Dalla ISO 19600 alla ISO 37301: l'evoluzione del Compliance Management System (CMS)

di Cindy Martine Grasso

Il 13 aprile 2021 è stata pubblicata la nuova norma ISO 37301:2021 "*Compliance Management Systems - Requirements with guidance for use*" (CMS), uno standard di grandissima importanza nel panorama delle norme ISO sui sistemi di gestione.

L'introduzione del nuovo schema è un ulteriore passo in avanti verso l'emergente corpus normativo sulla *governance* delle organizzazioni intrapreso dal Comitato Tecnico Internazionale ISO/TC 309 "*Governance of Organizations*", istituito nel 2017 per aiutare le organizzazioni a sviluppare il sistema che regola il modello di gestione, di controllo e di responsabilità necessario a realizzare la propria missione nel lungo termine.
Attraverso lo sviluppo di norme nell'ambito della *governance* organizzativa, il comitato ISO si propone di facilitare le organizzazioni a dimostrare il loro impegno nei confronti delle parti interessate attraverso evidenze e attività di reporting, incoraggiando gli organi di governo a prendere le giuste decisioni, assicurando il rispetto delle finalità, dei valori e degli obiettivi dell'organizzazione.
Il comitato ha potuto beneficiare del supporto del gruppo di esperti che ha elaborato la UNI ISO 37001:2016 "*Anti-bribery Management Systems - Requirements with guidance for use*" che specifica i requisiti e fornisce una guida per stabilire, mettere in atto, mantenere, aggiornare e migliorare un sistema di gestione per la prevenzione della corruzione. La norma, sebbene non affronti in modo specifico condotte fraudolente e altri reati relativi ad anti-trust/concorrenza, riciclaggio di denaro sporco o altre attività legate a pratiche di malcostume e disoneste, si prefigge di aiutare un'organizzazione a prevenire, rintracciare e affrontare la corruzione.
Il lavoro del Comitato Tecnico Internazionale ISO/TC 309 ha portato all'emanazione solo quest'anno di tre nuovi standard di assoluta rilevanza in ambito *governance*:

1. ISO 37000:2021 "*Governance of Organizations – Guidance*", documento che fornisce indicazioni per guidare gli organi di governo su come adempiere alle proprie responsabilità in modo che le organizzazioni possano raggiungere il loro scopo.

2. ISO 37002:2021 "*Whistleblowing Management Systems - Guidelines*", norma che

specifica le linee guida per istituire, attuare e mantenere un efficace sistema di gestione per il *Whistleblowing* basato sui principi di fiducia, imparzialità e protezione.

3. ISO 37301:2021 "*Compliance Management Systems - Requirements with guidance for use*", standard che riguarda la conformità alle regole che un un'organizzazione deve definire considerando il suo campo di attività e il settore nel quale opera.

Entriamo ora nel vivo dell'analisi del recente *Compliance Managemnet System*, oggetto del nostro approfondimento.

La norma ISO 37301:2021 "*Compliance Management Systems - Requirements with guidance for use*" (CMS) specifica i requisiti e fornisce linee guida per istituire, sviluppare, attuare, valutare, mantenere e migliorare un efficace sistema di gestione per la *compliance* all'interno di un'organizzazione.
Essa è applicabile a tutti i tipi di organizzazione indipendentemente da tipo, dimensione e natura delle relative attività, così come dal fatto che l'organizzazione stessa appartenga al settore pubblico, privato o al settore no-profit.

Benché tecnicamente si tratti di una prima edizione, la ISO 37301 rappresenta l'evoluzione della norma conosciuta in Italia come UNI ISO 19600:2016 "*Compliance Management Systems - Guidelines*". Il 90% del nuovo standard è comunque basato sulla ISO 19600, per cui le aziende che si sono precedentemente allineate a questa non avranno bisogno di attuare cambiamenti radicali.

L'aspetto sicuramente più innovativo e di rilevanza prioritaria rispetto alla precedente ISO 19600 riguarda la certificabilità del nuovo standard. La ISO 19600, essendo una norma *type B* e dunque non certificabile, si limitava a indicare le linee guida, i criteri e i principi di carattere generale, non permettendo che il sistema implementato potesse essere certificato da un Organismo di Terza Parte. La nuova ISO 37301 è invece una norma *type A*, cioè certificabile e dunque riportante i requisiti prescrittivi

compatibili con una vera e propria certificazione dello standard ISO.

Anche il CMS, come tutte le norme introdotte dal 2012, nasce sotto il *framework* del HLS - *High Level Structure*, un documento elaborato dall'ISO con l'ambizioso obiettivo di definire una terminologia e una struttura di base e delle parti di testo comuni per tutte le norme di sistemi di gestione, presenti e future. La necessità di definire una struttura univoca a tutti i MSS è un'esigenza da tempo nota ad ISO, in particolare per migliorare l'integrazione tra i vari sistemi di gestione nel costituire un singolo sistema integrato e facilitarne l'impiego da parte delle aziende e delle altre organizzazioni certificate.
Gli standard che condividono la medesima *High Level Structure* hanno una struttura del documento che presenta i seguenti titoli:
• scopo e campo di applicazione;
• riferimenti normativi;
• termini e definizioni;
• contesto dell'organizzazione;
• leadership;
• pianificazione;
• supporto;
• attività operative;
• valutazione delle prestazioni;
• miglioramento.
Inoltre, ogni standard può essere corredato da alcuni allegati. Ad esempio, lo standard ISO 37301 è corredato da un allegato A corposo e dettagliato.

