

**LA NUOVA NORMA
UNI ISO 37301:2021**

Sistemi di Gestione per la Compliance, Requisiti

-

**Istruzioni applicative per aziende e
professionisti**

di

**Stefano Aldini, Andrea Baldin, Emanuele Montemarano,
Claudio Perissinotti Bisoni, Emanuele Riva e
Giovanna Raffaella Stumpo**

Coordinamento scientifico a cura di Giovanna Raffaella Stumpo

©2022 UNI - Milano

TUTTI I DIRITTI SONO RISERVATI

Nessuna parte del libro può essere riprodotta o diffusa con un mezzo qualsiasi, fotocopie, microfilm, o altro senza il consenso scritto dell'editore.

ALL RIGHTS RESERVED

No part of this work may be reproduced, stored in a retrieval system or transmitted in any form or by any means electronic, photocopying, recoding or otherwise, without the written permission from the publisher.

*Questa pubblicazione non è un documento normativo.
La responsabilità dei concetti espressi è unicamente dell'autore.*

Autori

Stefano Aldini - Andrea Baldin - Emanuele Montemarano
Claudio Perissinotti Bisoni - Emanuele Riva - Giovanna Raffaella Stumpo

Coordinamento scientifico a cura di Giovanna Raffaella Stumpo

Editore

UNI - Ente Italiano di Normazione
Via Sannio, 2 - 20137 Milano
Italia
Tel. 02 700241 - Fax. 02 70024481
www.uni.com

Grafica di copertina realizzata da UNI

1ª edizione - Settembre 2022

Stampato da UNI - Milano (MI)

ISBN 978-88-95730-62-2

Indice

Prefazione - <i>Ruggero Lensi</i>	1
Introduzione - <i>Filippo Trifiletti</i>	3
Capitolo 1 Norma UNI ISO 37301:2021 - Inquadramento nell'ambito delle altre norme ISO - <i>Claudio Perissinotti Bisoni</i>	5
Figura 1 Struttura e standard del ISO/TC 309	7
Figura 2 Struttura e standard del ISO/TC 309	10
Capitolo 2 Norma UNI ISO 37301:2021- Esperienze applicative a livello internazionale - <i>Stefano Aldini</i>	11
2.1 La norma UNE 19601 in Spagna	11
2.2 Il modello esimente della responsabilità penale delle persone giuridiche in Spagna	17
Capitolo 3 Norma UNI ISO 37301:2021 e Sistema di Gestione per la compliance - <i>Stefano Aldini, Giovanna Raffaella Stumpo, Andrea Baldin</i>	21
3.1 Scopo, Riferimenti normativi, Termini e definizioni rilevanti - <i>Stefano Aldini</i>	21
Tabella 1 Termini e Definizioni UNI ISO 37301:2021 (Estratto)	24
3.2 Pianificare il Sistema di Gestione per la Compliance	25
3.2.1 Contesto e Stakeholders rilevanti	25
3.2.2 Obblighi di compliance	27
3.2.3 Campo di applicazione del Sistema di Gestione per la Compliance	29
3.2.4 Compliance Risk Assessment	32
Tabella 2 Riferimenti tecnici per il processo di valutazione dei rischi (Estratto)	34
Tabella 3 Circostanze rilevanti per il riesame periodico della valutazione dei rischi	35
3.2.5 Pianificazione delle azioni di trattamento dei rischi e delle opportunità, obiettivi di miglioramento e pianificazione delle modifiche	36
Tabella 4 Requisiti degli obiettivi per la compliance e regole di pianificazione (Estratto)	38
3.3 Valutazione della performance del Sistema di Gestione per la Compliance	39
3.3.1 Monitoraggio, misurazione, analisi e valutazione	42
3.3.1.1 Fonti di feedback sulle prestazioni della compliance, indicatori, reporting e registrazioni	43
3.3.1.2 Fonti di feedback	43
Tabella 5 Ricercare e rilevare feedback sulle prestazioni di compliance - Esempi di fonti suggeriti nella guida all'utilizzo	44
3.3.1.3 Indicatori	45

