



ESHQ Consulting

WEBINAR

**I MODELLI ORGANIZZATIVI
231, I SISTEMI DI GESTIONE
AZIENDALI E IL RUOLO
DELLA NUOVA UNI ISO
37301:2021**

4 Novembre 2021

**La norma UNI ISO
37301:2021 a
supporto
dell'esimenza dei
Modelli 231**

Alessandro Foti

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

Safety
DAYS



UNI ISO 37301:2021

Introduzione (sintesi)

La **compliance** è un processo su base continuativa e il risultato di un'organizzazione che soddisfa i propri obblighi. La compliance è resa sostenibile incorporando essa stessa nella **cultura dell'organizzazione** e nei **comportamenti e attitudini** delle persone che lavorano al suo interno. Pur mantenendo la propria indipendenza, è preferibile che la **gestione per la compliance** sia **integrata con gli altri processi gestionali** dell'organizzazione e con i requisiti e le procedure operative.





UNI ISO 37301:2021

Termini e definizioni

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.

Condotta: Comportamenti e prassi che impattano sugli esiti per clienti, collaboratori, fornitori, mercati e comunità.

Rischio di compliance: Probabilità di accadimento e relative conseguenze di una non compliance in riferimento agli obblighi di compliance dell'organizzazione.



Reati 231 e 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)



UNI ISO 37301:2021

Introduzione (sintesi)

1. *Compliance* **integrata** con gli altri processi gestionali dell'organizzazione
2. Dimostrazione dell'impegno dell'Organizzazione (Ente) a **conformarsi alle leggi**
3. Valutare, gestire e minimizzare i **rischi correlati alla compliance**
4. Il non rispetto della *compliance* determina **sanzioni** da imporre a seguito di violazioni di leggi pertinenti.
5. Benchmark per gli **organismi legislativi** e giudiziari
6. **Salvaguardia dell'integrità** dell'Organizzazione ed evitare/minimizzare il mancato rispetto dei propri obblighi di compliance.
7. Aumento della fiducia di **terze parti** nella capacità dell'organizzazione.



MOG231 vs UNI ISO 37301:2021

Principi generali

Linee Guida 231 di Confindustria

- 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.

ISO 37301 - Campo di applicazione (§ 4.3)

- 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**



MOG231 vs UNI ISO 37301:2021

Impegno dell'Organizzazione/Ente

Linee Guida 231 di Confindustria

Contenuti minimi del Codice etico

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**

Approvazione da parte del vertice aziendale (CdA)

ISO 37301 - Obblighi di compliance (§ 4.5)

- 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*.

