MODELLO DI ORGANIZZAZIONE E CONTROLLO EX D.LGS. 231/2001

PARTE GENERALE

Rev	Data	Motivo	Approvazione
00		Prima adozione	Determina Amministratore Unico

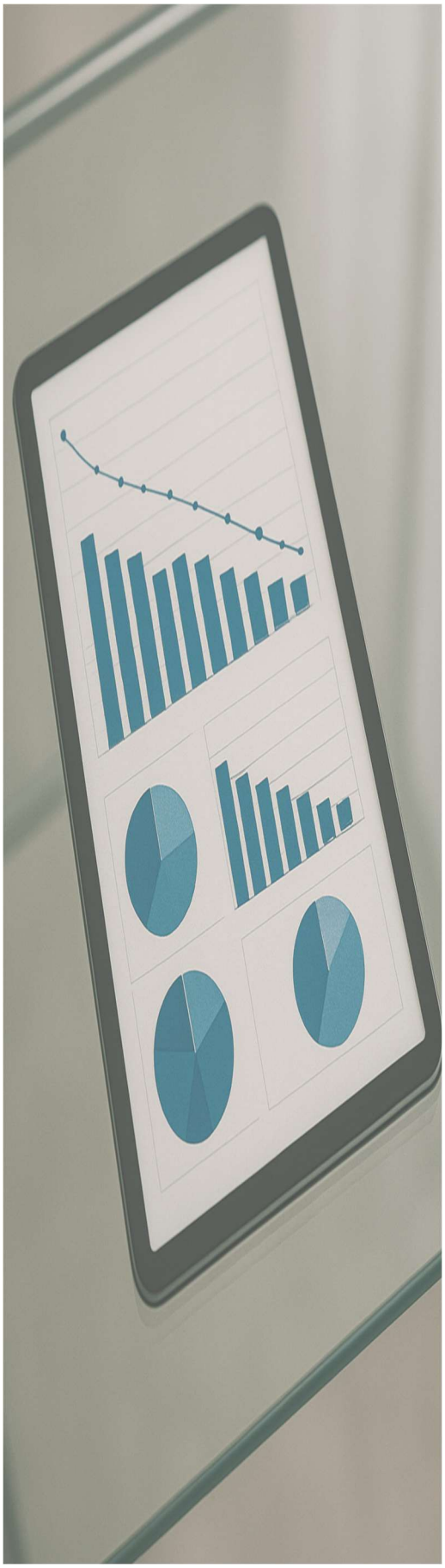


Tabella delle definizioni

Ai fini del presente documento si applicano i termini e le definizioni seguenti.

TABELLA DEI TERMINI E DELLE DEFINIZIONI			
Termine	**Definizione**	**Note**	**Riferimento normativo**
Alta direzione	persona che, al livello più elevato, guida e tiene sotto controllo un'organizzazione		ISO 37301, punto 3.3
Attività sensibile	attività dell'impresa nell'ambito della quale possono essere commessi reati previsti dal d.lgs. 231/2001		Art. 6, D.Lgs. 231/2001
Audit	processo sistematico e indipendente per ottenere evidenze e valutarle con obiettività, al fine di determinare in quale misura i criteri dell'audit sono stati soddisfatti.	Esiste audit interno (di prima parte) o un audit esterno (di seconda parte o di terza parte) Nota 2 Un audit interno è condotto dall'organizzazione stessa o da una parte esterna per suo conto. Nota 3 Le "evidenze dell'audit" ed i "criteri dell'audit" sono definiti nella UNI EN ISO 19011	ISO 37301, punto 3.18
Azione correttiva	azione per eliminare la causa di una non conformità per prevenirne la ripetizione.		ISO 37301, punto 3.17
Compliance	rispetto degli obblighi: soddisfacimento di tutti gli obblighi di compliance di un'organizzazione		ISO 37301, punto 3.26
Funzione di compliance	persona o gruppo di persone con responsabilità e autorità per il funzionamento del sistema di gestione per la compliance		ISO 37301, punto 3.23
Interesse/vantaggio	requisiti necessari per la sussistenza della responsabilità dell'ente collettivo, ai sensi del D.Lgs. 231/2001. L'interesse consiste nella finalizzazione del reato ad avvantaggiare l'ente; il vantaggio consiste nel risultato utile o profitto effettivamente conseguito dall'ente in seguito alla commissione del reato";		Art. 5, D.Lgs. 231/2001
Miglioramento continuo	attività ricorrente per migliorare le prestazioni		ISO 37301, punto 3.12
Modello di Organizzazione, Gestione e Controllo	documento che contiene una pluralità di misure organizzative, gestionali e di controllo finalizzate alla prevenzione dei reati previsti dal d.lgs. 231/2001		Art. 6, D.Lgs. 231/2001
Organizzazione	persona o gruppo di persone avente funzioni proprie con responsabilità, autorità e relazioni per conseguire i propri obiettivi		ISO 37301, punto 3.1

Organismo di Vigilanza	organo della società munito di autonomi poteri di iniziativa e di controllo deputato a monitorare il funzionamento del Modello organizzativo e curarne l'aggiornamento"	Nozione sostanzialmente coincidente con quella di "Organo di governo" contenuta nella UNI ISO 37301 :2021: "Persona o gruppo di persone che detiene la responsabilità e autorità finali nei confronti delle attività, della governance e delle politiche di un'organizzazione e al quale riferisce l'alta direzione e rispetto alla quale l'alta direzione è chiamata a rispondere	Art. 6, D.Lgs. 231/2001
Parte interessata (termine preferito) **stakeholder** (termine ammesso):	persona od organizzazione che può influenzare, essere influenzata, o percepire sé stessa come influenzata, da una decisione o attività.		ISO 37301, punto 3.2
Procedura	modo specificato per svolgere un'attività o un processo		ISO 37301, punto 3.31
Processo	Insieme di attività correlate o interagenti che utilizzano o trasformano input per consegnare un risultato.		ISO 37301, punto 3.8
Rischio	qualsiasi variabile o fattore che nell'ambito dell'azienda, da soli o in correlazione con altre variabili, possano incidere negativamente sul raggiungimento degli obiettivi indicati dal decreto 231	Per la ISO 37301, punto 3.7 è l'effetto dell'incertezza in relazione agli obietti	Art. 6, D.Lgs. 231/2001
Sistema di gestione	insieme di elementi correlati o interagenti di un'organizzazione finalizzato a stabilire politiche, obiettivi e processi per conseguire tali obiettivi		ISO 37301, punto 3.4
Soggetto apicale	soggetto munito di poteri di rappresentanza della società o al quale compete l'amministrazione o la direzione e controllo della stessa		Art. 5, D.Lgs. 231/2001

ACRONIMI	
AU	Amministratore Unico
MOG	Modello di Organizzazione, Gestione e Controllo
OdV	Organismo di Vigilanza
PG	Procedura Gestionale
PO	Procedura Operativa

SEZIONE PRIMA

INTRODUZIONE AL D.LGS. 231/2001

1. IL D.LGS 231/2001: PRINCIPALI CONTENUTI

1.1. Premessa

Con il **Decreto Legislativo 8 giugno 2001, n. 231** (di seguito, anche "Decreto" o "D.Lgs. 231/2001"), recante **la disciplina della "Responsabilità amministrativa degli enti"**, è stata introdotta nell'ordinamento italiano la responsabilità delle persone giuridiche **per alcuni reati commessi nel loro interesse o vantaggio**. Questa forma di responsabilità **si affianca a quella tradizionalmente prevista per le persone fisiche** e deriva dalla commissione di reati specificamente indicati nella Parte Speciale del Decreto. I soggetti attivi sono persone fisiche che rivestono funzioni apicali o che operano sotto la direzione e il controllo altrui all'interno dell'organizzazione. Il D.Lgs. 231/2001 rappresenta un'importante **innovazione normativa, finalizzata a contrastare la criminalità d'impresa**, riconoscendo che determinati illeciti possono riflettere non solo iniziative individuali, ma anche politiche aziendali più ampie. In questo contesto si parla di corporate crime, evidenziando la diretta imputazione del reato alla società, oltre che al singolo autore materiale.

La previsione della responsabilità amministrativa degli enti trova fondamento anche in fonti sovranazionali, quali la Convenzione di Bruxelles del 26 luglio 1995 sulla tutela degli interessi finanziari della Comunità Europea, la Convenzione di Bruxelles del 26 maggio 1997 sulla lotta alla corruzione di funzionari pubblici e la Convenzione OCSE del 17 dicembre 1997 sulla lotta alla corruzione di pubblici ufficiali stranieri.

In origine limitata a un numero ristretto di reati, la disciplina si è progressivamente ampliata per effetto di successivi interventi legislativi, includendo numerose fattispecie penalmente rilevanti. Tra queste si annoverano, a titolo esemplificativo:

- ✓ Indebita percezione di erogazioni, truffa in danno dello Stato, di un ente pubblico o dell'Unione europea o per il conseguimento di erogazioni pubbliche, frode informatica in danno dello Stato o di un ente pubblico e frode nelle pubbliche forniture (Art. 24, D. Lgs. n. 231/2001);
- ✓ Delitti informatici e trattamento illecito di dati (Art. 24-bis, D. Lgs. n. 231/2001);
- ✓ Delitti di criminalità organizzata (Art. 24-ter, D. Lgs. n. 231/2001);
- ✓ Peculato, indebita destinazione di denaro o cose mobili, concussione, induzione indebita a dare o promettere utilità, corruzione (Art. 25, D. Lgs. n. 231/2001);
- ✓ Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento (Art. 25-bis, D. Lgs. n. 231/2001);
- ✓ Delitti contro l'industria e il commercio (Art. 25-bis.1, D. Lgs. n. 231/2001);
- ✓ Reati societari (Art. 25-ter, D. Lgs. n. 231/2001);
- ✓ Reati con finalità di terrorismo o di eversione dell'ordine democratico (Art. 25-quater, D. Lgs. n. 231/2001);

- ✓ Pratiche di mutilazione degli organi genitali femminili (Art. 25-quater.1, D. Lgs. n. 231/2001);
- ✓ Delitti contro la personalità individuale (Art. 25-quinquies, D. Lgs. n. 231/2001);
- ✓ Abuso di mercato (Art. 25-sexies, D. Lgs. n. 231/2001);
- ✓ Reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro (Art. 25-septies, D. Lgs. n. 231/2001);
- ✓ Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio (Art. 25-octies, D. Lgs. n. 231/2001);
- ✓ Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori (art. 25-octies.1, D.Lgs. n. 231/2001);
- ✓ Delitti in materia di violazione del diritto d'autore (Art. 25-novies, D. Lgs. n. 231/2001);
- ✓ Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (Art. 25-decies, D. Lgs. n. 231/2001);
- ✓ Reati ambientali (Art. 25-undecies, D. Lgs. n. 231/2001);
- ✓ Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (Art. 25-duodecies, D. Lgs. n. 231/2001);
- ✓ Razzismo e Xenofobia, (Art. 25-terdecies, D.lgs. n. 231/2001);
- ✓ Frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati (Art. 25-quaterdecies, D.lgs. 231/2001);
- ✓ Reati tributari (Art. 25-quinquiesdecies del D.lgs. 231/2001);
- ✓ Contrabbando (Art. 25-sexiesdecies del D.lgs. 231/2001);
- ✓ Delitti contro il patrimonio culturale (art. 25-septiesdecies d.lgs. 231/2001);
- ✓ Riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici (art. 25-duodevicies d.lgs. 231/2001);
- ✓ Responsabilità degli enti per gli illeciti amministrativi dipendenti da reato (Art. 12, L. n. 9/2013, costituiscono presupposto per gli enti che operano nell'ambito della filiera degli oli vergini di oliva);
- ✓ Reati transnazionali (L. n. 146/2006).

Oggi, la responsabilità amministrativa degli enti copre un vasto spettro di reati che interessano molteplici settori, con l'obiettivo di incentivare le imprese a dotarsi di modelli organizzativi idonei a prevenire la commissione di illeciti.

Alla luce del costante aggiornamento normativo che interessa il catalogo dei reati presupposto, si precisa che l'elenco sempre aggiornato degli stessi è riportato nel documento allegato al presente Modello, denominato **Allegato 1 – Matrice dei reati presupposto**.

1.2. L'ambito di applicazione soggettiva del d.lgs. 231/2001

L'art. 1 del D.Lgs. 231/2001 definisce l'ambito soggettivo di applicazione della disciplina, stabilendo che essa si applica agli enti forniti di personalità giuridica, alle società e alle associazioni anche prive di personalità giuridica. Sono dunque destinatari del Decreto:

- ✓ Le **persone giuridiche private riconosciute**, comprese le fondazioni (artt. 14 ss. c.c.), ossia enti privati cui viene riconosciuta la personalità giuridica attraverso apposite procedure;

- ✓ Tutte le **società**, tra cui:
  - Società per azioni (tranne quelle in formazione);
  - Società in accomandita per azioni;
  - Società a responsabilità limitata, anche unipersonali;
  - Società partecipate dallo Stato o da enti pubblici;
  - Società estere con sede secondaria in Italia;
  - Società cooperative, di mutua assicurazione, semplici, in nome collettivo, in accomandita semplice;
  - Società di intermediazione mobiliare (SIM), società di investimento a capitale variabile (SICAV), società di gestione di fondi comuni;
  - Società sportive.
- ✓ Le **associazioni non riconosciute**, ossia enti privi di personalità giuridica che svolgono attività non a fini di lucro (artt. 36 ss. c.c.).
- ✓ I **consorzi con attività esterna**, anche se non costituiti in forma societaria, dotati di autonomia patrimoniale (art. 2615 c.c.).

Sono, invece, esclusi dal campo di applicazione del Decreto:

- ✓ Lo **Stato**, gli **enti pubblici territoriali** (Regioni, Province, Comuni) e gli **enti pubblici non economici**;
- ✓ Gli enti che esercitano funzioni di rilievo costituzionale (ad es. partiti politici, sindacati);
- ✓ Gli enti pubblici associativi che, pur caratterizzati da tendenze privatistiche, conservano natura pubblica per disposizioni di legge (es. Ordini professionali, Croce Rossa Italiana);
- ✓ Gli enti pubblici erogatori di servizi pubblici (istituzioni assistenziali, scuole, università, aziende ospedaliere);
- ✓ Gli enti che perseguono fini pubblici (INPS, INAIL, CNR, ISTAT, ENEA, ecc.).

Non sono esclusi, invece, gli **enti pubblici economici**, ossia soggetti di diritto pubblico che operano sul mercato secondo regole privatistiche (ad es. istituti di credito di diritto pubblico).
La giurisprudenza ha inoltre chiarito che la disciplina si applica anche alle **società straniere con sede principale all'estero**, purché operanti stabilmente in Italia. In tal senso si è espresso il Tribunale di Milano (27 aprile 2004), affermando che l'assenza di obblighi analoghi nella normativa del paese d'origine non esonera la società estera dal rispetto delle previsioni del D.Lgs. 231/2001, qualora operi sul territorio italiano. Il criterio applicativo si fonda, infatti, sul luogo di commissione del reato presupposto.
Diversamente, l'art. 4 del Decreto disciplina i casi di **reati commessi all'estero da società con sede principale in Italia**. In tali ipotesi, la società può essere ritenuta responsabile qualora:

a) abbia la sede principale in Italia;
b) ricorrano le condizioni previste dagli artt. 7, 8, 9 e 10 del codice penale;
c) nei casi in cui sia richiesta l'autorizzazione del Ministro della giustizia per procedere penalmente, tale richiesta sia estesa anche all'ente.

1.3. Presupposti e natura della responsabilità dell'ente

Ai sensi del D.Lgs. 231/2001, la responsabilità dell'ente si fonda sulla presenza congiunta di tre condizioni oggettive:

- ✓ la commissione di un reato rientrante tra quelli indicati nel Decreto (c.d. **reato presupposto**);
- ✓ la commissione del reato da parte di una persona fisica che riveste funzioni apicali o sottoposte all'altrui direzione o vigilanza all'interno dell'ente;
- ✓ la realizzazione del reato **nell'interesse o a vantaggio dell'ente**.

Tuttavia, la sola sussistenza di questi elementi non è sufficiente a configurare la responsabilità dell'ente. Il legislatore ha infatti ancorato tale responsabilità a un **deficit organizzativo**, richiedendo che l'ente risponda solo se non abbia adottato ed efficacemente attuato modelli di organizzazione e gestione idonei a prevenire la commissione di reati. Si tratta di una responsabilità definita come **colpa di organizzazione**, che esclude un'automatica imputazione all'ente per i reati commessi dai propri soggetti apicali o subordinati.

La giurisprudenza ha chiarito che la responsabilità dell'ente non sorge quando il reato sia stato commesso nell'interesse esclusivo della persona fisica, per fini personali o estranei all'attività dell'impresa. In particolare, la Corte di Cassazione ha evidenziato che la responsabilità dell'ente richiede, oltre al nesso oggettivo tra reato e interesse/vantaggio dell'ente, anche la mancata adozione di adeguati modelli di prevenzione (**culpa in vigilando**).

1.4. Autonomia della responsabilità della società

Un aspetto qualificante della disciplina è l'autonomia della responsabilità della società rispetto a quella della persona fisica che ha materialmente commesso il reato. L'art. 8 del D.Lgs. 231/2001 stabilisce, infatti, che l'ente può essere chiamato a rispondere anche quando:

- ✓ l'autore del reato non sia stato identificato o non sia imputabile;
- ✓ il reato si estingua per cause diverse dall'amnistia (ad esempio, prescrizione o morte dell'autore del reato).

Questa previsione risponde all'esigenza di evitare che l'ente possa sottrarsi alla responsabilità in ragione della complessità dell'organizzazione o dell'impossibilità di identificare il soggetto responsabile. È il caso, ad esempio, delle ipotesi di imputazione soggettivamente alternativa, in cui risulti evidente la riconducibilità del reato ai vertici aziendali, ma non sia possibile attribuire con certezza la responsabilità a uno specifico amministratore. Unica eccezione a tale principio riguarda l'amnistia propria, la quale preclude l'esercizio dell'azione anche nei confronti dell'ente, salvo che quest'ultimo non rinunci volontariamente a tale causa estintiva al fine di ottenere una pronuncia assolutoria nel merito. In ogni caso, resta ferma la distinzione tra l'illecito penale imputabile alla persona fisica e quello amministrativo imputabile all'ente, trattandosi di responsabilità autonome e non alternative.

