DATI COPERTINA E PREMESSA DEL PROGETTO

UNI1611084

Lingua

Italiana

Titolo Italiano

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

Titolo Inglese

Guidelines for the integration of the UNI ISO 37301: 2021 compliance management system to support the Organizational Management and Control Models and the Supervisory Bodies in accordance with Legislative Decree 231/2001

Commissione Tecnica

Organo Competente

UNI/CT 016/GL 09 - Governance delle organizzazioni

Coautore

Sommario

La norma 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 al fine di agevolare gli Enti nello sviluppo di modelli efficaci sulla base dei principi e requisiti espressi dalle norme tecniche nazionali ed internazionali UNI ISO. Inoltre, la norma può guidare gli Organismi di Vigilanza nel riferirsi ad uno strumento sistemico nello svolgimento del proprio compito di vigilanza e controllo sul Modello dell'Ente.

I destinatari di questo documento sono invitati a presentare, insieme ai loro commenti, la notifica di eventuali diritti di brevetto di cui sono a conoscenza e a fornire la relativa documentazione.

Questo testo NON è una norma UNI, ma è un progetto di norma sottoposto alla fase di inchiesta pubblica, da utilizzare solo ed esclusivamente per fini informativi e per la formulazione di commenti. Il processo di elaborazione delle norme UNI prevede che i progetti vengano sottoposti all'inchiesta pubblica per raccogliere i commenti degli operatori: la norma UNI definitiva potrebbe quindi presentare differenze -anche sostanziali- rispetto al documento messo in inchiesta.

Questo documento perde qualsiasi valore al termine dell'inchiesta pubblica, cioè il:

2024-06-07

UNI non è responsabile delle conseguenze che possono derivare dall'uso improprio del testo dei progetti in inchiesta pubblica.

Relazioni Nazionali

Relazioni Internazionali

Premessa

La presente norma è stata elaborata sotto la competenza della Commissione Tecnica UNI Gestione per la qualità e metodi statistici

---

1 Scopo e campo di applicazione

La presente norma 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 al fine di fine di agevolare gli Enti nello sviluppo di modelli efficaci sulla base dei principi e requisiti espressi dalle norme tecniche nazionali ed internazionali UNI ISO. Inoltre, la presente norma può guidare gli Organismi di Vigilanza nel riferirsi ad uno strumento sistemico nello svolgimento del proprio compito di vigilanza e controllo sul Modello dell'Ente.

2 Riferimenti normativi

La presente norma rimanda, mediante riferimenti datati e non datati, a disposizioni contenute in altre pubblicazioni. Tali riferimenti normativi sono citati nei punti appropriati del testo, e sono di seguito elencati. Per i riferimenti non datati, vale l'ultima edizione della pubblicazione alla quale si fa riferimento (compresi gli aggiornamenti).

UNI 11883:2022 *Attività professionali non regolamentate - Figure professionali operanti nell'ambito della gestione per la compliance - Requisiti di conoscenza, abilità, autonomia e responsabilità*

UNI EN ISO 19011:2018 *Linee guida per audit di sistemi di gestione*

UNI ISO 37000:2021 *Governance delle organizzazioni - Guida*

UNI ISO 37002:2021 *Sistemi di gestione per il whistleblowing - Linee Guida*

UNI ISO 37301:2021 *Sistemi di gestione per la compliance - Requisiti con guida per l'utilizzo*

3 Termini e definizioni

Ai fini della presente norma si applicano i termini e le definizioni seguenti.

3.1

organizzazione

persona o gruppo di persone avente funzioni proprie con responsabilità, autorità e relazioni per conseguire i propri obiettivi.

Nota 1: Il concetto di organizzazione comprende, in termini non esaustivi, singoli operatori, società, gruppi, aziende, imprese, autorità, partnership, enti di beneficenza o istituzioni, o loro parti o combinazioni, costituiti in persona giuridica o meno, pubblici o privati.

Nota 2: Se l'organizzazione è parte di un'entità (organizzativa) più ampia, il termine "organizzazione" si riferisce unicamente alla parte dell'entità più ampia che ricade all'interno del campo di applicazione del sistema di gestione per la compliance.

3.2

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.

3.3

alta direzione

persona o gruppo di persone che, al livello più elevato, guida e tiene sotto controllo un'organizzazione.

Nota 1: L'alta direzione ha il potere di delegare le autorità e mettere a disposizione le risorse all'interno dell'organizzazione.

Nota 2: Se il campo di applicazione del sistema di gestione copre solo una parte di un'organizzazione, il termine "alta direzione" si riferisce a coloro che guidano e tengono sotto controllo quella parte dell'organizzazione stessa.

Nota 3: Ai fini del presente documento, il termine "alta direzione" si riferisce al più alto livello della direzione esecutiva.

3.4

sistema di gestione

insieme di elementi correlati o interagenti di un'organizzazione finalizzato a stabilire politiche, obiettivi e processi per conseguire tali obiettivi.

3.5

politica

orientamenti e indirizzi di un'organizzazione espressi in modo formale dalla sua alta direzione.

Nota 1 Una politica può anche essere formalmente espressa dall'organismo di governo di un'organizzazione.

3.6

obiettivo

risultato da conseguire.

Nota 1: Un obiettivo può essere strategico, tattico od operativo.

Nota 2: Gli obiettivi possono riguardare differenti discipline (quali finanziari, di salute e sicurezza, e ambientali) e si possono applicare a livelli differenti (come quello strategico, dell'intera organizzazione, di progetto, di prodotto e di processo).

Nota 3: Un obiettivo può essere espresso in altre forme, per esempio come un esito atteso, una finalità, un criterio operativo, come un obiettivo per la compliance, o ancora attraverso l'utilizzo di altre parole di significato analogo (per esempio intento, scopo, o traguardo).

Nota 4: Nel contesto dei sistemi di gestione per la compliance, gli obiettivi per la compliance sono fissati dall'organizzazione, in coerenza con la politica per la compliance, per conseguire specifici risultati.

3.7

rischio

effetto dell'incertezza in relazione agli obiettivi.

Nota 1: Un effetto è uno scostamento - positivo o negativo - da quanto atteso.

Nota 2: L'incertezza è lo stato, anche parziale, di carenza di informazioni relative alla comprensione o conoscenza di un evento, delle sue conseguenze o della loro probabilità.

Nota 3: Il rischio è spesso caratterizzato dal riferimento a potenziali "eventi" (come definito nella Guida ISO 73:2009) e "conseguenze" (come definito nella Guida ISO 73:2009), o da una loro combinazione.

Nota 4: Il rischio è frequentemente espresso in termini di combinazione delle conseguenze di un evento (compresi cambiamenti nelle circostanze) e della "probabilità" (come definito nella Guida ISO 73:2009) associata al suo verificarsi.

3.8

processo

insieme di attività correlate o interagenti che utilizzano o trasformano input per consegnare un risultato.

Nota 1: Se il "risultato" di un processo è chiamato output, prodotto o servizio, ciò dipende dal contesto di riferimento.

3.9

competenza

capacità di applicare conoscenze e abilità per conseguire i risultati attesi.

3.10

informazione documentata

informazioni che devono essere tenute sotto controllo e mantenute da parte di un'organizzazione e il mezzo che le contiene.

Nota 1 Le informazioni documentate possono essere in un qualsiasi formato, su qualsiasi mezzo e provenire da qualsiasi fonte.

Nota 2 Le informazioni documentate possono riferirsi a:

- il sistema di gestione, compresi i relativi processi;
- le informazioni prodotte per il funzionamento dell'organizzazione (documentazione);
- l'evidenza dei risultati conseguiti (registrazioni).

3.11

prestazioni (performance)

risultati misurabili.

Nota 1: Le prestazioni possono riguardare risultanze sia quantitative sia qualitative.

Nota 2: Le prestazioni possono riguardare la gestione di attività, processi, prodotti (compresi i servizi), sistemi od organizzazioni.

3.12

miglioramento continuo (continual improvement)

attività ricorrente per migliorare le prestazioni.

3.13

efficacia

grado di realizzazione delle attività pianificate e di conseguimento dei risultati pianificati.

3.14

requisito

esigenza o aspettativa che può essere esplicita, generalmente implicita, oppure obbligatoria.

3.15

conformità

soddisfacimento di un requisito.

3.16

non conformità

mancato soddisfacimento di un requisito.

Nota 1: Una non conformità non è necessariamente una noncompliance.

3.17

azione correttiva

azione per eliminare la causa di una non conformità e per prevenirne la ripetizione.

3.18

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.

Nota 1: Un audit può essere un audit interno (di prima parte) o un audit esterno (di seconda parte o di terza parte) e può essere un audit combinato (che combina due o più discipline).

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 ISO 19011.

Nota 4: L'indipendenza può essere dimostrata attraverso l'assenza di responsabilità circa l'attività sottoposta ad audit o libertà da pregiudizi e conflitti di interesse.

3.19

misurazione

processo per determinare un valore.

3.20

monitoraggio

determinazione dello stato di un sistema, di un processo o di un'attività.

Nota 1: Per determinare lo stato può essere necessario verificare, sorvegliare od osservare criticamente.

3.21

organismo di governo

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.

Nota 1: Non tutte le organizzazioni, in particolare quelle di piccole dimensioni, dispongono di un organismo di governo separato dall'alta direzione.

Nota 2: Un organismo di governo può comprendere, in termini non esaustivi, un consiglio direttivo, comitati del consiglio, un consiglio di supervisione o fiduciari.

3.22

personale

singole persone in una relazione riconosciuta come rapporto di lavoro dalla legislazione nazionale o nella pratica, o in qualsiasi rapporto contrattuale che, per la relativa attività, dipende dall'organizzazione.

3.23

funzione di compliance

persona o gruppo di persone con responsabilità e autorità per il funzionamento del sistema di gestione per la compliance.

Nota: È preferibile che una singola persona sia assegnata alla supervisione del sistema di gestione per la compliance.

3.24

rischio di compliance

probabilità di accadimento e relative conseguenze di una noncompliance in riferimento agli obblighi di compliance dell'organizzazione.

3.25

obblighi di compliance; obblighi (da rispettare)

requisiti rispetto ai quali un'organizzazione deve obbligatoriamente conformarsi, così come quelli a cui un'organizzazione sceglie volontariamente di conformarsi.

3.26

compliance; rispetto degli obblighi

soddisfacimento di tutti gli obblighi di compliance di un'organizzazione.

3.27

non compliance (non compliance); mancato rispetto degli obblighi

non soddisfacimento di obblighi di compliance.

3.28

sistema di gestione per la compliance

sistema di gestione in riferimento alla compliance.

Nota 1: Un sistema di gestione per la compliance può essere parte di un sistema di gestione integrato complessivo di un’organizzazione.

Nota 2: Nel seguito della presente norma, per designare il sistema di gestione per la compliance è utilizzato l’acronimo CMS - Compliance Management System

[FONTE: UNI 11883:2022]

3.29

gestione per la compliance (compliance management):

gestione in riferimento alla compliance.

Nota 1: La gestione per la compliance comprende la definizione della politica per la compliance, gli obiettivi per la compliance, nonché le strutture organizzative (a partire dalla funzione di compliance) e processi per raggiungere tali obiettivi, attraverso pianificazione, supporto, attività operative, valutazione delle prestazioni e miglioramento.

[FONTE: UNI 11883:2022]

3.30

manager della compliance (Compliance Manager):

figura professionale operante nell'ambito della gestione per la compliance ad un livello politicostrategico.

Nota 1: Alla figura professionale in oggetto è associato un livello EQF/QNQ di autonomia e responsabilità pari a 7 (vedere punto 5.4 della UNI 11883:2022).

Nota 2: La figura professionale assume un ruolo di leadership ai fini dell'adozione, progettazione e attuazione di un sistema di gestione per la compliance, interfacciandosi prevalentemente con l'organismo di governo, l'alta direzione e con gli attori della catena del valore (value chain) dell'organizzazione, per quanto applicabile, in coerenza con i compiti e le attività specifiche di cui al punto 4.4 e le conoscenze e abilità di cui al punto 5.4 della UNI 11883:2022

Nota 3: Alcune denominazioni di figure professionali associate a tale livello professionale possono essere, in termini non esaustivi: abilitatore, consulente senior, direttore della compliance (chief compliance officer, compliance director, compliance head), esploratore, evangelista (evangelist), leader della compliance (compliance leader), temporary manager.

[FONTE: UNI 11883:2022]

3.31

cultura della compliance

valori, etica, convinzioni e condotta che esistono all'interno di un'organizzazione e interagiscono con le strutture ed i sistemi di controllo dell'organizzazione stessa al fine di produrre norme comportamentali che favoriscono la compliance.

3.32

condotta

comportamenti e prassi che impattano sugli esiti per clienti, collaboratori, fornitori, mercati e comunità.

3.33

terza parte

persona od organismo che è indipendente dall'organizzazione.

Nota: Tutti i soci in affari sono terze parti, ma non tutte le terze parti sono tali.

3.34

procedura (procedure)

modo specificato per svolgere un'attività o un processo.

4 Contesto dell'organizzazione

4.1 Comprendere l'organizzazione e il suo contesto

La comprensione dell'organizzazione e del suo contesto è uno dei passaggi iniziali fondamentali per conoscere i processi aziendali rilevanti dell'Ente al fine dell'inquadramento degli ambiti di attuazione del Modello di Gestione, Organizzazione e controllo (da adesso Modello 231) ai sensi del D. Lgs.231/2001 (da adesso, anche "D.Lgs.231" o "decreto 231" o "231") e al fine dell'implementazione del Sistema di Gestione per la Compliance conforme alla norma UNI ISO 37301:2021 (da adesso, anche "UNI ISO 37301").

