Compliance?

La Funzione Compliance anche in tale settore può svolgere un ruolo chiave in termini di gestione dei rischi e di garanzia di conformità. In particolare, la stessa può:

- effettuare **attività di identificazione, gestione e controllo dei rischi** derivanti dalle attività di export;
- **supportare le organizzazioni** nella predisposizione della documentazione relativa **all'ottenimento di licenze, autorizzazioni e certificazioni** ai fini del corretto e regolare svolgimento delle attività di export;
- **efficientare la gestione dei rischi** nell'ambito dell'impresa per mezzo della **predisposizione di organizzativi e di piani di formazione** ad hoc finalizzati all'introduzione della materia dell'Export Compliance;
- svolgere **attività di due diligence su terze parti** per verificare l'eventuale presenza delle medesime nelle cd. blacklists dell'Unione Europea o di altri Paesi;
- predisporre ed implementare dei cd. **Export Compliance Administration Program**, mediante l'adozione di un insieme di procedure formalizzate che vanno a rappresentare un ICP (Internal Compliance Program) basato sui dettami delle normative di settore e focalizzato sull'Export Compliance ed in sinergia con il sistema di controllo interno implementato dall'organizzazione;
- **redigere pareri di Export Compliance** per singole operazioni di export o a questioni di particolare complessità.

Regolamento UE 2016/679, “GDPR”

Negli ultimi anni lo sviluppo tecnologico ha condotto all’ottimizzazione di molteplici attività, portando, tuttavia, con sé molteplici problematiche relative alla gestione dei dati che circolano mediante i sistemi informatici.
Con specifico riguardo alla **protezione delle persone fisiche rispetto al trattamento dei dati personali** e alla libera circolazione di tali dati, il legislatore europeo è intervenuto con l’emanazione - da ultimo - del **Regolamento (UE) 2016/679**, ***General Data Protection Regulation***, (cd. “**GDPR**”).
Nell’ambito delle disposizioni poste a garanzia dei dati personali, il legislatore individua diversi soggetti coinvolti nel cd. “**trattamento**” **dei dati personali** - inteso come *“qualsiasi operazione o insieme di operazioni, compiute con o senza l’ausilio di processi automatizzati e applicati ai dati personali o insieme di dati personali, come la raccolta, la registrazione, l’organizzazione, la strutturazione, la conservazione, l’adattamento o la modifica, l’estrazione, la consultazione, l’uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l’interconnessione, la limitazione, la cancellazione o la distruzione”* - quali:

SOGGETTO	RUOLO E RESPONSABILITÀ
Interessato	Colui al quale appartiene il dato personale oggetto del trattamento ed al quale sono riconosciuti tutti i diritti a ciò attinenti.
Titolare	La persona fisica o giuridica che determina le finalità del trattamento ed impartisce istruzioni vincolati nei confronti dei responsabili.
Responsabile	La persona fisica o giuridica che tratta i dati personali per conto del Titolare, designata per contratto o altro atto giuridico.
Incaricato	La persona fisica titolare o il responsabile del trattamento designato, nell’ambito dell’organizzazione, per lo svolgimento di specifiche attività inerenti al trattamento.
Responsabile della protezione dei dati (“DPO”)	Il cd. “facilitatore della compliance” individuato anche come una sorta di “Garante Privacy” interno all’organizzazione definito Data Protection Officer (“DPO”) e designato nei casi espressamente previsti dalla normativa (art. 37 GDPR). Il DPO è un professionista, interno o esterno all’ente, dotato di competenze giuridiche, informatiche e di risk management la cui responsabilità principale è quella di informare e fornire consulenza al titolare e al responsabile del trattamento circa i contenuti degli obblighi su loro gravanti, nonché di svolgere attività di sorveglianza e di cooperazione e contatto con il Garante.

Nell'ambito del **trattamento dei dati personali** si annidano **molteplici rischi che l'ente deve necessariamente prevedere, gestire e mitigare**, quali ad esempio la perdita, il furto, la divulgazione non autorizzata dei dati personali, l'alterazione o la distruzione degli stessi a causa di incidenti o eventi avversi. Ai fini della gestione di tali ultimi rischi e della conformità ai dettami normativi posti a protezione dei dati personali, è necessario che l'ente si serva dell'operato della **Funzione Compliance**, o nei casi previsti del **DPO**, per rispettare i principi, adottare procedure organizzative e di sicurezza in tale ambito.

Focus

Qual è il ruolo della Funzione Compliance?

La **Funzione Compliance**, talvolta, può essere chiamata a ricoprire il ruolo di **Data Protection Officer** – cd. "DPO", quale responsabile della conformità in materia di trattamento dei dati personali in seno alla compliance che ha il compito di sviluppare un programma interno di conformità al GDPR.
Al responsabile di tale ufficio può alle volte essere affidato tale ruolo, data la similarità delle rispettive incombenze, tra le altre:

- lo sviluppo di un privacy compliance program;
- il supporto all'organizzazione nel fornire contributi utili a considerare elementi di conformità "by design" relativa a processi, prodotti e servizi;
- l'esecuzione periodica di controlli relativamente all'attuazione ed al rispetto delle prescrizioni in materia di trattamento dei dati, nell'ambito dei quali avrà necessità di raccogliere periodicamente, attraverso appositi "flussi informativi", informazioni relative alle innovazioni introdotte in azienda dal punto di vista organizzativo, tecnologico, di business;
- la pianificazione e l'esecuzione di sessioni formative rivolte alla compagine societaria così da consolidare una cultura di conformità alle disposizioni di cui al GDPR;
- Posto ciò, tuttavia, risulta preferibile segregare i ruoli di chi implementa un programma di compliance e di chi è chiamato a controllarne la sua adeguatezza, pertanto affidare il ruolo di DPO ad un soggetto altro, interno od esterno all'ente, rispetto al Chief Compliance Officer.

Environmental, social, governance ("ESG")

Nel contesto sociale ed economico contemporaneo è diventata sempre più avvertita la necessità di **garantire la sostenibilità dell'operato tanto del singolo quanto delle organizzazioni economiche**.
Ciò posto, è venuto in rilievo il nuovo termine "**Environmental, Social e Governance" (cd. "ESG")** per indicare tutte quelle attività espletate dalle organizzazioni che perseguono gli obiettivi di business, ma che tengono ormai in debito conto tutti gli aspetti di natura ambientale, sociale e di governance che vengano in rilievo, data l'odierna rilevanza dei fattori ESG in termini di ritorno economico, finanziario e reputazionale per un'impresa.
Tale termine è costituito da **tre fattori fondamentali ai fini della misurazione e la determinazione della sostenibilità** e **dell'impatto etico di un ente**, nel dettaglio:

- **Environmental: l'impatto** delle organizzazioni **nell'ambito delle sfide ambientali** attraverso una attenta valutazione delle condotte dell'ente sulla base di specifici criteri;
- **Social: l'impatto sociale** delle organizzazioni, nel senso della capacità delle medesime di fare la differenza, in termini positivi, sul tessuto sociale nel quale operano.
- **Governance:** l'idoneità dell'assetto organizzativo, del governo societario degli enti ai fini del perseguimento degli obiettivi ESG.

In tale contesto risulta evidente che gli Organi amministrativi, ma soprattutto le **funzioni di controllo dell'impresa** debbano essere allineati – mediante il continuo confronto ed un operare sinergico - ed impegnati nel raggiungimento degli obiettivi di sostenibilità, oggi imprescindibili per un'ottima reputazione di un'organizzazione nel mercato di riferimento.

Focus

Qual è il ruolo della Compliance?