ISO/TC 309, con lo sviluppo della nuova 37301, ambisce a portare la normazione oltre il management, verso i vertici delle organizzazioni: *board*, consigli di amministrazione, organismi di governo in senso lato. È infatti la *governance* a definire il complesso quadro di politiche aziendali e l'osservanza delle regole dettate dall'organizzazione, necessarie a raggiungere sul mercato gli obiettivi nel rispetto delle leggi. Non si parla più infatti solo di *Top Management*, come siamo abituati nei MSS, ma di tre livelli di *Leadership*: un *Governing Body*, che ha il compito di sovraintendere all'operato del *Top Management* al di sotto del quale, in un livello più gestionale, troviamo i *Managers*.
La norma definisce di "vitale" importanza che l'Organismo di Governo dimostri il proprio impegno in maniera chiara e visibile, con azioni e decisioni e comunicando il proprio impegno in maniera capillare a tutto il personale e alle parti interessate.

Lo standard ISO 37031 già nella sua introduzione, specifica che le organizzazioni che mirano ad avere successo a lungo termine devono stabilire e mantenere una cultura della conformità, considerando le esigenze e le aspettative delle parti interessate. La *compliance* è quindi non solo la base, ma anche un'opportunità, per un'organizzazione di successo e sostenibile.
L'organizzazione deve quindi considerare un'ampia gamma di questioni:
• il modello di *business*, compresa la strategia, la natura, le dimensioni e la complessità di scala e la sostenibilità delle attività e delle operazioni dell'organizzazione;
• la natura e l'ambito dei rapporti d'affari con terzi;
• il contesto legale e regolamentare;
• la situazione economica;
• i contesti sociali, culturali e ambientali;
• le strutture interne, politiche, processi, procedure e risorse, compresa la tecnologia;
• la sua cultura della *compliance*;
Viene introdotto così il concetto di cultura della *compliance* aziendale: l'idea che ci siano dei principi, dei valori, dei comportamenti, dunque dei *mindset* aziendali condivisi e promossi anche attraverso l'esempio di chi sta al vertice. Dunque, promuovere in maniera proattiva la Compliance Culture invitando a sviluppare un meccanismo di Whistleblowing per assicurare l'anonimato e la riservatezza nel caso in cui un operatore o collaboratore dell'organizzazione, volesse riferire delle noncompliance senza il timore di ritorsioni.

Come specificato all'interno dell'allegato A, il *Compliance Management System* dovrebbe essere basato sui principi di:
• buon governo;
• proporzionalità;
• integrità;
• trasparenza;
• responsabilità;
• sostenibilità.

In particolare la norma pone le sue basi su tre obiettivi principali dello sviluppo sostenibile.
Ricordiamo che gli obiettivi di sviluppo sostenibile mirano ad affrontare un'ampia gamma di questioni relative allo sviluppo economico e sociale, che includono la povertà, la fame, il diritto alla salute e all'istruzione, l'accesso all'acqua e all'energia, il lavoro, la crescita economica inclusiva e sostenibile, il cambiamento climatico e la tutela dell'ambiente, l'urbanizzazione, i modelli di produzione e consumo, l'uguaglianza sociale e di genere, la giustizia e la pace.
Con particolare rilevanza agli obiettivi:
• promuovere una crescita economica duratura, inclusiva e sostenibile, la piena occupazione e il lavoro dignitoso per tutti;
• promuovere società pacifiche e inclusive orientate allo sviluppo sostenibile, garantire a tutti l'accesso alla giustizia e costruire istituzioni efficaci, responsabili e inclusive a tutti i livelli;
• rendere le città e gli insediamenti umani inclusivi, sicuri, resilienti e sostenibili.

Sui principi di *compliance* si basano le *Compliance Obligations*, cioè i requisiti ai quali un'organizzazione deve obbligatoriamente conformarsi, come leggi, regolamenti, permessi, licenze, guide, trattati, convenzioni, protocolli e anche sentenze delle corti di giustizia o dei tribunali e i requisiti ai quali un'organizzazione decide di conformarsi volontariamente, accordi, politiche, procedure, principi volontari o codici di buona condotta.

Nel punto 4.6 del sistema, è esplicitamente richiesto un processo di *Compliance Risk Assessment*, ovviamente in linea con la ISO

31000:2018, il *framework* di gestione del rischio secondo ISO, che prevede come metodologia quella del ciclo PDCA *Plan/Do/Check/Act*. Il ciclo PDCA, sviluppato negli anni 20 da *Walter Shewhart*, è stato successivamente reso popolare da *W. Edwards Deming* e consiste sinteticamente in quattro fasi:
• *plan*: cosa fare e come farlo per soddisfare politica e obiettivi che si sono determinati;
• *do*: porre in atto quanto pianificato;
• *check*: verificare se si è fatto quanto pianificato e se quanto fatto risulta efficace al raggiungimento degli obiettivi;
• *act*: come e cosa migliorare.