I riferimenti al D.Lgs.231/2001 sono presenti nel capitolo *II.INDIVIDUAZIONE DEI RISCHI E PROTOCOLLI* della Linea Guida di Confindustria; prima, nel paragrafo *1. "PREMESSA"* dove, sullo specifico punto si dice:

" [...] Fermo restando l'esigenza che ogni impresa costruisca e mantenga in efficienza il proprio sistema di gestione dei rischi e di controllo interno, anche in ottica di "compliance integrata", di seguito si propone un approccio coerente con i principali framework di riferimento in tema di controllo interno e di gestione dei rischi.". E ancora: "Le fasi principali in cui il sistema di prevenzione dei rischi 231 dovrebbe articolarsi sono le seguenti:

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. [.] a seconda della tipologia di reato, gli ambiti di attività a rischio potranno essere più o meno estesi. [.];"*

Nel medesimo capitolo troviamo un secondo riferimento al "contesto", esattamente al paragrafo *4. MODALITÀ OPERATIVE DI GESTIONE DEI RISCHI*, che recita testualmente:

"[.]. I modelli che verranno quindi predisposti ed attuati a livello aziendale saranno il risultato dell'applicazione metodologica documentata, da parte di ogni singolo ente, delle indicazioni qui fornite, in funzione del proprio ***contesto*** *operativo interno (struttura organizzativa, articolazione-territoriale, dimensioni, ecc.) ed esterno (settore economico, area geografica, contesto naturalistico, ecc.), nonché dei singoli reati ipoteticamente collegabili alle specifiche attività dell'ente considerate a rischio.[.]"*

I riferimenti al sistema di gestione per la compliance (di cui alla norma UNI ISO 37301:2021) sono presenti nel medesimo punto di cui all'oggetto (4.1 COMPRENDERE L'ORGANIZZAZIONE E IL SUO CONTESTO) che recita testualmente: "L'organizzazione deve determinare i fattori esterni ed interni che sono rilevanti per le sue finalità e che influenzano la sua capacità di conseguire i risultati attesi per il proprio sistema di gestione per la compliance.

A tal fine, l'organizzazione deve considerare un'ampia gamma di fattori quali, in termini non esaustivi:

- *il **modello di business**, compresi strategia, natura, dimensione e grado di complessità e sostenibilità delle attività generali e operative dell'organizzazione;*
- *la natura e l'ambito delle relazioni di business con terze parti;*
- *il **contesto legale e regolamentare;***
- *la situazione economica;*
- *i **contesti sociale, culturale e ambientale;***
- *le **strutture, politiche, processi, procedure e risorse interne, comprese le tecnologie;***
- *la propria cultura della compliance."*

Si riporta l'esempio: PRODOTTI SOSTENIBILI: L'IMPORTANZA DELL'ANALISI DEL CONTESTO.

VALUTAZIONE DEI RISCHI UNI ISO 37301

PRODOTTI SOSTENIBILI - L'IMPORTANZA DELL'ANALISI DEL CONTESTO
Avere una catena di fornitura sostenibile è un aspetto sempre più strategico per le aziende, come anche la verifica degli indicatori ESG. Molte aziende investono su prodotti "green", accompagnati da asserzioni riferite al consumo sostenibile, che contribuiscono a determinare le scelte dei consumatori/clienti. La sostenibilità, quindi, è un tema rilevante per qualsiasi realtà imprenditoriale, indipendentemente dalla dimensione o dal settore di appartenenza; tuttavia, sono differenti le modalità con cui ci si approccia al tema in base al proprio livello di engagement, alle risorse impiegate, agli strumenti e alle azioni messe in campo. In questo ambito è di fondamentale importanza l'Analisi del contesto di mercato e del posizionamento dei principali competitor nell'area e una corretta gap analysis al fine di definire un piano d'azione per l'adozione degli standard ESG internazionali. Solo una attenta e competente analisi può identificare e minimizzare il rischio di investimenti errati, che potrebbero ad esempio determinare il mancato successo del prodotto nel mercato e quindi perdite di profitto.

4.2 Comprendere le esigenze e le aspettative delle parti interessate

Le parti interessate (o stakeholder) sono descritti dall'ISO e dalla HS (Harmonized Structure, ex HLS) come "*persona od organizzazione che può influenzare, essere influenzata o percepire sè stessa come influenzata, da una decisione o attività*" (vedere punto 3.2.). Nel Decreto Legislativo 8 giugno 2001, n. 231 e nelle Linee Guida 231 di Confindustria non esiste un termine uguale o analogo a "parti interessate" o "Stakeholder". Al fine di identificare correttamente le sovrapposizioni e le sinergie tra il sistema di gestione della compliance UNI ISO 37301:2021 ed i Modelli di Organizzazione, Gestione e Controllo conformi al D. Lgs. 231/2001 possiamo identificare come "parti interessate" dall'applicazione del D. Lgs. 231/2001 e delle Linee Guida di Confindustria coloro che, per il loro specifico ruolo o posizione, hanno interesse nella corretta applicazione dei sistemi di gestione e controllo che possiamo identificare con:

- gli **azionisti dell'Ente**, che sono i principali soggetti danneggiati da una eventuale condanna per responsabilità dell'organizzazione conseguente a condotte colpose o dolose da parte di soggetti che operino in nome e o per conto dell'Ente stesso;
- l'**Organo amministrativo**, che svolge un ruolo centrale nella guida strategica dell'organizzazione
  - a cui è affidata la gestione ordinaria e straordinaria dell'organizzazione, di regola con facoltà di delegare le proprie attribuzioni a uno o più dei suoi componenti;
- **l'Organismo di Vigilanza** che, come previsto dall'art. 6 del decreto 231, vigila sul funzionamento e sull'osservanza del modello curandone il relativo aggiornamento. L'Organismo deve essere posto nelle condizioni di assolvere realmente ai complessi e delicati compiti di cui la legge lo investe, cioè la vigilanza sul funzionamento e sull'osservanza del modello curandone il relativo aggiornamento.

In riferimento alla norma UNI ISO 37301:2021, questo ambito è ben declinato nel medesimo punto di cui all'oggetto (*4.2 COMPRENDERE LE ESIGENZE E LE ASPETTATIVE DELLE PARTI INTERESSATE*) che recita testualmente:

"L'organizzazione deve determinare:

- *le parti interessate rilevanti per il sistema di gestione per la compliance;*
- *i requisiti rilevanti di tali parti interessate;*
- *quali di questi requisiti sono trattati nell'ambito del sistema di gestione per la compliance."*

È evidente che nelle norme ISO con il termine "parti interessate" si intende una accezione molto più ampia rispetto all'ambito 231; le norme ISO includerebbero anche ad esempio il personale interno all'organizzazione e i fornitori. Le Parti interessate rilevanti devono essere identificate nella fase iniziale, prima della progettazione e implementazione del Sistema di Gestione, parallelamente all'analisi del contesto. È anche evidente che gli Stakeholder possono differire da una norma (o sistema di gestione) ISO all'altra, in funzione dello "scope of work" della norma stessa (o del sistema di gestione).

4.3 Determinare il campo di applicazione del sistema di gestione per la compliance e dei Modelli 231

Così come la comprensione dell'organizzazione e del suo contesto (punto 4.1), anche la determinazione del campo di applicazione è uno dei passaggi iniziali fondamentali per inquadrare l'ampiezza dei processi sia la realtà dimensionale strutturale/organizzativa dell'Ente e per comprendere i processi aziendali rilevanti dell'Ente sia ai fini del Modello 231 che ai fini del Sistema di Gestione per la Compliance conforma alla norma UNI ISO 37301:2021.

Partendo questa volta dalla norma UNI ISO 37301:2021, la declinazione la troviamo nel punto *4.3 DETERMINARE IL CAMPO DI APPLICAZIONE DEL SISTEMA DI GESTIONE PER LA COMPLIANCE* che recita testualmente:

"L'organizzazione deve determinare i confini e l'applicabilità del sistema di gestione per la compliance per stabilirne il campo di applicazione. NOTA Lo scopo e campo di applicazione del sistema di gestione per la compliance è finalizzato a chiarire i principali rischi di compliance che l'organizzazione deve affrontare ed i confini geografici od organizzativi, o entrambi, ai quali si applica il sistema stesso, specialmente se l'organizzazione è parte di un'entità organizzativa di dimensioni maggiori.

Nel determinare il campo di applicazione, l'organizzazione deve considerare:

- *i fattori esterni e interni di cui al punto 4.1;*
- *i requisiti di cui ai punti 4.2, 4.5 e 4.6.*

Il campo di applicazione deve essere disponibile come informazione documentata."

In particolare, per le norme ISO il campo di applicazione chiarisce se l'organizzazione detiene il controllo su altre organizzazioni, specificando le caratteristiche di tale controllo, ad esempio: partecipazioni al capitale, vincoli contrattuali.

Nel caso del D.Lgs.231/2001, non esiste una analoga definizione di "campo di applicazione". In ogni caso, è possibile mutuare la definizione dell'ISO mettendola in relazione con i concetti espressi nel D.Lgs.231/2001 e dalle Linee Guida di supporto all'attuazione della norma stessa con la seguente possibile definizione:

"L'Ente dovrebbe determinare i confini e l'applicabilità dei reati contemplati nel "catalogo 231" per stabilirne il campo di applicazione. NOTA Lo scopo e campo di applicazione del Modello di Organizzazione, Gestione e Controllo è finalizzato a individuare le aree a rischio di reato che l'Ente deve presidiare e i confini organizzativi e il perimetro di attività (si veda per la definizione di queste ultime il Capitolo V. LA RESPONSABILITA' DA REATO NEI GRUPPI DI IMPRESE nelle Linee Guida 231 di Confindustria).

È importante documentare lo svolgimento di questa analisi iniziale per poter dimostrare l'attività svolta dall'organizzazione/Ente nell'individuazione dei rischi, dei presidi e degli ambiti ritenuti rilevanti per la successiva costruzione del Sistema di gestione ovvero del Modello 231.

4.4 Sistema di gestione per la compliance a supporto dei Modelli 231

Una rilevante area di sinergia tra il D.Lgs. 231/2001 e i Sistemi di Gestione ISO, è sicuramente la costruzione di un Sistema di Gestione per la Compliance come definito dalla norma UNI ISO 37301:2021

che miri, tra l'altro, alla valorizzazione, anche ai fini 231, delle attività di controllo previste, ad esempio, in altri ambiti di compliance specialistici.Le Linee Guida di Confindustria, così come quelle emesse da altre associazioni di categoria (si citano anche, tra le altre, quelle dell'emesse dall'ANCE denominate "Codice di comportamento delle imprese di costruzione") forniscono una rinnovata spinta all'importanza dei Sistemi di Gestione come base per la costruzione di un sistema di prevenzione dei reati (rif. 3.1 SISTEMA INTEGRATO DI GESTIONE DEI RISCHI delle Linee Guida di Confindustria), questo al fine di potere dimostrare sia l'adeguatezza del Modello stesso rispetto all'Ente che lo ha implementato (tailor made) che la sua efficace attuazione attraverso un organico sistema di gestione composto da manuali, procedure, istruzioni operative, moduli di registrazione, etc. Tale orientamento permetterebbe inoltre all'Ente/organizzazione di dimostrare in modo inequivocabile, la volontà dell'Ente di regolamentare i propri processi sensibili propedeutici alla prevenzione del reato dando regole chiare e oggettive che, se violate, fanno ricadere la responsabilità sull'autore stesso della violazione (fermo restando gli obblighi di vigilanza, da parte dell'OdV e dell'applicazione delle sanzioni disciplinari in caso di violazione da parte dell'Ente).

Al fine di comprendere meglio l'importanza dei sistemi di gestione ISO a supporto dei Modelli 231, estrapoliamo di seguito alcuni passaggi delle Linee Guida stesse che ci possono aiutare nella comprensione di tale sinergia (Linee Guida di Confindustria - *II. INDIVIDUAZIONE DEI RISCHI E PROTOCOLLI - 3. PASSI OPERATIVI PER LA REALIZZAZIONE DI UN SISTEMA DI GESTIONE DEL RISCHIO*":

"*Premesso che i modelli organizzativi devono essere idonei a prevenire i reati di origine sia dolosa che colposa previsti dal decreto 231, [...] Occorre comunque tenere presente [...] che gli stessi reati possono essere commessi anche una volta implementato il modello [...] (e) l'agente [...] potrà attuare il suo proposito criminoso soltanto aggirando fraudolentemente le indicazioni dell'ente.*"

E ancora (Linee Guida di Confindustria - *II. INDIVIDUAZIONE DEI RISCHI E PROTOCOLLI - 3.1 SISTEMA INTEGRATO DI GESTIONE DEI RISCHI*":

"É 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 quest'ottica, un approccio integrato dovrebbe, quindi, contemplare ***procedure comuni*** *che garantiscano efficienza e snellezza e che non generino sovrapposizione di ruoli (o mancanza di presidi), duplicazioni di verifiche e di azioni correttive, in termini più ampi, di conformità rispetto alla copiosa normativa di riferimento, laddove tali ruoli rispettivamente incidano e insistano sui medesimi processi.*

Le società tenute al rispetto delle diverse normative dovrebbero valutare l'opportunità di ***predisporre o integrare tali procedure*** *tenendo conto delle peculiarità sottese a ciascuna di esse, portando a sintesi gli adempimenti, individuando le modalità per intercettare e verificare gli eventi economici e finanziari dell'impresa nell'ottica del corretto agire.*

Per dare attuazione a una gestione integrata di questo tipo occorre quindi anche definire specifici e continui meccanismi di coordinamento e collaborazione tra i principali soggetti aziendali interessati tra i quali, a titolo esemplificativo, il Dirigente Preposto, la funzione Compliance, l'Internal Audit, il Datore di lavoro, il responsabile AML[1] (per le imprese che ne sono tenute), il Collegio sindacale, il Comitato per il controllo

[1] Per Responsabile AML si intende il Responsabile Antiriciclaggio

interno e la revisione contabile (ai sensi dell'art.19, d.lgs. n. 39/2010) e l'OdV (che ha pur sempre il compito di vigilare sul funzionamento e l'osservanza del modello e di curarne l'aggiornamento).”

È chiara l'importanza data dal legislatore, anche attraverso una interpretazione attuativa fornita dalle associazioni di categoria attraverso le specifiche linee guida, ad un Sistema di Gestione attivo, vivo, dinamico e funzionale, come può essere quello declinato dalle norme ISO.

In riferimento alla norma UNI ISO 37301:2021, questo ambito è ben descritto nel punto *4.4 SISTEMA DI GESTIONE PER LA COMPLIANCE* che recita testualmente:

“L'organizzazione deve stabilire, attuare, mantenere e migliorare in modo continuo un sistema di gestione per la compliance, compresi i processi necessari e le loro interazioni, in conformità ai requisiti del presente documento.

Il sistema di gestione per la compliance deve riflettere i valori, gli obiettivi e la strategia dell'organizzazione, nonché i relativi rischi di compliance, considerando il contesto dell'organizzazione stessa”.

Si riporta di seguito un esempio che evidenzia l'importanza di un sistema per la compliance nel processo di qualifica dei fornitori: LAVORO CON FORNITORI ESTERNI: RISPETTO DEL QUADRO LEGISLATIVO.

VALUTAZIONE DEI RISCHI UNI ISO 37301

LAVORI CON FORNITORI ESTERNI - RISPETTO DEL QUADRO LEGISLATIVO

In materia di compliance l'esternalizzare la realizzazione di un servizio è un passaggio strategico e importante per ogni azienda. Non devono essere sottovalutati anche gli aspetti di compliance o conformità normativa.

