fieldfisher

Il sistema di gestione della Compliance ISO 37301 a supporto dei Modelli 231/01

club 231

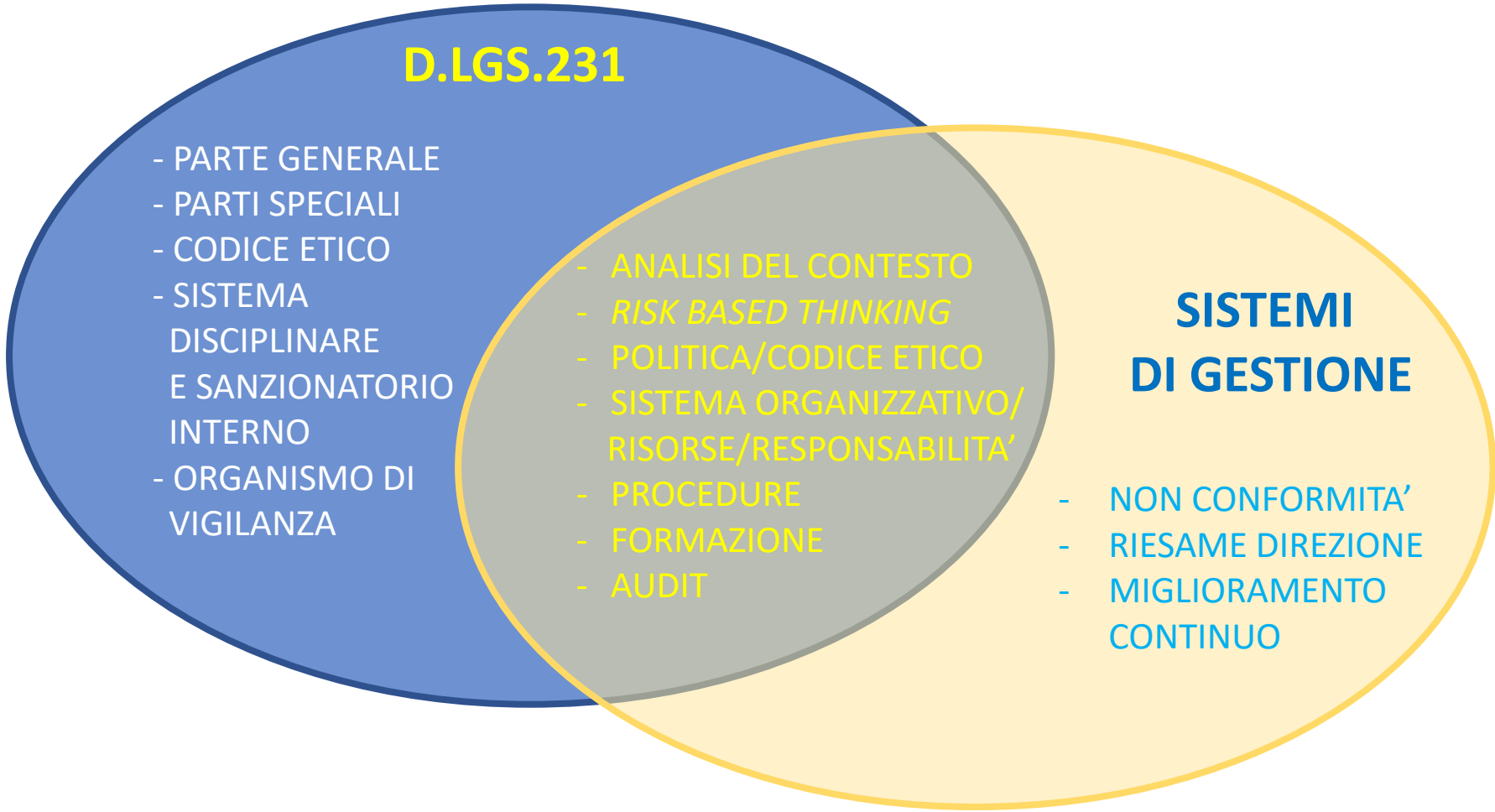
Roma,

21 giugno 2022

Terzo incontro 2022

Alessandro Foti
Coordinatore UNI/CT 016/GL 09 «Governance delle organizzazioni»
Coordinatore AIAS GTS "Sistemi di gestione"

Sistemi di Gestione ISO vs D.Lgs.231: analogie e differenze



Sistemi di Gestione ISO vs D.Lgs.231: analogie e differenze

Scopo e finalità

Norme ISO

- i sistemi di gestione ISO sono volontari
- adottati per garantire **il raggiungimento dello "Scopo" della norma** di riferimento
- **miglioramento continuo**

Scopo:

- rispondere ai dettami della norma volontaria che li descrive
- obiettivo verificato dall'organismo di parte terza durante gli audit di certificazione.

