ODCEC m@ster

ORDINE DEI DOTTORI COMMERCIALISTI E DEGLI ESPERTI CONTABILI
MILANO

FONDAZIONE COMMERCIALISTI ODCEC di MILANO

La responsabilità amministrativa degli enti ex D. Lgs. 231/2001

IL RISK ASSESSMENT 231

MARIO CHIODI

06 ottobre 2023

Il successo sostenibile e i rischi d'azienda

- L'acronimo **ESG** indica tre **fattori fondamentali per verificare, misurare e sostenere l'impegno in termini di sostenibilità di una impresa o di una organizzazione.**
- Nello specifico, gli **indicatori ESG** rappresentano una serie di **criteri di misurazione delle attività ambientali, sociali e della *governance* di una organizzazione**, che si concretizzano in un insieme di *standard* operativi a cui si devono ispirare le *operations* di un'azienda.
- Negli ultimi anni le imprese si stanno interrogando su come integrare i processi aziendali che governano la gestione dei rischi d'impresa e le tematiche di sostenibilità.

Il successo sostenibile e i rischi d'azienda

Secondo il Codice di Corporate Governance (2020) delle società quotate, l'organo di amministrazione guida la società perseguendone il **successo sostenibile.**

Il successo sostenibile e i rischi d'azienda

Il successo sostenibile, quindi la creazione di **valore di lungo periodo**, non può prescindere da un sistema di gestione dei rischi.

Gino Zappa, nel lontano 1956, affermava che:
«sebbene fattore perturbatore, il rischio è l'elemento che forse meglio caratterizza l'azienda, al punto che, in assenza del rischio, l'attività aziendale non è neppure concepibile».

ESG RISKS

I rischi e il SCI

Processo	Risk Exposure	Controls
Gestione flussi finanziari	Rischio finanziario Rischio 231 (corruzione, etc.) Cyber risk Altro	Assetto organizzativo SCI (controlli di linea, di secondo e terzo livello) Sistema amministrativo contabile Flussi informativi

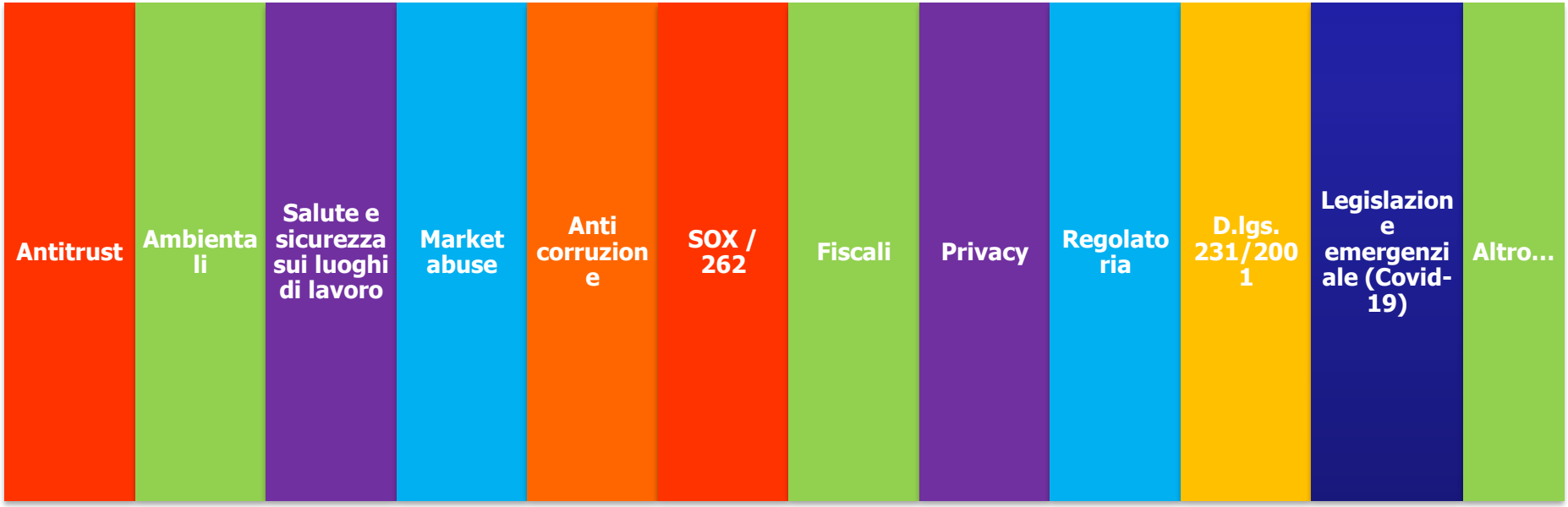
Rischio inerente –
Presidi di controllo =
Rischio residuo

L'obiettivo è la mitigazione dei rischi

Senza ingessare la società e valorizzando, ove possibile, i controlli esistenti/flussi informativi esistenti

I rischi di compliance

Il rischio di compliance è *«il rischio di incorrere in sanzioni giudiziarie o amministrative, perdite finanziarie rilevanti o danni di reputazione in conseguenza di violazioni di norme imperative (di legge o di regolamenti) ovvero di autoregolamentazione (es. statuti, codici di condotta, codici di autodisciplina)».*



I rischi di compliance sono molteplici e dinamici in funzione della variazione del contesto di riferimento