In caso di appalto di opere o di servizi, il committente imprenditore o datore di lavoro è obbligato a richiedere copia degli attestati di versamento delle ritenute operate sulle retribuzioni corrisposte al personale impiegato nell'appalto e di verificarne la congruità.

Anche il rispetto degli obblighi in materia di sicurezza sul lavoro porta l'azienda committente alla richiesta e verifica di una serie di documenti dell'appaltatore al fine di accertarne la regolarità sia tecnico professionale sia amministrativa/contributiva.

La valutazione del rischio compliance è un elemento strategico per il committente al fine di qualificare fornitori affidabili e conformi a loro volta alle normative di salute e sicurezza e a quelle retributive verso i loro addetti.

Il discostamento dalla compliance da parte del fornitore potrebbe significare, infatti, coinvolgimenti in reati colposi nel caso di violazione della normativa di salute e sicurezza (art. 26 del D.lgs. 81), o anche sanzioni o ammende per la mancata regolarità contributiva dei fornitori.

4.5 Obblighi di compliance, anche in relazione ai reati 231

Questo adempimento va letto in combinato disposto col requisito *4.3 DETERMINARE IL CAMPO DI APPLICAZIONE DEL SISTEMA DI GESTIONE PER LA COMPLIANCE E DEI MODELLI 231:* per la norma UNI ISO 37301 viene chiarito che l'organizzazione/Ente deve identificare lo scopo e il campo di applicazione del sistema di gestione per la compliance (nel sistema 231 il riferimento è al proprio Modello) al fine di chiarire i principali rischi di compliance (nel sistema 231 il riferimento è al rischio della commissione dei reati presupposto) che l'organizzazione/l'Ente deve affrontare nello sviluppo del proprio sistema di gestione (nel sistema 231 il riferimento è al proprio Modello). Per le Linee Guida di Confindustria si chiede di dotarsi di strumenti attuativi per rendere operativo tale impegno.

A tale fine, può essere utile alla comprensione leggere quanto scritto testualmente dalla norma UNI ISO 37301:2021, al punto *4.5 OBBLIGHI DI COMPLIANCE*:

"L'organizzazione deve identificare sistematicamente gli obblighi di compliance che derivano dalle proprie attività, prodotti e servizi, e valutare il relativo impatto sulle proprie attività operative.

L'organizzazione deve disporre di processi in funzione al fine di:

a) *identificare obblighi di compliance nuovi o modificati per assicurare la compliance su base continuativa;*

b) *valutare l'impatto dei cambiamenti identificati e attuare ogni necessaria modifica nella gestione degli*

obblighi di compliance.

L'organizzazione deve mantenere informazioni documentate dei propri obblighi di compliance."

Mutuando tale definizione anche ai fini del D.Lgs.231/2001, potremmo leggere questo adempimento come segue:

l'Ente dovrebbe identificare sistematicamente i "reati 231" astrattamente applicabili alla propria organizzazione (nota: processo di "Risk mapping") e riconducibili alle aree/processi correlati ad attività, prodotti e servizi, e valutarne i relativi impatti".

L'Ente dovrebbe disporre di processi in funzione al fine di:

c) identificare obblighi di compliance ai fini 231, nuovi o modificati per assicurare la compliance su base continuativa;

d) valutare l'impatto dei cambiamenti identificati e attuare ogni necessaria modifica nella gestione degli obblighi di compliance ai fini 231.

L'organizzazione dovrebbe mantenere informazioni documentate dei propri obblighi di compliance 231.

Anche in questo caso va evidenziato come, sia il D.Lgs.231/2001 sia la norma ISO, esprimono il requisito di fornire evidenza documentale di tale processo per poter dimostrare in modo tangibile ed oggettivo questo processo in quanto risulta essere la modalità più "solida" per potere dimostrare l'attività svolta, sia ai fini ISO per il rispetto degli obblighi di compliance, molto più ampi, che quelli ai fini del Modello 231 dell'Ente, limitatamente al catalogo dei reati presupposto.

4.6 Analisi e valutazione dei rischi di compliance in relazione a risk assessment e gap-analysis per la costruzione del Modello 231

Tra tutti i requisiti citati, l'attività di risk assessment è quella più importante: solo un corretto, attento e adeguato processo di analisi e valutazione dei rischi ci può permettere di identificare i capi-saldi che consentono all'organizzazione/ente di costruire un Sistema di Gestione per la Compliance, conforme agli standard ISO, ovvero costruire un Modello di Organizzazione, Gestione e Controllo ai sensi del D.Lgs.231/2001.

I riferimenti al D.Lgs.231/2001 sono presenti nel capitolo II.INDIVIDUAZIONE DEI RISCHI E PROTOCOLLI della Linea Guida di Confindustria, analizzando prima, nel paragrafo *1. "PREMESSA"* dove, sullo specifico punto si dice testualmente:

"[...] Le fasi principali in cui il sistema di prevenzione dei rischi 231 dovrebbe articolarsi sono le seguenti:

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.* ***Per "rischio" si intende 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*** *(in particolare all'art. 6, comma 1, lett. a); pertanto, a seconda della tipologia di reato, gli ambiti di attività a rischio potranno essere più o meno estesi. Per esempio, in relazione al rischio di omicidio colposo o lesioni colpose gravi o gravissime commessi con violazione delle norme in materia di salute e sicurezza sul lavoro, l'analisi dovrà verosimilmente estendersi alla totalità delle aree ed attività aziendali;*

[.] Il sistema delineato, per operare efficacemente, deve tradursi in un processo continuo o comunque svolto con una periodicità adeguata, da rivedere con particolare attenzione in presenza di cambiamenti aziendali (apertura di nuove sedi, ampliamento di attività, acquisizioni, riorganizzazioni, modifiche della struttura organizzativa, ecc.), ovvero di introduzione di nuovi reati presupposto della responsabilità dell'ente in via normativa."

Figura1 — "Processo di risk management secondo il Decreto 231 e le Linee guida Confindustria"

In riferimento alla norma UNI ISO 37301:2021, il processo di identificazione e valutazione del rischio è trattato nel punto *4.6 PROCESSO DI VALUTAZIONE DEI RISCHI DI COMPLIANCE* che recita testualmente:

"L'organizzazione deve identificare, analizzare e ponderare i propri rischi di compliance sulla base di un processo di valutazione dei rischi di compliance.

L'organizzazione deve identificare i rischi di compliance mettendo in relazione i propri obblighi di compliance con le proprie attività, i propri prodotti, servizi e aspetti rilevanti delle proprie attività operative.

L'organizzazione deve valutare i rischi di compliance in termini di processi affidati all'esterno e di terzi parti.

I rischi di compliance devono essere valutati su base periodica e ogni qual volta vi siano cambiamenti sostanziali a livello di condizioni o di contesto organizzativo.

L'organizzazione deve conservare informazioni documentate circa il processo di valutazione dei rischi di compliance e le azioni per affrontare i propri rischi di compliance."

Come è facile intravedere nella comparazione dei due testi, il processo di identificazione e valutazione dei rischi espresso nell'ambito del D.Lgs.231/2001 e nell'ambito ISO sono simili; questo ci aiuta molto nell'ottica di una sinergia di strumenti aziendali e nella integrazione dei due ambiti. In questo processo di possibile sinergia e integrazione, bisogna però prestare molta attenzione al concetto di rischio, in quanto i due ambiti lo intendono in maniera parzialmente difforme.

Nell'ambito "231" per "rischio" si intende "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 (in particolare all'art. 6, comma 1, lett. a); pertanto, a seconda della tipologia di reato, gli ambiti di attività a rischio potranno essere più o meno estesi."

Nelle definizioni della norma UNI ISO 37301:2021 troviamo le seguenti definizioni:

*"- **rischio** (risk): effetto dell'incertezza in relazione agli obiettivi*

Nota 1: Un effetto è uno scostamento - positivo o negativo - da quanto atteso.

Nota 2: L'incertezza è lo stato, anche parziale, di carenza di informazioni relative alla comprensione o conoscenza di un evento, delle sue conseguenze o della loro probabilità.

Nota 3: Il rischio è spesso caratterizzato dal riferimento a potenziali "eventi" e "conseguenze", o da una loro combinazione.

Nota 4: Il rischio è frequentemente espresso in termini di combinazione delle conseguenze di un evento (compresi cambiamenti nelle circostanze) e della "probabilità" associata al suo verificarsi.

- ***rischio di compliance** (compliance risk): probabilità di accadimento e relative conseguenze di una non compliance in riferimento agli obblighi di compliance dell'organizzazione"*

Nel mettere in correlazione le due diverse tipologie di processo di analisi e valutazione, laddove implementati in combinato disposto nell'ambito del sistema di gestione integrato aziendale, bisogna tenere conto di entrambe le definizioni per essere certi che il processo adottato risponda alle esigenze normative di entrambi i contesti.

Si riporta un esempio sull'importanza di monitorare il rischio, stabilendo dei punti critici di controllo: SICUREZZA ALIMENTARE: GESTIONE DEL RISCHIO RESIDUO

VALUTAZIONE DEI RISCHI UNI ISO 37301

SICUREZZA ALIMENTARE - GESTIONE DEL RISCHIO RESIDUO
Spetta agli operatori del settore alimentare e dei mangimi controllare e garantire che nelle imprese da essi controllate gli alimenti o i mangimi soddisfino le disposizioni della legislazione alimentare inerenti alle loro attività in tutte le fasi della produzione, della trasformazione e della distribuzione e verificare che tali disposizioni siano soddisfatte con l'obiettivo di ottenere prodotti alimentari il più possibile sicuri.
La legislazione alimentare prevede che gli operatori predispongano ed attuino adeguate procedure operative, basate sul sistema **HACCP "Hazard Analysis Critical Control Point"**, che consiste nell'identificazione di potenziali problemi inerenti la sicurezza degli alimenti e nella definizione di modalità per prevenirli aumentare la garanzia della sicurezza degli alimenti al fine di evitare intossicazioni alimentari dovute a prodotti non sicuri.
È altresì necessario stabilire i punti critici di controllo, i limiti critici che differenziano l'accettabilità dalla inaccettabilità ed è anche necessario stabilire e applicare procedure di sorveglianza efficaci per ridurre il rischio residuo.
Stabilire, ad esempio, un'azione correttiva errata, per monitorare un punto critico sotto controllo (per evitare il superamento dei limiti critici stabiliti), espone ad un ulteriore rischio non solo di intossicazione alimentare, ma di perdita economica per il ritiro del prodotto dal mercato e perdita di immagine del produttore.

5 Leadership

5.1 Leadership e impegno

5.1.1 Organismo di governo e alta direzione

Nelle attività di progettazione di un Modello Organizzativo ai sensi del D.Lgs. n. 231/2001 in linea con i requisiti della UNI ISO 37301 occorre identificare correttamente i soggetti che, secondo la norma tecnica, sono assegnatari delle principali responsabilità per la progettazione ed attuazione di un sistema di gestione della compliance. Ai sensi della UNI ISO 37301 assumono rilevanza le definizioni di "organismo di governo" e "alta direzione": se l'organismo di governo - definito come "*persona o gruppo di persone che detiene la responsabilità e autorità finali nei confronti delle attività, della governance e delle politiche di un'organizzazione, al quale riferisce l'alta direzione e rispetto alla quale l'alta direzione è chiamata a rispondere*" - può essere agevolmente identificato nell'organo che, all'interno della

Organizzazione, detiene istituzionalmente i poteri di gestione ed amministrativi (ad es., il Consiglio di Amministrazione o l'Amministratore Unico nel sistema amministrativo tradizionale delle società commerciali); per l'alta direzione - definita quale "*persona o gruppo di persone che, al livello più elevato, guidano e tengono sotto controllo un'organizzazione*" - è viceversa opportuno effettuare una apposita verifica, potendosi addivenire a conclusioni differenti in base alla concreta distribuzione dei poteri direttivi (ad esempio, la qualifica potrebbe essere ascritta all'Amministratore Delegato ed ai suoi primi riporti, individuati anche in relazione al settore di riferimento della UNI ISO 37301).

Le figure dell'organismo di governo e dell'alta direzione non sono presenti nel D.Lgs. n. 231/2001 e nelle Linee Guida di Confindustria. Anche nell'ottica di addivenire ad un coordinamento tra le due normative, può tuttavia rinvenirsi un profilo di coincidenza tra l'organismo di governo della UNI ISO 37301 e l'"organo dirigente" di cui all'art. 6, comma 1, lett. a) del D.Lgs. n. 231/2001.

Quanto al ruolo da assegnare all'organismo di governo e all'alta direzione, la UNI ISO 37301 stabilisce che essi "*devono dimostrare leadership e impegno in riferimento al sistema di gestione per la compliance:*

- *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:

- *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 (vedere punto 5.3.2);*
- *assicurare che sia definito un sistema per far emergere e trattare le preoccupazioni, in conformità al punto 8.3"* 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. Per l'alta direzione non vi è, allo stato, alcun riferimento terminologico analogo nel D.Lgs. 231/2001 e/o nelle Linee Guida di Confindustria, prospettandosi pertanto la presenza di un nuovo "attore" nel "sistema 231", da identificarsi sulla base della UNI ISO 37301.

5.1.2 Cultura della compliance

La norma UNI ISO 37301 stabilisce i seguenti requisiti sulla "cultura della compliance":

"L'organizzazione deve sviluppare, mantenere e promuovere una cultura della compliance a tutti i livelli dell'organizzazione.

L'organismo di governo, 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.

L'alta direzione deve incoraggiare comportamenti tali da creare e supportare la compliance. Essa deve prevenire e non tollerare comportamenti in grado di compromettere la compliance stessa".

Nell'ottica di valorizzare la cultura della compliance - intesa come 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 - si riportano i fattori in grado di supportarne lo sviluppo, che includono tra gli altri (cfr. punto A.5.1.2 della UNI ISO 37301):

- un chiaro insieme di valori resi pubblici;
- un management che attua e rispetta attivamente e visibilmente i valori;
- una formazione su base continua sulla compliance, compresi aggiornamenti della formazione a tutti il personale e alle parti interessate rilevanti;
- una comunicazione su base continua delle questioni relative alla compliance;
- un esercizio della disciplina pronto e proporzionato nel caso di violazioni di obblighi di compliance volontari o negligenti.