D.Lgs. 231/2001

- i modelli sono volontari
- il "Modello di Organizzazione, Gestione e Controllo" ha la finalità di definire un **contesto** all'interno del quale, se rispettate le misure prescrittive e preventive e supportati da una corretta vigilanza, **non debba essere possibile commettere un "reato 231" se non in modo fraudolento** eludendo il sistema di prevenzione e controllo impostato dall'Ente.

COLLEGAMENTO: un sistema di gestione, se adattato ed integrato con le finalità del MOG, aiuta a identificare, progettare, implementare e rivedere idonei presidi di controllo per supportare una Organizzazione a dotarsi di basi solide atte a fornire comprovate evidenze di "adeguatezza" e di "effettività", fondamentali per provare a dimostrare l'esimenza dei Modelli aziendali.

Sistemi di Gestione ISO vs D.Lgs.231: analogie e differenze

D.Lgs. 231 e ISO 37301

- La norma ISO 37301 è trasversale e copre tutti gli adempimenti di *Compliance* che un'azienda deve tenere monitorati e a cui deve adempiere e dimostrare di adempiere.

- La ISO 37301 si differenzia dalle altre norme ISO, orientate ad un ambito specifico (ISO 45001; ISO 14001; ISO 37001; ISO 27001; etc.)

- I reati non correlabili ad una norma ISO specifica potrebbero beneficiare della struttura della ISO 37301 (es. reati tributari; reati societari; etc.)

- Il beneficio del Sistema di Gestione richiamato dalle norme ISO risiede nel garantire:
  - ✓ **conformità** rispetto all'oggetto della norma stessa;
  - ✓ **approccio sistematico** (ciclo di *Deming*): valutazione iniziale dei processi specifici; progettazione di procedure e regole predeterminate; misure di controllo; attuazione delle regole; verifica della loro corretta attuazione; revisione del sistema e avvio di un nuovo ciclo secondo il principio del miglioramento continuo.

Reati 231 e le norme ISO

REATI 231	ISO 45001	ISO 14001	ISO 9001	ISO 37001	ISO 27001	ISO 37301	MOG 231
Art. 24 - Indebita percezione di erogazioni, truffa in danno dello Stato, di un ente pubblico o dell'UE o per il conseguimento di erogazioni pubbliche, …						X	X
Art. 24-bis - Delitti informatici e trattamento illecito di dati					X	X	X
Art. 24-ter -Delitti di criminalità organizzata						X	X
Art. 25 - Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e abuso d'ufficio				X		X	X
Art. 25-bis - Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento						X	X
Art. 25-bis.1 - Delitti contro l'industria e il commercio			X			X	X
Art. 25-ter - Reati societari						X	X
Art. 25-quater - Reati con finalità di terrorismo o di eversione dell'ordine democratico previsti dal Codice penale e dalle leggi speciali						X	X
Art. 25- quarter.1 - Pratiche di mutilazione degli organi genitali femminili						X	X
Art. 25- quinquies - Delitti contro la personalità individuale						X	X
Art. 25-sexies - Reati di abuso di mercato						X	X
Art. 187- quinquies TUF - Altre fattispecie in materia di abusi di mercato						X	X
Art. 25-septies - Reati di omicidio colposo e lesioni colpose gravi o gravissime	X					X	X
Art. 25-octies - Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio						X	X
Art. 25-novies - Delitti in materia di violazione del diritto d'autore						X	X
Art. 25-decies - Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria						X	X
Art. 25-undecies - Reati ambientali		X				X	X

La norma ISO 37301 abbraccia tutti gli obblighi di compliance di una Organizzazione (Ente)