Considerate le competenze tecnico-professionali della Funzione Compliance è chiaro che la medesima possa svolgere un **ruolo rilevante per il raggiungimento degli obiettivi di sostenibilità** dell'impresa, in quanto **risulta in grado di**:

- monitorare costantemente l'addivenirsi delle prescrizioni normative in ambito ESG;
- promuovere l'adeguamento dell'organizzazione interna (es. policies, procedure di selezione di gestione degli outsourcer, definizione del sistema di deleghe e procure, piani strategici) alle prescrizioni normative e agli standard ESG;
- promuovere e coadiuvare l'ente nell'adozione di modelli organizzativi e di governance che siano funzionali in termini di sostenibilità ambientale, tenendo conto delle istanze degli investitori, del mercato e degli obiettivi di business;
- supportare il Top Management e l'organo di gestione nella elaborazione di strategie di gestione dei rischi ESG (es. violazioni del diritto della concorrenza, scarsità di risorse naturali, abusi dei diritti umani, discriminazione sul posto di lavoro, frodi contabili o fiscali, violazioni dei dati e altro ancora) ad esempio attraverso eventuali ESG Compliance Programs;
- pianificare e fornire adeguata formazione e la responsabilizzazione di tutta la compagine societaria in ambito ESG.

2.2
Le principali normative nazionali

D.LGS. N. 231/2001

Il D.lgs. n. 231/2001, contenente la "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica", ha introdotto nell'ordinamento nazionale la cd. **responsabilità amministrativa derivante da reato degli enti** che considera l'Ente quale autonomo ed ulteriore centro d'imputazione rispetto all'autore della condotta criminosa.
Si addiviene, pertanto, al superamento del dogma "societas delinquere non potest" alla lettera del quale soltanto una persona fisica può rispondere dell'illecito penale e non anche una persona giuridica.
L'**art. 1, comma 2**, del decreto prescrive che **possono incorrere** in questo tipo di responsabilità gli enti forniti di personalità giuridica e le società e le associazioni anche prive di personalità giuridica. Sono **invece esclusi**, lo Stato e gli enti pubblici territoriali, gli altri enti pubblici non economici e gli enti che svolgono funzioni di rilievo costituzionale.
È necessario precisare che, ai sensi dell'**art. 5** del decreto in argomento, **l'ente potrà essere chiamato a rispondere ed eventualmente considerato responsabile soltanto laddove**:

- si configuri **uno dei reati tassativamente elencati nel decreto agli artt. 24 e ss.**;
- il **fatto criminoso sia stato posto in essere nel suo interesse o a suo vantaggio**;
- la **condotta sia stata realizzata da soggetti apicali**, ossia che rivestono, anche di fatto, funzioni di rappresentanza, amministrazione o direzione o da soggetti sottoposti alla loro vigilanza, a prescindere dal fatto che siano dipendenti dell'ente o esterni ad esso.

CONDIZIONE ESIMENTE DELLA RESPONSABILITÀ DELL'ENTE

Si precisa che la **responsabilità dell'ente è presunta** qualora l'illecito sia stato realizzato dai cd. **soggetti apicali**, di cui all'art. 5 pocanzi citato. Da tale presunzione **deriva un'inversione dell'onere della prova a carico dell'ente** medesimo che, **al fine di escludere la propria respon-**

sabilità - a norma **dell'art. 6 del D.lgs. 231/2001** - deve provare che:

- l'ente si sia **dotato di un modello di organizzazione, gestione e controllo** che è stato **attuato efficacemente**;
- il compito di vigilare sul funzionamento e l'osservanza dei modelli, di curare il loro aggiornamento sia stato affidato al cd. **Organismo di Vigilanza** dotato di autonomi poteri di iniziativa e di controllo;
- il reato sia stato commesso mediante **elusione fraudolenta del modello**;
- **la vigilanza** da parte dell'Organismo di Vigilanza **non sia stata omessa o insufficiente**.

Se, invece, il **reato è stato commesso dai sottoposti**, **l'ente risponde** solo **se la commissione dell'illecito è stata resa possibile dall'inosservanza degli obblighi di direzione e vigilanza**. Al contrario, l'ente non risponde se essi hanno agito nell'esclusivo interesse proprio o di terzi.
Qualora accertata la responsabilità amministrativa dell'Ente, quest'ultimo vedrà applicarsi **una sanzione o più sanzioni congiuntamente** tra cui: sanzioni pecuniarie, interdittive, la confisca o, ancora, la pubblicazione della sentenza di condanna.

Focus

Qual è il ruolo della Compliance nell'ambito di operatività del Decreto 231?

La Funzione Compliance coadiuva il Management nell'adozione del Modello di organizzazione, gestione e controllo ed in particolare può occuparsi di:

- coordinare le attività di predisposizione e aggiornamento del Modello, nonché tutte le azioni per garantirne l'efficacia efficace;
- recepire le indicazioni dell'Organismo di Vigilanza afferenti al Modello;
- definire i principi etici e morali da inserire nel Modello e nel Codice Etico e di Condotta;
- supportare l'Organismo di Vigilanza nella raccolta ed analisi dei flussi informativi richiesti dal D.lgs. 231/2001;
- supportare la definizione e la realizzazione di attività formative in materia di conformità.

Whistleblowing: D.LGS. N. 24/2023

Il termine "**whistleblowing"** è di matrice anglosassone e si riferisce a quello **strumento volto a garantire un'informazione tempestiva circa eventuali fatti illeciti posti in essere a danno o ad opera dell'organizzazione.** Più nel dettaglio, tale strumento consente ad uno o più membri di un'organizzazione o anche da persone esterne all'organizzazione, ma che con essa mantengono specifici rapporti, di comunicare il rischio del concretizzarsi o la già avvenuta realizzazione di un'azione illecita, una condotta immorale o illegittima (cd. "wrongdoing"), quale atto contrario ai principi etici posti alla base dell'operato dell'organizzazione - compresi i comportamenti penalmente rilevanti - realizzata da un determinato soggetto interno all'ente.
Dato il proliferare del fenomeno corruttivo in tutti i settori di attività e, soprattutto, nell'ambito privato oltre che quello pubblico, è venuta in rilievo la necessità di implementare tale sistema di tutela nel settore privato con **Direttiva Europea sul Whistleblowing (2019/1937)**, avente ad oggetto la protezione delle persone che segnalano violazioni del diritto dell'UE ed adottata dal Parlamento Europeo e dal Consiglio del 23 ottobre 2019 e che impone a tutti gli Stati membri dell'Unione Europea di adottare misure idonee a prevedere l'obbligo per le aziende con più di 50 dipendenti di dotarsi di un canale per le segnalazioni whistleblowing.
A tal riguardo, il legislatore nazionale ha provveduto a recepire le prescrizioni della summenzionata Direttiva Europea attraverso il ***Decreto Legislativo del 10 marzo 2023 n. 24 di "Attuazione Della Direttiva (UE) 2019/1937 Del Parlamento Europeo e del Consiglio, del 23 Ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'unione"***.
Lo scopo primario del Decreto n. 24/2023 è quello di disciplinare, sulla base delle disposizioni della direttiva europea, la protezione dei cosiddetti whistleblowers e, dunque, delle persone che segnalano violazioni di disposizioni normative nazionali o dell'Unione Europea che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato, di cui siano venute a conoscenza in un contesto lavorativo pubblico o privato.
Più in generale, il Decreto mira a promuovere la cultura della legalità e della compliance nei contesti organizzativi, tramite l'armonizzazione della disciplina del whistleblowing alle indicazioni delle Istituzioni euro-unitarie e alle best practices internazionali.