Benché all'interno del D.Lgs. n. 231/2001 non vi sia un esplicito e specifico richiamo al requisito della cultura della compliance, esso può ritenersi insito nell'approccio metodologico declinato dal Legislatore del 2001. Nel momento in cui l'esimente da responsabilità trova fondamento, tra gli altri, nell'adozione ed efficace attuazione del Modello Organizzativo - da intendersi, lo si ricorda, quale complesso delle misure e dei presidi di controllo volti a prevenire la commissione dei reati-presupposto mediante la mitigazione del rischio a un livello accettabile - si attribuisce rilevanza decisiva all'auto-organizzazione degli Enti in chiave penal-prevenitva. In questa prospettiva, il Modello Organizzativo, proprio nella sua consistenza regolatoria endoaziendale, è destinato a costituire il primario riferimento delle regole e dei principi da seguire e, pertanto, a divenire rappresentazione documentata della "cultura di compliance" esistente in seno all'Ente.

Infatti, nel novero dei fattori di sviluppo declinati dalla UNI ISO 37301 si rinvengono elementi e protocolli richiamati espressamente sia nel D.Lgs. 231/2001 che nelle Linee Guida Confindustria:

- il “chiaro insieme di valori resi pubblici” è nozione sostanzialmente sovrapponibile al “Codice Etico" richiamato dalle Linee Guida Confindustria;
- la formazione e la comunicazione costituiscono, a loro volta, protocolli generali a cui è riservata
- apposita disciplina nelle Linee Guida Confindustria;
- la comunicazione delle questioni relative alla compliance trova corrispondenza in uno dei contenuti minimi obbligatori dei Modelli Organizzativi, ossia la previsione di “obblighi di informazione nei confronti dell’organismo deputato a vigilare sul funzionamento e l’osservanza dei modelli” (cfr., art. 6, comma 2, lett. d, D.Lgs. 231/2001), potendosi peraltro sussumere nell’alveo delle "questioni relative alla compliance” anche l’istituto del whistleblowing disciplinato dall’art. 6, comma 2-bis, del D.Lgs. 231/2001, che sancisce la necessità di approntare e promuovere un efficace sistema di trasmissione delle segnalazioni di condotte indebite;
- l’esercizio della disciplina menzionato dalla UNI ISO 37301 trova, a sua volta, corrispondenza nel “sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello” cfr., art. 6, comma 2, lett. e, D.Lgs. 231/2001).

5.1.3 Governance della compliance

La UNI ISO 37301 stabilisce che “*L'organismo di governo e l'alta direzione devono assicurare che siano attuati i seguenti principi:*

- *accesso diretto all'organismo di governo da parte della funzione di compliance;*
- *indipendenza della funzione di compliance;*
- *appropriate autorità e competenza della funzione di compliance*.”

L'accesso diretto può comprendere: una linea diretta di reporting all'organismo di governo, l'emissione di rapporti periodici all’organismo di governo e la partecipazione nelle riunioni di quest'ultimo. L'indipendenza significa l'assenza di indebite interferenze o pressioni, o entrambe, in riferimento alle attività della funzione di compliance”.

Come noto, il D.Lgs. n. 231/2001 si limita a delineare, in linea generale, i principali compiti dell’Organismo di Vigilanza (la vigilanza sul funzionamento e l’osservanza del Modello Organizzativo e la cura del relativo aggiornamento), fornendo cenni in merito alle sue caratteristiche e requisiti.

Sul punto, vanno considerate le indicazioni delle Linee Guida Confindustria, segnatamente quelle riepilogative ed illustrative dei requisiti dell’Organismo di Vigilanza.

Il richiamo all’accesso diretto all’organismo di governo trova, difatti, riscontro nel requisito della “autonomia” declinato da Confindustria, a mente del quale occorre, tra gli altri, prevedere che l’OdV riporti al massimo vertice operativo aziendale, a cui è peraltro destinato il report periodico dell’Organismo, da inviare all’organo dirigente con cadenza almeno semestrale.

Anche per le “appropriate autorità” della Funzione Compliance rileva il requisito della “autonomia” dell’OdV, nelle sue ulteriori accezioni riportate dalle Linee Guida Confindustria (i) autonomia sul piano gerarchico e organizzativo, consistente nella necessità che “*la posizione dell’OdV nell’ambito dell’ente deve garantire l’autonomia dell’iniziativa di controllo da ogni forma di interferenza o condizionamento da parte di qualunque componente dell’ente e, in particolare, dell’organo dirigente*”; (ii) autonomia sul piano funzionale ed operativo, da intendersi quale facoltà di stabilire senza condizionamenti o sindacati esterni le regole di funzionamento, mediante redazione di un regolamento interno, così come l’ambito delle proprie attività; (iii) autonomia sul piano economico, dovendosi stanziare un budget a disposizione

dell'OdV per l'espletamento delle attività che richiedessero l'esercizio del potere di spesa (ad es., per il ricorso a consulenti esterni, l'adesione a newsletter normative, ecc.); (iv) autonomia sul piano ispettivo, essendo previsto che *" l'OdV deve avere libero accesso presso tutte le funzioni della società - senza necessità di alcun consenso preventivo - onde ottenere ogni informazione o dato ritenuto necessario per lo svolgimento dei compiti previsti dal decreto 231*".

L'indipendenza e la competenza, che la UNI ISO 37301 associa alla Funzione Compliance, sono requisiti validi (rectius, necessari) anche per l'Organismo di Vigilanza. Quanto all'indipendenza, le Linee Guida di Confindustria statuiscono che occorre scongiurare il rischio di condizionamenti o mancanza di terzietà in capo all'Organismo nel suo complesso, così come rispetto ai singoli membri. Quanto all'Organismo, non dovrebbero essergli attribuiti compiti operativi, esulanti dalla vigilanza sul Modello Organizzativo. Quanto ai singoli membri, si afferma con chiarezza che "*il modello non deve sovrapporre la figura del controllore e del controllato. I compiti dell'OdV non possono essere esercitati nei propri confronti ma esigono che il* soggetto vigilato sia distinto dal componente dell'OdV". Non potendosi, afferma Confindustria, attribuire ad eventuali membri interni una assoluta indipendenza, in caso di organo collegiale il grado di indipendenza dell'Organismo va valutato nella sua globalità.

L'organismo è interno all'ente e deve essere dotato di autonomi poteri di iniziativa e di controllo. E proprio quest'ultimo riferimento agli "autonomi poteri" può ritenersi satisfattivo, almeno in parte, del richiamo alla "appropriata autorità" di cui alla UNI ISO 37301[2].

Per quanto attiene alle "competenze", le Linee Guida Confindustria richiamano il concetto di "professionalità", da intendersi riferita "al bagaglio di strumenti e tecniche che l'OdV deve possedere per poter svolgere efficacemente la propria attività", i quali riguardano in primis i controlli interni e il diritto penale.

5.2 Politica per la compliance in relazione al Codice etico

Il requisito della "politica per la compliance", presente nella norma UNI ISO 37301, non trova un espresso corrispondente nell'ambito del D.Lgs. n. 231/2001. Un riferimento può, quindi, andare al Codice Etico e di Comportamento, indicato dalle Linee Guida Confindustria quale uno dei principali Protocolli generali di controllo sia per i reati dolosi che per quelli colposi. I due documenti pur avendo finalità non del tutto sovrapponibili, è auspicabile che dialoghino e si integrino reciprocamente. In particolare, Confindustria statuisce che "*l'adozione di principi etici, ovvero l'individuazione dei valori aziendali primari cui l'impresa intende conformarsi è espressione di una determinata scelta aziendale e costituisce la base su cui impiantare il sistema di controllo preventivo. Deve costituire profilo di riferimento per ogni realtà imprenditoriale la raccomandazione di un elevato standard di professionalità, nonché il divieto di comportamenti che si pongano in contrasto con le disposizioni legislative e con i valori deontologici*".

Al pari di quanto sopra, l'appendice alla norma UNI ISO 37301, al punto A.5.2, definisce la politica per la compliance come necessario strumento per stabilire "*i principi generali e l'impegno all'azione per un'organizzazione al fine di conseguire la compliance*".

È evidente che la norma UNI ISO 37301, oltre ad utilizzare una terminologia diversa, risulti meno dettagliata rispetto a quanto stabilito dalle Linee Guida di Confindustria, le quali, peraltro,

[2] La governance per la compliance di cui alla UNI ISO 37301 non può essere confusa o assimilata all'OdV di cui alla 231.

dedicano un intero capitolo al Codice Etico e/o di Comportamento (vedere *capitolo III CODICE ETICO O DI COMPORTAMENTO E SISTEMA DISCIPLINARE*).

La UNI ISO 37301, infatti, stabilisce al riguardo quanto segue:

"*L'organismo di governo e l'alta direzione devono stabilire una politica per la compliance che:*

a) sia appropriata alle finalità dell'organizzazione;

b) costituisca un quadro di riferimento (framework) per fissare gli obiettivi per la compliance;

c) comprenda l'impegno a soddisfare i requisiti applicabili;

d) comprenda l'impegno per il miglioramento continuo del sistema di gestione per la compliance.

La politica per la compliance deve:

- *essere allineata ai valori, obiettivi e strategie dell'organizzazione;*
- *richiedere il rispetto degli obblighi di compliance dell'organizzazione;*
- *supportare i principi di governance della compliance in conformità al punto 5.1.3;*
- *fare riferimento alla funzione di compliance e descriverla;*
- *delineare le conseguenze di non essere conformi agli obblighi, politiche, processi e procedure relativi alla compliance;*
- *incoraggiare l'emergere di preoccupazioni e proibire ogni forma di ritorsione;*
- *essere scritta in un linguaggio diretto in modo che il personale possa comprenderne facilmente principi e intenti;*
- *essere attuata e fatta rispettare in modo appropriato;*
- *essere disponibile come informazione documentata;*
- *essere comunicata all'interno dell'organizzazione;*
- *essere disponibile alle parti interessate, per quanto appropriato*".

5.3 Ruoli, responsabilità e autorità

5.3.1 Organismo di governo e alta direzione

Ai vertici aziendali compete di guidare e sensibilizzare tutti, coloro che operano all'interno dell'organizzazione al rispetto del Modello, del Codice Etico e dei protocolli annessi, così da garantire e supportare l'efficacia del sistema di gestione per la compliance adottato dall'ente.

La UNI ISO 37301, in proposito, stabilisce quanto segue: "*L'organismo di governo e l'alta direzione devono assicurare che le responsabilità e le autorità per i ruoli pertinenti siano assegnate e comunicate*

all'interno dell'organizzazione." Per quanto attiene l'individuazione dell'Alta Direzione e dell'Organo Direttivo nell'ambito del D.Lgs. n. 231/2001, si rinvia a quanto osservato nell'ambito del par. 5.1.1.

L'organismo di governo e l'alta direzione devono assegnare le responsabilità e autorità per:

a) assicurare che il sistema di gestione per la compliance sia conforme ai requisiti del presente documento;

Rispetto a tale compito, il riferimento in ambito 231 può essere rinvenuto nell'art. 6, comma 1, lett. b, del Decreto 231, laddove si subordina l'esenzione da responsabilità, tra gli altri, alla nomina di un organismo

- dotato di autonomi poteri di iniziativa e di controllo - cui assegnare il compito di vigilare sul funzionamento e l'osservanza del Modello Organizzativo: la promozione della conformità ai requisiti della UNI ISO 37301, difatti, presenta sostanziali analogie, sul piano concettuale e teleologico, con la verifica della adeguatezza del Modello Organizzativo a prevenire la commissione dei reati-presupposto richiamati dal medesimo Decreto 231.

b) riferire all'organismo di governo e all'alta direzione sulle prestazioni del sistema di gestione per la compliance.

Sul punto, pur in assenza di previsioni di carattere legislativo, certamente rilevante è il richiamo alle Linee Guida Confindustria, laddove contemplano un periodico flusso informativo, con cadenza almeno semestrale, dell'OdV verso l'organo amministrativo (ed al Collegio Sindacale) al fine di rappresentare le attività di verifica e controllo svolte e i relativi esiti (cfr., Linee Guida Confindustria, pag. 81).

"L'organismo di governo deve:

- *assicurare che l'alta direzione sia misurata a fronte del raggiungimento degli obiettivi per la compliance;*
- *esercitare una supervisione sull'alta direzione in riferimento alle attività operative del sistema di gestione per la compliance.*

L'alta direzione deve:

- *allocare risorse appropriate e adeguate per stabilire, sviluppare, attuare, valutare, mantenere e migliorare il sistema di gestione per la compliance;*
- *assicurare che siano in funzione sistemi efficaci di reporting tempestivo sulle prestazioni relative alla compliance;*
- *assicurare l'allineamento tra i traguardi di natura strategica e operativa e gli obblighi di compliance;*
- *stabilire e mantenere meccanismi di accountability, comprese azioni disciplinari e relative conseguenze;*
- *assicurare l'integrazione delle prestazioni relative alla compliance nelle valutazioni delle prestazioni del personale".*

Questa parte del requisito non trova una perfetta correlazione nell'ambito del D.Lgs. 231/2001 e dei Modelli Organizzativi, in ragione della più volte segnalata assenza delle figure dell'organismo di governo e dell'Alta Direzione, richiamate dalla UNI ISO 37301. Ciò premesso, va tuttavia segnalato che analoghe prescrizioni si rinvengono in sostanza anche nel Decreto e nelle Linee Guida: (i) lo stanziamento di un budget annuale in favore dell'OdV costituisce uno degli strumenti per

promuovere la necessaria autonomia dell'Organismo (cfr., Linee Guida Confindustria, pag. 77-81); (ii) in aggiunta alle risorse economiche stanziate dall'organo amministrativo, all'OdV va riconosciuta anche la facoltà di avvalersi dell'ausilio delle strutture della società e di consulenti esterni (cfr., Linee Guida Confindustria, pag. 81); (iii) la presenza di un Sistema Disciplinare, volto a sanzionare le violazioni del Modello Organizzativo, costituisce, secondo quanto indicato dallo stesso Legislatore, uno dei contenuti minimi del Modello Organizzativo (cfr., art. 6, comma 2, lett. e).

5.3.2 Funzione di compliance e Organismo di Vigilanza

La UNI ISO 37301 riserva un ruolo centrale alla "Funzione di Compliance", cui è assegnata la responsabilità "*delle attività operative del sistema di gestione per la compliance*".

Fermo restando che l'obbligo di conformità legislativa è esteso e diffuso all'intera organizzazione, dall'Organo di governo a tutti coloro che lavorano a nome e per conto dell'organizzazione stessa, la funzione di Compliance è centrale nella garanzia del coordinamento interno all'azienda del rispetto della conformità legislativa e può essere letta su piani diversi." Un primo livello è quello interno all'organizzazione, nella lettura più stretta alla sola norma UNI ISO 37301, dove il ruolo di Responsabile della funzione Compliance potrebbe essere associato anche alla figura del Compliance Manager[3] e relative declinazioni o a figure analoghe che rispondano ai requisiti della norma stessa.