Il processo di valutazione dei rischi di *compliance* costituisce la base per l'attuazione del CMS e per la scelta, definita con un approccio integrato, di risorse e processi per gestire i rischi.
Vediamo più da vicino questo elemento cardine, necessario ad identificare, analizzare e valutare i rischi di *compliance*.
Il pensiero basato sul rischio è un concetto radicato nella nostra mente che agisce in modo automatico e istintivo. Nella vita quotidiana, generalmente, non seguiamo un processo strutturato ma portiamo avanti un ragionamento abbastanza coerente, che a volte conduce a decisioni non del tutto adeguate al raggiungimento degli obiettivi prefissati.
Nella vita delle organizzazioni il *risk-based thinking* è essenziale per il mantenimento di un efficace sistema di gestione. A differenza della vita privata, nelle aziende è necessario che si passi da un «ragionamento abbastanza coerente» a un «processo strutturato».
È necessario quindi considerare il rischio qualitativamente e in base al contesto dell'azienda per ottenere i benefici che il pensiero basato sul rischio può fornire, quali:
• miglioramento del governo dell'organizzazione;
• aumento della fiducia degli stakeholder;
• introduzione di cultura e di gestione proattiva per il miglioramento;
• aumento solidità organizzazione e riduzione di perdite;
• miglioramento del processo decisionale;
• identificazione dei rischi prima possibile e gestione sistematica;
• miglioramento processo di identificazione preventiva di vulnerabilità e minacce;
• garanzia di essere conformi alle leggi.

Peculiare è l'introduzione della funzione di *compliance*. Nella ISO 37301 è esplicitamente richiesta, come requisito di norma, l'istituzione di una *Compliance Function*, che tenga conto delle *Compliance Obbligations* e dei conseguenti *Compliance Risk*. Tre sono i principi cardine che governano la funzione di *compliance*:
• indipendenza dalla struttura organizzativa;
• accesso diretto all'organismo di governo e all'alta direzione;
• livello di autorità e competenza complessivo adeguato ad una funzione così rilevante.

La *Compliance Function* deve poter avvalersi di un suo comitato all'interno del quale scambiare le informazioni, condividere gli indirizzi, gestire in maniera efficiente la politica dei controlli interni, giovandosi della trasversalità comune anche ad altre funzioni preposte a vigilare in qualche misura sui comportamenti dei dipendenti quali, ad esempio, il DPO, il *risk manager*, l'*internal auditor*, ma anche l'HR ed il legale.

A tal proposito, il Comitato Tecnico Internazionale ISO/TC 309 sta concludendo in questi mesi una nuova norma afferente all'ambito delle attività professionali non regolamentate, che definisce i requisiti relativi alle attività professionali delle figure operanti nell'ambito della disciplina della gestione della *compliance* (*Compliance Management Professionals*), ossia:
• tecnico della *compliance (Compliance Technician)*;
• specialista della *compliance (Compliance Specialist)*;
• manager della *compliance (Compliance Manager)*;
La futura norma prevede la definizione di tre distinti livelli professionali, i cui relativi compiti e attività specifiche riflettono la volontà di intercettare i differenti livelli organizzativi ai quali si presume debbano

operare tali figure, in coerenza con le rispettive definizioni, ossia i livelli: operativo, tattico-manageriale e politico-strategico.

In uno scenario normativo in continua evoluzione, caratterizzato da mercati instabili ed incerti, ora le organizzazioni hanno l'opportunità di conformarsi a uno *standard* univoco e riconosciuto, che rappresenta una linea guida di *best practice* internazionale.
La ISO 37301 si pone, infatti, l'obiettivo di orientare le imprese nell'adozione di un efficace complesso di misure organizzative e protocolli volti a governare i rischi aziendali, creando inevitabilmente delle interconnessioni con i diversi sistemi di organizzazione, gestione e controllo tra cui il modello organizzativo 231/2001.
L'adozione e la concreta attuazione di quest'ultimo, nonché il suo stato di aggiornamento e adeguatezza, è pertanto uno degli obiettivi di quei sistemi di *compliance* che la ISO 37301 si propone di disciplinare e certificare. A loro volta, i modelli organizzativi 231, nel definire adeguati presidi per la prevenzione dei reati presupposto, non possono rinunciare a descrivere e disciplinare il sistema di verifiche e controlli interni di *compliance*, in assenza del quale le realtà più complesse e articolate sarebbero esposte a rischi non accettabili.
Il recente standard ISO 37301:2021 ha voluto rispondere alla necessità di trovare soluzioni "integrate", capaci di far dialogare efficacemente presidi, procedure, organi di controllo e flussi informativi riferibili a sistemi normativi differenti, evitando sovrapposizioni e reciproche interferenze.