1.5. Le sanzioni

L'art. 9 del D.Lgs. 231/2001 individua le sanzioni applicabili agli enti riconosciuti responsabili di illeciti amministrativi dipendenti da reato. Esse sono:

Tipologia di Sanzione	Descrizione
Sanzioni pecuniarie	**Le sanzioni pecuniarie sono** determinate dal giudice attraverso **un sistema basato su "quote"** in numero non inferiore a cento e non superiore a mille e di importo variabile fra un minimo di Euro 258,22 a un massimo di Euro 1.549,37. Nella commisurazione della sanzione pecuniaria il giudice determina: (i) il numero delle quote, tenendo conto della gravità del fatto, del grado della responsabilità della società nonché dell'attività svolta per eliminare o attenuare le conseguenze del fatto e per prevenire la commissione di ulteriori illeciti; (ii) l'importo della singola quota, sulla base delle condizioni economiche e patrimoniali della società. Sono previste però riduzioni delle sanzioni pecuniarie in caso di: ✓ Interesse prevalente dell'autore/terzi senza vantaggio per l'ente ✓ Danno patrimoniale tenue ✓ Risarcimento integrale del danno ✓ **Adozione di Modello Organizzativo idoneo.**
Sanzioni interdittive	**Le sanzioni interdittive si applicano esclusivamente per determinati reati espressamente previsti dal Decreto**, quando l'ente ha tratto un profitto di rilevante entità dal reato e la sua commissione è stata favorita da gravi carenze organizzative; oppure in caso di reiterazione degli illeciti. Le sanzioni interdittive sono: ✓ Interdizione dall'esercizio dell'attività; ✓ Sospensione o revoca di autorizzazioni, licenze o concessioni; ✓ Divieto di contrattare con la Pubblica Amministrazione (salvo prestazioni di pubblico servizio); ✓ Esclusione da agevolazioni, contributi e finanziamenti, con eventuale revoca di quelli già concessi; ✓ Divieto di pubblicizzare beni o servizi. Esse possono essere applicate anche in via definitiva nei seguenti casi: ✓ profitto di rilevante entità con condanne per sanzioni interdittive temporanee già riportate almeno tre volte negli ultimi sette anni; ✓ utilizzo stabile della società o di un'unità organizzativa per la commissione di reati.
Confisca	**Viene sempre disposta con la condanna**, per il prezzo o profitto del reato. Può riguardare anche beni di valore equivalente. Cassazione (sentenza n. 10561/2014): applicabile anche per reati non presupposto, se il profitto resta disponibile alla società.
Pubblicazione della sentenza	**Disposta** dal giudice **quando** viene **applicata una sanzione interdittiva**.
Nomina del commissario	Alternativa alla sanzione interdittiva per evitare l'interruzione dell'attività quando: ✓ L'ente svolge servizio di pubblica utilità ✓ La sospensione ha effetti negativi sull'occupazione. I profitti derivanti dalla prosecuzione saranno confiscati.

1.6. Le misure cautelari interdittive e reali

Nei confronti della società sottoposta a procedimento può essere applicata, in via cautelare, una sanzione interdittiva ovvero disposto il sequestro preventivo o conservativo.

La **misura cautelare interdittiva** è disposta in presenza di due requisiti:

- ✓ quando risultano gravi indizi per ritenere la sussistenza della responsabilità della società per un illecito amministrativo dipendente da reato. I gravi indizi sussistono ove risulti una delle condizioni previste dall'art. 13 del Decreto: la società ha tratto dal reato – compiuto da un suo dipendente o da un soggetto in posizione apicale - un profitto di rilevante entità e la commissione del reato è stata determinata o agevolata da gravi carenze organizzative; in caso di reiterazione degli illeciti;
- ✓ quando vi sono fondati e specifici elementi che fanno ritenere concreto il pericolo che vengano commessi illeciti della stessa indole di quello per cui si procede.

Le **misure cautelari reali** si concretizzano nel sequestro preventivo e nel sequestro conservativo.

Il sequestro preventivo è disposto in relazione al prezzo o al profitto del reato, laddove il fatto di reato sia attribuibile alla società, non importando che sussistano gravi indizi di colpevolezza a carico della società stessa.

Il sequestro conservativo è disposto in relazione a beni mobili o immobili della società nonché in relazione a somme o cose alla stessa dovute, qualora vi sia fondato motivo di ritenere che manchino o si disperdano le garanzie per il pagamento della sanzione pecuniaria, delle spese del procedimento e di ogni altra somma dovuta all'erario dello Stato.

1.7. Delitti tentati

Nelle ipotesi di commissione, nelle forme del tentativo, dei delitti sanzionati sulla base del D. Lgs. 231/2001, le sanzioni pecuniarie (in termini di importo) e le sanzioni interdittive (in termini di durata) sono ridotte da un terzo alla metà. È esclusa l'irrogazione di sanzioni nei casi in cui l'ente impedisca volontariamente il compimento dell'azione o la realizzazione dell'evento (art. 26 D. Lgs. 231/2001). L'esclusione di sanzioni si giustifica, in tal caso, in forza dell'interruzione di ogni rapporto di immedesimazione tra ente e soggetti che assumono di agire in suo nome e per suo conto.

1.8. Le azioni esimenti dalla responsabilità amministrativa

L'art. 6, comma I, del Decreto prevede una forma specifica di esimente dalla responsabilità amministrativa qualora il reato sia stato commesso da soggetti in c.d. «**posizione apicali**» e la Società provi che:

a) l'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto illecito, un modello idoneo a prevenire la realizzazione degli illeciti della specie di quello verificatosi;

b) ha affidato ad un organo interno – c.d. Organismo di Vigilanza, dotato di autonomi poteri di iniziativa e di controllo – il compito di vigilare sul funzionamento e sull'efficace osservanza del modello in questione, nonché di curarne l'aggiornamento;

c) i soggetti in c.d. «posizione apicali» hanno commesso il reato eludendo fraudolentemente il modello;

d) non vi è stato omesso o insufficiente controllo da parte del c.d. Organismo di Vigilanza.

L'art. 6, comma II, del Decreto dispone inoltre che il modello debba rispondere alle seguenti esigenze:

- ✓ individuare i rischi aziendali, ovvero le attività nel cui ambito possono essere commessi i reati;
- ✓ escludere che un qualunque soggetto operante all'interno della Società possa giustificare la propria condotta adducendo l'ignoranza delle discipline aziendali ed evitare che, nella normalità dei casi, il reato possa essere causato dall'errore – dovuto anche a negligenza o imperizia – nella valutazione delle direttive aziendali;
- ✓ introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello;
- ✓ individuare modalità di gestione delle risorse finanziarie idonee a impedire la commissione di tali reati;
- ✓ prevedere un sistema di controlli preventivi tali da non poter essere aggirati se non intenzionalmente;
- ✓ prevedere obblighi di informazione nei confronti dell'Organismo di Vigilanza deputato a controllare sul funzionamento e l'osservanza del modello.

L'art. 7 del Decreto prevede una forma specifica di esimente dalla responsabilità amministrativa, qualora il reato sia stato commesso dai c.d. «**subalterni**», ma sia accertato che la Società, prima della commissione del reato, abbia adottato un modello idoneo a prevenire reati della stessa specie di quello verificatosi.

In concreto la Società, per poter essere esonerata dalla responsabilità amministrativa, deve implementare un sistema articolato e completo di procedure e controlli interni. Questo sistema deve essere strutturato in modo da garantire la massima trasparenza e correttezza nella gestione delle attività aziendali, prevenendo efficacemente il rischio di commissione dei reati previsti dalla normativa. In particolare, è chiamata a dotarsi dei seguenti elementi costitutivi di un Modello di Organizzazione, Gestione e Controllo dei rischi di commissione di reati (MOG):

CODICE ETICO
Adozione di un documento formale che stabilisca principi di comportamento in relazione alle fattispecie di reato rilevanti

STRUTTURA ORGANIZZATIVA
Definizione di un'organizzazione che garantisca chiara attribuzione dei compiti, segregazione delle funzioni e controllo dei comportamenti

PROCEDURE FORMALIZZATE
Implementazione di procedure manuali ed informatiche per regolamentare lo svolgimento delle attività, con particolare attenzione alla segregazione dei compiti nelle aree a rischio

POTERI AUTORIZZATIVI
Assegnazione di poteri di firma coerenti con le responsabilità organizzative e gestionali definite

COMUNICAZIONE INTERNA
Diffusione capillare al personale del Codice Etico, delle procedure e di tutti gli strumenti di prevenzione

SISTEMA SANZIONATORIO
Predisposizione di un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello

ORGANISMO DI VIGILANZA
Costituzione di un organo autonomo e indipendente con adeguata professionalità, in grado di valutare l'adeguatezza del modello, vigilare sul suo funzionamento e curarne l'aggiornamento.

L'adozione di questi elementi costituisce non solo un requisito per l'esonero dalla responsabilità, ma rappresenta anche un'importante opportunità per migliorare i processi interni, rafforzare la governance aziendale e promuovere una cultura della legalità e dell'etica all'interno dell'azienda.

1.9. Procedimento di accertamento dell'illecito

La responsabilità per illecito amministrativo derivante da reato viene accertata nell'ambito di un procedimento penale. A tale proposito, l'art. 36 del D. Lgs. 231/2001 prevede che "*La competenza a conoscere gli illeciti amministrativi dell'ente appartiene al giudice penale competente per i reati dai quali gli stessi dipendono. Per il procedimento di accertamento dell'illecito amministrativo dell'ente si osservano le disposizioni sulla composizione del tribunale e le disposizioni processuali collegate relative ai reati dai quali l'illecito amministrativo dipende*".

Altra regola, ispirata a ragioni di effettività, omogeneità ed economia processuale è quella dell'obbligatoria riunione dei procedimenti: il processo nei confronti dell'ente dovrà rimanere riunito, per quanto possibile, al processo penale instaurato nei confronti della persona fisica autore del reato presupposto della responsabilità dell'ente (art. 38 del D. Lgs. 231/2001). Tale regola trova un contemperamento nel dettato dell'art. 38, comma 2, del D. Lgs. 231/2001 che, viceversa, disciplina i casi in cui si procede separatamente per l'illecito amministrativo. L'ente partecipa al procedimento penale con il proprio rappresentante legale, salvo che questi sia imputato del reato da cui dipende l'illecito amministrativo; quando il legale rappresentante non compare, l'ente costituito è rappresentato dal difensore (art. 39, commi 1 e 4, del D. Lgs. 231/2001).

1.10. Vicende modificate della società

Il D.Lgs. 231/2001 disciplina la responsabilità patrimoniale degli enti in relazione a operazioni societarie straordinarie quali trasformazione, fusione, scissione e cessione d'azienda. Secondo l'art. 27, l'ente risponde delle sanzioni pecuniarie con il proprio patrimonio o fondo comune, evidenziando una responsabilità autonoma rispetto ai singoli membri e all'autore del reato.

Gli articoli 28-33 regolano la responsabilità dell'ente nelle diverse vicende modificative:

Trasformazione (art. 28): la responsabilità per reati precedenti rimane invariata.

Scissione (art. 30): la società scissa resta responsabile per i reati precedenti. Gli enti beneficiari sono solidalmente responsabili entro il limite del patrimonio ricevuto, con obblighi più estesi se ricevono il ramo di attività interessato.

Cessione o conferimento d'azienda (art. 33): il cessionario è solidalmente responsabile per sanzioni pecuniarie entro il valore dell'azienda ceduta e nei limiti indicati; le sanzioni interdittive non si trasferiscono.

Fusione (art. 29): l'ente risultante risponde per i reati delle società fuse.

Fusione e scissione (art. 31): le sanzioni pecuniarie sono commisurate alle condizioni economiche dell'ente originario; le interdittive possono essere convertite in pecuniarie se eliminate le carenze organizzative e risarciti i danni.

2. MODELLI DI ORGANIZZAZIONE GESTIONE E CONTROLLO

2.1. Il Valore esimente di un modello di organizzazione

Aspetto fondamentale del D.Lgs. 231/2001 è l'attribuzione di un valore esimente ai modelli di organizzazione, gestione e controllo della società. In caso di reato commesso da un soggetto in posizione apicale, infatti, la società **non risponde se prova**, tra i vari aspetti, **che l'organo dirigente ha adottato ed efficacemente attuato**, prima della commissione del fatto, modelli di organizzazione e di gestione idonei a prevenire reati della specie di quello verificatosi (art. 6, comma 1, D. Lgs. 231/2001).

Adozione del modello: Il D. Lgs. 231/2001 delinea il contenuto dei modelli di organizzazione e di gestione prevedendo che gli stessi, in relazione all'estensione dei poteri delegati e al rischio di commissione dei reati, come specificato dall'art. 6, comma 2, debbano:

- ✓ individuare le attività nel cui ambito possano essere commessi reati;
- ✓ prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni della società in relazione ai reati da prevenire;
- ✓ individuare modalità di gestione delle risorse finanziarie idonee a impedire la commissione dei reati;
- ✓ prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei modelli;
- ✓ introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello

Efficace attuazione: L'art. 7, comma 4, del D. Lgs. 231/2001 definisce, inoltre, i requisiti dell'efficace attuazione dei modelli organizzativi:

- ✓ la verifica periodica e l'eventuale modifica del modello quando sono scoperte significative violazioni delle prescrizioni ovvero quando intervengono mutamenti nell'organizzazione e nell'attività;
- ✓ un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.

2.2. Modelli di riferimento per l'adozione di un MOG

L'art. 6, comma 3, del D. Lgs. 231/2001 prevede che "*I modelli di organizzazione e di gestione possono essere adottati, garantendo le esigenze di cui al comma 2, sulla base di codici di comportamento redatti dalle associazioni rappresentative degli enti, comunicati al Ministero della giustizia che, di concerto con i Ministeri competenti, può formulare, entro trenta giorni, osservazioni sulla idoneità dei modelli a prevenire i reati*".

Confindustria ha definito le "Linee guida per la costruzione dei modelli di organizzazione, gestione e controllo ex D. Lgs. n. 231/2001", diffuse in data 7 marzo 2002, integrate in data 3 ottobre 2002 con appendice relativa ai c.d. reati societari (introdotti nel D. Lgs. 231/2001 con il D. Lgs. n. 61/2002) e aggiornate, da ultimo, al giugno 2021 (di seguito, "Linee guida di Confindustria") fornendo, tra l'altro, indicazioni metodologiche per l'individuazione delle aree di rischio (settore/attività nel cui ambito possono essere commessi reati), la progettazione di un sistema di controllo (i c.d. protocolli per la programmazione della formazione ed attuazione delle decisioni dell'ente) e i contenuti del modello di organizzazione, gestione e controllo.

Il presente Modello **è ispirato alle «Linee guida** per la costruzione di modelli di organizzazione, gestione e controllo deliberato *ex* d.lgs. 231/01» **approvate** e divulgate **da Confindustria** ed aggiornate nel giugno del **2021 nonché** ai principi delineati dalla **UNI ISO 37301:2021 sui "Sistemi di Gestione della Compliance".**

2.3. Le linee Guida Confindustria 2021

Le Linee Guida di Confindustria sono state approvate dal Ministero della Giustizia con il D.M. 4.12.2003. L'ultimo aggiornamento, pubblicato nel giugno 2021, è stato approvato dal Ministero della Giustizia, che ha giudicato tali Linee Guida idonee al raggiungimento delle finalità previste dal Decreto.

Le fasi fondamentali che le **Linee Guida Confindustria** individuano nella costruzione dei Modelli possono essere così schematizzate:

una **prima fase** consiste nell'**identificazione dei rischi**, ossia l'analisi del contesto aziendale per evidenziare dove (in quale area/settore di attività) e secondo quali modalità si possono verificare eventi pregiudizievoli per gli obiettivi indicati dal Decreto;

una **seconda fase** consiste nella **progettazione del sistema di controllo** (c.d. protocolli per la programmazione della formazione ed attuazione delle decisioni della società), ossia nella valutazione del sistema esistente all'interno della società ed il suo eventuale adeguamento, in termini di capacità di contrastare efficacemente, cioè ridurre ad un livello accettabile, i rischi identificati.

Fase di identificazione dei rischi

Da un punto di vista concettuale, **la riduzione del rischio comporta** il dovere **di intervenire su** due fattori determinanti:

- ✓ **la probabilità di accadimento dell'evento;**
- ✓ **l'impatto dell'evento stesso.**

Per operare efficacemente, il sistema delineato non può però ridursi a un'attività saltuaria, ma **deve tradursi in un processo continuo da reiterare con particolare attenzione ai momenti di cambiamento aziendale.**

Va peraltro osservato che la premessa per la costruzione di un sistema di controllo preventivo adeguato passa attraverso la definizione del "**rischio accettabile**".

Se nell'ambito della progettazione di sistemi di controllo a tutela dei rischi di *business*, il rischio è ritenuto accettabile quando i controlli aggiuntivi "costano" più della risorsa da proteggere (es. le comuni automobili sono dotate di antifurto e non anche di un vigile armato), **nel contesto del d.lgs. n. 231** del 2001, invece, la logica economica dei costi non può essere un riferimento utilizzabile in via esclusiva. È dunque importante che ai fini dell'applicazione delle norme del decreto sia definita una soglia effettiva che consenta di porre un limite alla quantità/qualità delle misure di prevenzione da introdurre per evitare la commissione dei reati considerati. D'altronde, in assenza di una previa determinazione del rischio accettabile, la quantità/qualità di controlli preventivi istituibili è virtualmente infinita, con le intuibili conseguenze in termini di operatività aziendale. Del resto, il generale principio, invocabile anche nel diritto penale, dell'esigibilità concreta del comportamento, sintetizzato dal brocardo latino *ad impossibilia nemo tenetur*, rappresenta un criterio di riferimento ineliminabile anche se, spesso, appare difficile individuarne in concreto il limite.

La nozione di "accettabilità" di cui sopra riguarda i rischi di condotte devianti dalle regole del modello organizzativo e non anche i sottostanti rischi lavorativi per la salute e la sicurezza dei lavoratori che, secondo i principi della vigente legislazione prevenzionistica, devono essere comunque integralmente eliminati in relazione alle conoscenze acquisite in base al progresso tecnico e, ove ciò non sia possibile, ridotti al minimo e, quindi, gestiti.