In un secondo livello, correlato al D.Lgs. n. 231/2001, tale ruolo va ricercato, quanto meno in prima battuta, con l'Organismo di Vigilanza delineato dall'art. 6, comma 1, lett. b), del Decreto. A ben vedere, tuttavia, i due organismi sono assegnatari di compiti e funzioni non del tutto sovrapponibili e coincidenti. Se, infatti, l'OdV ha - anzi, dovrebbe avere - esclusivamente compiti di vigilanza e di cura dell'aggiornamento del Modello, dovendosi evitare qualsiasi assegnazione di compiti operativi (cfr., in particolare le Linee Guida Confindustria, pag. 77 e ss.), la UNI ISO 37301 assegna alla Funzione Compliance anche adempimenti non riconducibili nell'alveo della mera vigilanza ma che si caratterizzano per una spiccata consistenza operativa.

Si riporta, sul punto, quanto indicato nel requisito 5.3.2:

- *facilitare l'identificazione degli obblighi di compliance;*

L'attività di monitoraggio normativo pare sussumibile in quelle di spettanza dell'OdV. L'obbligo di vigilanza sull'idoneità del Modello e di cura del suo aggiornamento, difatti, non può prescindere dalla conoscenza della normativa applicabile e delle relative novità e modifiche, in presenza delle quali è chiamato a inoltrare all'organo amministrativo specifiche proposte di aggiornamento del Modello.

- *documentare il processo di valutazione dei rischi di compliance (vedere punto 4.6);*

Il processo di valutazione dei rischi esula dai compiti dell'OdV. Se è vero, difatti, che la vigilanza sull'adeguatezza del Modello, intesa quale sua idoneità a prevenire la commissione dei reati- presupposto mediante la riduzione del rischio a un livello accettabile, include inevitabilmente una prognosi sulla completezza dei risultati del risk assessment, è altrettanto vero che quest'ultimo non dovrebbe essere svolto dall'Organismo di Vigilanza. In caso contrario, sarebbe prospettabile una

[3] Si veda anche la norma UNI 11883:2022 - Attività professionali non regolamentate - Figure professionali operanti nell'ambito della gestione per la compliance - Requisiti di conoscenza, abilità, autonomia e responsabilità, 06/10/2022

situazione di conflitto di interesse, poiché l'OdV si troverebbe a doversi pronunciare sull'adeguatezza di un'attività svolta da sé stesso.

- *allineare il sistema di gestione per la compliance agli obiettivi per la compliance;*

Anche tale funzione esula dall'ambito di intervento dell'OdV, poiché implica un intervento di carattere operativo che non pare compatibile con l'attività di vigilanza propria dell'Organismo.

- *monitorare e misurare le prestazioni relative alla compliance;*

Laddove si ritenga che tale funzione riguardi la verifica sui comportamenti dei destinatari del sistema di gestione per la compliance, può concludersi nel senso della sostanziale sovrapponibilità di questo compito con la vigilanza sull'osservanza del Modello Organizzativo, richiamata dall'art. 6, comma 1, lett. b) del Decreto.

- *analizzare e valutare le prestazioni del sistema di gestione per la compliance per identificare ogni esigenza di azioni correttive;*

La funzione può ritenersi coincidente con i compiti di vigilanza sull'adeguatezza del Modello Organizzativo e di cura dell'aggiornamento dello stesso, richiamati dall'art. 6, comma 1, lett. b) del Decreto. Ed in effetti, anche le Linee Guida di Confindustria chiariscono che tra i compiti dell'OdV vi è quello di "*formulazione delle proposte all'organo dirigente per gli eventuali aggiornamenti ed adeguamenti del Modello, da realizzare mediante le modifiche ed integrazioni rese necessarie da: significative violazioni delle prescrizioni del Modello stesso; rilevanti modificazioni dell'assetto interno della società, delle attività di impresa o delle relative modalità di svolgimento; modifiche normative*" (cfr., Linee Guida Confindustria, pagg. 80-81).

- *stabilire un reporting relativo alla compliance e un sistema documentale;*

Nel declinare i contenuti minimi del Modello Organizzativo, l'art. 6, comma 2, lett. d) prescrive la necessità di prevedere obblighi di informazione nei confronti dell'OdV, con l'obiettivo di promuovere la conoscenza, da parte dell'Organismo, delle informazioni e dei documenti necessari o comunque utili all'efficace espletamento dell'incarico. Se, quindi, è confermata anche in ambito 231 la rilevanza di progettare ed attuare un idoneo sistema di flussi informativi, il Decreto 231 non assegna espressamente tale compito all'OdV, delineandolo come uno dei contenuti del Modello, come tale approvato dall'organo dirigente. Va, tuttavia, considerato che l'Organismo, nell'esercizio dei propri "*autonomi poteri di iniziativa e di controllo*" potrebbe decidere di integrare le regole del Modello Organizzativo mediante la definizione di un più puntuale sistema di flussi informativi, individuando anche la relativa periodicità e gli *owner* del flusso.

Quanto ai flussi "in uscita", si è già ricordato che le Linee Guida Confindustria raccomandano un flusso informativo almeno semestrale verso l'organo amministrativo ed il Collegio Sindacale, al fine di rappresentare le attività di verifica e controllo svolte dall'OdV e i relativi esiti (cfr., Linee Guida Confindustria, pag. 81).

- *assicurare che il sistema di gestione per la compliance sia riesaminato a intervalli pianificati (vedere punti 9.2 e 9.3);*

L'attività in esame trova una corrispondenza con i compiti dell'OdV rispetto al requisito 9.2., riguardante gli audit interni, atteso che le attività di verifica costituiscono uno degli elementi centrali dell'operato dell'Organismo. Come si dirà in merito al requisito 9.2., in seno al Decreto 231

ed alle Linee Guida Confindustria non è presente una specifica disciplina in materia di programmazione delle attività di verifica.

Per quanto attiene il requisito 9.3, se è vero che all'OdV è ascrivibile il compito di trasmettere la propria relazione periodica all'organo dirigente, va considerato che l'Organismo non dispone dell'autorità e/o degli strumenti per "assicurare" che la relazione sia anche esaminata, potendo tutt'al più svolgere un'attività di mero controllo. In ogni caso, la programmazione delle attività di verifica da parte dell'OdV è una prassi consolidata richiamata anche dalle prassi consolidate[4].

- *stabilire un sistema per far emergere preoccupazioni e assicurare che quest'ultime siano affrontate.*

Anche in tal caso, le analogie con il Decreto 231 sono parziali.

Quest'ultimo, difatti, prevede l'obbligo per gli enti, che siano dotati di un Modello Organizzativo, di implementare appositi meccanismi e canali informativi volti a consentire la segnalazione di potenziali condotte indebite (whistleblowing).

A ben vedere, tuttavia, il sistema di segnalazione richiamato dal Decreto 231 è uno dei contenuti obbligatori del Modello Organizzativo, come tale approvato dall'organo dirigente, e non rientra nelle prerogative o nei compiti dell'OdV.

"La funzione di compliance deve esercitare una supervisione affinché:

- *le responsabilità riguardanti il conseguimento degli obblighi di compliance identificati siano allocate in modo appropriato all'interno dell'organizzazione;*
- *gli obblighi di compliance siano integrati in politiche, processi e procedure;*
- *tutte le persone pertinenti siano formate, come richiesto;[5]"*
- *siano stabiliti indicatori di prestazione relativi alla compliance.*

La correlazione con l'OdV non sembra prospettabile in questo caso, poiché l'attività di "supervisione" non pare possa essere circoscritta ad un intervento di mero controllo, comportando viceversa un contributo ulteriore anche in termini di sovrintendenza operativa delle attività, come tale non associabile al ruolo dell'OdV, normativamente limitato alla sola "vigilanza".

"La funzione di compliance deve assicurare:

- *personale con accesso alle risorse relative alle politiche, processi e procedure riguardanti la compliance;*
- *assistenza all'organizzazione su questioni correlate alla compliance. [6]"*

Queste funzioni paiono implicare la necessità, rispettivamente, di un intervento operativo nella promozione delle attività di comunicazione e di un contributo di natura "consulenziale" verso l'organizzazione. Per tali aspetti, non sembrano trovare una correlazione nella sfera di intervento dell'OdV.

[4] "Principi consolidati per la redazione dei modelli organizzativi e l'attività dell'organismo di vigilanza e prospettive di revisione del d.lgs. 8 giugno 2001, n. 231"
[5] UNI ISO 37301, punto 5.3
[6] UNI ISO 37301, punto 5.3

"L'organizzazione deve assicurare che alla funzione di compliance sia dato accesso a:

- *i decisori senior e l'opportunità di contribuire sin dalle fasi iniziali dei processi decisionali;*
- *tutti i livelli dell'organizzazione;*
- *tutto il personale, informazioni documentate e dati necessari;*
- *consulenza competente in riferimento a leggi, regolamenti, codici e specifiche organizzative pertinenti"*[7].

In ambito 231, un riferimento utile è costituito, *in primis*, dalla richiamata necessità che l'OdV sia dotato "di autonomi poteri di iniziativa e di controllo" (art. 6, comma 1, lett. b, Decreto 231). Le Linee guida Confindustria declinano la "autonomia" dell'Organismo in più prospettive, tra cui: (i) libero accesso presso tutte le funzioni della società - senza necessità di alcun consenso preventivo - onde ottenere ogni informazione o dato ritenuto necessario per lo svolgimento dei compiti previsti dal decreto 231; (ii) facoltà di utilizzare il budget stanziato dall'organo dirigente per il ricorso a consulenti.

Il riferimento alla possibilità della Funzione Compliance di contribuire ai processi decisionali non può, invece, trovare una correlazione, attesa la più volte riferita esigenza di evitare di coinvolgere l'OdV in attività operative "*che, facendolo partecipe di decisioni dell'attività dell'ente, potrebbero pregiudicare la serenità di giudizio al momento delle verifiche*"[8].

In sintesi, dalla disanima sopra riportata è quindi evidente quanto sia importante che, anche nel caso di imprese che abbiamo implementato un Modello 231, la figura di Responsabile della funzione Compliance sia ricoperta da una funzione interna all'azienda ovvero nominata dall'azienda nell'ambito della propria organizzazione (ad esempio, Compliance Manager, Internal Audit, ecc.) distinto rispetto all'OdV che svolge un ruolo autonomo ed indipendente per le competenze e le responsabilità espressamente assegnate a questo organismo dal D.Lgs.231 e declinate dalle Linee Guida di Confindustria.

5.3.3 Management

La norma UNI ISO 37301 stabilisce che: *"Il management deve essere responsabile in riferimento alla compliance nell'ambito delle proprie aree di responsabilità:*

- *cooperando e supportando la funzione di compliance e l'incoraggiamento del personale a fare altrettanto;*
- *assicurando che il personale sotto il proprio controllo sia conforme agli obblighi, politiche, processi e procedure di compliance dell'organizzazione;*
- *identificando e comunicando i rischi di compliance nelle proprie attività operative;*
- *integrando degli obblighi di compliance nelle prassi e procedure di business esistenti nell'ambito delle proprie aree di responsabilità;*
- *partecipando e supportando le attività di formazione in materia di compliance;*

[7] UNI ISO 37301, punto 5.3
[8] GIP Tribunale di Roma, 4 aprile 2003

- *sviluppando consapevolezza, da parte del personale, circa gli obblighi di compliance, indirizzando le persone a soddisfare i requisiti di formazione e competenza;*

- *incoraggiando il proprio personale a far emergere preoccupazioni relative alla compliance, supportandoli e impedendo ogni forma di ritorsione;*

- *partecipando attivamente alla gestione e risoluzione di incidenti e questioni correlati alla compliance, come richiesto;*

- *assicurando che, una volta sia stata identificata l'esigenza di azioni correttive, quest'ultime siano raccomandate e attuate".*

In ambito 231, salvo il riferimento all'adozione ed efficace attuazione del Modello Organizzativo a cura dell'organo dirigente, manca un riferimento esplicito ai compiti ed alle funzioni del management rispetto alla compliance.

Ciò premesso, le Linee Guida di Confindustria si soffermano sulla struttura del Modello Organizzativo ed in particolare sulle componenti di un idoneo sistema di controllo preventivo, i cc.dd. "Protocolli". Sebbene non si rinvenga una compiuta sovrapponibilità con quanto indicato dalla UNI ISO 37301, sono ravvisabili alcune analogie, ove si consideri che nelle Linee Guida Confindustria:

- è sancita la necessità di informare le risorse aziendali sui Protocolli che costituiscono il Modello e, in genere, su "*tutto quanto contribuisca a fare trasparenza nell'operare quotidiano*"[9];
- assume rilevanza l'adozione di procedure manuali ed informatiche atte ad orientare i comportamenti dei propri destinatari, anche nell'assolvimento degli obblighi di compliance, costituisce un importante presidio di controllo ai fini del buon funzionamento del sistema di gestione adottato dall'ente (Cfr. Linee Guida di Confindustria, pag. 52);
- particolare risalto è attribuito alle iniziative in materia di formazione, rispetto a cui dovrebbe porsi l'obbligo di partecipazione e contemplarsi una verifica di apprendimento dei contenuti del training;
- trova apposita disciplina il whistleblowing, con l'obiettivo di incentivare il contributo delle risorse e favorire l'emersione di condotte o pratiche indebite di cui siano venuti a conoscenza, prevedendo altresì specifiche forme di tutela del segnalante anche rispetto a eventuali atti discriminatori o ritorsivi.

5.3.4 Personale

Con riguardo al Personale, la UNI ISO 37301 prevede espressamente che le risorse debbano:

"- aderire agli obblighi, politiche, processi e procedure relativi alla compliance dell'organizzazione;

- *riferire preoccupazioni, questioni e malfunzionamenti relativi alla compliance;*

- *partecipare alla formazione, come richiesto".*

All'interno del Decreto 231 non si rinvengono espliciti riferimenti ad obblighi analoghi in capo al Personale.

[9] Linee Guida di Confindustria, pag. 53

A ben vedere, le disposizioni del Decreto 231 in materia di whistleblowing non prospettano un "dovere" di segnalazione in capo ai destinatari, limitandosi a prescrivere che i Modelli prevedano "uno o più canali che consentano (...) di presentare (...) segnalazioni". In altri termini, non vi è allo stato alcun obbligo legislativo di inoltrare una segnalazione in caso si venga a conoscenza di condotte indebite.

Diversamente, le Linee Guida di Confindustria dispongono che l'obbligo di informazione all'OdV va esteso "*ai dipendenti che vengano in possesso di notizie relative alla violazione del Modello o alla commissione dei reati, in specie all'interno dell'ente, ovvero a pratiche non in linea con le norma di comportamento che l'ente è tenuto ad emanare nell'ambito del Modello disegnato dal decreto 231*" (cfr., Linee Guida Confindustria, pag. 91).