Nello specifico, il Decreto in parola:

- individua i soggetti obbligati all'implementazione di un sistema di segnalazione (destinatari);
- disciplina le modalità e le tempistiche del processo di gestione della segnalazione;
- prevede una tutela dalle ritorsioni nei confronti del soggetto segnalante (dipendenti ai clienti, fornitori, ex dipendenti, ed altri);
- assicura la protezione del soggetto segnalante dal licenziamento nonché da qualsiasi atto di demansionamento o altre forme di discriminazione.

Focus

Qual è il ruolo della Compliance?

La Funzione Compliance, soprattutto nelle imprese di grandi dimensioni, **ha le competenze ed i requisiti idonei alla gestione, ovvero a fornire il contributo interno alla gestione, del canale delle segnalazioni di illeciti**. La medesima risulta avere piena conoscenza del contesto aziendale e normativo di riferimento tanto da essere in grado di **ricevere le segnalazioni, valutarle e, se del caso, avviare le investigazioni interne** mantenendo sempre un contegno imparziale rispetto ai fatti.

Tale ruolo della Compliance, nell'ambito del whistleblowing, rappresenta **un'opportunità per l'ente ai fini di effettiva prevenzione degli illeciti, di disfunzioni o frodi interne**.

Alla conclusione delle attività, la Funzione Compliance si occuperà di riportare e rendicontare le attività espletate e le risultanze delle stesse agli organi di governo societario, e di informare il segnalante circa la fondatezza della segnalazione e degli sviluppi della stessa.

Il coinvolgimento della Funzione Compliance nel processo di gestione delle segnalazioni determina, altresì, la necessità di prevedere specifiche forme di tutela anche a beneficio della stessa, la quale dovrebbe essere tenuta indenne da azioni ritorsive o discriminatorie per aver fornito il proprio contributo all'emersione di eventuali condotte poste in essere in violazione di policy, procedure, principi etici ed in generale del sistema dei controlli interni. Tali tutele dovrebbero essere riflesse in norme o regolamenti aziendali approvati dagli Organi di gestione.

Antitrust: L. 287/1990 e D.LGS. N. 206/2005

Il termine "**Antistrust"** rappresenta quel complesso di disposizioni normative che mirano, **da un lato, a tutelare i diritti del consumatore e, dall'altro, a garantire il corretto funzionamento dei mercati**, in particolare, la leale concorrenza dei molteplici operatori economici che nei medesimi si muovono tale che si addivenga ad un efficientamento della distribuzione di beni e servizi.
Il legislatore, nell'obiettivo di impedire alle organizzazioni di operare in modo sleale, ostacolando o influenzando la regolare competizione economica e consolidando le posizioni di monopolio, ha provveduto ad istituire il cd. "**diritto alla concorrenza**".
Sulla base di tale assunto, **l'Italia si è adoperata nell'introduzione di tale impianto di tutele con** la **Legge n. 287 del 10 ottobre 1990 recante *"Norme per la tutela della concorrenza e del mercato"* (cd." Legge Antitrust").**

La legge 10 ottobre 1990 n. 287 introduce **due fondamentali forme di violazione del diritto alla concorrenza**: **(I)** l'abuso di posizione dominante e **(II)** l'intesa restrittiva della concorrenza.
Nell'ottica di garantire il corretto funzionamento dei mercati e, dunque, l'osservanza delle regole che li disciplinano, i dettami normativi contemplano l'istituzione di un Organismo ad hoc che si occupi di espletare tale attività nel territorio nazionale: l'**Autorità Garante della Concorrenza e del Mercato (AGCM)** quale ente amministrativo indipendente, noto anche come Antitrust, che è tenuto a vigilare su: **(I)** abusi di posizione dominante; **(II)** la presenza di intese e/o cartelli lesivi o restrittivi per la concorrenza e; **(III)** operazioni di concentrazione che superano un certo valore.

L'ente si occupa, altresì, di tutelare il consumatore nei casi in cui le imprese, invece di competere tra loro, si accordino e coordinino i loro comportamenti sul mercato restringendo la concorrenza, danneggiando i consumatori o gli altri concorrenti.
A valle degli accertamenti di eventuali violazioni, l'Antitrust potrà irrogare sanzioni **amministrative pecuniarie** anche piuttosto impattanti sul fatturato degli enti economici destinatari (sanzioni di diversi milioni o miliardi di euro per le più grandi multinazionali) e, ovviamente, sulla loro reputazione.

In tale sede è opportuno sottolineare che nel 2005, in attuazione della **Direttiva Europea (29/2005/CE)**, le competenze dell'Autorità Garante della Concorrenza e del Mercato sono state ampliate attraverso l'introduzione di specifiche disposizioni poste a **tutela del consuma-**

tore contro tutte le pratiche commerciali scorrette poste in essere dalle imprese nei confronti dei consumatori. In particolare, il legislatore nazionale ha voluto disciplinare e dare rilievo ai casi in cui, ad esempio, un'impresa tenti di falsare le scelte economiche del consumatore attraverso l'omissione di informazioni rilevanti oppure la diffusione di informazioni non veritiere. A tal riguardo, nell'ambito delle competenze dell'Antitrust in materia di tutela del consumatore, viene in rilievo il potere dell'Autorità di accertare l'eventuale vessatorietà di clausole contrattuali inserite dalle imprese nei contratti stipulati con i consumatori.
In tutti i casi sopra citati, è stato riconosciuto all'Antitrust il potere di intervenire, anche in via cautelare, imponendo specifiche **sanzioni alle imprese** che operino in danno dei consumatori.
La prescrizioni di cui alla Direttiva sono state oggetto di recepimento nel nostro ordinamento giuridico con il **Decreto legislativo 6 settembre 2005, n. 206**, cd. "**Codice del Consumo**", relativo al riassetto delle disposizioni vigenti in materia di tutela dei consumatori, che comprende la maggior parte delle disposizioni emanate dall'Unione Europea nell'ambito della tutela e protezione del consumatore.

L'approvazione del Codice del Consumo va considerata una svolta importante nella tutela dei consumatori italiani, in quanto ha messo in atto **un'opera di riorganizzazione della materia**, conducendo a definire specifiche regole attinenti alle fasi del rapporto di consumo, alla pubblicità e alla corretta informazione, ai contratti con i consumatori, alla sicurezza dei prodotti, all'accesso alla giustizia e, ancora, alle associazioni rappresentative di consumatori.

Circolare n. 285/2013 di Banca d'Italia sulle *Disposizioni di vigilanza per le banche*

La Circolare n. 285/2013, emessa dalla Banca d'Italia, riguarda la "Supervisione delle banche - Disposizioni di vigilanza per le banche" e stabilisce le principali regole prudenziali e i requisiti di vigilanza applicabili alle banche operanti in Italia. Questa circolare è stata emessa per garantire la stabilità finanziaria, la solidità e l'affidabilità del sistema bancario italiano. La circolare si occupa di molteplici argomenti, tra cui:

- **Requisiti patrimoniali**: individuazione dei requisiti minimi di capitale che le banche devono mantenere per assorbire le perdite e far fronte ai rischi di credito, di mercato e operativi;
- **Governance e organizzazione**: definizione di best practice in materia di governance e organizzazione interna delle banche, includendo requisiti per la struttura organizzativa, la gestione dei conflitti di interesse e le funzioni di controllo interno (es. Compliance, Internal Audit e Risk Management);
- **Rischi e controlli interni**: indicazione alle banche di identificazione misurazione, gestione e monitoraggio di vari tipi di rischio a cui sono esposte, come il rischio di credito, il rischio di mercato, il rischio operativo, il rischio di liquidità e il rischio di interesse. Le banche devono implementare un efficace sistema di controllo interno per mitigare e gestire questi rischi;
- **Remunerazione e incentivazione**: determinazione dei principi e criteri per l'adozione di politiche di remunerazione e incentivazione che siano coerenti con una gestione sana e prudente delle banche e che non incentivino la presa di rischi eccessivi o comportamenti scorretti;
- **Trasparenza e divulgazione delle informazioni:** imposizione della garanzia di comunicazione chiara, tempestiva e accurata delle informazioni relative alla loro situazione finanziaria, alla gestione dei rischi e alla governance interna, sia nei confronti degli azionisti e degli investitori, sia nei confronti dei clienti e del pubblico in generale;
- **Vigilanza consolidata**: la circolare prevede disposizioni per la vigilanza consolidata dei gruppi bancari, stabilendo i requisiti per la supervisione e il controllo delle attività delle banche che fanno parte di un gruppo.