3.3.1.4	Reporting	45
3.3.1.5	Registrazioni	46
3.3.2	Audit Interni	47
Tabella 6	Flusso di processo di un programma di audit interni secondo la UNI EN ISO 19011:2018	49
Tabella 7	Le principali fasi della conduzione dell'audit secondo la UNI EN ISO 19011:2018	50
3.3.3	Riesame di Direzione	50
Tabella 8	Monitoraggio dell'efficacia del Sistema di Gestione per la Compliance - Esempi di "COSA MONITARE" suggeriti nella guida all'utilizzo	53
Tabella 9	Monitoraggio dell'efficacia delle prestazioni della compliance - Esempi di "COSA MONITARE" suggeriti nella guida all'utilizzo	54
3.4	Miglioramento	54
3.4.1	Miglioramento continuo	54
3.4.2	Non Conformità ed Azioni Correttive	55
3.5	Leadership ed Impegno della Direzione (Top Management) nel disposto del Capitolo 5 della norma UNI ISO 37301:2021 - <i>Giovanna Raffaella Stumpo</i>	58
3.5.1	Premessa	58
Tabella 10	Articolazione del Capitolo 5 dello standard dedicato alla Leadership (Estratto dall'indice della UNI ISO 37301:2021)	60
Tabella 11	Chiarimenti sul concetto di "Leadership e impegno della Direzione" (Fonte: Appendice Informativa A) ...	61
3.5.2	Cultura, Governance e Politica della Compliance	62
Tabella 12	Benefici derivanti dalla scelta di implementare una solida cultura di compliance (Estratto dall'introduzione della UNI ISO 37301:2021)	64
Tabella 13	Caratteristiche della politica per la compliance (Estratto dall'Appendice Informativa A)	64
3.5.3	Ruoli, Responsabilità ed Autorità	65
3.5.3.1	L'Organo di Governo e l'Alta direzione	65
3.5.3.2	La Funzione di compliance	66
Tabella 14	L'impegno della Direzione a supporto della Funzione di compliance (Fonte: Capitolo 5 - Paragrafo 5.3.2 della UNI ISO 37301:2021)	69
3.5.3.3	Il Management	69
Tabella 15	Funzioni del Management a supporto dei Vertici nella gestione della compliance (Fonte: Capitolo 5 - Paragrafo 5.3.3 della UNI ISO 37301:2021)	70
3.5.3.4	Il personale.....	70
3.6	Attuazione del Sistema di Gestione per la Compliance e controlli operativi	71
3.6.1	Premessa	71
3.6.2	Pianificazione e controlli operativi	72
3.6.2.1	Il quadro dei controlli e le procedure	72
Tabella 16	Pianificazione e controlli operativi (Nelle Linee interpretative della UNI ISO 37301:2021 gli strumenti sono specificati e si richiede che siano integrati con funzioni e regole)	74