Quanto alla formazione, un elemento di correlazione si rinviene nelle Linee Guida di Confindustria, "*laddove si precisa che deve essere sviluppato un adeguato programma di formazione modulato in funzione dei livelli dei destinatari; è opportuno prevedere il contenuto dei corsi di formazione, la loro periodicità, l'obbligatorietà della partecipazione ai corsi, i controlli di frequenza e di qualità sul contenuto dei programmi, l'aggiornamento sistematico dei contenuti degli eventi formativi in ragione dell'aggiornamento del Modello*"[10] .

6 Pianificazione

6.1 Azioni per affrontare rischi e opportunità, anche in relazione ai presidi di controllo 231

Con riguardo alla pianificazione del sistema di gestione per la compliance, la UNI ISO 37301 stabilisce che "*l'organizzazione deve considerare i fattori di cui al punto 4.1 Comprendere l'organizzazione e il suo contesto ed i requisiti di cui al punto 4.2 Comprendere le esigenze e le aspettative delle parti interessate e determinare i rischi e le opportunità che è necessario affrontare per:*

- *fornire assicurazione che il sistema di gestione per la compliance possa conseguire gli esiti attesi;*
- *prevenire, o ridurre, gli effetti indesiderati.*
- *conseguire il miglioramento continuo.*

All'interno del Decreto 231 non si ravvisa una indicazione analoga, potendosi fare riferimento unicamente a quanto previsto, in linea del tutto generale, circa la necessità di adottare ed attuare efficacemente un Modello Organizzativo idoneo a prevenire la commissione dei reati-presupposto richiamati dal Decreto 231, che possono essere messi in relazione con "gli effetti indesiderati" di cui alla UNI ISO 37301. Sebbene non vi sia un esplicito riferimento al "miglioramento continuo", il quale, come noto, costituisce un fattore di matrice precipuamente tecnica e non giuridica, va comunque segnalato che il legislatore ha attribuito espressa rilevanza alla necessità di curare, attraverso l'impulso dell'OdV (art. 6, comma 1, lett b, del Decreto 231), l'aggiornamento del Modello Organizzativo, da intendersi - come chiarito anche dalle Linee Guida Confindustria - in una prospettiva di sua evoluzione e miglioramento

[10] Linee Guida Confindustria, pagg. 53-56).

in considerazione di novità normative, modifiche organizzative o significative violazioni del Modello stesso.

"Nel pianificare il sistema di gestione per la compliance, l'organizzazione deve considerare:

- *i propri obiettivi per la compliance* (vedere punto 6.2);
- *gli obblighi di compliance identificati* (vedere punto 4.5)*;*
- *i risultati del processo di valutazione dei rischi di compliance* (vedere punto 4.6)*"*[11]*.*

Non si ravvisano, sul piano legislativo, norme del tutto sovrapponibili a quelle della UNI ISO 37301. Alcune analogie possono riscontrarsi dall'esame dell'art. 6, comma 2, del Decreto 231, che individua i contenuti minimi del Modello Organizzativo:

a) individuare le attività nel cui ambito possono essere commessi reati;

b) prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire;

c) individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei reati;

d) prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento

e l'osservanza del Modello;

e) introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello.

I contenuti sub a) e b) implicano la necessaria considerazione dei risultati del risk assessment svolto preliminarmente alla progettazione del Modello.

Le Linee Guida di Confindustria richiamano, in relazione alla fase di progettazione del sistema di controllo "*la valutazione del sistema esistente all'interno dell'ente per la prevenzione dei reati ed il suo eventuale adeguamento in termini di capacità di contrastare efficacemente, ossia ridurre ad un livello accettabile, I rischi identificati*" [12]

"L'organizzazione deve pianificare:

a) le azioni per affrontare tali rischi e opportunità;

b) le modalità per:

1) integrare e attuare le azioni nei processi del proprio sistema di gestione per la compliance;

2) valutare l'efficacia di tali azioni"[13].

Rispetto a tale requisito, non si riscontrano punti di esplicita correlazione con il Decreto 231 o le Linee Guida di Confindustria.

[11] UNI ISO 37301 punto 6.1
[12] Linee Guida Confindustria, pag. 50.
[13] UNI ISO 37301 punto 6.1

6.2 Obiettivi per la compliance e pianificazione per il loro raggiungimento

La UNI ISO 37301 prevede che "*L'organizzazione deve stabilire gli obiettivi per la compliance relativi alle funzioni e ai livelli pertinenti.*

Gli obiettivi per la compliance devono:

a) essere coerenti con la politica per la compliance;

b) essere misurabili (se praticabile);

c) tenere in considerazione i requisiti applicabili;

d) essere monitorati;

e) essere comunicati

f) essere aggiornati per quanto appropriato;

g) essere disponibili come informazioni documentate.

Nel pianificare come raggiungere i propri obiettivi per la compliance, l'organizzazione deve determinare:

- *cosa sarà fatto;*
- *quali risorse saranno richieste;*
- *chi ne sarà responsabile;*
- *quando sarà completato;*
- *come saranno valutati i risultati*".

Nell'ambito del Decreto 231 e delle Linee Guida Confindustria non si ravvisa una disciplina specifica riservata agli obiettivi. Ed a ben vedere, l'obiettivo che è associato alla adozione ed efficace attuazione del Modello Organizzativo è principalmente quello di prevenire la commissione dei reati-presupposto (art. 6, comma 1, lett. A).

Le Linee Guida Confindustria indicano, quale obiettivo dell'attività di progettazione del sistema di controllo, la costruzione ed attuazione di un sistema in grado di ridurre il rischio di commissione dei reati ad un livello "accettabile". La nozione di "rischio accettabile" è diversamente definita in relazione alla natura dolosa o colposa del reato: nel primo caso, la soglia di accettabilità consiste nella progettazione di un sistema di controllo che possa essere aggirato solo "fraudolentemente"; per i reati colposi, in assenza della coscienza e volontà di cagionare un determinato evento, la soglia di rischio accettabile "*è rappresentata dalla realizzazione di una condotta in violazione del modello organizzativo di prevenzione (...), nonostante la puntuale osservanza degli obblighi di vigilanza previsti dal Decreto 231 da parte dell'Organismo di Vigilanza*" (cfr., Linee Guida Confindustria, pag. 41).

Al di là di tali spunti, non si rinvengono puntuali previsioni o disposizioni concernenti la fase di programmazione e raggiungimento degli obiettivi.

6.3 Pianificazione delle modifiche

Ai sensi della UNI ISO 37301, "*Quando l'organizzazione determina l'esigenza di modifiche al sistema di gestione per la compliance, queste devono essere effettuate in modo pianificato.*

L'organizzazione deve prendere in considerazione:

- *le finalità delle modifiche e le loro potenziali conseguenze;*
- *la progettazione e l'efficacia operativa del sistema di gestione per la compliance;*
- *la disponibilità di risorse adeguate;*
- *l'allocazione o riallocazione di responsabilità e autorità.*

Il requisito può essere posto in correlazione con il disposto dell'art. 7, comma 4, lett. a) del Decreto 231, a mente del quale "*l'efficace attuazione del modello richiede una verifica periodica e l'eventuale modifica dello stesso quando sono scoperte significative violazioni delle prescrizioni ovvero quando intervengono mutamenti nell'organizzazione*".

Anche le Linee Guida di Confindustria confermano che il sistema di controllo, per poter operare efficacemente, "*deve tradursi in un processo continuo o comunque svolto con periodicità adeguate, da rivedere con particolare attenzione in presenza di cambiamenti aziendali ovvero di introduzione di nuovi reati presupposto della responsabilità dell'ente in via normativa*" (cfr., Linee Guida Confindustria, pag. 3940).

Il processo di modifica del Modello Organizzativo vede il coinvolgimento dell'Organismo di Vigilanza, che ha il compito, tra gli altri, di curarne l'aggiornamento. Come già indicato, l'adempimento di tale compito si traduce (cfr., Linee Guida Confindustria, pag. 80-81) nella "*formulazione delle proposte all'organo dirigente per gli eventuali aggiornamenti e adeguamenti del Modello, da realizzare mediante le modifiche e integrazioni rese necessarie da:*

- *significative violazioni delle prescrizioni del Modello stesso;*
- *rilevanti modificazioni dell'assetto interno della società, delle attività d'impresa o delle relative modalità di svolgimento;*
- *modifiche normative".*

In ambito 231, pertanto, la fase di pianificazione delle modifiche e la relativa metodologia non trovano esplicita valorizzazione.

7 Supporto

Al punto *5.3* "Ruoli, responsabilità e autorità" si è potuto approfondire l'organizzazione in riferimento alla sua Governance, con ruoli di indirizzo e controllo ovvero ruoli manageriali e ruoli più prettamente operativi di attuazione delle disposizioni aziendali. Nel presente punto si analizza come le disposizioni normative del sistema di gestione UNI ISO 37301 e le disposizioni contenute nel D. Lgs.231 possano darsi reciproco supporto, partendo da una definizione chiara che l'organizzazione dovrebbe mettere in atto in termini di risorse, competenze e consapevolezza.

7.1 Risorse

Il tema dell'organizzazione, sia in termini di risorse coinvolte nella corretta e adeguata gestione dei sistemi di gestione aziendale che in un adeguata organizzazione dei presidi di controllo ai fini della prevenzione dei reati che possono determinare la responsabilità amministrativa dell'Ente è sviluppato in modo speculare sia dalla UNI ISO 37301 che dalle Linee Guida di Confindustria.

La UNI ISO 37301, in proposito, stabilisce che "l'organizzazione deve determinare e fornire le risorse necessarie per l'istituzione, l'attuazione, il mantenimento e il miglioramento continuo del sistema di gestione per la compliance.", principio generale sviluppato in modo più esaustivo nei successivi punti *7.2* "*Competenza*" e punto *7.3* "*Consapevolezza".*

Nel medesimo senso le Linee Guida di Confindustria, le quali descrivono in modo più dettagliato questi ambiti facendo anche un distinguo tra la prevenzione dei reati cd "dolosi" dalla prevenzione di quelli cd. "colposi". Tali aspetti sono declinati al punto *4. Modalità operative di gestione dei rischi; A) Sistemi di controllo preventivo dei reati dolosi* dove, tra le componenti di un sistema di controllo preventivo generalmente ritenute necessarie per garantire l'efficacia del Modello viene richiesto, al secondo comma, un *Sistema organizzativo sufficientemente aggiornato, formalizzato e chiaro; "ciò vale soprattutto per l'attribuzione di responsabilità, le linee di dipendenza gerarchica e la descrizione dei compiti, con specifica previsione di principi di controllo quali, ad esempio, la contrapposizione di funzioni; deve inoltre tenere traccia della copertura temporale degli incarichi [...]. Nell'ambito del sistema organizzativo, attenzione andrà prestata ai sistemi premianti dei dipendenti. Essi sono necessari per indirizzare le attività del personale operativo e manageriale verso il conseguimento degli obiettivi aziendali. Tuttavia, se basati su target di performance palesemente immotivati ed inarrivabili, essi potrebbero costituire un velato incentivo al compimento di alcune delle fattispecie di reato previste dal decreto 231.*". Inoltre, al successivo quarto comma, si fa un esplicito riferimento ai "*Poteri autorizzativi e di firma*", altro requisito ritenuto indispensabile per una corretta Governance dell'organizzazione e per individuare in modo chiaro chi ha poteri per agire in nome e/o per conto dell'organizzazione (ad esempio, figure Apicali e manageriali) e chi, non avendo poteri di autorizzazione e firma formalmente attribuiti, può operare solamente sotto la supervisione e il controllo di un suo superiore. Viene inoltre ricordato che i Poteri "*vanno assegnati in coerenza con le responsabilità organizzative e gestionali. Talune funzioni possono essere delegate a un soggetto diverso da quello originariamente titolare. Ma occorre definire preliminarmente in modo chiaro e univoco i profili aziendali cui sono affidate la gestione e la responsabilità delle attività a rischio reato, avendo riguardo anche al profilo dell'opponibilità delle procure a terzi. La delega deve costituire lo strumento per un più efficace adempimento degli obblighi imposti dalla legge all'organizzazione complessa, non per un agevole trasferimento di responsabilità.".*

Un tema importante su cui le Linee Guida di Confindustria si soffermano è legato al **potere di spesa**, per dare attuazione alla procura ovvero alla delega ricevuta. Su questo punto si chiarisce che "*può rivelarsi utile una puntuale indicazione delle soglie di approvazione delle spese effettuate dal delegato. In particolare, 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 dell'ente 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 limitazioni delle deleghe e dei poteri di spesa conferiti;*

- *preveda soluzioni dirette a consentire un controllo sull'esercizio dei poteri delegati;*
- *disponga l'applicazione di sanzioni in caso di violazioni 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.*

È, inoltre, importante prevedere un sistema coerente e integrato che comprenda tutte le deleghe o procure aziendali (comprese quelle in materia antinfortunistica ed in quella ambientale), periodicamente aggiornate alla luce sia delle modifiche normative, che delle eventuali variazioni nel sistema organizzativo aziendale." Merita una nota specifica, soprattutto per gli ambiti legislativi ma, indirettamente, anche per gli adempimenti richiesti dalla norma UNI ISO 37301 il tema della **documentabilità del sistema di procure e deleghe;** su questo ambito le Linee Guida di Confindustria recitano "*Sarebbe poi opportuno garantire la documentabilità del sistema di deleghe, al fine di rendere agevole una sua eventuale ricostruzione a posteriori.*"

Particolare enfasi viene poi attribuita a tale aspetto organizzativo nell'ambito del capitolo *4. Modalità operative di gestione dei rischi; B) Sistemi di controllo preventivo dei reati colposi in materia di tutela della salute e sicurezza sul lavoro e dell'ambiente dove*, ad integrazione di quanto già scritto nell'ambito dei reati dolosi, si dà enfasi al combinato disposto degli aspetti legislativi e, in particolare, a quanto previsto nell'art. 30, comma 3, d.lgs. n. 81/2008 in tema di sicurezza e salute dei lavoratori; alle figure "consulenziali" della sicurezza espressamente previste a supporto dell'organizzazione (RSPP, Medico Competente; RLS; etc.) oltre alle figure deputate alla prevenzione dei reati ambientali richiamati dall'articolo 25-undecies del decreto 231. In tema di delega per i reati colposi, si fa esplicito riferimento agli artt.16 e 17 del D.Lgs.81/2008 (delega e sub-delega di funzione) oltre ad affrontare lo spinoso tema delle deleghe ambientali per le quali occorre considerare che, a differenza della delega di funzioni disciplinata nel Testo Unico in materia di Salute e Sicurezza sul Lavoro, quella "ambientale" non è codificata dal Testo Unico Ambientale (d.lgs.152/2006).