Casi dei reati dolosi

Riguardo al sistema di controllo preventivo da costruire in relazione al rischio di commissione delle fattispecie di reato contemplate dal d.lgs. n. 231 del 2001, **la soglia concettuale di accettabilità, nei casi di reati dolosi, è rappresentata da un sistema di prevenzione tale da non poter essere aggirato se non fraudolentemente.** Questa soluzione è in linea con la logica della "elusione fraudolenta" del modello organizzativo quale esimente espressa dal citato decreto legislativo ai fini

dell'esclusione della responsabilità amministrativa della società (art. 6, comma 1, lett. c), «le persone hanno commesso il reato eludendo fraudolentemente i modelli di organizzazione e di gestione».

Casi dei reati colposi

Diversamente, **nei casi di reati di omicidio colposo e lesioni personali colpose commessi con violazione delle norme in materia di salute e sicurezza sul lavoro, la soglia concettuale di accettabilità, agli effetti esimenti del d.lgs. n. 231 del 2001, è rappresentata dalla realizzazione di una condotta** (non accompagnata dalla volontà dell'evento-morte/lesioni personali) **che viola il modello organizzativo di prevenzione** (e dei sottostanti adempimenti obbligatori prescritti dalle norme prevenzionistiche) **nonostante la puntuale osservanza degli obblighi di vigilanza previsti dal d.lgs. n. 231 del 2001 da parte dell'apposito organismo di vigilanza**. Ciò in quanto l'elusione fraudolenta dei modelli organizzativi appare incompatibile con l'elemento soggettivo dei reati di omicidio colposo e lesioni personali colpose, di cui agli artt. 589 e 590 c.p.

*** *** ***

In conclusione, secondo le Linee Guida Confindustria, **la realizzazione di un sistema di gestione del rischio deve muovere dal presupposto che i reati possano comunque essere commessi anche una volta attuato il modello**.

Laddove si tratti di reati dolosi, il modello e le relative misure devono cioè essere tali che l'agente non solo dovrà "volere" l'evento reato (es. corrompere un pubblico funzionario), **ma potrà attuare il suo proposito criminoso soltanto aggirando fraudolentemente** (es. attraverso artifizi e/o raggiri) **le indicazioni della società**. L'insieme di misure che l'agente sarà costretto a "forzare" nel caso in cui sia sua intenzione delinquere, dovrà essere realizzato in relazione a quelle specifiche attività considerate a rischio e ai singoli reati ipoteticamente collegabili alle stesse.

Nell'ipotesi di reato colposo, invece, l'evento dannoso e pericoloso, anche se preveduto non è mai voluto dall'agente e si verifica a causa di negligenza, imprudenza o imperizia, ovvero per inosservanza di leggi, regolamenti, ordini o discipline. In tale settore, pertanto, **assume particolare rilievo il rispetto dei protocolli e delle norme cautelari, volte ad evitare il verificarsi di eventi che costituiscono l'oggetto di protezione di norme cautelari.**

Fase di progettazione del sistema di controllo

Nella definizione del Modello di Organizzazione, Gestione e Controllo, le Linee Guida di Confindustria prevedono le seguenti fasi progettuali:

INFORMAZIONE E FORMAZIONE DEL PERSONALE

- **Attività di formazione e informazione** del personale ai fini di una concreta attuazione del modello di organizzazione

PROCEDURE E SISTEMI DI CONTROLLO DI GESTIONE

- Procedure per regolare lo svolgimento delle attività, prevedendo opportuni controlli, e per segnalare tempestivamente possibili criticità

IDENTIFICAZIONE DEI RISCHI

- **Analisi del contesto aziendale** per evidenziare in quali aree di attività e secondo quali modalità si possano verificare eventi pregiudizievoli per gli obiettivi indicati dal D.lgs. 231/2001.

PREDISPOSIZIONE DI UN SISTEMA DI CONTROLLO:

- **Previsione di principi etici e di regole comportamentali** (CODICE ETICO)
- **Sistema organizzativo formalizzato e chiaro** (con poteri di firma coerenti con le responsabilità organizzative)

Le Linee Guida di Confindustria precisano, **inoltre**, che le componenti del sistema di controllo sopra descritte devono conformarsi ad **una serie di principi di controllo**, tra cui:

tracciabilità, verificabilità, coerenza e congruità di ogni operazione, transazione e azione

applicazione del **principio di** separazione delle funzioni e **segregazione dei compiti** (nessuno può gestire in autonomia un intero processo)

documentazione dei controlli effettuati

Il sistema di controllo integrato

Le nuove Linee Guida predisposte da Confindustria hanno in particolar modo incentrato la propria attenzione su aspetti valorizzati nel modello di organizzazione e controllo che la società ha adottato.

In particolare, molto interessante è la grande importanza data con le nuove Linee Guida alla valorizzazione di un sistema integrato di gestione dei rischi.

Sul punto, con tale documento si chiarisce che "***È ormai dato acquisito che il rischio di compliance, ossia di non conformità alle norme, comporta per le imprese il rischio di incorrere in sanzioni giudiziarie o amministrative, perdite finanziarie rilevanti o danni reputazionali in conseguenza di violazioni di norme imperative ovvero di autoregolamentazione, molte delle quali rientrano nel novero dei reati di cui al D.lgs. 231/2001*"**. In effetti, la gestione dei numerosi obblighi di *compliance*, secondo un approccio tradizionale, potrebbe risultare connotata da una pluralità di processi, informazioni potenzialmente incoerenti e controlli potenzialmente non ottimizzati.

Sempre secondo le già menzionate Linee Guida, il passaggio ad una *compliance* integrata potrebbe permettere alla Società di:

a) razionalizzare le attività (in termini di risorse, persone, sistemi, ecc.);

b) migliorare l'efficacia ed efficienza delle attività di compliance;

c) facilitare la condivisione delle informazioni attraverso una visione integrata delle diverse esigenze di compliance, anche attraverso l'esecuzione di *risk assessment* congiunti, e la manutenzione periodica dei programmi di compliance.

Ciò comporta la necessità di individuare specifici e continui meccanismi di coordinamento e collaborazione tra i principali soggetti aziendali interessati tra i quali rientrano, a mero titolo esemplificativo, il Dirigente Preposto, il Datore di lavoro, il Revisore Unico e l'OdV.

A maggior ragione, nel caso in cui la Società miri all'ottenimento di certificazioni, pur avendo tali sistemi una funzione diversa dai modelli di organizzazione e gestione previsti dal decreto 231 diviene importante valorizzare la sinergia tra il Modello di organizzazione e controllo ex D.lgs. 231 e, la documentazione (articolata di solito in manuali interni, procedure, istruzioni operative e registrazioni) dei sistemi aziendali in materia antinfortunistica (ISO 45001), ambientale (ISO14001), di sicurezza informatica (ISO 27001), di qualità (ad esempio ISO 9001) anticorruzione (ISO 37001), ma anche del sistema di gestione del rischio del trattamento dei dati personali. **L'analisi del rischio deve quindi considerare policies e procedure esistenti, punto di partenza della compliance integrata.**

Valuecube s.r.l., alla luce di quanto sopra, ha adottato procedure operative che fungono da punto di contatto e coordinamento con tutte le altre procedure aziendali adottate prevedendo, tra l'altro, un'apposita regolamentazione dei flussi informativi all'ODV, tale da consentire proprio l'instaurazione di continui meccanismi di coordinamento e controllo dei principali soggetti aziendali.

2.4. I principi della ISO 37301: Sistemi di gestione per la compliance

Il modello di organizzazione e controllo adottato da Valuecube s.r.l. è stato predisposto seguendo anche gli standard di riferimento elaborati dalla UNI ISO 37301, che disciplina i sistemi di gestione per la *compliance*.

La *compliance* può essere definita come l'insieme delle regole emanate dal Legislatore, dai Ministeri, dagli Enti Pubblici Territoriali, ma anche da Authority di Garanzia, Organismi di controllo pubblici (ad esempio Consob, Banca d'Italia), Enti di certificazione pubblici e privati, Enti di gestione delle procedere nei rapporti con gli enti pubblici...che le aziende devono rispettare per una corretta condotta degli affari. La *compliance* presenta soprattutto aspetti "normativi", ma comprende anche regole etiche, morali, sociali e organizzative

Si tratta di un sistema di gestione che permette ad un'organizzazione di dimostrare il proprio impegno a conformarsi a leggi, requisiti regolamentari, codici di settore e specifiche organizzative, così come a norme di buona *governance*, generalmente accettate come migliori prassi, alle aspettative in termini etici e della comunità.

L'approccio dell'organizzazione in riferimento alla *compliance* è determinato dalla *leadership* che applica i valori fondamentali, e dagli standard generalmente accettati riguardanti la buona *governance*, l'etica e la comunità. Incorporare la *compliance* nel comportamento delle persone che lavorano per l'organizzazione dipende soprattutto dalla *leadership*, a tutti i livelli, e dai chiari valori di un'organizzazione, così come dal riconoscimento e dall'attuazione di misure per promuovere un comportamento conforme.

Se questo non si riscontra a tutti i livelli dell'organizzazione, c'è il rischio di *non compliance*.

Come indicato nell'introduzione della ISO 37301, **le organizzazioni che ambiscono ad avere successo** nel lungo periodo necessitano di stabilire e mantenere **una cultura della *compliance***, che consideri le esigenze ed aspettative delle parti interessate. La *compliance* è pertanto non solo la base, ma anche un'opportunità, per un'organizzazione di successo e sostenibile. Si tratta quindi di un processo su base continuativa che deve essere incorporato nella cultura dell'organizzazione, nei comportamenti e nelle attitudini delle persone che lavorano al suo interno.

Sono aspetti che sono richiamati anche nel Codice Etico adottato dalla Società.

Pur mantenendo la propria indipendenza, è preferibile che la gestione per la *compliance* venga integrata con gli altri processi gestionali dell'organizzazione e con i requisiti e le procedure operative, come il Modello di Organizzazione, Gestione e Controllo ex D.Lgs. 231/2001.

Le organizzazioni sono sempre più convinte, applicando valori vincolanti e un'appropriata gestione per la *compliance*, di poter salvaguardare la loro integrità ed evitare o minimizzare il mancato rispetto dei propri obblighi di *compliance*. L'integrità e un'efficace *compliance* sono pertanto elementi chiave di una buona e competente gestione.

La *compliance* contribuisce altresì al comportamento socialmente responsabile dell'organizzazione, comportando numerosi **benefici** per la stessa:

A) **incremento delle opportunità di business e di sostenibilità**

B) protezione e **accrescimento della reputazione** e della credibilità dell'organizzazione

C) **considerazione delle aspettative delle parti interessate**

D) **dimostrazione dell'impegno** dell'organizzazione **nel gestire i propri rischi** relativi alla *compliance* in modo efficace ed efficiente

E) **aumento della fiducia di terze parti** nella capacità dell'organizzazione di conseguire il successo durevole (*sustained success*)

F) **minimizzazione dei rischi di violazione** che comportano conseguenti costi e danni alla reputazione

Concludendo, il valore aggiunto di un sistema di gestione certificato secondo la ISO 37301:2021 rappresenta una *best practice* a livello internazionale, perché aumenta la fiducia degli stakeholders verso l'azienda che così incentiva i suoi affari e protegge la sua reputazione. Tale sistema è poi pienamente integrabile con i sistemi di gestione Qualità, Sicurezza, Ambiente od altri eventuali schemi certificabili.

2.5. La UNI 11961:2024 "*Linee Guida per relazione tra ISO 37301:2021 e MOG*"

Nella predisposizione e redazione del presente Modello di Organizzazione e Controllo ex D.Lgs. 231/2001 si è provveduto a tenere in considerazione altresì il contenuto della norma UNI 11961:2024, pubblicata il 17 dicembre 2024, che definisce le linee guida per mettere in relazione il sistema di gestione per la compliance UNI ISO 37301:2021 e i Modelli di Organizzazione, Gestione e Controllo conformi al D.lgs. 231/2001 per agevolare le società nello sviluppo di modelli efficaci sulla base dei principi e requisititi espressi dalle norme tecniche nazionali ed internazionali UNI ISO.

Si tratta di una norma che ha messo a confronto il D.lgs. 231/201, le Linee Guida Confindustriale e la norma UNI ISO 37301:2021, con l'obiettivo di armonizzare e integrare i sistemi di gestione della compliance con il MOG, proponendo anche un metodo pratico per attuarla.

Tra i principali aspetti di integrazione individuati dalla norma vi è proprio un approccio basato sul rischio in relazione al contesto organizzativo: in effetti, sia la UNI ISO 37301:2021 che il D.lgs.

231/2001 richiedono una valutazione del rischio di non conformità.

Questa norma rappresenta un passo significativo verso la creazione di un sistema integrato che collega i reati contemplati nel "catalogo 231" con la norma ISO 37301, la quale richiede un approccio sistemico al rispetto di tutti gli obblighi legislativi cui un'azienda è sottoposta. L'integrazione proposta permette alle aziende di dimostrare l'adeguatezza ed efficacia dei propri modelli, basandosi non solo su parti generali e speciali, ma anche su procedure realizzate e monitorate nell'ambito del sistema di gestione ISO.

Implementare un Sistema di Gestione per la Compliance conforme alla UNI ISO 37301:2021, integrato con il Modello 231 secondo le linee guida della UNI 11961:2024, può rafforzare la posizione dell'azienda in sede processuale, dimostrando l'efficacia delle misure adottate per prevenire reati e garantire la conformità normativa.

2.6. Riferimenti normativi e legislativi

In conclusione, il presente Modello di Organizzazione, Gestione e Controllo rimanda ai riferimenti normativi e legislativi di seguito elencati:

D.lgs. 231/2001	Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'articolo 11 della legge 29 settembre 2000, n. 300
Linee guida UNI INAIL	emanate da INAIL nel 2001
Linee guida per la costruzione dei modelli di organizzazione, gestione e controllo	emanate da Confindustria nel giugno 2021
Criteri guida per la redazione di codici di comportamento delle associazioni rappresentative degli enti	emanate dal Ministero della Giustizia nel febbraio 2025;
UNI ISO 37301:2021	Sistemi di gestione per la compliance
UNI 11961:2024	Linee guida per l'integrazione del sistema di gestione per la compliance UNI ISO 37301:2021 a supporto dei modelli Organizzativi di Gestione e Controllo e degli Organismi di Vigilanza in conformità al D.lgs. 231/2001.
UNI ISO 31008:2018	Gestione del Rischio
UNI EN ISO 9001:2015	Sistemi di gestione per la qualità
UNI EN ISO 14001:2015	Sistemi di gestione ambientale
UNI ISO 45001:2018	Sistemi di gestione per la salute e sicurezza sul lavoro

SEZIONE SECONDA
ADOZIONE DEL MODELLO ORGANIZZATIVO

1. FASE DI IDENTIFICAZIONE DEI RISCHI (ANALISI DEL CONTESTO AZIENDALE)

1.1. La Storia della Società

Valuecube S.r.l., con sede a Siena, affonda le proprie radici nei primi anni 2000, pur derivando da un progetto avviato già nel decennio precedente. L'esperienza fondativa nasce infatti negli anni '90 all'interno di una realtà differente, ma caratterizzata dallo stesso nucleo di competenze, visione e risorse professionali.

La svolta organizzativa decisiva si è concretizzata circa dieci anni fa, con il trasferimento dell'intera operatività nella nuova struttura attuale. Questo passaggio ha consentito di mantenere la continuità tecnica, introducendo al contempo un modello più moderno, flessibile e orientato all'innovazione.

I primi progetti sviluppati da Valuecube si sono basati su prodotti e soluzioni già consolidati nella precedente configurazione societaria. Tuttavia, è stato con l'introduzione delle normative di Basilea e con l'incremento della complessità regolamentare nel settore bancario e finanziario che l'azienda ha colto un'importante opportunità di crescita, specializzandosi progressivamente in ambiti quali la gestione del rischio, la compliance e l'adeguamento normativo.

Negli ultimi anni, una nuova direttrice strategica ha guidato l'evoluzione dell'offerta: la crescente attenzione al rischio climatico e ambientale. Da questa prospettiva è nata una linea di prodotti ad alto contenuto specialistico, progettati per valutare gli impatti fisici e finanziari dei cambiamenti climatici e delle transizioni energetiche. Tali soluzioni rappresentano oggi una componente centrale del portafoglio aziendale.

1.2. Descrizione del *business* e della struttura aziendale

Valuecube s.r.l. si occupa dello sviluppo di applicazioni software di nuova concezione destinate al mondo creditizio e della finanza, rispondenti ai più avanzati standard metodologici e tecnologici.

Fornisce inoltre servizi di consulenza e formazione nell'ambito del risk management, banking regulation, corporate finance e portfolio management.

La società è organizzata in modo dinamico e trasversale. I progetti nascono quasi sempre da un confronto tra il team funzionale, che si relaziona direttamente con il cliente, e la parte tecnica. Infatti, da un punto di vista organizzativo, la Società è suddivisa in due aree di intervento: la prima è la c.d. "Area Fin", che si occupa di interfacciarsi con i clienti; la seconda, la c.d. "Area IT" si occupa invece,

di concerto con l'Area Fin e nel rispetto di quanto pattuito con cliente, di progettare il software o la banca dati commissionata. L'esigenza del cliente, analizzata da una specifica figura di riferimento nonché dal team tecnico, viene trasformata in un progetto concreto per il quale viene definita la tecnologia da usare, viene strutturato ed organizzato il lavoro così come pianificati i tempi di realizzazione. Avviata la produzione del progetto, il responsabile dello stesso gestisce le evoluzioni successive, le manutenzioni, gli aggiornamenti normativi, e tutti gli avanzamenti.

Dal punto di vista tecnico, la società si avvale della più moderna e aggiornata platform engineering, che consente di garantire un alto standard qualitativo per ogni progetto realizzato.

Il mercato principale di riferimento è quello finanziario e bancario. La società lavora da anni con grandi realtà italiane, tra cui anche clienti istituzionali. Non partecipa spesso a bandi pubblici, ma ha avuto esperienze anche in quel contesto (es. Banca d'Italia, Mediocredito Centrale).