Dunque, la Circolare n. 285/2013, tra le altre cose, dispone che le banche assicurino la completezza, l'adeguatezza, la funzionalità e l'affidabilità del sistema dei controlli interni, utilizzando specifici presidi per ciascuna tipologia di rischio aziendale individuato e strutturando un sistema definito di compiti e responsabilità funzionale all'adeguata gestione d'impresa.
Le funzioni che si occupano, tra gli altri attori aziendali, dell'implementazione e del concreto funzionamento di tale ultimo sistema dei controlli interni sono le Funzioni aziendali di controllo. In particolare, la Funzione Compliance che presiede, secondo un approccio risk-based, alla gestione del rischio di non conformità alle normative di etero-regolamentazione e di auto-regolamentazione con riguardo a tutta l'attività aziendale.

Focus

Qual è il ruolo della Compliance?

La Funzione Compliance anche in tale ambito si adopera in maniera proattiva, nell'ottica di intercettare e, quindi, minimizzare il rischio antitrust attraverso:

- la definizione di campagne di formazione interna aziendale;
- la predisposizione di policies aziendali e procedure di Gruppo e locali, laddove vi sia una presenza territoriale dell'impresa al di fuori dei confini europei;
- implementare un ICP (*internal compliance program*) volto a monitorare il rischio antitrust e, se del caso, funzionale a poter beneficiare di una riduzione delle sanzioni qualora si dimostri che il programma antitrust sia stato definito, sviluppato completamente ed efficacemente attuato.

CAPITOLO 3

Aspetti di processo

3.1 Identificazione e monitoraggio del perimetro normativo applicabile

Art. 13

La Funzione Compliance identifica di volta in volta il **perimetro normativo applicabile all'organizzazione**, costituito dall'insieme delle norme, delle regole e dei principi rilevanti per l'azienda siano essi di carattere cogente che di adozione volontaria, tenendo conto del settore di operatività, delle dimensioni e della natura della medesima. La Funzione Compliance identifica ed estrapola da tale perimetro normativo i requisiti, i vincoli e gli obblighi che dovranno **indirizzare l'operato dell'organizzazione**.

Art. 14

L'attività di identificazione e **monitoraggio del perimetro normativo applicabile** viene aggiornata nel continuo, affinché l'organizzazione possa tempestivamente adattarsi ed intervenire all'esito di modifiche nel perimetro normativo applicabile ovvero di modifiche nell'assetto dell'organizzazione, della sua configurazione amministrativa o operativa, del suo ambito di intervento e delle geografie in cui essa opera, che comportino la necessità di considerare nuovi requisiti, vincoli ed obblighi ovvero il venir meno degli stessi anche in parte.

Come identificare il perimetro normativo applicabile?

Il primo passo per la corretta identificazione del perimetro normativo applicabile è rappresentato da un'attenta valutazione del mandato della Funzione, che dovrà delineare contenuti ed ambiti di intervento della Funzione, avuto riguardo agli obiettivi che il top management intende assegnare alla stessa e delle aree normative già presidiate da altre funzioni ed attori dell'organizzazione.
Sulla scorta dei **confini tracciati dal mandato della Funzione**, il **perimetro delle norme applicabili** deve essere rilevato e censito **partendo** da una attenta **valutazione del settore in cui l'azienda opera** ed una successiva accurata inventariazione delle fonti che permetterà la rilevazione iniziale e la successiva selezione di quelle applicabili. L'attività di benchmarking degli operatori comparabili per settore, configurazione organizzativa, dimensioni ed assetto di business aiuterà l'ulteriore affinamento della mappatura.

3.2
Identificazione e valutazione dei rischi e dei controlli

Art. 15

La Funzione Compliance identifica e valuta i rischi di non compliance e identifica il sistema dei controlli a mitigazione di tali rischi, valutandone l'adeguatezza. I rischi possono essere identificati a fronte dell'analisi di processi, transazioni, aree organizzative, aree geografiche, operazioni straordinarie, terze parti con cui l'organizzazione intrattiene relazioni di affari così come dall'attività di altre funzioni aziendali quali ad esempio la Funzione di Risk Management, laddove presente.

Art. 16

La Funzione Compliance supporta l'organizzazione nell'identificazione di criticità ed aree di miglioramento, connesse alla mancata o parziale mitigazione dei rischi identificati, proponendo azioni rimediali ed iniziative tese al miglioramento del sistema dei controlli, in considerazione delle caratteristiche, delle dimensioni, della complessità della struttura organizzativa e del business.

Art. 17

Nell'esecuzione di attività di valutazione dei rischi e dei controlli, la Funzione Compliance adotta le metodologie ritenute più idonee in funzione delle caratteristiche, delle dimensioni, della complessità della struttura organizzativa del business, ed in considerazione della natura e della specifica connotazione dei rischi identificati. La metodologia di valutazione dei rischi e dei controlli viene condivisa con il top management ovvero con altre funzioni o attori aziendali in relazione al complessivo disegno di governo del sistema di controllo interno e di gestione dei rischi ed approvata dal consiglio di amministrazione.

Art. 18

La Funzione Compliance promuove la definizione e l'implementazione di sistemi di identificazione e valutazione dei rischi di frode, in quanto rischi di non compliance, valutando l'opportunità di coinvolgere funzioni ed altri attori interni competenti rispetto ad ambiti tecnici rilevanti allo scopo. Ove tale compito sia stato demandato ad altra funzione secondo le regole organizzative statuite dal top management, la Funzione Compliance valuta la coerenza dei criteri di definizione del risk assessment antifrode rispetto agli obiettivi di compliance dell'azienda, segnalando eventuali difformità o punti di miglioramento.

Art. 19

Gli elementi minimi di un sistema di identificazione e valutazione dei rischi e dei controlli si sostanziano nella mappatura dei rischi e nel documento di valutazione dei rischi dei controlli corredato da una proposta di piano di azione.

Focus

Che cosa sono i rischi di non compliance?

Con il termine rischi di non compliance si fa riferimento a qualsiasi evento che determini il mancato o parziale rispetto dei requisiti, dei vincoli e degli obblighi identificati in relazione al complesso di norme, regole e dei principi considerati rilevanti per l'organizzazione. Tali rischi si sostanziano nella possibilità che l'organizzazione incorra in sanzioni giuridiche, anche di natura penale, perdite economiche, finanziare o patrimoniali, danni reputazionali o altre conseguenze legate alla capacità di preservare una sostenibile prospettiva di esercizio dell'attività di impresa nell'ecosistema di mercato e dei portatori di interesse.

In tale ambito vanno ricompresi i rischi di frode, intese quali condotte penalmente rilevanti che aggrediscono il patrimonio societario/aziendale attraverso l'inganno/artifizio/raggiro, ovvero quelle attività disoneste e ingannevoli volte a sottrarre valore all'organizzazione e che possono arrecare danni sia economici che reputazionali. Tra le varie ipotesi di frodi aziendali ritroviamo, ad esempio l'appropriazione indebita, che riguarda il furto o l'uso improprio delle risorse aziendali; le false comunicazioni sociali e/o falsificazione del bilancio per distrazione di risorse economiche e, ancora, la corruzione tra privati.