Pertanto, è necessario fare riferimento alle pronunce giurisprudenziali, anche di legittimità, che hanno chiarito la specificità delle delega cd. ambientale rispetto a quella in materia antinfortunistica, prevedendo la necessità che il contenuto della delega sia chiaro e inequivoco e si riferisca espressamente alle misure di rispetto della normativa ambientale. In quest'ottica, la giurisprudenza ammette la validità della "delega ambientale" in presenza delle seguenti condizioni:

i) specificità e inequivoca indicazione dei poteri delegati;

ii) dimensioni dell'azienda (in una organizzazione complessa è impensabile non farvi ricorso);

iii) capacità tecnica e idoneità del soggetto delegato;

iv) autonomia (gestionale e finanziaria) ed effettivi poteri del delegato;

v) accettazione espressa della delega[14].

[14] v. Cass, sez. III pen., 12 ottobre 2009, n. 39729

7.2 Competenza e Formazione

In tema di competenza, la norma UNI ISO 37301 declina in modo semplice e chiaro i principi generali da tenere conto per il personale che opera in nome e per conto dell'azienda; in particolare, al punto 7.2.1 *Generalità* si dice che "*l'organizzazione deve:*

- *determinare le competenze necessarie per le persone che svolgono attività lavorative sotto il suo controllo e che influenzano le sue prestazioni relative alla compliance;*
- *assicurare che queste persone siano competenti sulla base di istruzione, formazione o esperienza appropriate;*
- *ove applicabile, intraprendere azioni per acquisire le necessarie competenze e valutare l'efficacia delle azioni intraprese.".*

Specifico richiamo viene fornito al tema della documentabilità delle scelte intraprese, adempimento questo rilevante sia per la norma UNI ISO 37301 che per il D.Lgs. 231; la norma in particolare specifica che "*Devono essere conservate appropriate informazioni documentate quale evidenza delle competenze*."

Anche il processo di selezione e impiego del personale è rilevante in quanto declinato nella norma ISO 37301 come requisito che, se non correttamente gestito, potrebbe portare a situazioni di non compliance, quindi di violazione della conformità legislativa.

Tale principio vale anche per la costruzione del Modello 231, nel cui ambito il processo di selezione del personale costituisce una delle attività sensibili in relazione al rischio di commissione di specifici reati presupposto ex D. Lgs. 231.

Nell'ambito delle competenze, sia la norma UNI ISO 37301 che il D.Lgs. 231 e le Linee Guida di Confindustria danno particolare enfasi al tema della **Formazione**. Per completezza nei contenuti, diamo particolare rilievo a quanto declinato al punto 7.2.3 *Formazione* della UNI ISO 37301, la quale ricorda che "*l'organizzazione deve erogare formazione su base regolare al personale pertinente, dal momento dell'entrata in servizio e ad intervalli pianificati determinati dall'organizzazione.*

La formazione deve essere:

a) appropriata ai ruoli del personale e ai rischi di compliance al quale il personale stesso è esposto;

b) valutata ai fini di efficacia;

c) riesaminata su base regolare.

Prendendo in considerazione i rischi di compliance[15] identificati, l'organizzazione deve assicurare che siano attuate procedure per trattare i temi della consapevolezza e formazione per terze parti che operano per conto dell'organizzazione stessa e che possono rappresentare un rischio di compliance per l'organizzazione. Le registrazioni relative alla formazione devono essere conservate come informazioni documentate."

In tema di formazione il D.Lgs.231/2001 non dà particolari indicazioni tranne che il modello dovrebbe essere "efficacemente attuato". A tale fine, le Linee Guida di Confindustria specificano l'importanza della formazione dando indicazioni sulla corretta programmazione e attuazione, specificando che:

[15] Rischio di non rispetto della conformità legislativa

- *"va indirizzata e differenziata in funzione dei destinatari: i dipendenti nella loro generalità, quelli che operano in specifiche aree di rischio/attività sensibili, i componenti degli organi sociali ecc.*
- *deve essere sviluppato un adeguato programma di formazione modulato in funzione dei livelli dei destinatari;*
- *il modello dovrebbe prevedere le modalità di erogazione della formazione (sessioni in aula, e-learning);*
- *è necessario assicurare adeguati test intermedi e finali di verifica del livello di apprendimento dei contenuti;*
- *implementare un idoneo sistema di monitoraggio dell'effettiva fruizione della formazione da parte dei destinatari, corredato da opportuni interventi correttivi a fronte di comportamenti anomali".*

7.3 Consapevolezza

Anche per questo requisito ci sono profonde sinergie tra la norma UNI ISO 37301 (con riferimento al capitolo 7.3) e le Linee Guida di Confindustria che affrontano il tema del Coinvolgimento al capitolo 4 Modalità operative di gestione dei rischi; Comunicazione e coinvolgimento nell'ambito dei reati colposi.

Mutuando quanto previsto dalla norma UNI ISO 37301 potremmo sintetizzare l'adempimento come segue: Le persone che svolgono un'attività lavorativa sotto il controllo dell'organizzazione devono essere consapevoli:

- della politica per la compliance;
- del proprio contributo all'efficacia del sistema di gestione per la compliance, compresi i benefici derivanti dal miglioramento delle prestazioni relative alla compliance;
- delle implicazioni derivanti dal non essere conformi ai requisiti del sistema di gestione per la compliance;
- dei mezzi e le procedure per far emergere preoccupazioni relative alla compliance (vedere punto 8.3);
- della relazione tra la politica per la compliance e gli obblighi di compliance pertinenti al loro ruolo;
- dell'importanza di sostenere una cultura della compliance;
- del codice etico e di comportamento;
- dei processi sensibili che potrebbero portare alla commissione del reato;
- dei presidi di controllo previsti dall'organizzazione per prevenire l'accadimento del reato presupposto;
- dei canali di segnalazione verso l'Organismo di Vigilanza di fatti/eventi rilevanti, come previsto dai flussi informativi ovvero segnalazioni di violazioni o potenziali violazioni (Whistleblowing);
- del sistema sanzionatorio e disciplinare, in caso di violazioni del Modello.

7.4 Comunicazione

Il tema della comunicazione riveste notevole rilevanza sia per la norma UNI ISO 37301 che per il D.Lgs.231 nella parte in cui prevede un Modello effettivamente attuato (ove il coinvolgimento e la partecipazione dell'intera organizzazione costituisce una condizione essenziale).. Anche in questo caso

prendiamo come riferimento quanto previsto dal punto *7.4. Comunicazione* della UNI ISO 37301, che recita quanto segue:

"L'organizzazione deve determinare le comunicazioni interne ed esterne pertinenti al sistema di gestione per la compliance, includendo:

a) l'argomento della comunicazione;

b) quando comunicare;

c) con chi comunicare;

d) come comunicare.

"L'organizzazione deve:

- considerare aspetti di diversità e potenziali barriere in termini di esigenze di comunicazione;

- assicurare che, nella definizione dei propri processi di comunicazione, siano considerati i punti di vista delle parti interessate;

- nella definizione dei propri processi di comunicazione:

- includere una comunicazione relativa alla propria cultura, obiettivi e obblighi di compliance;

- assicurare che le informazioni relative alla compliance da comunicare siano coerenti con le informazioni generate nell'ambito del sistema di gestione per la compliance e che esse siano affidabili;

- rispondere a comunicazioni rilevanti circa il proprio sistema di gestione per la compliance;

- conservare informazioni documentate come evidenza delle proprie comunicazioni, per quanto appropriato;

- comunicare al proprio interno informazioni rilevanti per il sistema di gestione per la compliance tra i vari livelli e funzioni dell'organizzazione, comprese le modifiche al sistema di gestione per la compliance, per quanto appropriato;

- assicurare che i propri processi di comunicazione consentano al personale di contribuire al miglioramento continuo del sistema di gestione per la compliance;

- assicurare che i propri processi di comunicazione consentano al personale di far emergere preoccupazioni;

- comunicare verso l'esterno informazioni rilevanti per il sistema di gestione per la compliance, come stabilito dai processi di comunicazione dell'organizzazione, includendo comunicazioni circa la propria cultura, i propri obiettivi e obblighi di compliance."

7.5 Informazioni documentate

Il tema della **documentabilità** e della **documentazione** è un tema che merita una particolare attenzione. La norma UNI ISO 37301 e, in generale, tutte le norma UNI ISO che attuano l'HS (Harmonized structure, ex HLS) hanno visto demandare all'organizzazione la scelta di quali informazioni documentare con una conseguente e graduale semplificazione della burocrazia che ha portato le procedure/istruzioni operative ad un livello di "prassi", pur mantenendo fermo l'obbligo di evidenza documentata

dell'attuazione del "processo" descritto dalla norma e dall'organizzazione (informazione documentata). Per quanto riguarda invece i presidi/principi di controllo previsti per la prevenzione del reato ex-D.Lgs. 231, le Linee Guida di Confindustria hanno ricordato al capitolo 5. I principi di controllo dove:

***"Ogni operazione, transazione, azione deve essere: verificabile, documentata, coerente e congrua"**.*

Per ogni operazione vi deve essere 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.

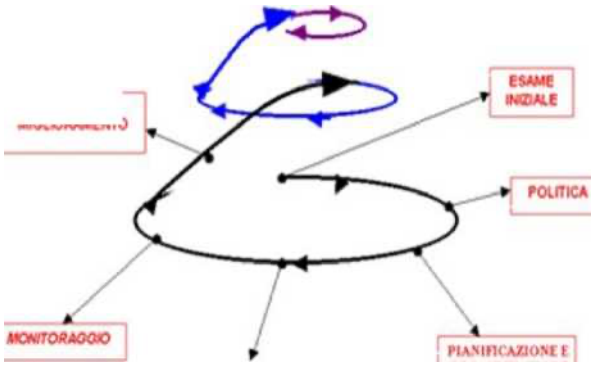
[■■■]

I controlli devono essere documentati".

Il sistema di controllo dovrebbe prevedere un sistema di reporting (eventualmente attraverso la redazione di verbali) adatto a documentare l'effettuazione e gli esiti dei controlli, anche di supervisione.

In particolare, i principi di controllo (ovvero di gestione regolata) possono riassumersi nello schema generale sotto riportato.

MIGLIORAMENTO



OKCAMlXUIon I

Si NS1BH I7ZAZIOM AZIONE

Figura2 — Principi di controllo (ovvero di gestione regolata) secondo le Linee guida Confindustria e le Linee Guida UNI INAIL per i sistemi di gestione per la salute e la sicurezza sul lavoro

Dove è chiaro a tutti coloro che conoscono i sistemi di gestione che il grafico fa riferimento al ciclo di Deming (detto anche ciclo PDCA) e del miglioramento continuo richiamato nelle Linee Guida UNI INAIL per i sistemi di gestione per la salute e la sicurezza sul lavoro.

In sintesi, è importante quindi evidenziare che, laddove il sistema di gestione per la compliance conforme alla UNI ISO 37301 verrà utilizzato a supporto dei Modelli di Organizzazione, Gestione e Controllo, l'organizzazione/l'ente dovrebbero prediligere la scelta di documentare procedure/protocolli e le evidenze di attuazione degli stessi rispetto alla scelta di operare mediante "prassi".

8 Attività operative

Secondo il ciclo di Deming, dalla fase PLAN, che comprende la valutazione degli aspetti considerati rilevanti per una corretta identificazione dei rischi di compliance (UNI ISO 37301) ovvero alla gap analysis e risk assessment per i processi sensibili che potrebbero portare, se non correttamente presidiati, alla commissione di un reato ex-D.Lgs. 231/2001, si passa alla fase DO. Questa fase prevede la messa in atto di tutte quelle misure per l'attuazione dei sistemi di prevenzione e controllo previsti dalla norma UNI ISO 37301 e dal D.Lgs. 231 e dalle Linee Guida di Confindustria, definito in modo sintetico come "Attività operativa".

8.1 Pianificazione e controllo operativi

La fase di attuazione prevede innanzitutto l'attuazione delle procedure/protocolli definiti per la compliance (UNI ISO 37301) ovvero per la prevenzione dei reati ex-D-Lgs.231/2001 attraverso la mitigazione del rischio a un livello considerato accettabile. A tale fine, entrambi i sistemi presi ad esame declinano adeguatamente la messa in atto delle "regole" definite dall'organizzazione/Ente ma la ISO 37301 (punto *8.1 Pianificazione e controlli operativi*) disegna con un approccio sistemico le modalità di attuazione che possono essere usate anche a supporto del D.Lgs. 231.

"L'organizzazione deve pianificare, attuare e tenere sotto controllo i processi necessari per soddisfare i requisiti e per attuare le azioni determinate al punto 6. (Pianificazione):

- *stabilendo i criteri per i processi;*
- *attuando il controllo dei processi, in conformità ai criteri.*

Le informazioni documentate devono essere disponibili nella misura necessaria ad avere fiducia che i processi siano stati effettuati come pianificato.

L'organizzazione deve tenere sotto controllo le modifiche pianificate e riesaminare le conseguenze dei cambiamenti involontari, intraprendendo azioni per mitigare ogni effetto negativo, per quanto necessario.

L'organizzazione deve assicurare che i processi, prodotti o servizi forniti dall'esterno, che sono rilevanti per il sistema di gestione per la compliance, siano tenuti sotto controllo. [...]

L'organizzazione deve assicurare che i processi affidati all'esterno siano tenuti sotto controllo e monitorati."

In combinato disposto è possibile leggere anche quanto previsto dalle Linee Guida di Confindustria al capitolo *4. Modalità operative di gestione dei rischi; iii.Valutazione/costruzione/adeguamento del sistema di controlli preventivi* che recita quanto segue:

"Il sistema di controlli preventivi dovrà essere tale da garantire che i rischi di commissione dei reati, secondo le modalità individuate e documentate nella fase precedente, siano ridotti ad un "livello accettabile", secondo la definizione esposta in precedenza. Si tratta, in sostanza, di progettare quelli che il decreto 231 definisce "specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire".

Sempre scorrendo il medesimo paragrafo delle Linee Guida di Confindustria troviamo un interessante stimolo relativo alla gerarchia dei controlli, dove si ricorda che:

"un 1° livello di controllo, che definisce e gestisce i controlli cosiddetti di linea, insiti nei processi operativi, e i relativi rischi. È svolto generalmente dalle risorse interne della struttura, sia in autocontrollo da parte dell'operatore, sia da parte del preposto/dirigente ma può comportare, per aspetti specialistici (ad esempio per verifiche strumentali) il ricorso ad altre risorse interne o esterne all'azienda."