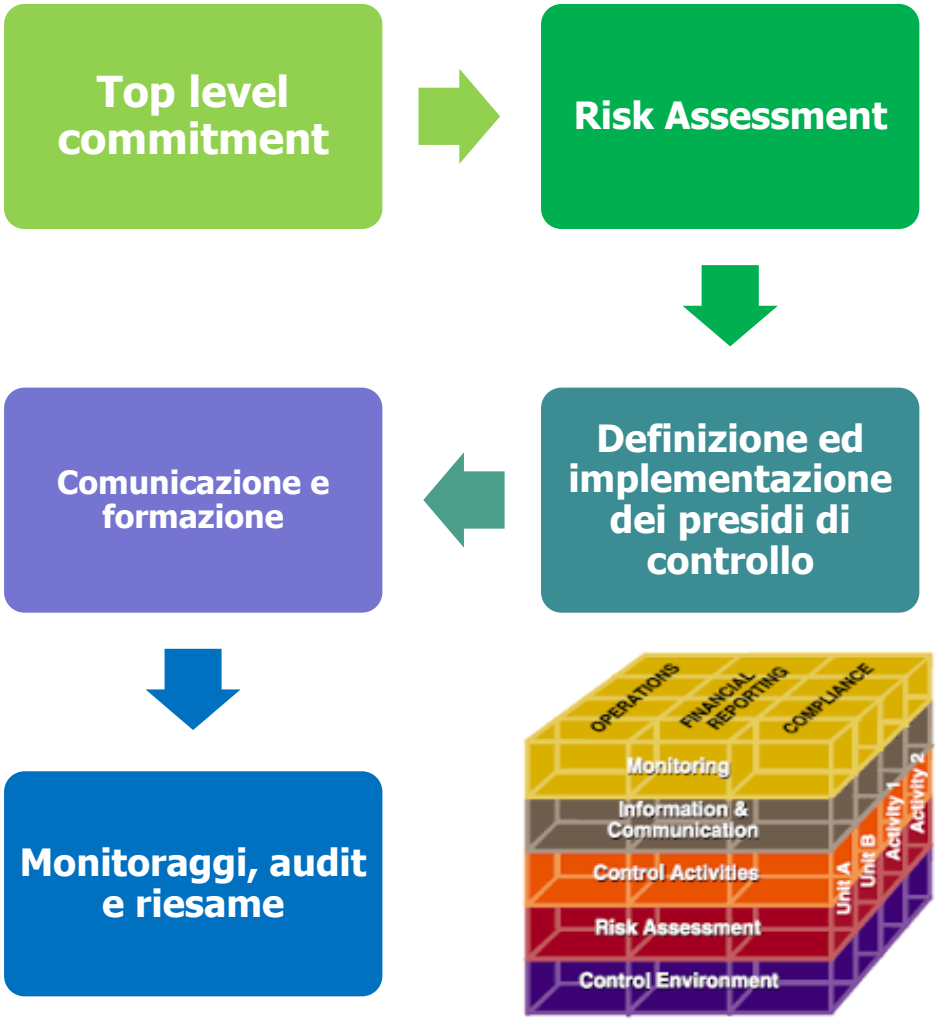
I rischi di compliance e il SCI

Obiettivo: Mitigare i rischi, che sono ineliminabili.

Proliferazione di Compliance program, policy e procedure anche, a volte, scoordinati tra di loro.

Proliferazione di organi, comitati e funzioni deputati al monitoraggio.

In alcuni casi sono obbligatori (si pensi alle funzioni compliance e antiriciclaggio nei soggetti vigilati)…



I rischi di compliance e il SCI

Obiettivo: Mitigare i rischi, che sono ineliminabili.

Per evitare di burocratizzare l'azienda ed ottenere un'efficace ed efficiente gestione dei rischi è necessario fare alcune considerazioni:

1) Il sistema di controllo interno è unico e centrale;

2) Uno o più presidi di controllo possono mitigare uno più rischi aziendali

Il D.Lgs. 231/2001

Il Decreto Legislativo 8 giugno 2001, n. 231 - recante *"Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica"* - ha introdotto una forma di **responsabilità "quasi penale" degli enti, che si aggiunge a quella della persona fisica che ha commesso o tentato il reato, nell'interesse o a vantaggio della Società.**

I presupposti della responsabilità dell'ente sono:

- **commissione di talune tipologie di reato**, tassativamente indicate dal legislatore, **da parte di soggetti funzionalmente legati all'ente (soggetti apicali e sottoposti)**;
- **realizzazione del reato nell'interesse o a vantaggio dell'ente**;
- **mancata predisposizione di un Modello di Organizzazione, Gestione e Controllo** idoneo alla **prevenzione** dei reati o sua inefficace attuazione.

Il D.Lgs. 231/2001

L'ESIMENTE - L'Ente non risponde se prova:

Adozione di un Modello di Organizzazione, Gestione e Controllo	L'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, Modelli di Organizzazione, Gestione e Controllo **idonei a prevenire reati** della specie di quello verificatosi.
Identificazione dell'Organismo di Vigilanza	Il compito di vigilare sul funzionamento e l'osservanza dei Modelli di curare il loro aggiornamento é stato affidato a un organismo dell'ente dotato di autonomi poteri di iniziativa e di controllo (Organismo di Vigilanza).
Inefficcace attuazione del Modello ed elusione fraudolenta dello stesso da parte dell'autore dell'illecito	Gli autori del reato, hanno commesso l'illecito **eludendo fraudolentemente** i Modelli di Organizzazione, Gestione e Controllo.

Modello 231

Il modello per essere

IDONEO

deve essere (anche)

SPECIFICO

La giurisprudenza ha indicato come sia necessaria la definizione di un **modello** elaborato **sulle specificità aziendali** e con **un elevato livello di personalizzazione**.