In che cosa consiste l'identificazione dei rischi di non compliance?

La Funzione Compliance identifica, ovvero coordina, l'identificazione dei **rischi di non compliance,** tenendo conto di tutte le aree di operatività dell'organizzazione ai fini dell'individuazione del livello del rischio al quale esse potrebbe essere esposta.

L'identificazione dei rischi di non compliance implica, dunque, la conoscenza degli obblighi di conformità che costituiscono il perimetro di intervento della Funzione Compliance e delle modalità di gestione di tali rischi che possono essere riconducibili a buone pratiche di controllo interno, frameworks, modelli di controllo definiti da norme cogenti o autoregolamentari, e, ancora, standard identificati da associazioni di categoria o altre organizzazioni di riferimento.

Una volta identificati i rischi di non compliance essi saranno analizzati considerando le potenziali conseguenze nelle quali potrebbe incorrere l'organizzazione, nonché le circostanze attuali e prospettiche che ne determinano la valutazione. L'analisi dei rischi di non conformità, dunque, terrà conto tanto della probabilità che essi si verifichino quanto delle conseguenze che deriverebbero dalla loro manifestazione.

In che cosa consiste la valutazione dei rischi di non compliance?

A valle dell'individuazione dei rischi di non compliance, la Funzione Compliance procederà con la valutazione degli stessi nell'ottica della pesatura di elementi che consentano l'attribuzione di un giudizio di rilevanza ai rischi stessi. All'esito della valutazione dei rischi la Funzione Compliance disporrà di informazioni più qualificate per la definizione delle priorità e per l'analisi di adeguatezza del sistema organizzativo e di controllo rispetto al livello di rischio individuato.

L'identificazione e **la valutazione dei rischi rilevanti per la Compliance sarà effettuata periodicamente** e, laddove necessario - ad esempio, quando si verifichino **cambiamenti di qualsiasi tipo all'interno dell'organizzazione, cambiamenti del quadro normativo regolamentare di riferimento** o **incidenti relativi al mancato rispetto degli obblighi di conformità** - dovrà essere rivista al fine di assicurare che gli obiettivi e l'ambito delle attività di monitoraggio e consulenza in materia di conformità siano sempre adeguati a scongiurare anche i rischi emergenti.

La **valutazione dei rischi**, come detto, può avvalersi di **metodi e tecniche alternative**, sintetizzate di seguito:

- **Le tecniche qualitative** di valutazione del rischio utilizzano metodi di assegnazione di un punteggio su una scala di severità definita (ad esempio punteggio alto, medio, basso) e possono prevedere la diretta attribuzione del punteggio al rischio o la valutazione dei fattori che ne determinano la severità (ad esempio, considerando il valore del rischio come risultante del prodotto fra valore della probabilità e valore dell'impatto);
- **Le tecniche quantitative** di valutazione del rischio utilizzano metodi che applicano tecniche matematiche e statistiche per calcolare il valore del rischio che può essere espresso come perdita attesa, in considerazione della quantificazione probabilistica di eventi (osservati e rappresentati da serie storiche, stimati in modelli di proiezione a scenario, acquisiti da benchmark, ecc.);
- **Le tecniche miste** combinano le tecniche suindicate.

Una ulteriore considerazione va espressa rispetto alle modalità ed alle tecniche di valutazione del sistema dei controlli che mitigano i rischi. È possibile valutare i controlli mitiganti in modo contestuale o in modo consequenziale rispetto ai rischi stessi. Ne derivano approcci differenti, come di seguito rappresentato:

- La **valutazione contestuale del rischio e dei controlli mitiganti** conduce all'espressione diretta del giudizio di rischiosità *netta* o *residuale*, intesa come valutazione del rischio, tenuti in considerazione i controlli adottati per la sua mitigazione;
- La **valutazione separata e consequenziale dei rischi e dei controlli mitiganti** conduce ad una preliminare valutazione del rischio "*lordo*" o "*inerente*", intesa quale valutazione del rischio espressa senza che sia tenuto in considerazione l'effetto mitigante dei controlli adottati. Si avrà, pertanto, un primo step di **valutazione del rischio potenziale** con successiva valutazione **del sistema dei controlli mitiganti** - che esprimerà la capacità dei controlli di contenere il rischio – ed uno step finale di *netting* cioè di **valutazione complessiva del rischio**, applicando al giudizio *lordo* o *inerente* alle considerazioni espresse in fase di valutazione dei controlli. Tale risultato finale sarà considerato la valutazione di rischiosità *netta* o *residuale*.

Quali tecniche risultano applicate in modo prevalente nell'esperienza applicativa delle Funzioni di Compliance?

L'esperienza applicativa ha **largamente preferito i metodi qualitativi** ed un approccio a due fasi di valutazione del rischio "lordo" o "inerente" e successivamente, all'esito della valutazione del controllo, l'espressione di un giudizio di rischiosità "netta" o "residuale". Quest'orientamento va interpretato in considerazione della natura dei rischi di compliance e degli aspetti normativi ad essi sottesi, sovente difficili da tradurre in serie storiche di accadimenti quantificabili in modo oggettivo; inoltre, la grande variabilità degli aspetti di contesto e dei fattori che qualificano gli eventi di rischio, rendono articolata l'applicazione di tecniche e metodi tipici della quantificazione del rischio. Un approccio che preserva un corretto rapporto costo/beneficio può essere rappresentato come segue:

FASE A | Valutazione del rischio inerente

- A seguito della mappatura dei rischi di compliance nei quali può incorrere l'organizzazione, è necessario procedere a stabilire e calcolare la **significatività** di un determinato rischio. A tal fine, il rischio può essere valutato tenendo in considerazione i fattori che ne determinano la severità complessiva: l'impatto e la probabilità.

  R (rischio) = P (probabilità) x I (impatto)

  Tale formula permette di determinare il **valore** del cd. **rischio inerente** che consiste nel rischio strettamente collegato ad un'attività dell'ente **al netto del sistema di misure interne adottate per**

la mitigazione del rischio medesimo. Dunque, la **significatività del rischio inerente** è data dalla **probabilità di accadimento dell'evento/del concretizzarsi di quello specifico rischio** e dell'i**mpatto** dello stesso sulla realtà aziendale in termini di raggiungimento degli obiettivi. A seguito della valutazione del rischio inerente, effettuata per mezzo della formula sopra esposta, è possibile assegnare al rischio inerente a un valore secondo una scala di punteggi prescelta (a titolo esemplificativo la scala di punteggi può essere determinata su matrice "4x4 Alto/Medio Alto/Medio Basso/Basso" ecc.).

FASE B | Valutazione delle misure di mitigazione e rischio residuo

- **Valutazione delle misure di mitigazione:** a questo punto è necessario che vengano individuati i **controlli mitiganti.** Sono definiti controlli mitiganti tutte le misure di tipo organizzativo, procedurale, transazionale, informatico, in grado di contenere la manifestazione o gli effetti del rischio: la classificazione dei controlli mitiganti può essere effettuata distinguendo misure di controllo (I) **attive preventive** e (II) **passive correttive**. Sono considerate misure di controllo attive preventive quelle misure (o quei controlli) in grado di prevenire l'accadimento, agendo sulla probabilità di accadimento del rischio; sono considerate misure di controllo passive correttive quelle misure (o quei controlli) in grado di intercettare l'evento attivando azioni informative, correttive o sanzionatorie.
- **Valutazione del rischio residuo ed assegnazione del giudizio finale**: Una volta adottate le misure di mitigazione per ciascun rischio inerente corrispondente è possibile determinare il grado di probabilità e di gravità che residuano e che daranno origine al **valore di rischio residuo**, ovvero, quel valore di rischio che permarrà nonostante le azioni poste in essere dall'organizzazione e che la stessa sa di correre e che ancora una volta potrà essere rappresentato secondo la scala di giudizio prescelta.