Il 2° livello e il 3° livello di controllo sono affrontatati in punti successivi della presente norma.

8.2 Definizione di controlli e procedure

Anche relativamente alla definizione dei controlli e delle procedure, sia l'ambito normativo della UNI ISO37301 che quello legislativo del D.Lgs.231 e delle Linee Guida di Confindustria definiscono elementi che possono essere trasversali e sinergici. A tal fine si citano i riferimenti di entrambe le fonti per avere una visione omnicomprensiva; il punto *8.2 Definizione di controlli e procedure* della UNI ISO 37301 ci ricorda che *"l'organizzazione deve attuare controlli per gestire i propri obblighi di compliance e rischi di compliance associati. Tali controlli devono essere mantenuti, riesaminati su base periodica e sottoposti a prova per assicurare la loro continua efficacia."*

Le Linee Guida di Confindustria riportano che i *"sistemi di controllo integrato [...] devono considerare tutti i rischi operativi, in particolare relativi alla potenziale commissione di reati-presupposto, in modo da fornire tempestiva segnalazione dell'esistenza e dell'insorgere di situazioni di criticità generale e/o particolare. Occorre definire opportuni indicatori per le singole tipologie di rischio rilevato (ad esempio accordi di intermediazione che prevedano pagamenti off-shore) e i processi di risk assessment interni alle singole funzioni aziendali."*

8.3 Far emergere le preoccupazioni (whistleblowing)

Il tema delle segnalazioni è di estrema attualità sia a livello europeo che a livello nazionale. In particolare, tale ambito è stato ampiamente sottoposto a legislazione oltre che a normazione (a tale fine, vedere la UNI ISO 37002 in tema di Sistemi di Gestione per il Whistleblowing). Per tale ragione, si rimanda alla specifica legislazione e normazione per gli approfondimenti del caso.

8.4 Processi di indagine

La gestione del processo di indagine è importante per dare credibilità e serietà al sistema di gestione ovvero al Modello di Organizzazione, Gestione e Controllo ai fini del D.Lgs. 231. Questo requisito può essere letto in modo più o meno esteso in funzione dell'applicazione in un sistema di gestione integrato aziendale che comprenda sia la norma che la legislazione in analisi, ma anche in funzione delle dimensioni dell'organizzazione ovvero dell'Ente.

Se confiniamo la lettura di questo adempimento alla norma UNI ISO 37301, ci limiteremo agli adempimenti relativi alle non compliance previste nel sistema di gestione per la Compliance. Ma se lo estendiamo ad un Modello ampio, nell'ottica di un Sistema di Gestione Integrato Aziendale, dovremo anche tenere conto del ruolo dell'Organismo di Vigilanza il quale ha, tra i suoi compiti, proprio la verifica degli ambiti legati a segnalazioni di violazioni, presunte ovvero conclamate.

Per quanto riguarda invece la gestione a livello sistemico è utile ricordare cosa prevede la norma UNI ISO 37301 al punto *8.4 Processi di indagine*:

"L'organizzazione deve sviluppare, stabilire, attuare e mantenere processi per valutare, ponderare, esaminare e chiudere i rapporti relativi a istanze di non compliance sospette o effettive.

Tali processi devono assicurare un processo decisionale equo e imparziale.

I processi di indagine devono essere condotti in modo indipendente e senza conflitto di interessi, da parte di personale competente.

L'organizzazione deve utilizzare l'esito delle indagini per il miglioramento del sistema di gestione per la compliance, per quanto appropriato (vedere punto 10).

L'organizzazione deve riferire, su base regolare, all'organismo di governo o all'alta direzione, circa il numero e gli esiti delle indagini.

L'organizzazione deve conservare informazioni documentate sulle indagini."

9 Valutazione delle prestazioni

La fase CHECK nel ciclo di Deming è considerata la fase del monitoraggio e controllo del buon funzionamento del sistema, non tanto attraverso il controllo quotidiano nell'operatività (attività queste che troviamo nella fase DO) quanto nella messa in atto di strumenti specifici per la periodica e puntuale verifica dell'andamento del sistema integrato, attraverso indicatori di prestazione, lo svolgimento di audit interni e il riesame della direzione al fine di verificare che il sistema di gestione sia conforme alle aspettative aziendali, alle prescrizioni della norma UNI ISO 37301 e alla legislazione applicabile. Questa fase può essere in parte integrata e mutuata con quanto previsto dal D.Lgs. 231/2001 ma si nota che, in buona parte, molti adempimenti di questo punto rimangono requisiti specifici della norma UNI ISO 37301.

9.1 Monitoraggio, misurazione, analisi e valutazione

Questo requisito è applicabile in via prioritaria alla norma UNI ISO 37301 e solo in parte può trovare un corrispettivo nel D.Lgs. 231/2001.

Sul tema le Linee Guida di Confindustria al capitolo 4. Modalità operative di gestione dei rischi introducono la distinzione tra reati dolosi e colposi. Per quanto riguarda i reati dolosi, al paragrafo Sistemi di controllo integrato, le Linee Guida riportano che "*occorre definire opportuni indicatori per le singole tipologie di rischio rilevato (ad esempio accordi di intermediazione che prevedano pagamenti offshore) e i processi di risk assessment interni alle singole funzioni aziendali*."

Una migliore e più approfondita declinazione è presente nei presidi di controllo dei reati colposi al paragrafo Sistema di monitoraggio, che recita: "*La gestione della salute e sicurezza sul lavoro dovrebbe prevedere una fase di verifica del mantenimento delle misure di prevenzione e protezione dei rischi adottate e valutate idonee ed efficaci. Le misure tecniche, organizzative e procedurali di prevenzione e protezione realizzate dall'azienda dovrebbero essere sottoposte a monitoraggio pianificato. L'impostazione di un piano di monitoraggio si dovrebbe sviluppare attraverso:*

- *programmazione temporale delle verifiche (frequenza);*
- *attribuzione di compiti e di responsabilità esecutive;*
- *descrizione delle metodologie da seguire;*

- *modalità di segnalazione delle eventuali situazioni difformi.*

Dovrebbe, quindi, essere previsto un monitoraggio sistematico delle citate misure le cui modalità e responsabilità dovrebbero essere stabilite contestualmente alla definizione delle modalità e responsabilità della gestione operativa."

Ai fini prettamente sistemici, mutuando la norma UNI ISO 37301 per raccogliere gli stimoli derivanti dalle Linee Guida di Confindustria, possiamo declinare il punto *9.1 Monitoraggio, misurazione, analisi e valutazione* come segue:

"L'organizzazione deve monitorare il sistema di gestione per la compliance per assicurare che gli obiettivi per la compliance siano raggiunti.

L'organizzazione deve determinare:

- *cosa è necessario monitorare e misurare;*
- *i metodi per il monitoraggio, la misurazione, l'analisi e la valutazione, per quanto applicabile, per assicurare risultati validi;*
- *quando il monitoraggio e la misurazione devono essere eseguiti;*
- *quando i risultati del monitoraggio e della misurazione devono essere analizzati e valutati.*

L'organizzazione deve conservare appropriate informazioni documentate quale evidenza dei risultati.

L'organizzazione deve valutare le prestazioni relative alla compliance e l'efficacia del sistema di gestione per la compliance [...]

L'organizzazione deve sviluppare, attuare e mantenere un insieme di indicatori appropriati che supportano l'organizzazione nella valutazione del raggiungimento dei propri obiettivi per la compliance e nella valutazione delle relative prestazioni.

L'organizzazione deve stabilire, attuare e mantenere processi per il reporting della compliance al fine di assicurare che:

a) siano definiti appropriati criteri per il reporting;

b) siano stabilite delle scadenze per un reporting su base regolare;

c) sia attuato un sistema di reporting delle eccezioni che faciliti un reporting ad hoc;

d) siano attuati sistemi e processi per assicurare l'accuratezza e la completezza delle informazioni;

e) siano fornite informazioni accurate e complete alle funzioni o aree appropriate dell'organizzazione per consentire che siano prese azioni preventive, correttive e di rimedio in modo tempestivo.

Al fine di supportare il processo di monitoraggio e riesame e dimostrare la conformità al sistema di gestione per la compliance, devono essere conservate registrazioni accurate e aggiornate delle attività di compliance dell'organizzazione."

È utile anche ricordare che i flussi informativi diretti all'OdV possono rientrare negli strumenti di monitoraggio del buon andamento del sistema ovvero come strumento per il presidio delle aree a rischio reato 231.

9.2 Audit interno

Lo strumento dell'audit è quello più diffuso ed efficace per verificare in modo diretto, seppure con un approccio statistico ma significativo, i processi aziendali posti sotto indagine. Partendo dalla norma UNI ISO 37301, al punto *9.2.1 Generalità* si ricorda che:

"L'organizzazione deve condurre, a intervalli pianificati, audit interni allo scopo di fornire informazioni per accertare se il sistema di gestione per la compliance:

a) è conforme ai:

- *requisiti propri dell'organizzazione relativi al suo sistema di gestione per la compliance;*
- *requisiti del presente documento;*

b) è efficacemente attuato e mantenuto."

Questa definizione può essere impiegata sia per quanto attiene gli audit cd di "prima parte" ai fini dei sistemi di gestione ISO[16] ovvero, secondo quanto descritto nelle Linee Guida di Confindustria al capitolo *4. Modalità operative di gestione dei rischi; iii. Valutazione/costruzione/adeguamento del sistema di controlli preventivi* che recita quanto segue:

"per le organizzazioni più strutturate e di dimensioni medio-grandi, un 3° livello di controllo, effettuato dall'Internal Audit, che fornisce assurance, ovvero valutazioni indipendenti sul disegno e sul funzionamento del complessivo Sistema di Controllo Interno, accompagnato da piani di miglioramento definiti in accordo con il Management."

Occorre ricordare che, ai fini delle norme internazionali ISO e regolamenti nazionali UNI, gli audit di 3° parte sono invece da considerarsi quelli svolti dagli organismi di certificazione, preferibilmente sotto accreditamento di Accredia ovvero inclusi nei patti di mutuo riconoscimento a livello europeo.

Gli audit di certificazione e le certificazioni sono comunque citati e rappresentati al *capitolo 3.1.3 I sistemi di certificazione* delle Linee Guida di Confindustria.

Infine, sempre ai fini 231, ricordiamo anche che, nell'ambito della sua indipendenza di azione, l'OdV può svolgere, direttamente o per tramite di specialisti terzi, audit specifici per valutare se i presidi di controllo del Modello 231 connessi ai processi sensibili siano adeguati e correttamente attuati.

9.3 Riesame di direzione

Il requisito relativo al Riesame della direzione (punto 9.3.) risulta specifico per la norma UNI ISO 37301 quindi non si ritiene utile una analisi dettagliata in comparazione col D.Lgs.231/2001.

10 Miglioramento

La fase ACT completa il ciclo di Deming in un processo idealmente infinito di miglioramento continuo e costante del sistema aziendale, principio che vale per i sistemi di gestione UNI ISO 37301 ma che è applicabile anche per i Modelli di Organizzazione, Gestione e Controllo conformi al D.Lgs.231/2001. Di

[16] Una guida sull'attività di audit di sistemi di gestione è specificata nella UNI ISO 19011

fatto l'organizzazione e l'Ente sono soggetti a mutamenti legati ai cambi organizzativi, alla variabilità dei processi di business (acquisizioni; dismissioni; etc.) su cui è progettato il sistema di gestione ovvero i Modelli 231, ma anche legati all'evoluzione legislativa e normativa ovvero a fatti/eventi accaduti che segnalano la necessità di rivedere i presidi di controllo per rinforzarli o riprogettarli.

10.1 Miglioramento continuo

Questo requisito è direttamente correlato alla premessa descritta al punto 10 ed è applicabile sia per la norma UNI ISO 37301 che per il D.Lgs.231/2001. Mutuando la norma UNI ISO, possiamo quindi definire il requisito come segue:

"L'organizzazione deve migliorare in modo continuo l'idoneità, l'adeguatezza e l'efficacia del sistema di gestione per la compliance."

10.2 Non conformità e azioni correttive

La gestione delle carenze ovvero delle violazioni rispetto al requisito atteso è un processo che, dal punto di vista della raccolta, registrazione e identificazione delle misure correttive potrebbe non avere grandi disallineamenti tra norma UNI ISO 37301 e D.Lgs. 231/2001; quello che cambia in modo significativo è il soggetto che dovrebbe valutare la non conformità (intesa, ai fini 231, come comportamenti violativi di una prescrizione, direttamente o indirettamente prevista dal Modello, che potenzialmente espone al rischio di commissione di un reato rilevante): infatti, ai fini della UNI ISO 37301 il soggetto chiamato a raccogliere e analizzare la carenza sarà interno (funzione compliance; funzione internal audit; ecc.) mentre, ai fini 231, tale compito è assegnato principalmente all'OdV.

Tornando alla fase preliminare di raccolta, registrazione e identificazione delle misure correttive è possibile usare la definizione del requisito punto *10.2 Non conformità e azioni correttive* della norma UNI ISO 37301 per entrambi gli ambiti in analisi:

"Quando si verifica una non conformità o una non compliance, l'organizzazione deve:

a) reagire alla non conformità o non compliance, e, per quanto applicabile:

1) intraprendere azioni per tenerla sotto controllo e correggerla;

2) affrontarne le conseguenze;

b) valutare l'esigenza di azioni per eliminare la(e) causa(e) della non conformità o della non compliance, in modo che non si ripeta o non si verifichi altrove:

1) riesaminando la non conformità o la non compliance o entrambe;

2) determinando le cause della non conformità o della non compliance, o entrambe;

3) determinando se esistono o possono verificarsi non conformità o non compliance, o entrambe, simili;

c) attuare ogni azione necessaria;

d) riesaminare l'efficacia di ogni azione correttiva intrapresa;

e) effettuare, se necessario, modifiche al sistema di gestione per la compliance.

Le azioni correttive devono essere adeguate agli effetti delle non conformità o non compliance, o entrambe, riscontrate. "

Bibliografia

[1] Decreto Legislativo 8 giugno 2001, n. 231 "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"

[2] Linee guida per la costruzione dei modelli di organizzazione, gestione e controllo ai sensi del decreto legislativo 8 giugno 2001, N. 231, GIUGNO 2021, Confindustria

[3] Principi consolidati per la redazione dei modelli organizzativi e l'attività dell'organismo di vigilanza e prospettive di revisione del d.lgs. 8 giugno 2001, n. 231, Consiglio nazionale dei dottori commercialisti e degli esperti contabili, febbraio 2019

[4] Linee Guida UNI INAIL per i sistemi di gestione per la salute e la sicurezza sul lavoro