Il Modello deve essere in grado di prevenire quei rischi-reato specifici della Società.

Modello 231

L'implementazione (*l'adozione*) e la "vita effettiva" (*l'attuazione*) del Modello 231 sono le attività attraverso cui si declina il giudizio di adeguatezza (o meno) e devono essere condotte in coerenza con:

- l'azienda e la sua storia;
- la normativa, anche internazionale;
- la giurisprudenza;
- le linee guida;
- la dottrina;
- Altro.

Il Modello è un «sistema» dinamico che «recepisce» e «sintetizza» molteplici indicazioni, esogene ed endogene all'organismo aziendale

Modello 231 – L'adozione

L'adozione è l'«atto» attraverso cui il Modello diventa operativo in ciascuna organizzazione aziendale. Di norma avviene mediante una specifica deliberazione del Consiglio di Amministrazione (o determinazione dell'Amministratore Unico).

Talune linee guida suggeriscono l'approvazione a livello assembleare (tematica da considerare in caso di coincidenza ODV-Collegio Sindacale)

Importante è che il Modello sia deciso ed approvato da chi abbia, effettivamente, il potere di determinare le scelte aziendali (il caso delle aziende che operano in Gruppo).

Il CdA non deve limitarsi ad approvare un **«pacchetto» di documenti** (il regolamento dell' OdV???)… ma deve rendere effettivo il Modello attraverso la diffusione a tutti i destinatari (interni ed esterni) nonché deve favorire specifiche sessioni formative sui contenuti dello stesso…ed essere d'esempio nell'attuazione.

Struttura tipo del Modello 231

Parte Generale

Nella Parte Generale è sintetizzato il quadro normativo di riferimento ed inoltre, sono descritti:

- ✓ descrizione della società e della governance
- ✓ la composizione ed il funzionamento dell'Organismo di Vigilanza;
- ✓ whistleblowing;
- ✓ le modalità di diffusione del Modello ed attività formative;
- ✓ il sistema sanzionatorio.

Parte Speciale

Nella Parte Speciale sono identificate, in relazione alla tipologia di attività svolta dalla Società:

- ✓ le fattispecie di reato rilevanti e le aree di rischio;
- ✓ i principi di comportamento;
- ✓ i flussi informativi all'Organismo di Vigilanza.

Codice Etico

Destinatari del Modello

- Amministratori
- Collegio sindacale
- Revisori
- Dipendenti
- Fornitori, consulenti, professionisti ed eventuali soggetti terzi nella misura in cui gli stessi possano essere coinvolti nello svolgimento di attività nelle quali sia ipotizzabile la commissione di uno dei reati presupposto di cui al Decreto
- Quanti agiscono sotto la direzione o la vigilanza dei vertici aziendali nell'ambito dei compiti e delle funzioni assegnate

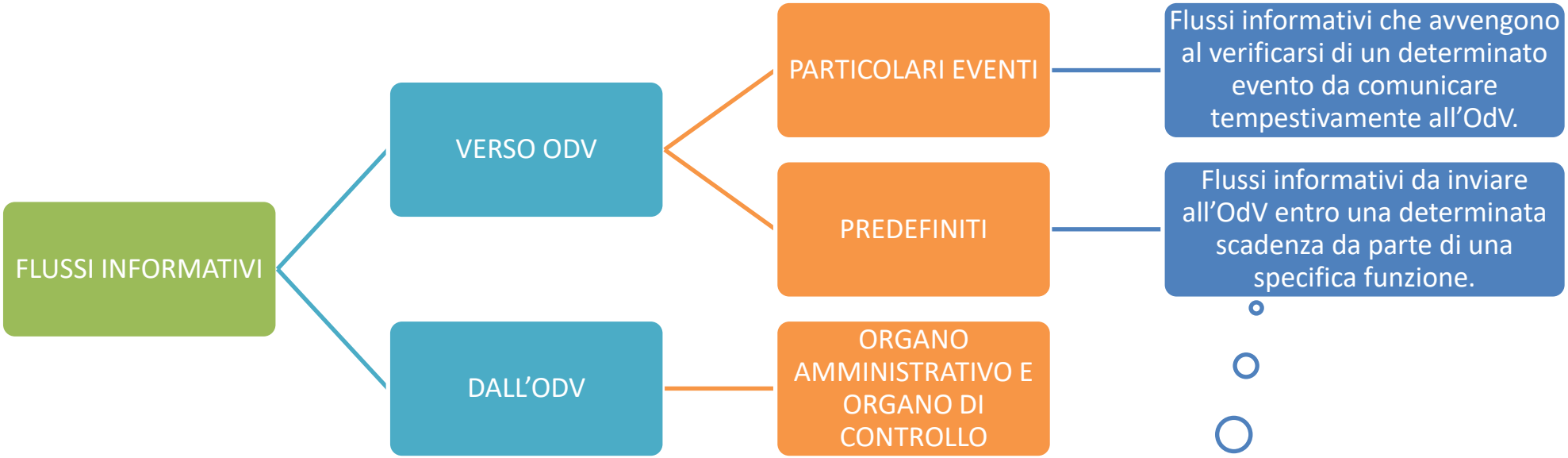
Formazione e informazione

La formazione assume carattere di **"obbligatorietà"** e dovrà essere "reiterata" per garantire l' effettivo aggiornamento

Prevedere test di apprendimento

Flussi informativi

I flussi informativi devono avere natura bidirezionale, consentendo ai destinatari del Modello di informare costantemente l'OdV e a quest'ultimo di interagire e retroagire con gli stessi soggetti.