La mira dell'attività di Risk Management e, quindi, dell'adozione di un sistema di gestione del rischio, non è quella di eliminare tutti i rischi - risultato onirico - ma di **raggiungere un equilibrio ottimale tra rischi e le opportunità** che sostenga il business ed il raggiungimento degli obiettivi d'impresa.

3.3
Il sistema dei controlli

Art. 20

La Funzione Compliance promuove il disegno, l'implementazione e la verifica del sistema dei controlli per l'adeguata mitigazione dei rischi di non compliance. Nel far ciò, la Funzione Compliance valuta preferenzialmente l'adozione di sistemi di gestione e/o modelli di compliance, intesi come framework organici di governo e controllo basati sulla coesistenza di più elementi quali a titolo esemplificativo policy, procedure, piani di formazione, piani di monitoraggio ed auditing, sistemi di segnalazione. In assenza di un sistema di gestione e/o modello di compliance la Funzione promuove l'adozione di uno o più degli elementi che ne costituiscono l'insieme.

Art. 21

Il sistema dei controlli definito può prevedere indirizzi, regole e standard di comportamento tesi a normare l'operato del personale interno o l'operato di soggetti terzi, all'esito dell'identificazione e della valutazione dei rischi; in quest'ultimo caso la Funzione Compliance valuta, di concerto con le altre funzioni interne preposte, gli strumenti applicativi idonei ed opportuni.

Art. 22

La Funzione Compliance promuove il periodico aggiornamento delle policy e delle procedure di compliance. L'aggiornamento deve tenere in considerazione l'adeguata copertura degli ambiti di rischio identificati in relazione al perimetro normativo e l'allineamento alla configurazione dell'organizzazione, dei riporti gerarchici e funzionali, dell'assetto dei ruoli e delle responsabilità, dei sistemi informatici e dei flussi di interazione sistemici.

3.4
Comunicazione e training

Art. 23

La Funzione Compliance promuove programmi ed iniziative tese all'adeguata formazione del personale interno sulle tematiche inerenti alle materie rientranti nel proprio perimetro di competenza e ai rischi identificati, ai sistemi di gestione e/o modelli di compliance, alle condotte attese per la preservazione di un ambiente di lavoro orientato all'etica, all'integrità ed alla conformità.

Art. 24

La Funzione Compliance promuove parimenti iniziative volte alla comunicazione e diffusione, all'interno ed all'esterno dell'organizzazione, del contenuto e dei principi espressi nei sistemi di gestione e/o modelli di compliance ovvero l'indirizzo delle politiche di compliance dell'organizzazione. Tale attività viene coordinata con i processi di comunicazione definiti, secondo le procedure e prassi dell'organizzazione.

Focus

Quali sono gli elementi minimi da garantire nel disegno e nell'implementazione di un programma di formazione di compliance?

Un corretto processo di formazione della compliance deve garantire i seguenti elementi:

- **la predisposizione di un piano formativo ad hoc**, composto da diverse sessioni di training pianificate durante l'anno e divise per specifici argomenti, oppure con cadenza occasionale a causa di variazioni della struttura organizzativa interna, di mutamenti delle responsabilità del personale o di novità normative.
- **l'individuazione del tema oggetto della formazione**, i quali contenuti possono essere generali, di alto livello (es. modifiche legislative) o specifici, (modifiche dei processi interni o riorganizzazione aziendale che abbiano anche comportato una modifica delle procedure e policy di riferimento);
- **l'individuazione dei destinatari della formazione**, avendo debito riguardo dei soggetti che risultano particolarmente coinvolti o interessati dalla stessa anche creando gruppi distinti di dipendenti, soggetti a diversi requisiti, per adattare il contenuto della forma-

zione e la sua frequenza alle esigenze specifiche di ciascuna risorsa, tale che siano in grado di gestire le attività di propria competenza e si assumano le responsabilità previste;

- **la predisposizione di un test finale di verifica** che permetta di constatare il concreto apprendimento delle nozioni da parte del personale coinvolto;
- **la corretta previsione e gestione** delle risorse messe a disposizione per avviare gli opportuni corsi di formazione.

La Funzione Compliance, coordinandosi con le altre funzioni dedicate alla materia, assicura che il personale dell'organizzazione riceva una formazione continua per migliorare la conoscenza degli obblighi di conformità che li riguardano, es. quelli relativi al rapporto di lavoro ordinario, alle procedure, le policies e ai controlli in essere di cui sono responsabili e ai rischi di inadempimento che ne derivano. Se da un lato, l'adeguata elaborazione di un piano formativo da parte della Funzione Compliance può rappresentare un parametro valutativo per la determinazione del corretto operato della stessa, dall'altro lato, la mancata partecipazione alle sessioni formative erogate ovvero il mancato raggiungimento degli obiettivi previsti all'esito delle stesse da parte degli esponenti della società deve essere valutata negativamente, financo rappresentare un presupposto per l'eventuale erogazione di sanzioni disciplinari.

3.5
Monitoraggio, testing (periodico e nel continuo)

Art. 25

La Funzione Compliance definisce ed attua piani di monitoraggio mirati alla verifica di efficacia dei presidi di controllo adottati ed alla verifica dello stato di attuazione di azioni correttive definite, interventi di progettazione organizzativa finalizzati all'introduzione o alla modifica di controlli ed in generale mirati a rilevare lo stato di attuazione di iniziative definite nell'ambito dei Sistemi di gestione o Modelli di compliance. Tali piani, ancorché inquadrati nell'ambito del secondo livello di controllo tipico della Funzione Compliance, possono essere strutturati secondo le modalità tipiche dell'auditing interno ovvero seguire modalità riferite ad indicazioni fornite da standard e raccomandazioni metodologiche specifiche in materia di monitoraggio._

Art. 26

La Funzione Compliance, nella predisposizione dei piani di monitoraggio, può ricercare integrazione e dialogo con gli altri attori del sistema di controllo interno e gestione dei rischi aziendali.

Focus

Quali sono le caratteristiche di un adeguato piano di monitoraggio/testing?

Le **attività di controllo sono generalmente programmate su base annuale** al fine di effettuare un monitoraggio periodico dell'adeguatezza e dell'efficacia delle procedure, dei processi e di tutto il sistema di gestione dei rischi adottato dall'azienda. Tuttavia, in ragione di specifiche esigenze collegate all'ambito di riferimento, a specifiche previsioni normativo-regolamentari o alla cadenza temporale dettata dai sistemi di gestione, dai modelli di compliance e/o da policy e procedure interne, tali attività possono essere schedulate con differente periodicità o rivalutate nel corso dell'anno al mutamento del contesto di rischio di riferimento.

I contenuti minimi di un piano di monitoraggio/auditing sono:

- la pianificazione dei controlli di monitoraggio/testing, orientata a criteri di copertura del rischio;
- l'analisi dei processi e delle attività fondamentali per il business, preliminare all'esecuzione dei controlli di monitoraggio/testing;

- la rilevazione del disegno del sistema che si intende sottoporre ad attività di monitoraggio/testing;
- La definizione degli obiettivi dell'attività di monitoraggio/testing: tali obiettivi distinguono principalmente verifiche del disegno (tese a verificare che il disegno dei processi e/o dei controlli risponda ai requisiti definiti) ovvero verifiche di efficacia (tese a verificare che l'applicazione dei controlli sia conforme al disegno definito);
- l'esecuzione delle attività di monitoraggio/testing;
- la rendicontazione interna delle risultanze, preferibilmente consequenziale rispetto alla condivisione con le funzioni e gli attori coinvolti;
- la definizione di azioni conseguenti alla rilevazione di criticità o aree di miglioramento;
- la pianificazione di follow-up.