La società partecipa regolarmente a convegni e seminari, in particolare quelli dell'ABI, dove presenta i suoi prodotti e soluzioni. Il rapporto con il mondo accademico è portato avanti direttamente da alcuni soci, che insegnano in Università e curano corsi legati al mondo della finanza e della gestione del rischio ambientale.

1.3. Descrizione dell'organizzazione societaria

Valuecube S.r.l. è una società di diritto italiano con una governance affidata a un Amministratore Unico, responsabile del coordinamento delle diverse funzioni aziendali e punto di raccordo strategico per le attività svolte dalle varie aree operative.

L'organigramma si caratterizza per una struttura snella ma ben delineata. Al vertice si colloca l'Amministratore Unico, il quale, oltre alle funzioni di indirizzo strategico, è direttamente coinvolto nella ricerca e sviluppo, nonché nell'ideazione di nuovi prodotti e soluzioni. Accanto a questa figura opera un Partner CEO, cui è affidata la gestione generale e l'organizzazione operativa della società.

La struttura è supportata da una rete di referenti funzionali, ciascuno responsabile di specifiche aree: Finanza (FIN), Information Technology (IT), Area Commerciale, Sicurezza Informatica, Qualità e Amministrazione. Il confronto tra i responsabili di funzione avviene con regolarità, privilegiando modalità snelle e informali che si sono dimostrate particolarmente efficaci. Inoltre, per garantire la conformità alle certificazioni ISO, l'azienda organizza incontri periodici volti all'analisi dei requisiti normativi e alla definizione di piani operativi coerenti.

Dal punto di vista tecnico, la figura del Chief Technology Officer (CTO) riveste un ruolo centrale: è coinvolto in tutte le fasi dei progetti, dalla progettazione all'implementazione, e interviene anche nella gestione di eventuali criticità. Il CTO partecipa inoltre ai colloqui tecnici per la selezione di nuove risorse e cura la supervisione delle procedure interne.

1.3.1. Organo Dirigente e Alta Direzione

L'Amministratore Unico, quale "Organismo di Governo" o "Organo Dirigente" ex art. 6 del D.Lgs 231/2001 svolge quindi un ruolo centrale nella guida strategica dell'azienda. Egli, inoltre, assieme al Partner CEO e al Head Advisory & Sales Manager fa parte altresì dell' "Alta Direzione", intesa quale gruppo di persone che a livello più elevato guida e tiene sotto controllo l'organizzazione e dimostra **leadership e impegno**:

- ✓ assicurando che siano stabiliti la politica e gli obiettivi per la compliance e che essi siano compatibili con gli indirizzi strategici dell'organizzazione;
- ✓ assicurando l'integrazione dei requisiti del sistema di gestione per la compliance nei processi di business dell'organizzazione;
- ✓ assicurando la disponibilità delle risorse necessarie al sistema di gestione per la compliance;
- ✓ comunicando l'importanza di una gestione per la compliance efficace, e della conformità ai requisiti del sistema di gestione per la compliance;
- ✓ assicurando che il sistema di gestione per la compliance consegua gli esiti attesi;
- ✓ guidando e supportando le persone affinché contribuiscano all'efficacia del sistema di gestione per la compliance;
- ✓ promuovendo il miglioramento continuo;
- ✓ fornendo supporto agli altri pertinenti ruoli gestionali per dimostrare la loro leadership, come essa si applica alle rispettive aree di responsabilità.

L'organismo di governo e l'alta direzione devono inoltre:

- ✓ stabilire e tener saldi i valori dell'organizzazione;
- ✓ assicurare che politiche, processi e procedure siano sviluppate e attuate per conseguire gli obiettivi per la compliance;
- ✓ assicurare che essi siano tenuti informati in modo tempestivo circa questioni riguardanti la compliance, compresi i casi di non compliance e assicurare che siano prese azioni appropriate;
- ✓ assicurare che sia mantenuto l'impegno verso la compliance e che le non compliance e relativi comportamenti siano trattati in modo appropriato;
- ✓ assicurare che le responsabilità relative alla compliance siano comprese nei mansionari, per quanto appropriato;
- ✓ designare o nominare una funzione di compliance;
- ✓ assicurare che sia definito un sistema per far emergere e trattare le preoccupazioni, riguardante il sistema di segnalazioni;
- ✓ rimettere in via esclusiva il compito (e la responsabilità) di promuovere l'adozione e l'efficace attuazione del Modello, così come – seppure solo implicitamente – di nominare l'Organismo di Vigilanza.

1.3.2. Il Management

All'interno dell'organizzazione è determinante poter individuare le figure responsabili della gestione di ogni specifico processo aziendale (process owner). Questi hanno il compito di:

- ✓ cooperare e supportare la funzione di compliance e l'incoraggiamento del personale a fare

altrettanto;

- ✓ assicurare che il personale sotto il proprio controllo sia conforme agli obblighi, politiche, processi e procedure di compliance dell'organizzazione;
- ✓ identificare e comunicare i rischi di compliance nelle proprie attività operative;
- ✓ integrare gli obblighi di compliance nelle prassi e procedure di business esistenti nell'ambito delle proprie aree di responsabilità;
- ✓ partecipare e supportare le attività di formazione in materia di compliance;
- ✓ sviluppare consapevolezza, da parte del personale, circa gli obblighi di compliance, indirizzando le persone a soddisfare i requisiti di formazione e competenza;
- ✓ incoraggiare il proprio personale a far emergere preoccupazioni relative alla compliance, supportandolo e impedendo ogni forma di ritorsione;
- ✓ partecipare attivamente alla gestione e risoluzione di incidenti e questioni correlati alla compliance, come richiesto;
- ✓ assicurare che, una volta sia stata identificata l'esigenza di azioni correttive, quest'ultime siano raccomandate e attuate".

1.3.3. La cultura della compliance e della legalità

In particolare, **l'organo dirigente, l'alta direzione e il management devono dimostrare** un **impegno** attivo, visibile, coerente e sostenuto **circa uno standard di comportamento e condotta** comuni che viene richiesto all'interno dell'organizzazione, **favorendo la c.d. "cultura della compliance"**, intesa come l'insieme di principi comportamentali volti ad assicurare che le attività aziendali siano svolte in conformità alle leggi e alle procedure adottate in seno all'organizzazione, che si sviluppa mediante:

A) L'adozione di un Codice Etico

B) L'attività di formazione e informazione

C) La costituzione di flussi informativi nei confronti dell'Organismo di Vigilanza

D) La creazione di un canale di segnalazione (whistleblowing)

E) Adozione di un chiaro sistema disciplinare

1.3.4. Il personale

Anche **il personale dipendente è coinvolto** nella fase di concreta attuazione del modello organizzativo. Secondo le linee guida di Confindustria, così come esplicitato dalla UNI 37301:2021, infatti, il personale è chiamato a:

- ✓ **aderire agli obblighi, politiche, processi e procedure**
- ✓ **riferire preoccupazioni, questioni e malfunzionamenti**
- ✓ **partecipare alla formazione**

1.3.5. Ruoli, responsabilità e autorità

Il sistema organizzativo di Valuecube s.r.l. si fonda su una chiara e formalizzata attribuzione di responsabilità, con individuazione di linee di dipendenza gerarchica, descrizione dei compiti, specifica previsione di principi di controllo anche della copertura temporale degli incarichi. L'attribuzione di compiti e responsabilità, funzione per funzione, viene riassunta nell'Organigramma Aziendale.

L'organigramma aziendale, aggiornato all'ultima versione, costituisce parte integrante del presente Modello ed è allegato allo stesso.

La modifica o l'aggiornamento dell'organigramma dovranno essere l'occasione per adeguare il Modello di Organizzazione, Gestione e Controllo alle esigenze di semplificazione delle procedure, fondando le stesse sul sistema delle deleghe da adottare in modo formale, seguendo le indicazioni della costante giurisprudenza della Corte di Cassazione e del d.lgs. 81/2008.

Deleghe e attribuzioni di funzioni

Stante la non complessità dell'organizzazione aziendale, la Società ha valutato l'opportunità di non adottare lo strumento della **delega di funzioni**, che consiste nel trasferimento di compiti amministrativi, gestionali ed esecutivi dal loro destinatario *ex lege* a terzi. L'istituto, nato per via giurisprudenziale, ha in seguito trovato un importante riconoscimento legislativo nell'art. 16 del d.lgs. 19 aprile 2008, n. 81, il Testo unico in materia di salute e sicurezza sul lavoro. Si tratta di una disposizione che, sebbene deputata a regolamentare la delega di funzioni nel settore dell'antinfortunistica sui luoghi di lavoro, nondimeno esprime regole e principi generali esportabili anche in altri settori del diritto penale, tanto da rappresentare una vera e propria norma di sistema.

Nello specifico, l'art. 16 d.lgs. 81/2008, circa i **requisiti di validità della delega**, richiede che:

- ✓ la delega risulti da atto scritto;
- ✓ il delegato possegga i requisiti di professionalità ed esperienza;
- ✓ al delegato vengano attribuiti poteri di organizzazione, gestione e controllo;
- ✓ al delegato venga attribuita "autonomia di spesa necessaria allo svolgimento delle funzioni";
- ✓ la delega venga accettata per iscritto;
- ✓ alla delega sia attribuita adeguata e tempestiva pubblicità.

Inoltre, ai sensi del comma 3 della disposizione, si precisa che permane in capo al delegante **l'obbligo di vigilanza** "in ordine al corretto espletamento da parte del delegato delle funzioni trasferite". Il D.Lgs. 106/2009 ha quindi introdotto una **presunzione legale** di adempimento dell'obbligo di vigilanza, "che si intende assolto in caso di adozione ed efficace attuazione del modello di verifica e controllo di cui all'art. 30, comma 4".

Al fine di ripartire in modo coerente e funzionale l'attribuzione di compiti e responsabilità in azienda occorre chiarire anche da un punto di vista definitorio la differenza tra:

Delega di funzioni (o procura): corrisponde ad una transizione di specifici doveri/poteri aventi rilevanza in sede penale e civile, unitamente ai poteri ed agli strumenti effettivi per adempiere alle attività delegate. Tali disposizioni possono essere formalizzate con atti notarili ma anche con atti che ricevano però adeguata pubblicità (ad esempio con pubblicazione nel Registro delle Imprese), tale da garantire l'opponibilità ai terzi dell'oggetto della delega.

Attribuzione di funzioni: Il termine "delega" può essere utilizzato in senso meno tecnico intendo esprimere una mera attribuzione di funzioni, incarico o poteri all'interno dell'organizzazione. Si tratta di un atto interno che può essere reso operativo tramite determine dell'A.U., approvazione di manuali, procedure o mansionari.

Valuecube s.r.l. assegna poteri autorizzativi e di firma in coerenza con le responsabilità organizzative e gestionali, così come sopra delineate ed individuate.

In ragione della propria struttura complessa la società intende consentire l'attribuzione di deleghe funzionali e poteri a singoli soggetti dotati di idonei requisiti di professionalità e di esperienza richiesti dalla specifica natura della funzione delegata.

Con il conferimento della delega sono conferiti al delegato al fine di adempiere ai poteri e alle mansioni attribuite:

- ✓ tutti i necessari poteri di organizzazione, gestione e controllo necessari e sufficienti, incluso il potere di utilizzo diretto, in piena autonomia e senza alcuna limitazione, delle somme stabilite dal budget annuale;
- ✓ il potere di avvalersi di ogni consulenza (sia di natura tecnica, che legale) per il migliore espletamento dei compiti e delle mansioni che gli sono state affidate;
- ✓ il potere di sub-delegare a soggetti ritenuti idonei e qualificati, gli adempimenti, le funzioni, le attività, le competenze e le relative responsabilità agli stessi conferite, sia tutte che in parte, ma comunque nei limiti posti dalla vigente normativa, conferendo a tali terzi tutti i poteri occorrenti;
- ✓ il potere di stipulare, modificare ed estinguere i contratti di acquisto di beni o servizi, necessari per lo svolgimento delle attività connesse alle predette funzioni delegate.

Inoltre, è opportuno che l'attribuzione delle deleghe e dei poteri di firma relativi alla gestione delle risorse finanziarie e all'assunzione e attuazione delle decisioni della società in relazione ad attività a rischio reato:

- ✓ sia formalizzata in conformità alle disposizioni di legge applicabili;

- ✓ indichi con chiarezza i soggetti delegati, le competenze richieste ai destinatari della delega e i poteri rispettivamente assegnati;
- ✓ preveda eventuali limitazioni delle deleghe e dei poteri di spesa conferiti;
- ✓ preveda soluzioni dirette a consentire un controllo sull'esercizio dei poteri delegati;
- ✓ sia disposta in coerenza con il principio di segregazione;
- ✓ sia coerente con i regolamenti aziendali e con le altre disposizioni interne applicati dalla società.

Individuazione di compiti e responsabilità

La società ritiene importante prevedere **un sistema coerente e integrato che comprenda tutte le deleghe o procure aziendali** (comprese quelle in materia antinfortunistica ed ambientale), periodicamente aggiornate alla luce sia delle modifiche normative, che delle eventuali variazioni nel sistema organizzativo. Ciò rappresenta un concreto passo operativo per la realizzazione di un sistema di gestione del rischio, in grado di creare:

- ✓ efficienza operativa, con articolazione delle responsabilità in coerenza con gli obiettivi aziendali;
- ✓ efficacia del processo decisionale, con allineamento nel tempo dei poteri attribuiti alla relativa responsabilità e posizione nell'organigramma;
- ✓ coerenza del sistema di attribuzione dei poteri, con conferimento di procura ai soggetti dotati di delega funzionale interna;
- ✓ chiarezza verso terzi e tutela della Società, con individuazione formale dei poteri attributi ai soggetti che possono assumere, in nome e per conto della Società stessa, obbligazioni verso terzi

A tal fine il sistema deve prevedere deleghe formalizzate in conformità alle disposizioni di legge applicabili con una chiara esplicitazione dei poteri assegnati, delle eventuali limitazioni di potere, dell'applicazione di sanzioni in caso di violazioni dei poteri delegati, del rispetto del principio di segregazione delle funzioni e dei ruoli, della coerenza con i regolamenti aziendali e con altre disposizioni interne applicate dalla società, comprese quelle in materia antinfortunistica ed ambientale, del periodico aggiornamento in funzione dei cambiamenti organizzativi, della documentabilità del sistema stesso delle deleghe (opponibile a terzi e che garantisca un'eventuale ricostruzione a posteriori.

Il sistema si completa con una matrice di attribuzione di deleghe e poteri, seguendo il modello di schematizzazione sotto riportato **(Allegato 2 – Matrice di attribuzione di deleghe e poteri).**

RUOLO E INQUADRAMENTO	SCOPO DELLA POSIZIONE	PRINCIPALI ATTIVITÀ	PRESIDIO RISCHI E COMPLIANCE	MODALITÀ DI FORMALIZZAZIONE DELLE RESPONSABILITÀ
INDICAZIONE DEL RUOLO E DELL'INQUADRAMENTO e INDICAZIONE DEI NOMINATIVI DEI RESPONSABILI	Descrizione dello scopo della posizione	Descrizione delle attività svolte	Rilevanza nella mappatura dei processi sensibili *Attuazione operativa delle procedure* *Ruolo dei flussi informativi verso l'ODV* *Contributo alla cultura della compliance* *Rilevanza rispetto alle attività di controllo* *Rilevanza rispetto alla formazione 231*	✓ Organigramma; ✓ Delega di funzione; ✓ Mansionario; ✓ Contratto; ✓ Nomina Datore Lavoro.

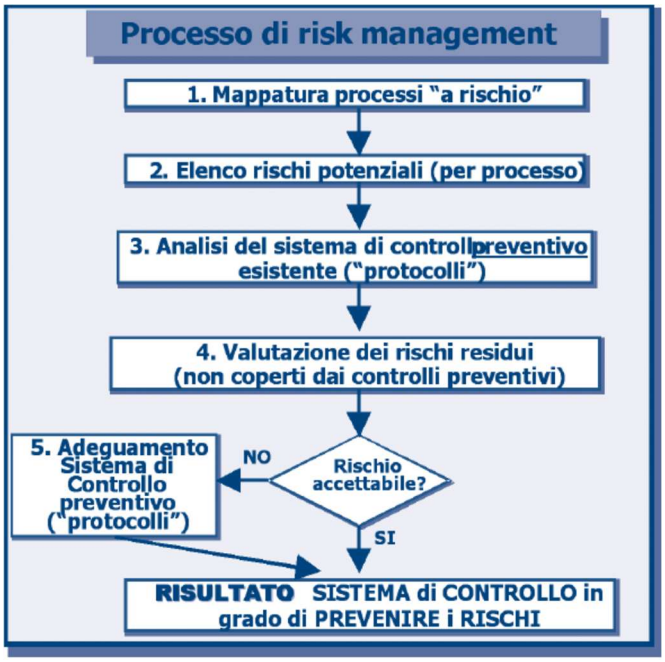
1.4. Analisi del rischio (*risk assessment*)

Le Linee Guida di Confindustria 2021 hanno precisato le fasi principali in cui il sistema di prevenzione dei rischi 231 dovrebbe articolarsi nel corso del *risk assessment*, ovvero:

a) **l'identificazione dei rischi potenziali**: ossia l'analisi del contesto aziendale per individuare in quali aree o settori di attività e secondo quali modalità si potrebbero astrattamente verificare eventi pregiudizievoli per gli obiettivi indicati dal decreto 231. Tale attività deve tradursi in un processo continuo o comunque svolto con periodicità adeguata, da rivedere con attenzione rispetto a cambiamenti aziendali o introduzione di nuovi reati presupposto.

b) **la valutazione del sistema di controllo in essere all'interno della società per la prevenzione dei reati** ed il suo eventuale adeguamento, in termini di capacità di contrastare efficacemente, cioè, ridurre ad un livello accettabile, i rischi identificati.

Nelle linee guida tale processo è stato esemplificato nel seguente grafico:



Rif. Pag. 40 Linee Guida Confindustria 2021

Nell'ambito dell'attività svolta, come prassi metodologica scelta, in ossequio anche alle indicazioni fornite dal Ministero della Giustizia con il documento "*Criteri guida per la redazione di codici di comportamento delle associazioni rappresentative degli Enti*" pubblicato nel febbraio 2025, si è preferito adottare una metodologia per la costruzione della parte speciale del modello e quindi anche per la fase di analisi del rischio, basata sui singoli processi, per correlare ad essi, le fattispecie presupposto rilevanti.