Valorizzare flussi informativi già presenti in azienda per altre finalità

Sistema sanzionatorio

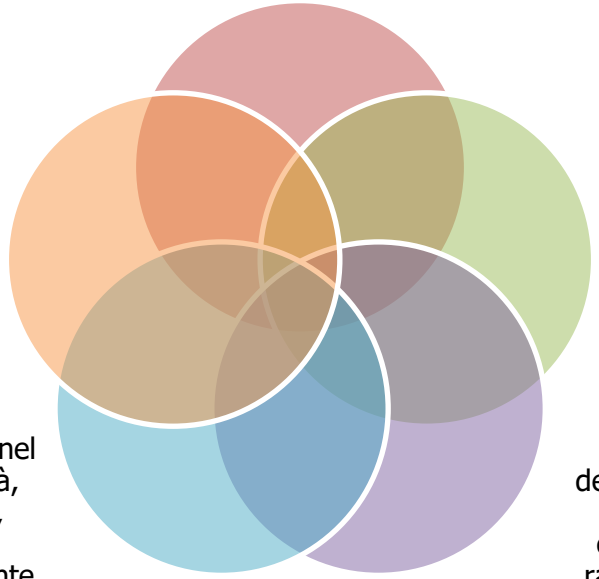
L'efficace attuazione del MOG esige, tra l'altro, l'adozione di un "Sistema Disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello", tanto nei confronti dei soggetti in posizione apicale (art. 6, comma 2, lett. e), quanto verso i soggetti sottoposti all'altrui direzione (art. 7, comma 4, lett. b).

Un adeguato Sistema Disciplinare, in generale, non può prescindere dal rispetto della legislazione vigente e deve essere articolato nel rispetto del principio della gradualità, prevedendo sanzioni proporzionate al ruolo ricoperto nell'organizzazione aziendale dall'autore dell'infrazione, all'infrazione stessa e all'impatto che questa comporta per la società in termini di esposizione al rischio reato.

Sistema sanzionatorio

deve essere elaborato per iscritto e adeguatamente diffuso, costituendo parte integrante dell'efficace attuazione del Modello, attraverso un'adeguata attività di informazione e formazione dei destinatari

deve garantire il contraddittorio, ovvero la possibilità a favore del soggetto a cui è stato contestato il comportamento di proporre, con ragionevole certezza, argomentazioni a sua difesa