Quali sono le modalità realizzative di un adeguato piano di monitoraggio/testing?

Le attività di monitoraggio e testing possono essere effettuate **mediante**:

- analisi documentale effettuata senza l'interazione di funzioni interne o attori aziendali;
- interviste con i responsabili delle aree interessate dal controllo e alcune delle risorse coinvolte per ottenere informazioni più dettagliate;
- analisi dei dati;
- metodologie miste che prevedono la combinazione dei punti precedenti.

Le attività di monitoraggio/testing possono riguardare soggetti o transazioni esterne all'organizzazione?

È possibile che, in ragione di esigenze connaturate ai rischi identificati e valutati ed al sistema di controllo definito, l'organizzazione ravvisi la necessità di rivolgere i controlli di monitoraggio/testing all'esterno. In tal caso l'oggetto della verifica può essere rappresentato dalla conformità del profilo societario, legale e reputazionale del terzo rispetto ai requisiti attesi ovvero dalla conformità di processi e transazioni rispetto a standard e controlli definiti dai sistemi di gestione, modelli di compliance o policy e procedure interne. In caso di verifiche sui terzi, ove tali attività comportino l'interfaccia con il terzo, la richiesta

di dati ed informazioni ovvero impatti sul trattamento di dati sensibili, la Funzione Compliance dovrà verificare la titolarità del mandato necessario all'effettuazione di tale verifica. A titolo esemplificativo la titolarità può essere definita da processi di controllo preliminari all'instaurazione di rapporti commerciali (es. processo di accreditamento di fornitore, partner, agente, ecc.) o connessa all'espletamento di verifiche propedeutiche alla realizzazione di operazioni straordinarie (es. due diligence in operazioni di M&A).

A titolo esemplificativo tali attività possono sostanziarsi in:

- **Integrity due diligence**: verifica del profilo societario, legale e reputazionale del terzo effettuata in fase preventiva o come monitoraggio successivo all'instaurazione di rapporti di affari fra la Società ed il terzo.
- **Transaction review**: verifica del profilo di rischio di transazioni intercorse fra la Società ed il terzo ovvero di transazioni effettuate dal terzo.
- **Third parties audit**: verifica di audit effettuata nei confronti del soggetto terzo, che può essere realizzata mediante modalità di visita in loco, remote audit, mystery shopping (verifica mascherata) o altri strumenti.

3.6
Investigazione interna e trattamento delle non conformità

Art. 27

La Funzione Compliance supporta, coordinandosi con le altre Funzioni all'uopo incaricate, la definizione e l'implementazione di processi finalizzati all'analisi, alla valutazione e all'investigazione interna delle non conformità. Tali processi devono garantire la preservazione di principi di indipendenza ed assenza di conflitti di interessi, conformità alle disposizioni normative in materia di privacy e data protection ossia adeguata e sicura custodia di dati ed informazioni. Ove tale compito sia stato demandato ad altra Funzione secondo le regole

organizzative statuite dal top management, la Funzione Compliance valuta la coerenza dei processi adottati rispetto agli obiettivi di compliance dell'azienda, segnalando eventuali difformità o punti di miglioramento.

Art. 28

La Funzione Compliance si assicura che i processi e le procedure di analisi, valutazione, investigazione interna delle non conformità prevedano adeguata tracciabilità delle valutazioni, affinché sia alimentato un processo di miglioramento continuo.

Focus

Qual è il ruolo della Compliance nell'ambito delle investigazioni interne e del trattamento delle non conformità?

Di norma, il ruolo di esecutore dell'investigazione interna viene attribuito in azienda ad altra Funzione (quale, a titolo meramente esemplificativo, Internal Audit, General Counsel) nel rispetto dei principi di competenza, indipendenza ed assenza di conflitto di interesse.
La Funzione Compliance, può svolgere un ruolo rilevante nell'eventuale supporto all'espletamento **delle attività di investigazione interna** alle organizzazioni, dato il largo ventaglio di competenze e di conoscenze che alla stessa si richiedono per espletare le attività di controllo di secondo livello.
Allo stesso modo alla Funzione Compliance può essere demandata la responsabilità di attivare e/o promuovere attività di investigazione all'esito di verifiche, ovvero alla ricezione di segnalazioni o flussi di informazioni, che evidenzino potenziali non conformità o sospetti in ordine al regolare svolgimento delle operazioni aziendali in ottemperanza alle norme interne o esterne.
All'esito di processi di investigazione interna che rilevino potenziali criticità delle procedure interne ed in generale di modelli e sistemi di gestione adottati a mitigazione dei rischi presidiati dalla Funzione Compliance, la stessa - dopo averne condiviso gli esiti e le proposte rimediali con l'Organo di gestione - si adopererà per adottare le condivise azioni di rimedio.

3.7
Sistemi di segnalazione

Art. 29

La Funzione Compliance promuove la definizione e l'implementazione di sistemi di segnalazione delle non conformità e degli illeciti coerentemente con i sistemi di gestione adottati, i modelli di compliance e le normative applicabili. Ove tale compito sia stato demandato ad altra funzione secondo le regole organizzative statuite dal top management, la Funzione Compliance valuta la coerenza dei sistemi di segnalazione adottati rispetto agli obiettivi di compliance dell'azienda, segnalando eventuali difformità o punti di miglioramento.

Focus

Cosa si intende per sistema di segnalazione?

Come sopra esposto, è chiaro che il sistema di segnalazione (tecnicamente conosciuto come "whistleblowing") mira **ad incentivare la collaborazione del personale dell'azienda e, se previsto, di soggetti esterni alla medesima, ai fini di prevenzione e contrasto dei fenomeni di non compliance o peggio criminosi** connessi alle transazioni dell'organizzazione e del contesto in cui essa opera. Tale obiettivo è perseguito mediante la predisposizione di appositi sistemi di segnalazione che permettono ai dipendenti (o altri soggetti autorizzati) di segnalare, senza temere ritorsioni, comportamenti illeciti di cui vengano a conoscenza nell'ambito dell'esercizio delle attività di propria competenza.

Come viene predisposto un sistema di segnalazione interno?

Ai fini dell'implementazione di un adeguato sistema di segnalazione, l'organizzazione si impegna nella **redazione ed adozione di specifiche procedure** finalizzate alla disciplina delle **segnalazioni interne** da parte di tutto il personale - ovvero i dipendenti e tutti coloro che svolgono la loro attività intrattenendo rapporti di svariata natura con l'organizzazione, quali i consulenti o collaboratori esterni - di circostanze che possano costituire una violazione normativa ovvero una violazione di sistemi di gestione, modelli di compliance, policy e procedure interne.

Quali sono i requisiti minimi di un sistema di segnalazione interno?