Sistemi di Gestione ISO vs D.Lgs.231: analogie e differenze

Impegno dell'Organizzazione/Ente

D.Lgs. 231/2001

- L'adozione di principi etici rilevanti ai fini della prevenzione dei reati 231 costituisce un elemento essenziale del sistema di controllo preventivo. Tali principi possono essere inseriti in un **codice etico o di comportamento.**
- I codici etici sono documenti ufficiali dell'ente che contengono **l'insieme dei diritti, dei doveri e delle responsabilità dell'ente** nei confronti dei "portatori d'interesse" (dipendenti, fornitori, clienti, Pubblica Amministrazione, azionisti, mercato finanziario, ecc.).
- I codici etici mirano a **raccomandare/promuovere o vietare determinati comportamenti**, indipendentemente da quanto previsto a livello normativo, e possono prevedere **sanzioni**
- I codici etici sono **documenti** voluti ed approvati dal massimo vertice dell'ente.

Norme ISO

Politica aziendale

ISO 37301 - Campo di applicazione

- L'organizzazione deve determinare i confini e l'applicabilità del sistema di gestione per la *compliance* (SGC) per **stabilirne il campo di applicazione**.
- 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/o i confini geografici od organizzativi […].
- Il campo di applicazione deve essere disponibile come **informazione documentata**

Sistemi di Gestione ISO vs D.Lgs.231: analogie e differenze

Campo di applicazione

D.Lgs. 231/2001

1. L'ente ha come principio imprescindibile il **rispetto di leggi e regolamenti** vigenti in tutti i paesi in cui esso opera.
2. Ogni operazione e transazione deve essere correttamente **registrata, autorizzata, verificabile, legittima, coerente e congrua**.
3. Principi base relativamente ai **rapporti con gli interlocutori dell'ente**

Norme ISO

ISO 37301 - 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 e 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*.

Approvazione da parte del vertice aziendale (CdA) → Organo di governo / Alta direzione

Sistemi di Gestione ISO vs D.Lgs.231: analogie e differenze

Risk based thinking

Legislazione

RISCHIO -> ACCEZIONE NEGATIVA

- Il rischio è inteso come un evento da temere, una parentesi negativa in un principio di equilibrio controllato
- Es. SSL = «probabilità di raggiungimento del livello potenziale di danno nelle condizioni di impiego o di esposizione ad un determinato fattore o agente oppure alla loro combinazione» dove il target è l'uomo

D.Lgs. 231/2001

- Rischio di commettere un «reato».
- Accezione prettamente negativa, come quella comunemente intesa nella legislazione vigente (antinfortunistica; ambientale; corruzione; etc.).

Norme ISO

- RISCHIO -> ACCEZIONE NEUTRA
  - Minaccia
  - Opportunità

- Minaccia di non raggiungere lo scopo e gli obiettivi del Sistema di Gestione afferente alla norma ISO di riferimento (minaccia)
- Opportunità, nella risoluzione di un problema, nel trovare possibili soluzioni che portino «valore» all'impresa

DIFFERENZE

Sistemi di Gestione ISO vs D.Lgs.231: analogie e differenze

Risk assessment/Risk mapping

Norme ISO

ISO 37301 - Valutazione dei rischi di compliance

I rischi di compliance comprendono:

a) **rischi di compliance intrinseci** (rischi affrontati dall'organizzazione in assenza misure di trattamento del rischio);

b) **rischi di compliance residui** (rischi non efficacemente tenuti sotto controllo mediante le misure esistenti di trattamento del rischio).

D.Lgs. 231/2001

- **Definizione di rischio**: capacità di commissione del reato in quanto i processi sensibili identificati, sia essi correlati a reati colposi o dolosi, non sono adeguatamente presidiati in termini di regole comportamentali (protocolli), organizzazione e governance, vigilanza e controllo nonché nell'attuazione di tutto quanto previsto nel sistema dei presidi identificati (efficacia/effettività del Modello).