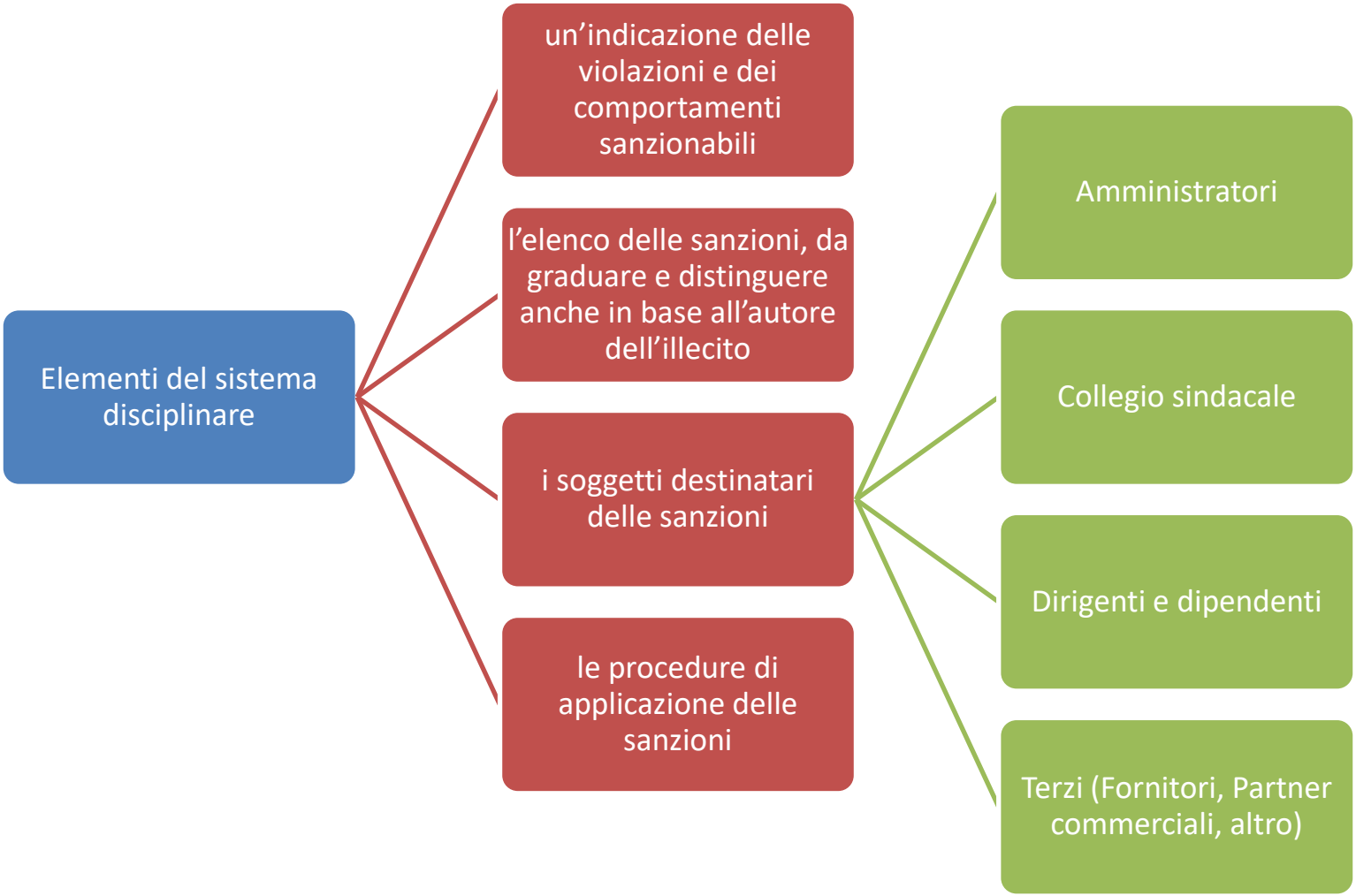


si affianca a quello esterno (penale o amministrativo), volto a sanzionare il trasgressore del Modello organizzativo indipendentemente dal fatto che da quella violazione sia scaturita la commissione di un reato

prevede sanzioni da comminare nel rispetto dei principi di specificità, tempestività ed immediatezza, nonché di idoneità a svolgere un'azione effettivamente deterrente, avendo una specifica funzione preventiva e non meramente ed esclusivamente punitiva

deve essere conciliabile con le norme, legislative e contrattuali, che regolano i rapporti intrattenuti dall'Ente con ciascuno dei soggetti ai quali si applica il Modello;

Sistema sanzionatorio



Codice etico

I codici etici sono documenti ufficiali dell'ente che contengono l'insieme dei diritti, dei doveri e delle responsabilità dell'ente nei confronti dei "portatori d'interesse" (dipendenti, fornitori, clienti, Pubblica Amministrazione, azionisti, mercato finanziario, ecc.).

Tali codici mirano a raccomandare, promuovere o vietare determinati comportamenti, indipendentemente da quanto previsto a livello normativo, e possono prevedere sanzioni proporzionate alla gravità delle eventuali infrazioni commesse.

I codici etici sono documenti voluti ed approvati dal massimo vertice dell'ente.

Fasi di costruzione/aggiornamento del Modello 231

Analisi preliminare

Analisi della storia della Società

FASE 1

Valutazione dei processi, rischi e controlli

FASE 2

Gap analysis ed action plan

FASE 3

Modello ex D. Lgs. 231/01

OBIETTIVI

Individuare e valutare le aree di rischio 231

Mappare le "attività sensibili" e i relativi meccanismi di controllo in essere

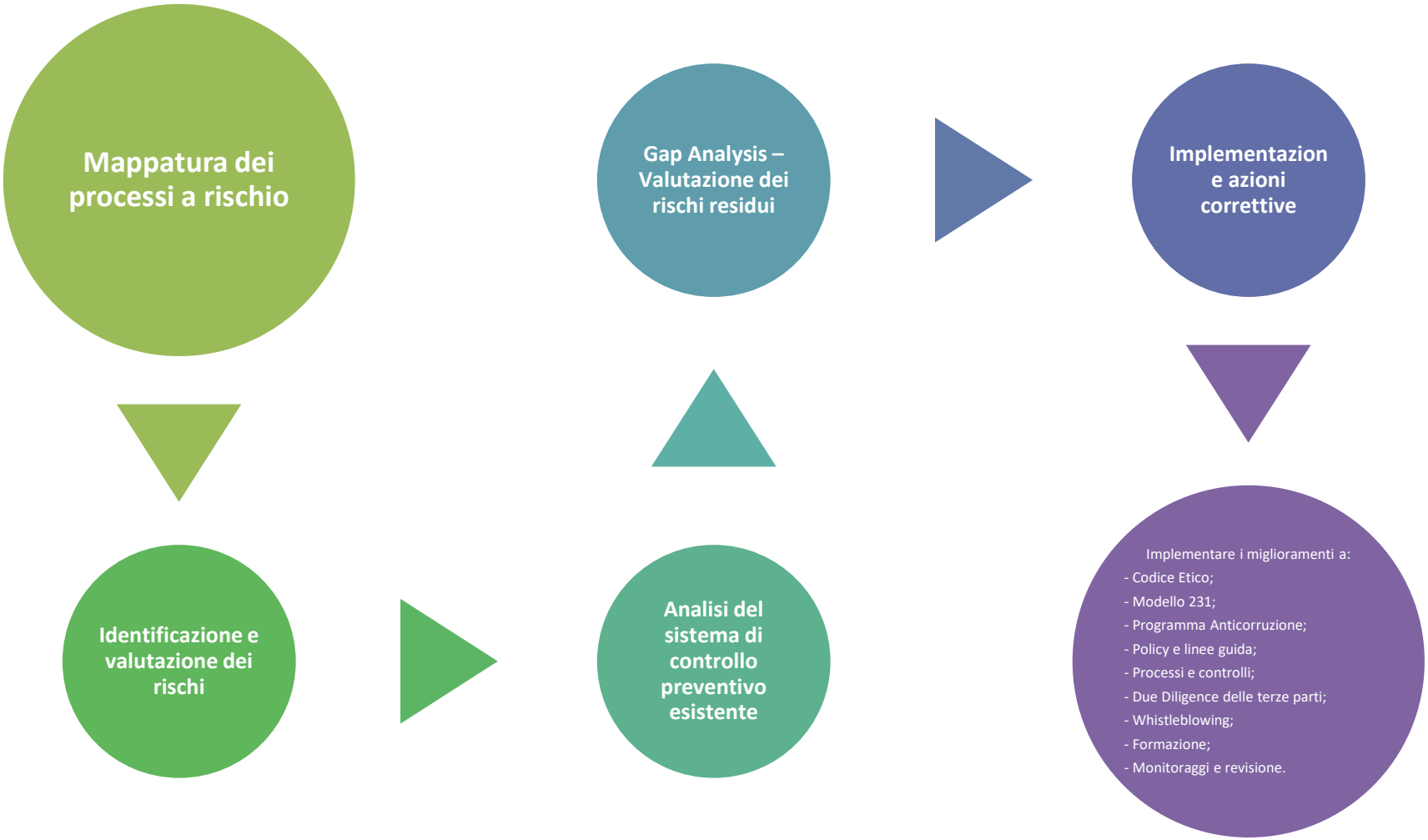
Individuare le opportunità di miglioramento e definire un piano di *remediation*