Anche in giurisprudenza sono stati analizzate e descritte le attività di analisi del rischio. In particolare, il Tribunale di Milano, con la sentenza n. 1070 del 22 aprile 2024 ha specificato sul punto che: "*La configurazione delle attività a rischio-reato, denominata anche "mappatura del rischio" (risk assessment), consiste in una fase cognitivo-rappresentativa funzionale alla percezione del rischio reato ed alla valutazione del suo grado di intensità. Infatti, come nel diritto penale individuale, sia il coefficiente psicologico che quello della colpa presuppongono che l'agente si sia rappresentato il rischio derivante dalla sua condotta attraverso le conoscenze disponibili in quel momento, allo stesso modo l'ente collettivo è chiamato a fare una ricognizione a tappeto dei fattori di rischio, il che risulta un'attività sicuramente più complicata rispetto a quanto avvenga nell'agile individuale, dal momento che ancora una volta si richiede un efficace metodo organizzativo di rilevamento e di valutazione.* ***La mappatura, pertanto, dovrà snodarsi attraverso un procedimento contraddistinto da: a) individuazione delle aree potenzialmente a rischio-reato con particolare riguardo alle aree c.d. strumentali, ovvero quelle che gestiscono strumenti finanziari, destinati a supportare la commissione dei reati stessi; b) rilevazione dei processi sensibili dai quali potrebbero derivare le ipotesi di reato perseguibili, il che significa selezionare le attività al cui espletamento è connesso il rischio di commissione di***

reati, indicando le direzioni ed i ruoli aziendali coinvolti; c) rilevazione e valutazione del grado di efficacia dei sistemi operativi e di controllo già in essere, allo scopo di reperire i punti di criticità rispetto alla prevenzione del rischio-reato; d) descrizione delle possibili modalità di commissione dei reati, allo scopo di forgiare le indispensabili 'cautele' preventive. *Sotto questo profilo particolarmente importante è un'attenta analisi dell'evoluzione dell'organigramma aziendale, che consiste nell'appurare, diacronicamente, gli eventuali mutamenti organizzativi intervenuti nel tessuto aziendale, allo scopo di verificare se siano stati indotti da disfunzioni operative o da violazioni comportamentali, che hanno reso un pregiudizio, anche solo potenziale all'ente. In altre parole, si tratta di verificare l'adeguatezza nel tempo del protocollo e la sua idoneità a conformarsi ai mutamenti strutturali avvenuti all'interno della società."*

È stato quindi analizzato tutto il sistema aziendale, comprendendo così anche i processi per i quali non sussiste il rischio di sanzioni ai sensi del D.Lgs. 231/2001, al fine di costruire un sistema di gestione di più ampia portata rispetto alle prescrizioni della normativa sulla responsabilità amministrativa degli enti.

In termini generali le aziende sviluppano il proprio *business* attivando tre processi principali, che a loro volta funzionano grazie all'utilizzo di alcune risorse, per la gestione delle quali è necessario attivare processi interni organizzativi, come di seguito riportato:

Processi Principali	Risorse Utilizzate	Processi Interni
✓ **il processo di acquisto** di beni e servizi per la produzione (ciclo passivo); ✓ **il processo di produzione** del bene e/o servizio (ovvero il ciclo produttivo); ✓ **il processo di vendita** del bene e/o del servizio (ovvero il ciclo attivo).	✓ beni strumentali materiali e immateriali; ✓ risorse umane; ✓ risorse finanziarie.	✓ la gestione amministrativa; ✓ la gestione finanziaria; ✓ la gestione del personale; ✓ la gestione dell'IT.

Partendo da tali premesse, **è stato studiato il funzionamento dell'organizzazione aziendale di Valuecube s.r.l.** al fine di cogliere nell'ambito di ogni processo lavorativo, **le aree e le attività a rischio ai sensi del D.Lgs. 231/2001**, nonché anche ai fini di una più ampia *compliance* aziendale, meglio descritte nella "parte speciale" del Modello di Organizzazione, Gestione e Controllo.

1.5. Valutazione dei rischi

Per lo svolgimento dell'attività di valutazione dei rischi si è provveduto ad utilizzare i seguenti criteri di classificazione del rischio di commissione dei reati rilevanti ai sensi del D.Lgs. 231/2001:

ALTAMENTE RILEVANTE	✓ Sono noti episodi in cui la commissione del reato ha causato un danno e/o ✓ Il pericolo esiste e può trasformarsi in un danno con una correlazione diretta e/o ✓ Il verificarsi dell'evento non susciterebbe sorpresa/incredulità in azienda e/o ✓ Vi è un elevato livello di rischio di impatto che l'impresa deve gestire e governare e/o ✓ Esiste una correlazione diretta tra il pericolo ed il verificarsi del danno ipotizzato e/o ✓ Si sono già verificati danni per la stessa mancanza rilevata nella stessa azienda o in aziende simili.
POTENZIALMENTE RILEVANTE	✓ Non sono noti episodi già verificati e/o ✓ L'evento può verificarsi solo in circostanze particolari e/o ✓ Il verificarsi dell'evento susciterebbe sorpresa in azienda e/o ✓ Vi è un trascurabile livello di rischio di impatto e/o ✓ Il pericolo può provocare un danno solo in circostanze sfortunate e/o ✓ Non si sono ancora verificati danni per la stessa mancanza rilevata nella stessa azienda o in aziende simili.
SCARSAMENTE RILEVANTE	✓ Il reato previsto è difficilmente compatibile con l'attività svolta dalla Società e/o ✓ L'evento si può verificare solo per una concatenazione di eventi improbabili e tra loro indipendenti e/o ✓ Vi è un rischio a livello di assenza di probabilità e perciò accettabili anche in assenza di azioni correttive e/o ✓ La mancanza rilevata può provocare un danno per la concomitanza di più eventi poco probabili e indipendenti e/o ✓ Non sono noti eventi o episodi già verificatisi.
NON APPLICABILE	✓ Qualora, per le caratteristiche della società, non vi siano i presupposti per la sua realizzazione.

Inoltre, al fine di una corretta valutazione, è opportuno tenere in considerazione le seguenti variabili:

- ✓ **Probabilità di accadimento:** determinata sulla base della frequenza storica, procedure interne e controlli esistenti.
- ✓ **Impatto potenziale:** considerato in termini di sanzioni amministrative e penali, danni reputazionali e finanziari.

1.6. La matrice del rischio di commissione dei reati

All'esito di un'approfondita analisi dei dati forniti (organigramma, DVR, contratti, precedenti giudiziari, procedure attualmente adottate, etc.) e sulla base di quanto emerso dalle interviste realizzate per redigere il Modello di Organizzazione, Controllo e Gestione ai sensi del d.lgs. 231/2001 al personale della società, è stato possibile suddividere l'attività svolta specificando per ciascun settore il rischio di commissione dei reati presupposto di cui al d.lgs. 231/2001.

L'analisi del rischio è quindi contenuta nel documento "Matrice del rischio" **(Allegato 3 – Matrice del rischio)**, parte integrante del Modello di Organizzazione e Controllo ex D.Lgs. 231/2001, che tiene conto per ogni area di rischio delle seguenti voci:

INDIVIDUAZIONE DEL RISCHIO				ATTIVITÀ DI MITIGAZIONE DEL RISCHIO					ESITO
AREA SENSIBILE	*DESCRIZIONE DEL RISCHIO*	*RIF. 231 e REATO*	*ESEMPI DI CONDOTTE*	*SEGREGAZION E DEI COMPITI*	*DELEGHE E POTERI*	*TRACCIABILITÀ*	*CERTIFICAZIONI E PROCEDURE SGI - ALTRI PROTOCOLLI*	*PROCEDURE SPECIFICHE EX DLGS 231*	*VALUTAZIO NE DEL RISCHIO*

Si tratta di un documento che deve essere sottoposto a riesame periodico, con aggiornamento della mappatura dei rischi e delle relative procedure preventive.

2. FASE DI PROGETTAZIONE DEL SISTEMA DI CONTROLLO

2.1. Gli strumenti di governance della società

I principali strumenti di governance di cui la società si è dotata possono essere così riassunti:

- ✓ lo Statuto di Valuecube s.r.l. che, oltre a descrivere l'attività svolta dalla società, contempla diverse previsioni relative alla gestione della medesima;
- ✓ l'organigramma e il mansionario aziendale che descrivono compiutamente le funzioni, i compiti ed i rapporti gerarchici esistenti nell'ambito della Società;
- ✓ l'individuazione della figura datoriale con tutti i più ampi poteri e con ampia autonomia finanziaria;
- ✓ le procedure aziendali che regolamentano i principali processi di business e, comunque, tutte le attività ritenute sensibili per l'applicabilità del d.lgs. 231/01;
- ✓ la documentazione aziendale relativa al sistema di gestione della salute e sicurezza sul lavoro;

L'insieme degli strumenti di *governance* adottati (qui sopra richiamati in estrema sintesi), del Codice Etico e delle previsioni del presente Modello consente di individuare, rispetto a tutte le attività, come siano formate e attuate le decisioni della società (cfr. art. 6, comma 2 lett. b, d.lgs. 231/01).

2.2. Il Codice etico

Valuecube s.r.l. intende operare secondo principi etici e regole di comportamento dirette ad improntare lo svolgimento dell'attività aziendale, il perseguimento dello scopo sociale e la sua crescita al rispetto delle leggi e regolamenti vigenti in Italia e tutti i Paesi in cui opera.

A tale fine, la Società ha adottato un Codice Etico volto a definire una serie di principi di "deontologia aziendale" e di regole comportamentali, che la società riconosce come proprie e delle quali esige l'osservanza sia da parte dei propri organi sociali e dipendenti, sia da parte di tutti coloro che cooperano con essa nel perseguimento degli obiettivi di business.

Il Codice Etico ha, pertanto, una portata di carattere generale e rappresenta un insieme di regole e principi, adottati spontaneamente da Valuecube s.r.l., che la stessa riconosce, accetta e condivide, diretti a diffondere una solida integrità etica e una forte sensibilità al rispetto delle normative vigenti.

Esso contiene l'insieme dei diritti, dei doveri e delle responsabilità della società nei confronti dei "portatori d'interesse" (dipendenti, fornitori, clienti, Pubblica Amministrazione, azionisti, mercato finanziario, ecc.).

In considerazione del fatto che il Codice Etico richiama principi di comportamento (tra cui, legalità, correttezza e trasparenza) idonei anche a prevenire i comportamenti illeciti di cui al D.Lgs. 231/2001, tale documento acquisisce rilevanza ai fini del Modello e costituisce, pertanto, un elemento complementare allo stesso.

Il Modello risponde, invece, a specifiche prescrizioni contenute nel D.Lgs. 231/2001, finalizzate espressamente a prevenire la commissione delle tipologie di reati previste dal decreto medesimo (per fatti che, apparentemente commessi nell'interesse o a vantaggio della Società, possono far sorgere a carico della stessa una responsabilità amministrativa da reato).

I principi e le regole contenuti nel presente Modello sono quindi coerenti con quelli previsti dal Codice Etico di Valuecube s.r.l. adottato in ottemperanza al d.lgs. 231/01.

Il Codice Etico, adottato dagli organi sociali competenti, reso noto a tutto il personale e pubblicato sul sito *web* aziendale esprime i principi etici e di deontologia che la Società riconosce come propri e sui quali richiama l'osservanza da parte di tutti coloro che operano per il conseguimento degli obiettivi della Società.

2.3. Il Modello Organizzativo adottato dalla società

In ossequio ai principi elaborati anche in giurisprudenza, il Modello di Organizzazione, Gestione e Controllo adottato da Valuecube s.r.l. è stato suddiviso in una Parte Generale e in una Parte Speciale: la prima rivolta ad individuare la fisionomia strutturale del Modello e la seconda indirizzata sia ad individuare le attività maggiormente esposte al rischio reato sia a formalizzare il contenuto delle cautele volte a prevenire il rischio reato attraverso singoli protocolli operativi richiamati nella Parte Speciale del modello.

2.3.1. Parte Generale:

In particolare, la Parte Generale del Modello, oltre a descrivere la configurazione giuridica societaria e i correlati organi di amministrazione e di controllo che la compongono, dando atto di eventuali modificazioni intercorse nel tempo, dovrebbe contenere al suo interno: il codice etico, che costituisce la tavola di valori ai quali la società si ispira; b) le linee dell'attività di informazione e di formazione del Modello e dei protocolli di prevenzione, c) le modalità di scoperta delle violazioni del Modello; d) il sistema disciplinare; e) l'istituzione, la composizione, il funzionamento e gli obiettivi dell'Organismo di Vigilanza, secondo il seguente schema:

Modello di Organizzazione e Controllo ex D.Lgs. 231/2001 **Parte Generale**	
Sezione Prima	**Introduzione alla disciplina del D.Lgs. 231/2001**
Sezione Seconda	**Adozione del modello organizzativo**
	Fase di identificazione dei rischi

	Fase di progettazione del sistema di controllo
Sezione Terza	**Attuazione del modello organizzativo**
	Principi di riferimento
	Documentazione dell'efficace attuazione del modello
Sezione Quarta	**Organismo di Vigilanza**
	Funzione di Controllo
	Flussi informativi
	Il Whistleblowing
Sezione Quinta	**Il sistema sanzionatorio**
Sezione Sesta	**Formazione e informazione**
Sezione Settima	**Adozione e aggiornamento del modello**

2.3.2. Parte Speciale

Il modello si completa poi con una c.d**. "parte speciale",** che è la sede in cui trova attuazione l'attività di mappatura del rischio in relazione alle diverse fattispecie di reato presupposto rilevanti ex lege, e in cui sono riportate le cautele finalizzate alla riduzione del rischio reato. La Parte Speciale del Modello descrive in particolare:

i) i reati presupposto;
ii) le attività e i processi "sensibili" per ciascuna categoria di reato;
iii) le misure di prevenzione dei reati, articolate in principi generali di comportamento e principi procedurali specifici.

Sono state inoltre predisposte specifiche procedure operative, che costituiscono parte integrante della parte speciale del modello.

2.4. Principi di Controllo

Valuecube s.r.l. gestisce i principali processi e le aree di attività a rischio sopra identificate, nel rispetto di principi che appaiono coerenti con le indicazioni fornite dal D.Lgs. 231/2001, garantendone una corretta e concreta applicazione. I principi che regolano le attività in tali aree e processi sono i seguenti:

- ✓ **esistenza di regole comportamentali di carattere generale a presidio delle attività svolte;**
- ✓ **esistenza e adeguatezza di procedure per la regolamentazione dello svolgimento delle attività nel rispetto dei principi di tracciabilità degli atti**, oggettivazione del processo decisionale e previsione di adeguati punti di controllo;
- ✓ **rispetto e attuazione concreta del generale principio di separazione dei compiti.** Il sistema interno aziendale garantisce l'applicazione del principio di separazione di funzioni, per cui l'autorizzazione all'effettuazione di un'operazione deve essere sotto la responsabilità di persona diversa da chi contabilizza, esegue operativamente o controlla l'operazione. Inoltre, è stato previsto che i poteri e le responsabilità siano chiaramente definiti e conosciuti all'interno dell'organizzazione; i poteri autorizzativi e di firma siano coerenti con le responsabilità organizzative assegnate e opportunamente documentati in modo da garantirne, all'occorrenza, un'agevole ricostruzione *ex post*.
- ✓ **esistenza di livelli autorizzativi a garanzia di un adeguato controllo del processo decisionale**, supportato da un sistema di deleghe ed eventuali procure riguardante sia i poteri autorizzativi interni, dai quali dipendono i processi decisionali dell'azienda in merito alle operazioni da porre in essere, sia i poteri di rappresentanza per la firma di atti o documenti destinati all'esterno e idonei a vincolare la Società nei confronti dei terzi (cosiddette "procure" speciali o generali);
- ✓ **esistenza di specifiche attività di controllo e di monitoraggio**, **documentata**. Il sistema di controllo prevede un sistema di *reporting* (attraverso la redazione di verbali) adatto a documentare l'effettuazione e gli esiti dei controlli, anche di supervisione.
- ✓ **verifica documentale.** Per ogni operazione si prevede l'esistenza di un adeguato supporto documentale su cui si possa procedere in ogni momento all'effettuazione di controlli che attestino le caratteristiche e le motivazioni dell'operazione e individuino chi ha autorizzato, effettuato, registrato, verificato l'operazione stessa.

La salvaguardia di dati e procedure in ambito informatico può essere assicurata mediante l'adozione delle misure di sicurezza già previste dal GDPR nonché dal decreto 196 del 2003 (Codice in materia di protezione dei dati personali) per tutti i trattamenti di dati effettuati con strumenti elettronici.

I protocolli contengono la disciplina più idonea a governare il profilo di rischio individuato, attraverso un insieme di regole originato da una dettagliata analisi di ogni singola attività e del relativo sistema di prevenzione del rischio. Essi rispondono, tra l'altro, all'esigenza di rendere documentabili e verificabili le varie fasi dei processi dagli stessi regolati, onde consentirne la tracciabilità.

Valuecube s.r.l. ha attribuito il compito di verifica della costante applicazione di tali principi, nonché l'adeguatezza e l'aggiornamento degli stessi ai responsabili delle Funzioni aziendali che sono chiamati a interfacciarsi con l'Organismo di Vigilanza, affinché lo stesso sia costantemente informato di eventuali

modifiche introdotte nell'organizzazione o nelle attività aziendali e al quale potranno essere richiesti pareri ovvero indicazioni di principio e di orientamento.

2.5. Destinatari e campo di applicazione del Modello di Organizzazione

Il MOG ha come destinatari (vale a dire come soggetti vincolati alla sua osservanza) l'organo amministrativo e i dipendenti della società (ovvero tutto il personale impiegato con contratto di lavoro dipendente, con contratto di lavoro interinale o con contratti di collaborazione, tra cui i contratti a progetto), anche con qualifica dirigenziale.

Sono destinatari delle disposizioni etiche e di condotta contenute nel MOG, in virtù di apposita clausola contrattuale, i partner commerciali (clienti, fornitori, distributori, concessionari, appaltatori, subappaltatori, partner d'affari, ecc.) e i consulenti esterni (lavoratori non subordinati, revisori, broker, agenti, ma anche liberi professionisti che supportano l'azienda nella propria gestione).