Tabella 17	Pianificazione e controlli operativi (Nelle Linee interpretative della UNI ISO 37301:2021 le specifiche quanto ai processi in outsourcing ed alla catena della fornitura).....	75
3.6.3	Far emergere le preoccupazioni (nella versione in lingua inglese della UNI ISO 37301:2021 "rising concerns")	76
3.6.4	I processi di indagine	76
3.7	Supporto e risorse del Sistema di Gestione per la Compliance - <i>Andrea Baldin</i>	79
3.7.1	Le Risorse - Premessa.....	79
3.7.1.1	La Competenza	80
3.7.1.2	Il Processo di impiego e la formazione.....	80
Tabella 18	La Formazione è obbligatoria internamente all'Organizzazione (Fonte: Capitolo 7 - Paragrafo 7.2.3 dello standard tecnico di riferimento)	82
3.7.1.3	La Consapevolezza	83
3.7.1.4	La Comunicazione interna ed esterna.....	83
Tabella 19	La Comunicazione esterna (Nelle Linee interpretative UNI ISO 37301:2021 tutte le indicazioni per organizzare al meglio il relativo processo, Fonte: Capitolo 7 - Paragrafo 7.4 dello standard tecnico di riferimento)	85
3.7.2	Le Regole organizzative (Nella terminologia ISO - Le informazioni documentate)	85
Tabella 20	Informazioni documentate (Nelle linee interpretative della UNI ISO 37301:2021 l'elencazione delle principali regole da documentare in modo formalizzato)	88
3.7.2.1	Creazione ed aggiornamento delle informazioni documentate	88
3.7.2.2	Controllo delle informazioni documentate	89
3.8	Profili di integrazione con i criteri ESG e con i Sistemi di Gestione aziendale ...	90
3.8.1	ESG e UNI ISO 37301:2021.....	90
3.8.1.1	ESG Rating	92
Figura 3	ESG e i 17 Obiettivi Agenda ONU 2030	93
Figura 4	Logo ONU Obiettivo 8 - 9 - 10 - 11	94
Figura 5	Logo ONU Obiettivo 16: Pace, giustizia e istituzioni solide	95
3.8.2	Profili di integrazione della UNI ISO 37301:2021 con altre norme ISO	96
Capitolo 4	Norma UNI ISO 37301:2021 e Modelli Organizzativi secondo il Dlgs. n. 231/2001 - <i>Emanuele Montemarano</i>	103
4.1	Collegamento tra la norma UNI ISO 37301:2021 e Dlgs. n. 231/2001.....	103
4.2	Funzione del Modello Organizzativo	105
4.3	Struttura del Modello Organizzativo all'interno di un Sistema di Gestione Integrato	106
4.4	Analisi del Contesto quale elemento introduttivo del Modello 231	107
4.5	Principi comportamentali alla base del Modello Organizzativo ex Dlgs. n. 231/2001	109
Tabella 21	Principi comportamentali alla base del MOG 231.....	110

4.6	Principi del sistema disciplinare	111
4.7	Funzione dell'Organismo di Vigilanza	113
4.8	Prerogative dell'Organismo di Vigilanza	114
Tabella 22	Prerogative dell'Organismo di Vigilanza	115
4.9	Procedura per l'esercizio del whistleblowing	116
Tabella 23	Un possibile modello di procedura di whistleblowing	117
4.10	Attività di analisi dei rischi di illecito aziendale	124
4.11	Attribuzione all'Organismo di Vigilanza della Funzione di compliance	125
Tabella 24	Parametri di riferimento atti a realizzare la Funzione di compliance in capo all'Organismo di Vigilanza	125
4.12	Riesame di Direzione sull'attuazione del Modello 231 dell'Organizzazione ..	126
Capitolo 5 Riflessioni su conformità, compliance e processo di certificazione - Emanule Riva		
5.1	Differenze tra i concetti di conformity e compliance	129
5.2	La Circolare tecnica ACCREDIA DC n.29/2021	134
Tabella 25	La circolare ACCREDIA DC n.29/2021 per punti (Estratto)	134
5.3	Ulteriori riflessioni conclusive	137
Testimonianze e Interviste		
Avv. Claudio Acampora - Cassa Forense		141
Avv. Vinicio Nardo - COA Milano		145
Dott.ssa Marcella Caradonna - CODCEC Milano		149
Dott. Demetrio Gilormo - AICQ SICEV		151
Dott. Federico Calvelli e Dott.ssa Cindy Martine Grasso - ASSOCOMPLIANCE		157
Ing. Francesco Solinas - AMT Genova		161
Bibliografia		
Sitografia		
Autori		
Ringraziamenti		

Prefazione

Viviamo in un mondo sempre più complesso.

Siamo passati in pochi anni da un contesto nel quale le principali preoccupazioni gestionali risiedevano nelle attività di core business, ovvero nella progettazione e realizzazione/erogazione di prodotti e servizi, ad una società dove si sono generati processi aggiuntivi - percepiti talvolta quali inutili sovrastrutture - che distolgono l'attenzione dagli obiettivi prioritari di produzione e di fatturato, aggiungendo costi alle Organizzazioni che riducono i loro margini di utili economici.

Molto spesso tali processi sono conseguenza di disposizioni cogenti, per cui il tema del rispetto della legalità, nella sua declinazione etica e deontologica, assume una dimensione sempre più rilevante nella capacità delle Organizzazioni di competere sui mercati, a livello nazionale, europeo ed internazionale.