Predisporre/aggiornare il Modello di Organizzazione, Gestione e Controllo articolato in tutte le sue componenti

Benefici dei risk assessment

- Fornire una realistica e completa visione delle aree di rischio e dei presidi di controllo;
- Concentrare l'attenzione e le risorse su quei processi e relazioni considerati più a rischio;
- Permettere all'organizzazione di individuare le aree in cui vi è:
  - un eccesso di controllo in base al rischio (spreco di risorse che rischia anche di ingessare il business);
  - una carenza di controllo (*gap analysis*);
- Individuare il corretto livello di profondità di due diligence delle terze parti *(risk-based due diligence)*;
- Individuare opportunità di miglioramento non solo di compliance, ma anche in termini di governance e riduzione dei costi ed efficienza organizzativa;
- Promuovere all'interno dell'organizzazione:
  - Cultura della legalità;
  - Approccio etico al business;
  - Consapevolezza dei rischi ai quali l'azienda e i singoli sono esposti;
  - Consapevolezza del sistema di controllo interno.

Fasi del risk assessment 231



Mappatura dei processi a rischio

Obiettivi

- Mappare le “attività sensibili”

Attività

- Raccolta ed analisi della documentazione societaria/organizzativa ed individuazione dei Process Owner
- Analisi del sistema di deleghe e procure;
- Interviste con i Process Owner;
- Formalizzazione e condivisione di una mappa delle aree sensibili.

Mappatura dei processi a rischio

Quali e quanti sono i processi a rischio 231?

Non è possibile definire a priori quali siano le attività a rischio reato 231 ma queste devono desunte all'interno della specifica realtà aziendale.

A scopo meramente didattico si può provare ad elencare dei possibili processi a rischio 231 all'interno di una organizzazione aziendale…

Mappatura dei processi a rischio - esempi

- Gestione delle attività commerciali
- Omaggi e spese di viaggio e ospitalità
- Predisposizione del bilancio di esercizio e gestione della fiscalità
- Gestione delle attività assembleari e operazioni sul capitale
- Donazioni ed erogazioni liberali
- Gestione delle sponsorizzazioni
- Gestione degli acquisti
- Conferimento degli incarichi di consulenza
- Selezione e gestione del personale
- Ottenimento di autorizzazioni e licenze
- Gestione delle attività ispettive
- Gestione della sicurezza informatica
- Gestione del sistema di prevenzione e protezione
- Gestione delle attività ad impatto ambientale
- Altro

Mappatura dei processi a rischio

Documentazione da analizzare

- la visura camerale;
- lo statuto societario;
- il bilancio d'esercizio;
- l'organigramma;
- il mansionario / job description;
- deleghe e poteri;
- le policy e procedure interne e/o di gruppo;
- la mappatura dei rapporti infragruppo;
- il Documento di Valutazione dei Rischi (DVR) ex D.Lgs. 81/08;
- la mappatura dei sistemi informativi;
- il modello SOD;
- altro…

Inoltre, è opportuno accertare la presenza di eventuali sistemi di gestione di qualità (ISO 9001), salute sicurezza sul lavoro (ISO 45001), ambiente (ISO 14001) e/o altra normativa interna di autodisciplina.

Individuazione dei potenziali rischi 231

Obiettivo

Simultaneamente alla mappatura dei processi interni è necessario individuare i relativi i rischi 231, cioè **individuare e analizzare i reati applicabili**, ovvero le categorie di reato che sono incluse nel catalogo dei reati e che fanno insorgere la responsabilità della Società ai sensi del Decreto

Individuazione dei potenziali rischi 231

L'**analisi dei rischi 231** dovrà considerare:

- la tipologia della clientela (pubblico/privato);
- le aree geografiche in cui la società opera (Italia e/o estero);
- la storia della società;
- il settore di appartenenza;
- la presenza di linee guida di settore;
- l'assetto societario (considerando anche la presenza di eventuali soci appartenenti alla Pubblica Amministrazione);
- l'appartenenza della società ad un gruppo;
- la presenza o meno di stabilimenti di produzione;
- altro.

Individuazione dei potenziali rischi 231

I rischi non devono essere solamente individuati ma anche esplicitati, comunicati e condivisi con il management.

I rischi potenziali per processo posso essere espressi nella forma delle modalità esemplificative di reato, quali ad esempio:

"La **gestione delle attività commerciali** potrebbe presentare profili di rischio in relazione ai reati contro la Pubblica Amministrazione nel caso in cui un soggetto sottoposto o apicale della Società:

- offra o prometta denaro od altra utilità ad un pubblico ufficiale, ad un incaricato di pubblico servizio o a soggetti da questi indicati o
- induca in errore un pubblico ufficiale mediante artifizi o raggiri (quali, ad esempio, la falsificazione o l'alterazione dei documenti predisposti per la Pubblica Amministrazione) al fine di acquisire la Pubblica Amministrazione di riferimento come cliente".