Nel caso in cui una o più attività sensibili siano esternalizzate, il contratto alla base del rapporto richiamerà i punti di controllo per ognuna di esse.

Le regole contenute nel MOG si applicano quindi a coloro che svolgono, anche di fatto, funzioni di gestione, amministrazione, direzione o controllo nella Società, ai soci e ai dipendenti, nonché a coloro i quali, pur non appartenendo alla Società, operano su mandato della medesima o sono legati contrattualmente alla stessa.

Valuecube s.r.l. divulga il presente MOG attraverso modalità idonee ad assicurarne l'effettiva conoscenza da parte di tutti i soggetti interessati e si impegna a promuovere adeguate e periodiche attività di formazione sui principi e sui contenuti del presente Modello. I soggetti ai quali il Modello si rivolge sono tenuti a rispettarne puntualmente tutte le disposizioni, anche in adempimento dei doveri di lealtà, correttezza e diligenza che scaturiscono dai rapporti giuridici instaurati con la Società.

Valuecube s.r.l. condanna qualsiasi comportamento difforme non solo alla legge, ma anche e soprattutto, per quel che qui importa, difforme al Modello e al Codice Etico; ciò anche laddove il comportamento illecito sia stato realizzato nell'interesse della Società, ovvero con l'intenzione di arrecare ad essa un vantaggio.

SEZIONE TERZA

ATTUAZIONE DEL MODELLO ORGANIZZATIVO

1. PRINCIPI DI RIFERIMENTO

Come indicato, al fini del rispetto del D.Lgs. 231/2001 non basta l'adozione ma serve altresì la concreta attuazione dei principi e dei protocolli indicati nel modello organizzativo.

Per fare ciò, con riferimento anche alle indicazioni fornite dagli standard ISO ed in particolare dalla norma ISO 37301:2021 è possibile prendere quale benchmark di riferimento il ciclo di Deming, meglio conosciuto come **ciclo PDCA (Plan-Do-Check-Act)**, ovvero quel metodo sistematico di azione che mira al miglioramento continuo, di seguito schematizzato.

Il ciclo si articola in quattro fasi:

FASE	DESCRIZIONE	ATTIVITÀ OPERATIVE
PLAN	**È la fase di pianificazione**, in cui l'azienda lavora per comprendere il suo funzionamento e il suo contesto (modello di business, contesto legale e regolamentare, sociale, culturale e ambientale, strutture, politiche, processi, procedure e risorse interne) oltre che la propria cultura della compliance. **Ha ad oggetto l'obiettivo dell'adozione ed efficace attuazione del modello organizzativo, per prevenire la commissione di reati presupposto.**	✓ **adottare il modello organizzativo.** In particolare: - con il risk *assessment* si individuano le attività in cui i reati possono essere commessi; - si regolamentano i presidi per impedire la commissione dei reati; - si individuano le modalità di gestione delle risorse finanziarie; - si regolamentano protocolli per la formazione; - si regolamentano i flussi informativi all'OdV; - si introduce un sistema disciplinare.
DO	**È la fase di attuazione** dei protocolli e/o procedure previsti nel modello organizzativo. L'intera organizzazione deve essere coinvolta, acquisendo consapevolezza attraverso anche attività di formazione. Fondamentale è poi la catena dei controlli. Comprende anche la fase del monitoraggio quotidiano delle attività svolte.	✓ **attuare le procedure/protocolli adottati;** ✓ **controllare il rispetto delle procedure attraverso processi documentati;** ✓ **far emergere le preoccupazioni attraverso canali di segnalazione (whistleblowing);** ✓ **esaminare e chiudere le non conformità (processo di indagine).**
CHECK	**È la fase di monitoraggio del funzionamento del sistema adottato.** A differenza del monitoraggio quotidiano (ricompreso nella fase del DO), consente di verificare i risultati ottenuti rispetto agli obiettivi del modello organizzativo.	✓ **effettuare verifiche programmate** sulla base delle informazioni documentate quale evidenza dei risultati ottenuti e definiti appropriati criteri di reporting. I flussi informativi diretti all'ODV rientrano tra gli strumenti di monitoraggio e come strumento di presidio per le aree a rischio 231; ✓ **effettuare audit interni:** verifica con approccio sistematico; ✓ **riesame della direzione:** l'organismo di governo e l'alta direzione a intervalli pianificati riesaminano il modello organizzativo sulla scorta delle comunicazioni dell'OdV.
ACT	**È la fase di adozione e attuazione dei miglioramenti** e completa il ciclo di Deming.	✓ **gestione delle non conformità:** l'OdV valuta la prescrizione che potenzialmente espone la società al rischio di commissione di reati; ✓ **miglioramento continuo:** si deve migliorare in modo continuo l'idoneità, l'adeguatezza ed efficacia del modello in base ai risultati della fase di check.

2. DOCUMENTAZIONE DELL'EFFICACE ATTUAZIONE DEL MODELLO

Ogni fase di attuazione del modello deve essere compiutamente documentata. Se è vero che tutte le norme UNI ISO basate sulla Harmonized Structure (HS, ex HLS), affidano all'organizzazione la responsabilità di decidere cosa documentare, favorendo una progressiva semplificazione burocratica a favore delle prassi operative - pur permanendo l'obbligo di produrre evidenze documentate sull'attuazione effettiva dei processi previsti dalla norma e definiti dall'organizzazione – per i principi di controllo finalizzati alla prevenzione dei reati ai sensi del D.Lgs. 231/2001, le Linee Guida di Confindustria (capitolo 5) indicano chiaramente che: "*ogni operazione, transazione, azione deve essere: verificabile, documentata, coerente e congrua*".

Tale principio, ben noto a chi opera nei sistemi di gestione, si inserisce nel modello del ciclo di Deming (PDCA) e del miglioramento continuo, richiamato anche nelle Linee Guida UNI-INAIL per i sistemi di gestione della salute e sicurezza sul lavoro.
In sintesi, se il sistema di gestione per la compliance conforme alla UNI ISO 37301 viene adottato a supporto del Modello di Organizzazione, Gestione e Controllo ex D.Lgs. 231 **si privilegia la formalizzazione e documentazione di procedure/protocolli, nonché delle evidenze della loro attuazione**, rispetto al ricorso a prassi non documentate.

Ogni operazione è supportata da un'adeguata documentazione, tale da consentire in ogni momento l'effettuazione di controlli che ne attestino caratteristiche, motivazioni e responsabilità (chi ha autorizzato, eseguito, registrato e verificato l'operazione).

A tal fine, il sistema di attuazione prevede l'adozione delle seguenti procedure e moduli gestionali:

Documentazione di competenza della Funzione di Compliance
PG. 01: Controllo della documentazione;
PG. 02: Prescrizioni legali; Mod 231 -02-1 Registro norme e leggi applicabili
PG. 03: Informazione/formazione del personale; Mod 231 -03-1 Piano di formazione Mod 231 -03-2 Registrazione partecipazione corsi Mod 231 -03-3 Scheda Personale di Informazione - Formazione
PG. 04: Comunicazione; Mod-231-04-1 Verbale informazione Mod-231-04-2 Comunicazione sito internet
PG. 05: Audit Mod-231 05-1 Piano degli audit Mod-231 05-2 Rapporto di audit Mod-231 05-3 Rapporto di non conformità
PG. 06: Riesame della Direzione Mod-231-06-1 Verbale Riesame della direzione
PG. 07: Flussi informativi Mod-231 07-1 Dossier Permanente
PG. 08: Whistleblowing

SEZIONE QUARTA
ORGANISMO DI VIGILANZA

1. L'ORGANISMO DI VIGILANZA AI SENSI DEL D.LGS. 231/2001

1.1. L'Organismo di Vigilanza di Valuecube s.r.l.

In ottemperanza alle previsioni del d.lgs. 231/2001, art. 6, comma 1, lett. a) e b), le società possono essere esonerate da responsabilità qualora l'organo dirigente, oltre ad aver adottato ed efficacemente attuato Modelli di Organizzazione, Gestione e Controllo, abbia affidato il compito di vigilare sul funzionamento e l'osservanza del modello ad un organismo dotato di autonomi poteri di iniziativa e controllo.

Requisiti fondamentali dell'O.d.V.

I requisiti principali dell'Organismo di Vigilanza sono:

- ✓ **Autonomia e indipendenza**
- ✓ **Professionalità**
- ✓ **Continuità di azione**

L'autonomia dell'O.d.V. è condizione indispensabile per il funzionamento del Modello. L'Organismo deve essere collocato al di fuori delle gerarchie societarie, in una posizione che lo ponga a fianco dell'organo di controllo, al quale deve riferire, ma dal quale non dipende gerarchicamente.

Aderendo alle *best practice* del settore e tenendo conto delle proprie dimensioni e complessità organizzativa, Valuecube s.r.l. ha optato per una soluzione che prevede **un organismo monocratico** individuato in un soggetto esterno alla compagine societaria. Questa scelta garantisce il rispetto dei requisiti di autonomia e indipendenza previsti dalla normativa e dalla giurisprudenza in materia.

La composizione collegiale dell'Organismo permette di disporre di competenze diversificate e complementari, elemento fondamentale per valutare adeguatamente l'efficacia del Modello di Organizzazione e per proporre eventuali aggiornamenti necessari in relazione all'evoluzione normativa, organizzativa o operativa della società.

1.2. La Funzione di Compliance

Per assicurare la continuità di azione, elemento essenziale per l'efficacia dei controlli, l'O.d.V. di Valuecube s.r.l. sarà supportato da una risorsa interna dedicata: il Security & IT Risk Manager che si occuperà anche dei compiti propri della Funzione di Compliance.

Infatti, con riferimento alla compliance in materia 231, fermo restando che, sulla base del D. Lgs. n. 231/2001, art. 6, comma 1, lett. a), la responsabilità di adottare e attuare efficacemente un Modello di organizzazione e di gestione idoneo spetta all'Organo Dirigente, la Società ha ritenuto importante avvalersi della collaborazione di una risorsa interna per collaborare con l'Organismo di Vigilanza.

I rapporti tra la Funzione di Compliance e l'Organismo di Vigilanza possono essere così sintetizzati in base ai compiti da svolgere:

Funzione di Compliance	Organismo di Vigilanza
	Facilitare l'identificazione degli obblighi di compliance: *l'Organismo di Vigilanza deve conoscere la normativa vigente e le sue evoluzioni, poiché ha il compito di proporre all'organo dirigente gli aggiornamenti necessari del Modello per garantirne l'idoneità.*
Documentare il processo di valutazione dei rischi: *la valutazione dei rischi non rientra tra i compiti dell'OdV, poiché svolgerla implicherebbe un conflitto di interesse: l'OdV dovrebbe vigilare sull'adeguatezza del Modello, ma non può essere anche responsabile della valutazione su cui tale giudizio si basa.*	
Allineare il sistema di gestione per la compliance agli obiettivi per la compliance: *intervento di carattere operativo.*	**Monitorare e misurare le prestazioni relative alla compliance:** *attività che coincide con vigilanza sull'osservanza del modello.*
	analizzare e valutare le prestazioni del sistema di gestione per la compliance per identificare ogni esigenza di azioni correttive: *l'OdV deve proporre modifiche al Modello in caso di violazioni, cambiamenti aziendali rilevanti o novità normative.*
Stabilire un reporting relativo alla compliance e un sistema documentale: *gestione e attuazione del sistema dei flussi informativi (individuazione della periodicità e degli owner del flusso).*	**Stabilire un reporting relativo alla compliance e un sistema documentale:** *gestione e attuazione del sistema dei flussi informativi (individuazione della periodicità e degli owner del flusso).*
Assicurare che il sistema di gestione per la compliance sia riesaminato a intervalli pianificati: *assicurare che la relazione dell'OdV venga esaminata dall'Organo Dirigente.*	**Invio della relazione sulle attività di verifica svolte:** *l'OdV si limita ad inviare annualmente il flusso informativo all'organo amministrativo.*

Stabilire un sistema per far emergere preoccupazioni e assicurare che quest'ultime siano affrontate: *la funzione di compliance ha un ruolo nella gestione attiva della compliance:* ✓ *le responsabilità in materia di compliance siano correttamente assegnate all'interno dell'organizzazione;* ✓ *gli obblighi di compliance siano integrati nelle politiche, procedure e processi aziendali;* ✓ *il personale coinvolto riceva un'adeguata formazione;* ✓ *siano definite modalità per monitorare la compliance.*	

Questa struttura organizzativa consente di coniugare l'indipendenza garantita dai membri esterni con la conoscenza dei processi interni necessaria per un efficace monitoraggio, rappresentando un equilibrio ottimale tra i diversi requisiti previsti dalle linee guida di riferimento.

1.3. Principi generali in tema di istituzione, nomina e sostituzione dell'Organismo di Vigilanza

L'Organismo di Vigilanza della Società è istituito con delibera dell'Amministratore Unico, resta in carica per tre anni dalla nomina ed è rieleggibile. L'Organismo di Vigilanza cessa per decorrenza del termine del periodo stabilito in sede di nomina, pur continuando a svolgere *ad interim* le proprie funzioni fino alla nomina del nuovo componente dell'Organismo di Vigilanza.

Se, nel corso della carica, un componente dell'Organismo di Vigilanza cessa dal suo incarico, l'organo amministrativo provvede alla sostituzione con propria delibera. Fino alla nuova nomina, l'Organismo di Vigilanza opera con gli altri componenti rimasti in carica e, in mancanza, con altro nominato *ad interim* dall'Amministratore Unico.

Il compenso per la qualifica di componente dell'Organismo di Vigilanza è stabilito, per tutta la durata del mandato, dall'Amministratore Unico.

La nomina quale componente dell'Organismo di Vigilanza è condizionata alla presenza di requisiti soggettivi di eleggibilità.

In particolare, all'atto del conferimento dell'incarico, **i soggetti designati a ricoprire la carica di componente dell'Organismo di Vigilanza devono rilasciare una dichiarazione nella quale si attesti l'assenza** di motivi di ineleggibilità quali:

✓ **funzioni di amministrazione** – nei tre esercizi precedenti alla nomina quale componente

dell'Organismo di Vigilanza – **di imprese sottoposte a fallimento**, liquidazione coatta amministrativa o altre procedure concorsuali;

- ✓ **sentenza di condanna** anche non passata in giudicato e, anche ai sensi dell'art. 444 c.p.p., in Italia o all'estero, **per i delitti richiamati dal d.lgs. 231/2001** o delitti comunque incidenti sulla moralità professionale;

- ✓ **condanna**, con sentenza anche non passata in giudicato, ovvero con provvedimento che comunque ne accerti la responsabilità, **a una pena che importa l'interdizione**, anche temporanea, dai pubblici uffici, ovvero l'interdizione temporanea dagli uffici direttivi delle persone giuridiche e delle imprese.

Laddove alcuno dei sopra richiamati motivi di ineleggibilità dovesse configurarsi a carico di un soggetto nominato, questi decadrà automaticamente dalla carica.

Nello svolgimento dei compiti affidatigli, l'O.d.V. potrà giovarsi – sotto la sua diretta sorveglianza e responsabilità – della collaborazione di tutte le funzioni e strutture della Società ovvero di consulenti esterni, avvalendosi delle rispettive competenze e professionalità. Tale facoltà consente all'Organismo di Vigilanza di assicurare **un elevato livello di professionalità e la necessaria continuità di azione**.

A tal fine **l'organo amministrativo assegna, ogni anno, un *budget* di spesa all'Organismo di Vigilanza**, tenuto conto delle richieste di quest'ultimo, che dovranno essere formalmente presentate all'organo amministrativo.

L'assegnazione del *budget* **permette** all'Organismo di Vigilanza **di operare in autonomia** e con gli strumenti opportuni per un efficace espletamento del compito assegnatogli dal presente Modello, secondo quanto previsto dal d.lgs. 231/2001.

Al fine di garantire la necessaria stabilità ai membri dell'Organismo di Vigilanza, la revoca dei poteri propri dell'Organismo di Vigilanza e l'attribuzione di tali poteri ad altro soggetto potrà avvenire soltanto per giusta causa mediante un'apposita delibera dell'organo amministrativo.

A tale proposito, per "giusta causa" di revoca dei poteri connessi con l'incarico di componente dell'Organismo di Vigilanza potrà intendersi, a titolo meramente esemplificativo:

- ✓ una *grave negligenza* nell'assolvimento dei compiti connessi con l'incarico quale (a titolo meramente esemplificativo): l'omessa redazione della relazione informativa semestrale all'organo amministrativo sull'attività svolta, l'omessa segnalazione all'A.U. o di violazioni accertate del Modello, con presunta commissione di reati;

- ✓ l'"*omessa o insufficiente vigilanza*" da parte dell'O.d.V. – secondo quanto previsto dall'art. 6, comma 1, lett. d), d.lgs. 231/2001 – risultante da una sentenza di condanna, passata in giudicato, emessa nei confronti della Società ai sensi del d.lgs. 231/2001 ovvero da provvedimento che comunque ne accerti la responsabilità;

In casi di particolare gravità, l'organo amministrativo potrà comunque disporre la sospensione dei poteri dell'Organismo di Vigilanza e la nomina di un Organismo *ad interim*.

1.4. Funzioni e poteri dell'Organismo di Vigilanza

Le attività poste in essere dall'Organismo di Vigilanza non possono essere sindacate da alcun altro organismo o struttura della Società, **fermo restando** però che l'organo dirigente è in ogni caso chiamato a svolgere un'attività di vigilanza sull'adeguatezza del suo operato, in quanto **l'organo dirigente ha la responsabilità ultima del funzionamento e dell'efficacia del Modello.**

All'Organismo di Vigilanza sono conferiti i poteri di iniziativa e controllo necessari per assicurare un'effettiva ed efficiente vigilanza sul funzionamento e sull'osservanza del Modello, secondo quanto stabilito dall'art. 6 del d.lgs. 231/2001.