I cambiamenti in atto hanno origine nel contesto interno ed esterno alle Organizzazioni, quali la richiesta di maggiori consapevolezza, responsabilità, trasparenza ed integrità, da a donne e uomini ai diversi livelli funzionali, soprattutto quelli apicali, e la profonda evoluzione della società legata sia all'aumento delle aspettative delle parti sociali che alle sfide delle trasformazioni tecnologico-digitale ed ecologico-ambientale.

La normazione non è stata a guardare ieri e nemmeno lo farà domani. Da una parte continua il suo centenario percorso nel contribuire ad interpretare in chiave misurabile i fenomeni evolutivi della società, fornendo a tutte le componenti scientifiche, economiche ed umanistiche, delle rappresentazioni dello stato dell'arte che possa costituire un modello di comunicazione, di confronto e di sviluppo. Dall'altra cerca di anticipare il futuro, sperimentando soluzioni che vogliono essere virtuose in un progressivo processo di sviluppo sostenibile, proponendosi quale agente trasformatore di una società che talvolta necessita di una "spinta gentile" per orientarsi.

È così che negli ultimi anni sono nate iniziative nella comunità delle norme volontarie che si sono discostate dallo strumento normativo tecnico tradizionale che puntava ad unificare i metodi di misurazione della prestazione dei prodotti.

Ricordiamo la positiva esperienza all'inizio degli anni 2000 che ha portato alla pubblicazione della ISO 26000 sulla responsabilità sociale - oggi UNI EN ISO 26000:2020 - strumento di base fondamentale per lo sviluppo di una cultura internazionale della sostenibilità.

Su questa scia, di particolare rilevanza è stata proprio la nascita del Comitato Tecnico internazionale ISO/TC 309, nato dall'esigenza di soddisfare le aspettative crescenti della società di disporre di strumenti e soluzioni per assicurare e riconoscere le pratiche di "buon governo" da parte delle Organizzazioni, e delle loro donne e dei loro uomini che desiderano operare e decidere "alla luce del sole": i popoli del mondo chiedono una gestione sana da parte di chi li rappresenta e li guida, sia nelle Organizzazioni private che nelle istituzioni pubbliche.

Sono già numerose le norme internazionali che sono state pensate, discusse, approvate e pubblicate nell'ambito dei lavori TC 309, ma la più importante è sicuramente la ISO 37301, adottata in Italia nel 2021 quale UNI ISO 37301, che stabilisce i requisiti di un Sistema di Gestione della cosiddetta "compliance".

Peccato non ci sia una parola italiana che rappresenti pienamente questo termine inglese. So bene che nella nostra lingua si indica la "conformità", ma la parola anglosassone comprende qualcosa di più, perché riesce ad andare oltre, alzando l'asticella da un livello tecnico orientato all'oggetto del quale si valuta la conformità ad un livello sociale che considera il soggetto che garantisce il rispetto della normativa in vigore, sia essa cogente o volontaria. Ed è proprio questo il grande valore della norma ISO: essere in grado di operare su scala internazionale tenendo in considerazione le specificità locali. In una visione di normazione integrata, il Sistema di Gestione consente di trattare con la medesima attenzione le disposizioni di Legge obbligatorie e la normazione ad applicazione volontaria, assicurando nel proprio contesto di riferimento, giuridico ed economico, una visione a 360° di tutti gli elementi necessari a garantire il rispetto degli elementi regolamentari, mettendo in atto comportamenti etici e deontologici.

Viviamo in un mondo sempre più complesso.

UNI può concorrere a semplificarlo, ma può soprattutto darci una chiave di lettura per orientarci in tale complessità con strumenti metodologici ed applicativi.

Con questo approccio vi invito quindi alla lettura del libro, ma soprattutto allo studio approfondito della UNI ISO 37301:2021.

Ruggero Lensi - Direttore Generale UNI

Introduzione

La catena che lega la normazione tecnica consensuale e l'accreditamento diventa sempre più solida e lunga.