Individuazione dei potenziali rischi 231

La **valutazione del rischio** inerente è data dall'interrelazione della probabilità e dell'impatto.

Si riporta a titolo di esempio una matrice probabilità-impatto con evidenza del rischio risultante.

Impatto	Rischio medio	Rischio elevato
	Rischio modesto	Rischio medio
	Probabilità	

Rischio inerente – Presidi di controllo = Rischio residuo

L'obiettivo è la mitigazione del rischio 231

Valutazione qualitativa

Senza ingessare la società e valorizzando i controlli esistenti

Analisi del sistema di controllo preventivo

Il sistema di controllo interno deve essere individuato, analizzato e valutato/valorizzato nella fase di costruzione del risk assessment.

L'implementazione di un sistema di controllo interno può determinare una riduzione del livello di rischiosità.

Tale capacità dipende da:

- disegno/architettura del controllo;
- efficace attuazione.

I presidi di controllo possono essere classificati in base al **grado di adeguatezza** degli stessi. Come per il rischio inerente, tale valutazione è soggettiva e possono essere utilizzati dei criteri quali-quantitativi.

Analisi del sistema di controllo preventivo

In linea generale un sistema di controllo interno dovrebbe essere strutturato secondo un sistema a tre linee di difesa, che prevede:

- i **controlli di primo livello**, i cosiddetti controlli di linea insiti nei processi operativi;
- i **controlli di secondo livello** eseguiti da funzioni aziendali specifiche, con lo scopo di disegnare e / o monitorare i controlli della prima linea di difesa;
- i **controlli di terzo livello**, svolti tipicamente dalla funzione di **Internal Audit**, che svolge attività di verifica e fornisce valutazioni indipendenti sul disegno del sistema di controllo interno.

Principio di proporzionalità: un sistema di controllo strutturato su tre linee di difesa è applicabile in organizzazioni di medio-grandi dimensioni.

Obiettivo: Valorizzare il sistema di controllo già esistente

Analisi del sistema di controllo preventivo

Si possono individuare molteplici presidi di controllo per prevenire i rischi 231 che possono essere classificati:

- di livello aziendale (*entity-level);*
- di livello di processo;
- preventivi;
- ex post.

Ogni singola Società ha già (consciamente o inconsciamente) istituito, anche se in forma embrionale, un sistema di controllo interno preventivo 231

Sono controlli che **già esistono** in azienda per altre finalità e/o per **mitigare altri rischi:** sistemi di certificazioni (qualità, ambiente, SSLL, sicurezza informatica), adeguata informazione finanziaria, anticorruzione, autoriciclaggio, altro…

Obiettivo: Valorizzare il sistema di controllo già esistente

Analisi del sistema di controllo preventivo

<u>Esempi di presidi di controllo 231 a livello di organizzazione:</u>

- adottare un **codice etico***;*
- adottare un sistema organizzativo sufficientemente aggiornato, formalizzato e chiaro;
- specifici programmi di **formazione** 231;
- un sistema di **whistleblowing** integrato;
- un **formalizzato processo approvativo** per le attività a rischio 231;
- sistema che garantisca la **tracciabilità ex post** delle attività e dei relativi presidi di controllo (rilevanza dei sistemi informativi aziendali)
- sistema di **deleghe e procure** che assegni ai vari soggetti coinvolti nel processo in oggetto gli ambiti di autonomia a livello economico;

Analisi del sistema di controllo preventivo

Esempi di presidi di controllo 231 a livello di organizzazione:

- chiare e trasparenti modalità di **gestione delle risorse finanziarie**, che prevedano tra gli altri deleghe formali per i rapporti bancari ed i pagamenti, meccanismo di firme incrociate, altro;
- policy aziendali di **gestione dei conflitti di interesse**;
- processo formalizzato di qualifica delle terze parti (**risk-based due diligence**);
- previsione di specifiche **clausole 231** nei contratti con le terze parti;
- processo di selezione dei fornitori che preveda la **comparazione di più offerte** (scegliendo una soglia di rilevanza);
- **processi segregati**, affinché un unico soggetto non gestisca in autonomia un intero processo e le responsabilità (proposta, approvazione, esecuzione, controllo, archiviazione) siano suddivise tra più soggetti;

Analisi del sistema di controllo preventivo

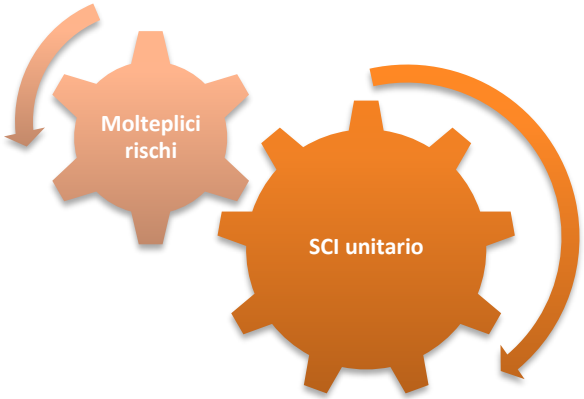
<u>Esempi di presidi di controllo 231 a livello di organizzazione:</u>

- previsione di periodiche **verifiche di compliance 231**;
- **rotazione del managemen**t a capo dei processi a più alto rischio (In particolare per soggetti controllati dalla Pubblica Amministrazione);
- minimizzare l'uso del **denaro contante** e della **piccola cassa**;
- **sistema di incentivazione** quali-quantitativo;
- **sistema sanzionatorio**.