Pertanto, a tale Organismo è affidato il **compito di vigilare** in generale:

✓ **sulla reale** (e non meramente formale) **efficacia del Modello e sulla sua adeguatezza** rispetto all'esigenza di prevenire la commissione dei reati per cui trova applicazione il d.lgs. 231/01	✓ **sull'osservanza delle prescrizioni del Modello da parte dei destinatari**	✓ **sull'aggiornamento del Modello** nel caso in cui si riscontrassero esigenze di adeguamento in relazione alle mutate condizioni aziendali o normative

In particolare, all'Organismo di Vigilanza sono affidati, per l'espletamento e l'esercizio delle proprie funzioni, i seguenti compiti e poteri:

- ✓ **effettuare verifiche mirate su specifiche attività a rischio** avendo libero accesso ai dati relativi;
- ✓ **promuovere l'aggiornamento della mappatura dei rischi** in caso di significative variazioni organizzative o di estensione della tipologia di reati presi in considerazione dal d.lgs. 231/2001;
- ✓ **monitorare le iniziative di informazione/formazione** finalizzate alla diffusione della conoscenza e della comprensione del Modello in ambito aziendale promosse dalla funzione competente;
- ✓ **raccogliere e gestire le informazioni** necessarie a fornire un quadro costantemente aggiornato circa l'attuazione del Modello;
- ✓ **esprimere**, sulla base delle risultanze emerse dalle attività di verifica e di controllo, **una**

valutazione periodica sull'adeguatezza del Modello rispetto alle prescrizioni del d.lgs. 231/2001, ai principi di riferimento, alle novità normative ed agli interventi giurisprudenziali di rilevo, nonché sull'operatività dello stesso;

- ✓ **segnalare eventuali violazioni di protocolli e carenze rilevate** in occasione delle verifiche svolte, affinché questi possa adottare i necessari interventi di adeguamento, coinvolgendo, ove necessario, l'organo amministrativo;
- ✓ **vigilare sull'applicazione coerente delle sanzioni previste dal codice disciplinare** nei casi di violazione del Modello, ferma restando la competenza dell'organo deputato per l'applicazione dei provvedimenti sanzionatori.

L'organo amministrativo della Società cura l'adeguata comunicazione alle strutture aziendali dei compiti dell'Organismo di Vigilanza e dei suoi poteri. L'O.d.V. è tenuto al vincolo di riservatezza rispetto a tutte le informazioni di cui è a conoscenza a causa dello svolgimento del suo incarico. La comunicazione di tali informazioni potrà essere rivolta solo ai soggetti specificamente individuati dal Modello e potrà essere effettuata con le peculiari modalità previste dal medesimo.

All'Organismo di Vigilanza vengono fornite dall'azienda adeguate risorse finanziarie e logistiche atte a sostenerne le spese e garantirne le attività.

1.5. Documentazione delle attività dell'Organismo di Vigilanza

La regolamentazione delle attività dell'Organismo di Vigilanza è affidata ad un regolamento interno che lo stesso organo di controllo dovrà approvare al momento del proprio insediamento.

Delle attività di verifica e di audit viene redatto apposito verbale, appositamente conservato con l'eventuale documentazione di corredo, e da cui risultano le problematiche trattate e quanto eventualmente deliberato.

Documentazione di Competenza dell'Organismo di Vigilanza
Mod-ODV 231 - Regolamento Organismo di Vigilanza
Mod-ODV 231- Registro Verbali ODV
Mod-ODV 231- Piano degli Obiettivi

2. FLUSSI INFORMATIVI

2.1. Obblighi di informazione nei confronti dell'Organismo di Vigilanza

L'Organismo di Vigilanza deve essere tempestivamente informato, mediante apposito sistema di comunicazione interna, in merito ad atti, comportamenti od eventi che possano determinare una violazione del Modello o che, più in generale, siano rilevanti ai fini del d.lgs. 231/2001.

Si tratta del **canale di comunicazione nella prassi definito come Flusso Informativo.**

Gli obblighi di informazione su eventuali comportamenti contrari alle disposizioni contenute nel Modello rientrano nel più ampio dovere di diligenza ed obbligo di fedeltà del prestatore di lavoro di cui agli artt. 2104 e 2105 c.c.. Valgono, in proposito, le seguenti prescrizioni di carattere generale:

- ✓ Devono essere raccolte eventuali segnalazioni relative: *i*) alla commissione, o al ragionevole pericolo di commissione, dei reati richiamati dal d.lgs. 231/2001; *ii*) alla violazione di norme poste a tutela della salute e sicurezza sul lavoro; *iii*) a "pratiche" non in linea con le norme di comportamento emanate dalla Società; *iv*) a comportamenti che, in ogni caso, possono determinare una violazione del Modello.
- ✓ Il dipendente che intenda segnalare una violazione (o presunta violazione) del Modello può contattare il proprio diretto superiore gerarchico ovvero, qualora la segnalazione non dia esito o si senta a disagio nel rivolgersi al suo diretto superiore per effettuare la segnalazione, riferire direttamente all'Organismo di Vigilanza.
- ✓ Al fine di raccogliere in modo efficace le segnalazioni sopra descritte, l'Organismo di Vigilanza provvederà a comunicare, a tutti i soggetti interessati, i modi e le forme di effettuazione delle stesse.
- ✓ L'Organismo di Vigilanza valuta, discrezionalmente e sotto la sua responsabilità, le segnalazioni ricevute e i casi in cui è necessario attivarsi.

I segnalanti in buona fede sono garantiti contro qualsiasi forma di ritorsione, discriminazione o penalizzazione ed in ogni caso è assicurata la riservatezza della identità del segnalante, fatti salvi gli obblighi di legge e la tutela dei diritti della Società o delle persone accusate erroneamente e/o in mala fede.

Oltre alle segnalazioni di cui sopra, devono essere inoltre obbligatoriamente trasmesse all'Organismo di Vigilanza le informazioni concernenti:

- ✓ Le decisioni relative alla richiesta, erogazione ed utilizzo di finanziamenti pubblici.
- ✓ I provvedimenti e/o notizie provenienti da organi di polizia giudiziaria, o da qualsiasi altra autorità, dai quali si evinca lo svolgimento di indagini, anche nei confronti di ignoti, per i reati contemplati dal d.lgs. 231/2001 o dalla normativa in materia di salute e sicurezza sul lavoro e che possano coinvolgere la Società.
- ✓ Le richieste di assistenza legale inoltrate da amministratori o dipendenti in caso di avvio di procedimento giudiziario nei loro confronti ed in relazione ai reati di cui al d.lgs. 231/2001 o alla normativa in materia di salute e sicurezza sul lavoro.
- ✓ Le commissioni di inchiesta o relazioni interne dalle quali emergano responsabilità per le ipotesi di reato di cui al d.lgs. 231/2001.
- ✓ Le notizie relative alla effettiva attuazione, a tutti i livelli dell'organizzazione societaria, del modello organizzativo, con evidenza dei procedimenti disciplinari svolti e delle eventuali sanzioni irrogate ovvero dei provvedimenti di archiviazione di tali procedimenti con le relative motivazioni.
- ✓ Reportistica periodica in materia di salute e sicurezza sul lavoro.
- ✓ Le comunicazioni inerenti modifiche organizzative e societarie.

Tutte le segnalazioni e le comunicazioni indirizzate all'Organismo di Vigilanza potranno essere inoltrate all'indirizzo email:

odv@valuecuberesearch.com

Nel caso di mancata osservanza del dovere di informazione sono applicabili le sanzioni disciplinari previste ed elencate nel Modello (d'ora in poi Modello 231).

Le schede dei flussi informativi periodici devono essere compilate ed inviate all'OdV in conformità a quanto regolamentato con la procedura gestionale PG. 07 – *Flussi informativi da e verso l'Organismo di Vigilanza*.

Ogni informazione, segnalazione, e relazione previste nel Modello sono conservate dall'Organismo di Vigilanza in un apposito archivio riservato. I componenti uscenti devono provvedere affinché il passaggio della gestione dell'archivio avvenga correttamente ai nuovi componenti.

2.2. Reporting dell'Organismo di Vigilanza verso gli organi societari

L'Organismo di Vigilanza riferisce in merito all'efficacia e osservanza del Modello, all'emersione di eventuali aspetti critici, alla necessità di interventi modificativi. A tal fine, l'Organismo di Vigilanza predispone:

- ✓ con cadenza annuale, una relazione informativa, relativa all'attività svolta da presentare all'organo amministrativo;
- ✓ immediatamente al verificarsi di violazioni accertate del Modello, con presunta commissione di reati, una comunicazione da presentare al Presidente e/o all'Amministratore Delegato.

Nell'ambito del *reporting* annuale vengono affrontati i seguenti aspetti:

- ✓ controlli e verifiche svolti dall'Organismo di Vigilanza ed esito degli stessi;
- ✓ stato di avanzamento di eventuali progetti di implementazione/revisione di processi sensibili;
- ✓ eventuali innovazioni legislative o modifiche organizzative che richiedono aggiornamenti nell'identificazione dei rischi o variazioni del Modello;
- ✓ eventuali sanzioni disciplinari irrogate dagli organi competenti a seguito di violazioni del Modello;
- ✓ altre informazioni ritenute significative; valutazione di sintesi sull'adeguatezza del Modello rispetto alle previsioni del d.lgs. 231/2001.

Gli incontri con gli organi societari cui l'Organismo di Vigilanza riferisce devono essere documentati. L'Organismo di Vigilanza cura l'archiviazione della relativa documentazione.

3. IL *WHISTLEBLOWING*

3.1. Oggetto della segnalazione

Il *whistleblowing* è un meccanismo di segnalazione ad opera di un dipendente o collaboratore di comportamenti aventi rilevanza penale ovvero di irregolarità gestionali in ragione delle funzioni svolte.

Oggetto della segnalazione, ai sensi dell'art. 2, comma 1, lett. a), d.lgs. 24/2023 può riguardare azioni od omissioni che siano idonee a ledere l'interesse pubblico o l'integrità della società di cui il whistleblower sia venuto a conoscenza nel suo contesto lavorativo. Possono costituire oggetto di segnalazione tutti quei fatti o comportamenti che potrebbero configurare una violazione:

a) di disposizioni nazionali o europee che consistono in illeciti riguardanti, a titolo esemplificativo i settori:

- ✓ degli appalti pubblici;
- ✓ dei servizi, prodotti o mercati finanziari;
- ✓ della prevenzione del riciclaggio e del finanziamento al terrorismo;
- ✓ della sicurezza e conformità dei prodotti;

- ✓ della sicurezza dei trasporti;
- ✓ della tutela dell'ambiente;
- ✓ della protezione dei consumatori;
- ✓ della tutela privata e protezione dei dati personali e sicurezza delle reti e dei sistemi informativi; oppure

b) di disposizioni europee che consistono in:

- ✓ atti od omissioni che ledono gli interessi finanziari dell'Unione Europea;
- ✓ atti ed omissioni riguardanti il mercato interno;
- ✓ atti e comportamenti che vanificano l'oggetto o le finalità delle disposizioni degli atti dell'Unione Europea nei settori richiamati nel punto a); oppure

c) di disposizioni nazionali che consistono in:

- ✓ illeciti amministrativi, contabili, civili o penali;
- ✓ condotte illecite rilevanti ai sensi del d.lgs. 231/2001;

d) dei modelli organizzativi e gestione ex d.lgs. 231/2001.

Affinché le segnalazioni possano consentire l'applicazione dello speciale regime di protezione, oltre al requisito della materia, devono sussistere anche altri requisiti, definiti dall'art. 1 d.lgs. 24/2023:

a) la violazione possa pregiudicare l'interesse pubblico o l'integrità della società;

b) sussistano fondati motivi che portino il segnalante a ritenere che l'informazione sia vera.

Non sono, invece, ricomprese nelle segnalazioni che darebbero diritto al segnalante ad ottenere una qualche forma di tutela quelle che siano:

a) legate ad un interesse di carattere personale del segnalante, che attengono esclusivamente ai propri rapporti individuali di lavoro o inerenti ai rapporti con le figure sovraordinate;

b) violazioni disciplinate in via obbligatoria dagli atti dell'Unione Europea o nazionali riguardanti le materie dei servizi, prodotti e mercati finanziari e prevenzione del riciclaggio e del finanziamento del terrorismo, così come indicate nella parte II dell'allegato alla Direttiva UE 2019/1937 (che costituiscono oggetto di apposita disciplina);

c) violazioni in materia di sicurezza nazionale, di appalti relativi ad aspetti di difesa o di sicurezza nazionale, purché non disciplinati da diritto derivato dell'Unione Europea.

Pertanto, il "segnalante" non deve utilizzare l'istituto in argomento per scopi meramente personali o per effettuare rivendicazioni di lavoro contro superiori gerarchici, per le quali occorre riferirsi alla disciplina e alle procedure di competenza di altri organismi o uffici.

Il segnalante non ha diritto alle tutele previste qualora l'oggetto della segnalazione, divulgazione o denuncia sia un'informazione palesemente priva di fondamento, già di dominio pubblico o acquisita sulla base di indiscrezioni o vociferazioni scarsamente attendibili.

Al momento della segnalazione è necessario eseguire una verifica, sulla base degli indizi concretamente in possesso per valutare se la segnalazione rientri tra quelle oggetto di tutela ex d.lgs. 24/2023.

3.2. Destinatari della disciplina

Destinatario della disciplina del whistleblowing è il personale della società, definito, ex art. 1, co. 1, lett. i-ter) del Testo unico Finanziario come: "i dipendenti e coloro che comunque operano sulla base di rapporti che ne determinano l'inserimento nell'organizzazione aziendale, anche in forma diversa dal rapporto di lavoro subordinato". Rientrano in questa categoria:

a) i lavoratori subordinati;

b) i lavoratori autonomi, compresi quelli indicati al capo I della l. n. 81/2017. Si tratta dei lavoratori con rapporti di lavoro autonomi disciplinati dal Titolo III del Libro V del codice civile ivi inclusi i contratti d'opera di cui all'art. 2222 del medesimo codice civile. Questi includono, ad esempio, i lavoratori autonomi che esercitano le professioni intellettuali per l'esercizio delle quali è necessaria l'iscrizione in appositi albi o elenchi come psicologi, architetti, geometri etc.;

c) i collaboratori di cui all'art. 409, n. 3 c.p.c. (rapporti di agenzia, di rappresentanza commerciale ed altri rapporti di collaborazione che si concretano in una prestazione di opera continuativa e coordinata, prevalentemente personale, anche se non a carattere subordinato come ad esempio, avvocati, ingegneri, assistenti sociali che prestano la loro attività lavorativa per un soggetto del settore pubblico organizzandola autonomamente, ovvero rapporto parasubordinato) e all'art. 2 d.lgs. 81/2015 (collaborazioni organizzate dal committente che si concretino in prestazioni di lavoro esclusivamente personali e continuative, le cui modalità di esecuzione siano organizzate dal committente anche con riferimento "ai tempi e al luogo di lavoro", la c.d. "etero-organizzazione") che operano presso l'azienda, fornendo beni o servizi;

d) i liberi professionisti e i consulenti che prestano la propria attività in favore della società;

e) i volontari;

f) i tirocinanti retribuiti e non;

g) i soci e le persone con funzioni di amministrazione, controllo, direzione, vigilanza o rappresentanza, anche se esercitate solo di fatto.

Questi soggetti sono destinatari delle tutele anche se la segnalazione giunga quando:

A) Il rapporto di lavoro non sia ancora iniziato, qualora le informazioni siano state acquisite durante il processo di selezione o nelle fasi precontrattuali.

B) Siano ancora nel periodo di prova.

C) Il rapporto contrattuale sia già cessato, se le informazioni sulle violazioni sono state acquisite in pendenza di rapporto.

Oltre a questi soggetti, **le tutele previste per il whistleblower si estendono** anche:

1) ai "facilitatori", ovvero, ai sensi della lett. h), art. 2, comma 1, d.lgs. 24/2023: "una persona fisica che assiste una persona segnalante nel processo di segnalazione, operante all'interno del medesimo contesto lavorativo e la cui assistenza deve essere mantenuta riservata". Rientra nella categoria dei facilitatori, ad esempio, il collega, anche di un altro ufficio, che assista il segnalante senza divulgare notizie. Non vi rientra il sindacalista che proceda alla segnalazione spendendo la sigla sindacale;

2) alle persone che, operando o avendo operato nello stesso contesto lavorativo del segnalante, siano a lui **legate da rapporto affettivo o di parentela** entro il quarto grado;

3) ai colleghi del segnalante che lavorano, al momento della segnalazione, **nello stesso contesto** lavorativo e che hanno, con lui, un rapporto abituale e corrente;

4) agli enti: a) di proprietà del segnalante che ha effettuato una segnalazione, divulgazione pubblica o denuncia. Si può trattare di enti nei quali il segnalante abbia una quota esclusiva o maggioritaria, ma non minoritaria; b) per i quali il soggetto che ha effettuato una segnalazione, divulgazione pubblica o denuncia lavora. Si pensi, ad esempio, al caso in cui l'impresa nella quale opera il segnalante abbia un contratto di fornitura; c) che operano nello stesso contesto lavorativo del segnalante che ha effettuato una segnalazione, divulgazione pubblica o denuncia. Si tratta del caso in cui vi sia un legame, ad esempio accordi, collaborazioni, scambi o confronti tra la società di proprietà del segnalante o, comunque, nel quale egli opera, e altri enti che potrebbero subire ritorsioni.

3.3. Procedura di gestione delle segnalazioni

La gestione del canale interno di segnalazione e del processo che ne consegue è attribuita all'OdV, in quanto si tratta di soggetto dotato di un adeguato livello di autonomia e competenza professionale.

Le segnalazioni possono essere presentate secondo una delle seguenti modalità:

- ✓ **piattaforma online** per la gestione delle segnalazioni da parte dei dipendenti e degli altri soggetti legittimati. Qualora volesse presentare la propria segnalazione con queste modalità, il segnalante deve accedere in una pagina dedicata del sito internet aziendale e compilare il relativo questionario (nel campo relativo alla e-mail è consigliabile indicare un indirizzo personale e non quello aziendale). Una volta compilato il questionario, il segnalante dovrà conservare il codice numerico fornito dal sistema e la password da lui scelta per verificare la presenza e prendere visione di comunicazioni da parte dell'O.d.V., mantenere interlocuzioni con lo stesso e verificare lo stato della segnalazione. Il segnalante potrà accedere alla propria segnalazione inserendo il codice numerico e la password negli appositi campi;
- ✓ **in forma orale**, mediante chiamate ovvero, su richiesta del segnalante, mediante un incontro diretto con l'OdV (da fissarsi entro un termine ragionevole).