ANALOGIE

Sistemi di Gestione ISO vs D.Lgs.231: analogie e differenze

Risk assessment/Risk mapping

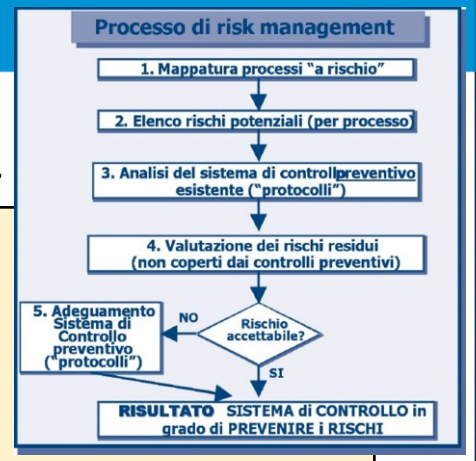
Norme ISO

ISO 37301 – VdR di compliance

L'organizzazione deve **identificare, analizzare e ponderare i propri rischi** di compliance:

- sulla base di un processo di valutazione del rischio 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.
- in termini di processi affidati all'esterno e di terzi parti.
- valutati su base periodica e ogni qual volta vi siano cambiamenti sostanziali a livello di condizioni o di contesto organizzativo.
- conservare informazioni documentate

D.Lgs. 231/2001



Per la costruzione del Modello è necessario procedere ad una accurata analisi dei rischi aziendali (***risk mapping***) e una loro valutazione in termini di possibilità di accadimento del reato (***risk assessment***), che preveda:

- la definizione di una mappa documentata, specifica ed esaustiva, dei processi aziendali a rischio;
- l'elaborazione di una mappa documentata delle potenziali modalità attuative degli illeciti nelle aree di rischio individuate;
- la valutazione delle probabilità di accadimento dell'evento e dell'impatto dell'evento stesso.

Approcci paralleli ma non sovrapponibili

Sistemi di Gestione ISO vs D.Lgs.231: analogie e differenze

Pianificazione e controlli operativi

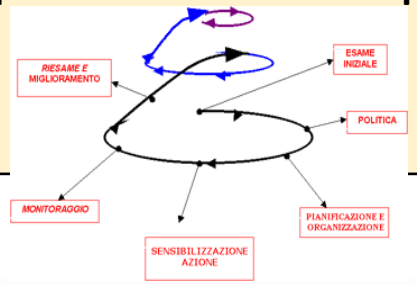
D.Lgs. 231/2001

Sistemi di controllo preventivo dei reati dolosi

- **Codice etico** o di comportamento con riferimento ai reati considerati.
- **Sistema organizzativo** sufficientemente aggiornato, formalizzato e chiaro.
- **Poteri** autorizzativi e di firma
- **Procedure**
- **Comunicazione** al personale e sua **formazione**
- Sistemi di **controllo** integrati

Sistemi di controllo preventivo dei reati colposi

Principi cardine dei sistemi di gestione



Norme ISO

ISO 37301 – Pianificazione e Controllo

- L'organizzazione deve pianificare, attuare e tenere sotto controllo i processi necessari per soddisfare i requisiti e per attuare le azioni determinate in fase di «Pianificazione», stabilendo i criteri per i processi e attuando il controllo dei processi, in conformità ai criteri.
- L'organizzazione deve tenere sotto controllo le modifiche pianificate e riesaminare le conseguenze dei cambiamenti involontari, intraprendendo azioni per mitigare ogni effetto negative […].
- 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.
- Le informazioni documentate devono essere disponibili

ANALOGIE

Sistemi di Gestione ISO vs D.Lgs.231: analogie e differenze

Certificazione

Norme ISO	D.Lgs. 231/2001
La norma **ISO 37301** è una norma di tipo A con possibilità quindi, come le altre norme analoghe, di ricevere una **certificazione di parte terza**	• i Modelli 231 non sono certificabili, • esistono degli strumenti analoghi per dimostrare l'adeguatezza e l'effettività del Modello stesso (in questi casi di parla di "attestazione" del Modello 231).

COLLEGAMENTO:

a) certificare l'intero sistema di gestione della *Compliance* conforme alla norma UNI ISO 37301:2021, tanto più se strettamente legato e permeato col Modello 231, dovrebbe permettere all'organizzazione di dimostrare che il proprio "Modello" di Compliance integrato viene anche controllato e "confermato" da un Organismo di Certificazione di parte terza;

b) la terzietà dell'**OdC** si andrà ad aggiungere alla terzietà dell' **OdV**.

Questa opportunità andrà a rinforzare ulteriormente la posizione dell'azienda nel caso si debba dimostrare l'esimenza del proprio Modello in sede giudiziaria