Sistema integrato di gestione dei rischi

Benefici compliance integrata

- Razionalizzazione delle attività in termini di risorse, persone, sistemi, ecc.
- Migliorare l'efficacia ed efficienza delle attività di gestione dei rischi
- Facilitare la condivisione delle informazioni attraverso una visione integrata delle diverse esigenze di compliance (e non solo), anche attraverso l'esecuzione di risk assessment integrati

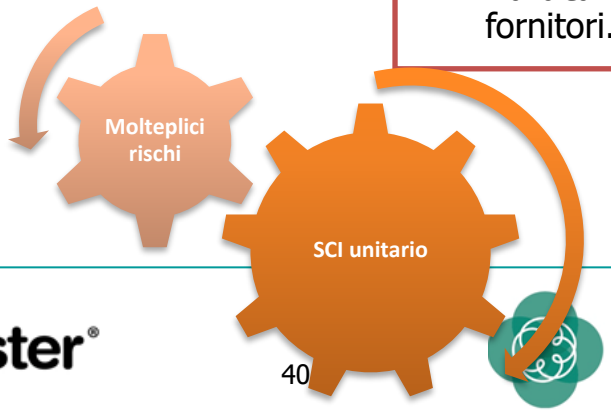


Sistema integrato di gestione dei rischi

Acquisti di beni e servizi

Rischi

- Operativi
- Corruzione
- Riciclaggio
- Criminalità organizzata
- Salute e sicurezza sui luoghi di lavoro
- Ambientali
- Fiscali
- Privacy
- Altro



Controlli

- **Qualifica dei fornitori:** che consenta di verificare la solidità finanziaria, l'attendibilità commerciale, tecnico-professionale ed etica,;
- **Anagrafica dei fornitori:** onde raccogliere e censire tutte le informazioni critiche e significative deli stessi;
- **Verifica della ragionevolezza/congruità** dell'operazione/acquisto;
- **Contratti/ordini scritti**, con chiara indicazione del prezzo del bene o del corrispettivo del servizio;
- **Verifica della rispondenza** della merce o servizio ricevuti rispetto a quanto effettivamente ordinato;
- Nei trasferimenti di denaro garantire la **piena coincidenza tra i destinatari/ordinanti i pagamenti e le controparti effettivamente coinvolte nelle transazioni**;
- **Valutazione periodica** delle prestazioni dei fornitori.

Gap Analysis – Valutazione dei rischi residui

Obiettivi

- Individuare le opportunità di miglioramento e definire un piano delle azioni correttive;

Attività

- Analisi comparativa tra il Modello Organizzativo e di controllo esistente ("AS IS") ed il modello astratto di riferimento ("TO BE") ai sensi del D.Lgs. n. 231/01;
- Individuazione delle azioni di miglioramento dell'attuale sistema di controllo;
- Condivisione delle possibili azioni di allineamento con il Management;
- Predisposizione di un action plan delle azioni condivise che identifica attività, priorità, responsabilità e tempi delle singole azioni.

Valutazione dei rischi residui

Determinato il **rischio residuo**, è necessario valutare se lo stesso sia **accettabile o meno**. La responsabilità di tale valutazione è dell'Organo Dirigente con il supporto dei soggetti che collaborano nella realizzazione del risk assessment e nella predisposizione del Modello.

Quando e come si può definire un rischio residuo accettabile?

Un rischio si può ritenere accettabile se la Società ha messo in piedi un sistema di prevenzione dei rischi reato tale da poter essere eluso solo <u>fraudolentemente</u>.

Tale assunto è coerente con quanto previsto art. 6, comma 1, lett. c del Decreto.

Rischio inerente – <u>Presidi di controllo</u> = Rischio residuo

L'obiettivo è la mitigazione del rischio 231

Valutazione dei rischi residui

La valutazione di adeguatezza del sistema di controllo interno e di accettabilità del rischio residuo non può prescindere dalle **linee guida di riferimento**, dalla **giurisprudenza** e dalle **best practices**.

I presidi di controllo possono essere molteplici, ma gli stessi devono essere **proporzionati** al livello di rischio, al disposto normativo ed alla struttura societaria.

Il sistema di controllo preventivo non può o non deve ingessare la società, ma deve essere funzionale ad essa per il raggiungimento dei propri obiettivi, in modo efficace ed efficiente.

Rischio inerente – Presidi di controllo = Rischio residuo

L'obiettivo è la mitigazione del rischio 231

Implementazione azioni correttive

A seguito dell'attività di risk asssessment può essere necessario implementare delle azioni correttive, con impatto ad esempio su:

- Codice Etico;
- Modello 231;
- Policy e linee guida;
- Procedure;
- Processi e controlli;
- Due Diligence delle terze parti;
- Whistleblowing;
- Formazione;
- Monitoraggi e revisione.

Aggiornamento del risk assessment…. e del Modello 231

La valutazione dinamica è necessaria per verificare l'adeguatezza e l'attualità del Modello 231 all'effettiva situazione dell'Ente ed al contesto normativo; più in particolare:

All'evoluzione delle strategie e degli obiettivi dell'Ente	**All'evoluzione dei fattori di rischio/normativi**
All'evoluzione del sistema informativo	**All'evoluzione dell'assetto organizzativo**

Altre evoluzioni "ambientali"

Il monitoraggio dovrà essere assicurato dall'Organismo di Vigilanza.

Q&A

GRAZIE!!!