Da un lato, si consolida il legame tradizionale, vuoi sul piano normativo (il regolamento che disciplina l'accreditamento, già dal 2008, ha imposto che gli accreditamenti vengano rilasciati in conformità con "norme armonizzate"), vuoi per i riconoscimenti che provengono da Mercato e Istituzioni.

Dall'altro, si è allungata la cordata, che ormai lega in modo inscindibile le attività di UNI-CEI ed ACCREDIA alla Metrologia, alle valutazioni di conformità - emesse sotto accreditamento e in conformità alle norme tecniche - e, *last but not least* alla sorveglianza del Mercato (anche questa disciplinata dall'Unione Europea, con lo stesso Regolamento n. 765/2008).

Anche in Italia, dunque l'Infrastruttura per la Qualità (IQ per l'Italia), si afferma progressivamente come un sistema integrato che agisce come forte elemento di sostegno, sia per le politiche di sviluppo economico, che per quelle rivolte alla sostenibilità ed alla sicurezza, nelle varie declinazioni che i concetti evoluti di ESG possono prevedere.

Questa affermazione vede nella pubblicazione promossa da parte di UNI del volume a cui ha contribuito Emanuele Riva, un ulteriore episodio del disegno di approfondimento culturale che lega i nostri due Enti e che tenta di allargare la rete degli interlocutori tradizionali. Se, un tempo, la comunicazione corporate era rivolta essenzialmente a Istituzioni ed imprese, è ormai necessario che anche i consumatori, gli studenti, gli Istituti d'Istruzione e di Ricerca raggiungano una maggiore familiarità con le diverse componenti dell'IQ.

E non è casuale che i processi della normazione tecnica si rivolgano sempre più spesso a tematiche non direttamente connesse ai processi della produzione industriale e dei servizi.

L'Italia si sta distinguendo in questo.

Basti ricordare norme e prassi di riferimento sviluppate negli ultimi anni per certificare professionalità rivolte alla cura della persona, o per la lotta al bullismo, la didattica a distanza e la parità di genere. Per non parlare dell'attenzione crescente rivolta ai temi della sanità e della sicurezza sociale (dispositivi di protezione individuale, professioni mediche, biobanche, etc.).

In un certo senso, la norma UNI ISO 37301, integrando in un sistema più completo ed organico il Sistema di Gestione anti-bribery regolato dalla 37001, soddisfa entrambe queste esigenze: il concetto più esteso di compliance potrà dare maggiori garanzie ai consumatori ed a tutti gli stakeholders di un impegno concreto e rigoroso per prevenire i fenomeni corruttivi, e di conseguenza assicurare la continuità imprenditoriale, anche nel caso in cui singoli episodi possano far venir meno l'eticità e la correttezza dei processi aziendali.

Non è casuale che proprio mentre il Governo e il Parlamento italiano si adoperavano, con l'applicazione della cd "Legge Severino", per favorire la trasparenza e contrastare la corruzione, la norma 37001 veniva sviluppata dall'ISO e immediatamente recepita in Italia, che è stato uno dei primi Paesi al Mondo a rilasciare certificazioni sotto la garanzia dell'accreditamento.

La crescita è stata subito rilevante.

Ad oggi si contano oltre 3.600 siti aziendali certificati in Italia, ma questo è ancora una goccia, nel mare dei 5 milioni di imprese italiane iscritte nei registri camerali.

Ci sono ora, dunque, con la norma 37301 tutte le prospettive per allargare ulteriormente la platea delle Organizzazioni certificate per l'antibribery o per ampliare i campi delle certificazioni già emesse, specie se si volessero approfondire le possibili relazioni e sovrapposizioni tra il Sistema di Gestione per la Compliance e i Modelli Organizzativi 231, e se si definissero opportune politiche di incentivazione, nelle fasi di selezione per il public procurement, o analogamente a quanto previsto per la certificazione dei Sistemi di Gestione per l'ambiente (riduzione delle fidejussioni per la V.I.A.), o per la sicurezza del lavoro (riduzione dei premi assicurativi).

Filippo Trifiletti - Direttore Generale di Accredia