I sistemi di segnalazione devono:

- individuare **i soggetti** che possono effettuare una segnalazione e l'**oggetto** della stessa;
- stabilire le **modalità** per effettuare le segnalazioni;
- assicurare l'implementazione di **un canale specifico, autonomo ed indipendente** per l'esecuzione della segnalazione;
- assicurare l'istituzione di **almeno un canale alternativo di segnalazione** idoneo a garantire, con **modalità informatiche**, la riservatezza dell'identità del segnalante;
- **garantire la riservatezza dei dati del segnalante** e **del presunto responsabile** della violazione;
- stabilire il **divieto di atti di ritorsione o discriminazione** nei confronti del segnalante;
- comminare **sanzioni nei confronti di chi viola le misure di tutela del segnalante** e di chi effettua con dolo o colpa grave segnalazioni infondate;
- indicare il **procedimento istruttorio delle segnalazioni** con l'indicazione delle tempistiche e delle fasi e, ancora, delle modalità di reporting tempestivo agli organi aziendali;
- individuare il **soggetto, la funzione o l'Organo deputato** alla **ricezione della segnalazione.**

Risulta, dunque, importante che il sistema di segnalazione contempli l'adozione di una **policy in materia di whistleblowing** e l'implementazione di **adeguati sistemi informatici**, come ad esempio piattaforme di supporto o software ad hoc gestiti anche da outsourcer, che assicurino la riservatezza dell'identità del segnalante.

3.8
Il sistema disciplinare

Art. 30

La Funzione Compliance congiuntamente alla funzione Risorse Umane o HR promuove - in coerenza con le disposizioni dettate dai sistemi di gestione, dai modelli di compliance, da requisiti definiti da norme, regolamenti ed istituzioni di riferimento nel campo della compliance e dei sistemi di controllo **- l'adozione di sistemi disciplinari tesi a prevedere l'applicazione di misure sanzionatorie o riparatorie** da porre in essere laddove i destinatari delle prescrizioni contenute nei sistemi di controllo adottino comportamenti non conformi.

Art. 31

Laddove i sistemi sanzionatori applicabili ai comportamenti non conformi in ambito compliance siano stati definiti da altre funzioni o attori aziendali, la Funzione Compliance valuta la **coerenza dei sistemi sanzionatori** adottati rispetto agli obiettivi di compliance dell'azienda, segnalando eventuali difformità o punti di miglioramento.

Focus

Qual è il principale riferimento codificato in azienda?

Le aziende, in ottemperanza alla normativa giuslavoristica, adottano il cosiddetto **codice disciplinare** che prescrive le condotte che il personale deve tenere, nell'ambito dello svolgimento delle proprie attribuzioni, al fine di supportare il raggiungimento degli obiettivi ed evitare di incorrere in sanzioni disciplinari. Ai fini dell'applicazione ed attuazione del codice disciplinare è necessaria la sua affissione in quei luoghi che ne permettano la conoscenza a tutti i lavoratori (bacheca aziendale, le diverse aree comuni, l'area in cui si timbra o spazi web aziendali).
Il codice disciplinare deve prevedere:

- le **condotte punibili** - quali quelle negligenti, imprudenti ed imperite o penalmente rilevanti o, ancora, condotte poste in essere in contrasto con l'impianto valoriale posto dal Codice Etico (non è necessario, tuttavia, che tutte le condotte punite ex post siano esattamente previste ex ante nel codice disciplinare);
- le **specifiche sanzioni** previste per ciascuna tipologia di comportamento;
- la **procedura disciplinare** che disciplini con precisione il procedimento disciplinare che verrà ad attivarsi.

3.9
Flussi di informazione e reporting

Art. 32

La Funzione Compliance opera secondo regole e processi codificati che prevedono il reporting delle proprie attività e degli esiti delle stesse, individuando criteri appropriati di selezione delle informazioni da riportare, delle tempistiche per garantire un reporting regolare, dei destinatari, delle modalità, dei canali ed eccezioni.

Art. 33

La Funzione Compliance si adopera affinché sia garantito il più completo e tempestivo scambio informativo con gli altri attori del sistema di controllo interno e gestione dei rischi, nei limiti del proprio mandato e del mandato conferito a tali funzioni. Parimenti, la Funzione Compliance stabilisce modalità, tempi e canali di condivisione delle informazioni con le funzioni o altri attori dell'azienda.

Focus

In cosa consiste il reporting e perché è importante la predisposizione di un vero sistema?

Il reporting consiste nella **rappresentazione e rendicontazione periodica** dei **risultati delle diverse attività della Funzione Compliance**, attraverso comunicazioni strutturate o non strutturate (es. report, lettere interne, comunicazioni e-mail, comunicazioni verbali, relazioni, ecc.).
Il sistema di reporting è lo strumento che serve per trasmettere tempestivamente al Management ed alle Funzioni Direttive, compresi i membri del consiglio di amministrazione, considerati i ruoli e le responsabilità dei soggetti coinvolti, le informazioni di natura economica, tecnica, organizzativa rilevati per l'operatività dell'impresa. In tale ambito è importante che tale flusso di comunicazioni comprenda aspetti legati agli esiti delle attività condotte dalla Funzione Compliance.

Quali sono le informazioni che costituiscono oggetto di reporting?

Il reporting verso il Top Management, ovvero verso funzioni e/o attori cui la Funzione riporta gerarchicamente o funzionalmente, conterrà al minimo i seguenti elementi informativi:

- informazioni di carattere generale sull'adeguatezza e l'efficacia delle politiche e delle procedure interne, violazioni e carenze nell'organizzazione interna;
- una sintesi della struttura e dell'organizzazione della Funzione Compliance;
- informazioni sulle modalità di monitoraggio e revisione degli obblighi imposti dalla normativa;
- una sintesi delle ispezioni in loco o delle revisioni documentali e delle attività di monitoraggio pianificate;
- un aggiornamento in merito ai corsi di formazioni erogati (anche con riferimento alle procedure operative adottate) e alle risultanze emerse;
- una sintesi dei provvedimenti adottati e in via di adozione per garantire la conformità ai requisiti applicabili modificati nonché il numero e le risposte fornite ai reclami ricevuti.

3.10
Valutazione e miglioramento della funzione e dei processi di compliance

Art. 34

La Funzione Compliance opera secondo principi di trasparenza, chiara definizione degli obiettivi e misurabilità dei risultati. In ragione di ciò, la Funzione Compliance definisce annualmente e condivide con l'alta direzione, ovvero verso funzioni e/o attori cui la Funzione riporta gerarchicamente gli obiettivi, un set di indicatori finalizzato all'oggettiva misurazione del livello di raggiungimento degli obiettivi.

Art. 35

La Funzione Compliance si adopera affinché sia alimentato un **processo di miglioramento continuo nella gestione della Funzione** stessa, **dei processi interni e delle attività**, tracciando e rendicontando dati che avvalorino tale percorso di miglioramento. Tali informazioni sono oggetto dei processi di reporting definiti.

Credits

Redazione
Consiglio Direttivo lab4compliance:
Giorgio Totis, Paolo Marpillero Errera,
Elda Varrone, Marino Giuseppe Sciascia

Partner Tecnico
EY Forensics & Integrity Services:
Fabrizio Santaloja, Piero Di Michele,
Massimiliano Carpino

Contributori esterni
prof. Giampaolo Gabbi - SDA Bocconi
School of Management
avv. Jean-Paul Castagno - Orrick,
Partner White Collar Criminal Defense

Contributori interni
Tutti gli associati di lab4compliance, appartenenti alle più diverse industry di riferimento, che hanno fattivamente contribuito alla creazione e revisione critica del documento. Impossibile elencarli tutti, ma un sincero grazie a ciascuno.

Partner Editoriale
Cast Edutainment Spa
Francesco Pipino, Rita Milazzo, Gianluca Chinnici,
Eleonora Chiomento, Marta Fontana

Realizzazione grafica

cast PUBLISHING | brought to you by cast EDUTAINMENT

Perché la compliance
è un partner strategico
per l’azienda.

Perché la compliance
riguarda tutti all’interno
della struttura aziendale,
a ogni livello.

Perché domani,
senza la compliance,
non si farà business.

lab4compliance