Ricevuta la segnalazione, l'Organismo di Vigilanza provvede, nel rispetto dei principi di imparzialità e riservatezza, a promuovere ogni attività ritenuta opportuna per l'accertamento dei fatti oggetto della segnalazione.

Può anche avvalersi del supporto e della collaborazione di strutture e funzioni aziendali quando, per la natura e la complessità delle verifiche, risulti necessario un loro coinvolgimento; come anche di consulenti esterni.

In ogni caso, durante tutta la gestione della segnalazione è fatto salvo il diritto alla riservatezza del segnalante.

In sintesi, le attività in cui si articola il processo gestionale delle segnalazioni sono:

- ✓ **Ricezione:** l'Organismo di Vigilanza riceve le segnalazioni;
- ✓ **Analisi preliminare:** L'Organismo di Vigilanza verifica la presenza di dati ed informazioni utili a consentire una prima valutazione della ammissibilità e fondatezza della segnalazione stessa.
- ✓ **Istruttoria:** l'O.d.V. valuta le segnalazioni ricevute avvalendosi, a seconda della loro natura, delle strutture interne della Società per lo svolgimento degli approfondimenti sui fatti oggetto di segnalazione. Può ascoltare direttamente l'autore della segnalazione – se noto – o i soggetti menzionati nella medesima;
- ✓ **Conclusione del processo:** all'esito dell'attività istruttoria l'O.d.V. assume, motivandole, le decisioni conseguenti, archiviando, ove del caso, la segnalazione o richiedendo alla Società di procedere alla valutazione ai fini disciplinari e sanzionatori di quanto accertato e/o agli opportuni interventi sul MOG.

Al fine di garantire la gestione e la tracciabilità delle segnalazioni e la ricostruzione delle diverse fasi del processo svolto, l'O.d.V. assicura l'archiviazione di tutta documentazione prodotta nell'ambito delle attività disciplinate nella presente procedura. I documenti cartacei sono archiviati presso un luogo identificato il cui accesso è consentito ai componenti dell'O.d.V. ovvero ai soggetti espressamente autorizzati dall'O.d.V. Al fine di garantire la gestione e la tracciabilità delle segnalazioni e delle relative attività, l'O.d.V. assicura l'archiviazione di tutta la correlata documentazione di supporto per un periodo di 5 anni dalla ricezione della segnalazione.

Valuecube s.r.l. si è dotata di una apposita procedura gestionale per la gestione delle segnalazioni (PG. 08 – Whistleblowing).

SEZIONE QUINTA
IL SISTEMA SANZIONATORIO

1. SISTEMA SANZIONATORIO

1.1. Principi generali

La predisposizione di un efficace sistema sanzionatorio per la violazione delle prescrizioni contenute nel Modello, è condizione essenziale per garantire l'effettività del modello stesso.

Al riguardo, infatti, l'articolo 6 comma 2 lettera e) e l'art. 7 comma 4 lett. b) del Decreto prevedono che il modello debba «*introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello*».

L'applicazione delle sanzioni disciplinari determinate ai sensi del Decreto prescinde dall'esito di eventuali procedimenti penali, in quanto le regole imposte dal Modello e dal Codice Etico sono assunte da Valuecube s.r.l. in piena autonomia, indipendentemente dalla tipologia di illecito che le violazioni del Modello o del Codice Etico stesso possano determinare.

In particolare, Valuecube s.r.l. si avvale di un sistema sanzionatorio che:

- ✓ individua esattamente le sanzioni disciplinari da adottarsi nei confronti di soggetti che pongano in essere violazioni, infrazioni, elusioni, imperfette o parziali applicazioni delle prescrizioni contenute nel modello, il tutto nel rispetto delle relative disposizioni dei CCNL e delle prescrizioni legislative applicabili;
- ✓ prevede un'apposita procedura di irrogazione delle suddette sanzioni, individuando il soggetto preposto alla loro irrogazione e in generale a vigilare sulla osservanza, applicazione ed aggiornamento del sistema sanzionatorio;
- ✓ introduce idonee modalità di pubblicazione e diffusione.

A tal fine, la Società prevede una graduazione delle sanzioni applicabili, in relazione al differente grado di pericolosità che i comportamenti possono presentare rispetto alla commissione dei reati presupposto. Si è pertanto creato un sistema disciplinare che, anzitutto, sanzioni tutte le infrazioni al modello, dalla più lieve alla più grave, mediante un sistema di gradualità della sanzione e che, secondariamente, rispetti il principio della proporzionalità tra la mancanza rilevata e la sanzione comminata.

Il presente sistema sanzionatorio ex D.Lgs. 231/2001, meglio specificato nell'allegato al modello organizzativo **(Allegato 4 – Sistema disciplinare)** può essere parte integrante di un più ampio regolamento disciplinare aziendale e costituisce espressione del potere riconosciuto al datore di lavoro

di impartire disposizioni anche per l'esecuzione e per la disciplina dell'attività lavorativa (art. 2104 c.c.) e viene affisso in ottemperanza alla disposizione di cui all' art. 7 della Legge 300/70 (Statuto dei Lavoratori).

In virtù dei principi esposti, il potere disciplinare di cui al d.lgs., 231/2001 è esercitato dal Datore di lavoro o da soggetto appositamente delegato, che si occuperà di gestire le procedure e le modalità previste dal vigente sistema disciplinare.

1.2. Sanzioni applicabili ai dipendenti

In caso di mancato rispetto delle prescrizioni indicate nel Modello, in proporzione alla gravità delle infrazioni verranno applicate nei confronti dei dipendenti le sanzioni qui di seguito indicate:

A) **Provvedimenti di richiamo verbale o di ammonizione scritta** per il lavoratore che violi, colposamente, le procedure interne previste dal presente Modello (a titolo meramente esemplificativo e non esaustivo, si rende passibile della sanzione qui descritta colui che non osservi le procedure previste; che ometta di comunicare all'Organismo di Vigilanza le informazioni prescritte, nelle forme e con le modalità stabilite dal Modello; che ometta di effettuare i controlli richiesti, ecc.), ovvero tenga, in relazione alle attività rilevanti per le aree a rischio di commissione di illecito, un comportamento non conforme alle disposizioni del Modello stesso.

B) **Provvedimento della multa non superiore a 3 ore di retribuzione** per il lavoratore che violi, ripetutamente con colpa oppure dolosamente, le procedure interne previste nel presente Modello; ovvero tenga, in relazione alle attività rilevanti per le aree a rischio di commissione di illecito, un comportamento non conforme alle disposizioni del Modello Organizzativo.

C) **Provvedimento della sospensione dal lavoro e dalla retribuzione fino ad un massimo di 3 giorni** per il lavoratore che a causa della violazione delle procedure interne previste dal presente Modello, ovvero attraverso l'adozione, in relazione alle attività rilevanti per le aree a rischio di commissione di illecito, di un comportamento non conforme alle prescrizioni del Modello Organizzativo, nonché compiendo atti contrari all'interesse di Valuecube s.r.l., ripetutamente con colpa oppure dolosamente, arrechi danno alla Società o la esponga ad una situazione oggettiva di pericolo per l'integrità e la conservazione del suo patrimonio

D) **Provvedimento del licenziamento** per il lavoratore che dolosamente assuma, in relazione alle attività rilevanti per le aree a rischio di commissione di illecito, un comportamento palesemente in violazione delle procedure interne previste dal presente Modello, che risulti idoneo e diretto in modo non equivoco a commettere uno qualsiasi dei reati presupposto elencati dal Decreto e, pertanto, in grado di ingenerare la responsabilità della Società a termini del Decreto, comportando la comminazione a carico della medesima delle sanzioni previste dal Decreto stesso.

Il tipo e la determinazione dell'entità di ciascuna delle sanzioni sopra esposte saranno commisurati, in conformità a quanto previsto dai CCNL vigenti in Valuecube s.r.l., in base:

- ✓ all'intenzionalità del comportamento o del grado di negligenza, imprudenza o imperizia del dipendente, anche con riguardo alla prevedibilità degli esiti della propria condotta;
- ✓ alla condotta complessiva del dipendente in seno alla Società, con particolare riferimento alla sussistenza o meno di precedenti disciplinari a carico del medesimo, nei limiti consentiti dalla legge;
- ✓ alle mansioni ed al livello di preparazione professionale del dipendente;
- ✓ alla posizione funzionale, all'interno della struttura organizzativa della Società, delle persone coinvolte nei fatti costituenti la violazione;
- ✓ ad ogni altra circostanza rilevante per la responsabilità disciplinare e penale del dipendente.

Il potere di procedere all'accertamento delle infrazioni, di adottare i relativi procedimenti disciplinari e di provvedere all'irrogazione delle conseguenti sanzioni spetta, nei limiti della rispettiva competenza, alla Direzione della Società. L'adeguatezza e l'efficacia del presente Sistema Disciplinare viene costantemente verificata dall'Organismo di Vigilanza.

1.3. Sanzioni applicabili a dirigenti, amministratori, collaboratori esterni e professionisti

In caso di mancato rispetto delle prescrizioni indicate nel Modello, in proporzione alla gravità delle infrazioni verranno applicate le sanzioni qui di seguito indicate:

- ✓ **Misure nei confronti dei dirigenti.** Si provvederà ad adottare nei confronti dei responsabili le misure ed i provvedimenti più idonei, in conformità a quanto previsto dal Contratto Collettivo Nazionale di Lavoro dei Dirigenti vigente in Valuecube s.r.l., fermo in ogni caso il provvedimento del licenziamento, ove ricorrano i presupposti di cui al presente Sistema Disciplinare.
- ✓ **Misure nei confronti degli Amministratori.** L'Organismo di Vigilanza ha l'obbligo di informare dei fatti, senza ritardo e per iscritto, l'Assemblea dei Soci, i quali procederanno a valutare e ad assumere tutte le opportune iniziative consentite dalla vigente normativa, ferma in ogni caso la revoca dall'incarico per l'Amministratore responsabile.

- ✓ Ogni violazione sarà ritenuta un grave inadempimento delle obbligazioni contrattualmente assunte e costituirà causa di risoluzione del contratto in essere tra la Società ed il/i Collaboratore/i o Partner responsabile/i. **Tale ipotesi dovrà essere espressamente ed adeguatamente disciplinata da apposita clausola risolutiva espressa del contratto concernente ogni singolo rapporto commerciale** o di collaborazione, al fine di terminare il relativo rapporto contrattuale, fatto salvo, in ogni caso, il diritto di Valuecube s.r.l. di pretendere il risarcimento dei danni, ove da tale comportamento derivi concreto nocumento alla Società.

SEZIONE SESTA: FORMAZIONE E INFORMAZIONE

1. PIANO DI FORMAZIONE E COMUNICAZIONE

Due elementi fondamentali per il corretto funzionamento del Modello sono la comunicazione e la formazione, da modulare in base ai destinatari: dipendenti in generale, soggetti operanti in aree a rischio o attività sensibili, componenti degli organi sociali, ecc.

1.1 Informativa

Per garantire l'efficacia del Modello, Valuecube s.r.l. si pone l'obiettivo di assicurare la corretta conoscenza, da parte di tutti i Destinatari, del modello di Organizzazione e Controllo nonché di ogni sua successiva modifica.

La comunicazione deve riguardare non solo il Codice Etico, ma anche gli strumenti organizzativi e operativi, quali i poteri autorizzativi, le linee di dipendenza gerarchica, le procedure, i flussi informativi e ogni altro elemento utile a garantire trasparenza nell'attività quotidiana. Essa deve essere capillare, chiara, efficace, dettagliata, provenire da livelli adeguati dell'organizzazione e ripetuta periodicamente. È inoltre necessario assicurare l'accessibilità alla documentazione che compone il Modello, anche tramite l'intranet aziendale.

A tal fine, Valuecube s.r.l. provvede alla diffusione del Modello mediante invio informatico ad ogni dipendente di:

1) un'informativa di carattere generale relativa al Decreto e alle linee guida adottate per la redazione del Modello;

2) la struttura e le principali disposizioni operative del Modello adottato da Valuecube s.r.l.;

3) la procedura di segnalazione all'O.d.V. e la scheda standard per la comunicazione – da parte dei soggetti in posizione apicale e dei dipendenti – di eventuali comportamenti, di altri dipendenti o di terzi, ritenuti potenzialmente in contrasto con i contenuti del Modello.

Al termine di ogni revisione del Modello, verrà inviato a tutti i dipendenti in organico una comunicazione – da parte degli organi individuati – per avvertire che Valuecube s.r.l. ha modificato il Modello di organizzazione, gestione e controllo ai sensi del Decreto, unitamente al testo modificato. Ai nuovi dipendenti verrà consegnata un'apposita informativa sul Modello contenente una nota informativa, nel corpo della lettera di assunzione, dedicata al Decreto ed alle caratteristiche del Modello.

1.2. Informativa a collaboratori esterni e partner

I soggetti esterni alla Società (*partner*, consulenti ecc.) saranno opportunamente informati in merito alla revisione, da parte di Valuecube s.r.l., del Modello includente il Codice Etico.

A tal fine Valuecube s.r.l. comunicherà a tutti i suddetti soggetti l'esistenza dell'indirizzo internet nel quale è possibile visionare il Modello di Organizzazione, Gestione e Controllo, unitamente al Codice etico. Verrà inoltre richiesto loro il formale impegno al rispetto delle disposizioni contenute nei suddetti documenti.

Per quanto riguarda i consulenti esterni che stabilmente collaborano con Valuecube s.r.l., sarà cura della società di prendere contatti con questi e accertarsi, tramite verifiche particolareggiate, che detti consulenti conoscano il Modello aggiornato della società e siano disposti a rispettarlo.

1.3 Formazione

Il livello di formazione e di informazione dei Destinatari ha un differente grado di approfondimento, con particolare attenzione verso quei soggetti che operano nei processi o nelle attività sensibili. L'attività di formazione è pertanto differenziata in funzione della qualifica dei Destinatari e del livello di rischio dell'area in cui operano.

L'azienda si impegna quindi ad implementare un programma formativo adeguato, calibrato in funzione del ruolo e del livello di responsabilità dei destinatari. Tale formazione deve illustrare non solo gli aspetti giuridici, ma anche le motivazioni di opportunità che sottendono le regole e le loro applicazioni concrete.

L'azienda definisce nel suo piano di formazione i contenuti dei corsi, la frequenza, l'obbligatorietà della partecipazione, i controlli di frequenza e qualità, nonché l'aggiornamento continuo dei materiali a seguito delle eventuali modifiche del Modello. Nel piano di formazione si indicano altresì le modalità di erogazione della formazione, prevedendo sessioni in aula e attività in modalità e-learning.

L'attività formativa sul D.Lgs. 231/2001 e sui contenuti del Modello adottato deve essere promossa e monitorata dall'Organismo di Vigilanza, con il supporto delle funzioni aziendali competenti o, se necessario, di consulenti esterni.

Per la formazione a distanza si prevedono fin dalla fase di progettazione test intermedi e finali per la verifica dell'apprendimento, nonché un sistema di monitoraggio dell'effettiva partecipazione, corredato da interventi correttivi in caso di criticità. In ogni caso, è auspicabile affiancare alla formazione e-learning anche momenti formativi tradizionali, in presenza, costruendo un approccio integrato e calibrato sul rischio, privilegiando le modalità più strutturate per i temi di maggiore complessità.

Sarà cura dell'O.d.V., d'intesa e in stretto coordinamento con l'organo amministrativo, valutare l'efficacia del piano formativo con riferimento al contenuto dei corsi, alle modalità di erogazione, ai destinatari, alla loro reiterazione, ai controlli sull'obbligatorietà della partecipazione e alle misure da

adottare avverso quanti non frequentino senza giustificato motivo.

A cadenza periodica, o comunque in caso di necessità, si procederà alla reiterazione dei corsi, al fine di verificare l'effettiva applicazione di quanto previsto dai documenti del Modello da parte dei Destinatari, nonché la loro sensibilizzazione ai temi e alle prescrizioni di cui al Modello medesimo, secondo modalità suggerite dall'Organismo di Vigilanza, in coordinamento con i direttori ed i responsabili delle funzioni aziendali.

SEZIONE SETTIMA: ADOZIONE E AGGIORNAMENTO DEL MODELLO

L'Amministratore Unico di Valuecube s.r.l., in qualità di organo dirigente, delibera in merito all'adozione e all'aggiornamento del Modello e al suo adeguamento in relazione a modifiche e/o integrazioni che si dovessero rendere necessarie in conseguenza di:

- ✓ modificazioni dell'assetto interno della Società e/o delle modalità di svolgimento delle attività d'impresa;
- ✓ cambiamenti delle aree di business;
- ✓ modifiche normative;
- ✓ risultanze dei controlli;
- ✓ significative violazioni delle prescrizioni del Modello.

Il Modello sarà, in ogni caso, sottoposto a procedimento di revisione ogniqualvolta l'organo amministrativo riterrà opportuno procedere a modifiche.

L'Amministratore Unico può delegare i compiti sopra descritti o ratificare l'operato del soggetto delegato.

La modifica delle procedure gestionali e operative richiamate nella parte speciale, così come degli allegati al modello di organizzazione sono di competenza dell'Alta Direzione.

ALLEGATI

Allegato 1 – Matrice dei reati presupposto

Allegato 2 – Matrice di attribuzione di deleghe e poteri

Allegato 3 – Matrice dei rischi

Allegato 4 – Sistema disciplinare

Allegato 5 – Procedure Operative

PR. OP. 01: Gestione del personale
PR. OP. 02: Salute e Sicurezza

Allegato 6 – Procedure Gestionali

PG. 01: Controllo della documentazione
PG. 02: Prescrizioni legali
Mod 231 -02-1 Registro norme e leggi applicabili
PG. 03: Informazione/formazione del personale
Mod 231 -03-1 Piano di formazione
Mod 231 -03-2 Registrazione partecipazione corsi
PG. 04: Comunicazione
Mod-231-04-1 Verbale informazione
Mod-231-04-2 Comunicazione sito internet
PG. 05: Audit
Mod-231 05-1 Piano degli audit
Mod-231 05-2 Rapporto di audit
Mod-231 05-3 Rapporto di non conformità
PG. 06: Responsabilità della Direzione
Mod-231-06-1 Verbale Riesame della direzione
PG. 07: Flussi informativi
Mod-231 07-1 Dossier Permanente
PG. 08: Whistleblowing