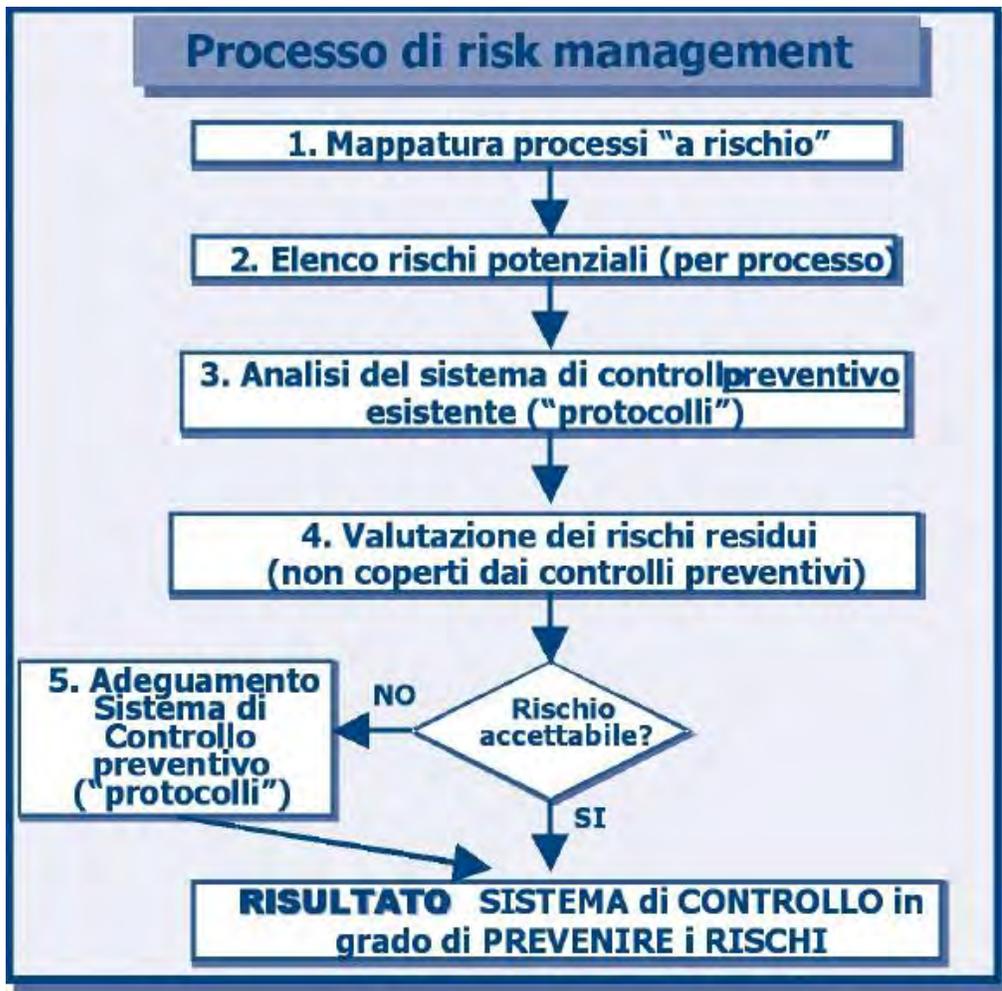
Organismo di governo
Alta Direzione



MOG231 vs UNI ISO 37301:2021

Identificazione e valutazione del rischio

Linee Guida 231 di Confindustria



ISO 37301 – Valutazione del rischio di compliance (§ 4.6)

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



Linee Guida 231 di Confindustria

- Il **rischio di compliance** 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 [...].
- Una **compliance integrata** potrebbe permettere invece agli Enti di [...] facilitare la condivisione delle informazioni attraverso una visione integrata delle diverse esigenze di compliance, anche attraverso l'esecuzione di **risk assessment congiunti**, e la manutenzione periodica dei programmi di compliance (ivi incluse le modalità di gestione delle risorse finanziarie [...]).
- un **approccio integrato** dovrebbe contemplare **procedure comuni** che [...] non generino **sovrapposizione di ruoli** (o **manca 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** [...] dovrebbero valutare l'opportunità di **predisporre o integrare tali procedure** [...]



MOG231 vs UNI ISO 37301:2021

Pianificazione e controlli operativi

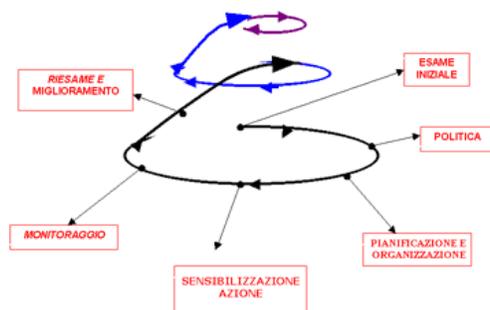
Linee Guida 231 di Confindustria

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



ISO 37301 – Pianif./Controllo (§ 8.1)

- 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



Gestione dei whistleblowing

Linee Guida 231 di Confindustria

Le imprese dotate del modello organizzativo 231 devono **disciplinare le modalità** per effettuare le segnalazioni e **le modalità di gestione delle stesse**, distinguendo fasi e responsabilità, eventualmente con una procedura ad hoc.

ISO 37002:2021
Whistleblowing
management systems
– Guidelines



Modelli 231 e certificazione delle norme ISO

Linee Guida 231 di Confindustria

3.1.3 I sistemi di certificazione

- Se una norma che espressamente stabilisce la presunzione di conformità del modello (art. 30, comma 5, decreto 81 del 2008) **non può valere di per sé a esimere l'ente da responsabilità in caso di concretizzazione del rischio reato**, perché residua un margine di discrezionalità giudiziale nel valutare l'effettiva attuazione del modello
- A maggior ragione **la sola adozione di un sistema di gestione certificato**, per di più non assistito da presunzione di conformità, non può mettere l'impresa al riparo da responsabilità da reato.
- In questo senso, per migliorare l'efficienza dei modelli organizzativi richiesti dal decreto 231, sarà importante valorizzare la **sinergia con la documentazione [...]** dei sistemi aziendali [...]

La norma ISO 37301 è una cosiddetta norma di tipo A, con possibilità quindi di **certificazione di parte terza**



Guida operativa per la costruzione e gestione del Modello 231

Aggiornata con le nuove Linee Guida di Confindustria e integrata con la norma UNI ISO 37001:2016 per l'anticorruzione e la UNI ISO 37301:2021 per la compliance

di **Alessandro Foti**

Edizione: novembre 2021 (III ed.)

È possibile acquistare i libri con un'**offerta riservata**:

SCONTO DEL 10% aggiuntivo rispetto a quello già previsto sul sito,

inserendo nel carrello il codice coupon: **SAFETYDAYS21**

Per acquistare il libro: www.epc.it



Sede Nord

Viale delle Industrie, 24
20090 Settala(MI)

Tel: 0247957969 02.95770601

Fax: 02.95844848

Sede Centro

Via di Casal Selce, 350
00166 Roma

Tel: 06.95557515 06.61901231

Fax: 06.61901231

Sede Sud

Via del Fante, 33 b sexies
91025 Marsala(TP)

Tel: 0923.1875100

e-mail: info@eshqconsulting.it

pec: info@pec.eshqconsulting.it

web: www.eshqconsulting.it

Seguici su: **LinkedIn**

CONTATTI

