L'evoluzione del *Compliance Management System*

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*", 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 da ISO, che già comprende le tematiche dell'*anti-bribery*, introdotte dalla norma UNI ISO 37001:2016 "Sistemi di gestione per la prevenzione della corruzione" e che prevede, entro la fine 2021, l'emanazione di due nuovi *standard*: la ISO 37000 "Linea Guida per la *Governance* delle Organizzazioni" e la ISO 37002 "Linea Guida per Sistemi di Gestione *Whistleblowing*".
Il recente CMS riguarda la conformità alle regole che un un'organizzazione deve definire considerando il suo campo di attività, cioè il settore nel quale opera.
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*".
L'aspetto sicuramente più innovativo e di rilevanza prioritaria rispetto alla precedente ISO 19600, riguarda la certificabilità del nuovo *standard*. Se la ISO 19600, essendo una norma *Type B*, si limitava a indicare le linee guida, i criteri e i principi di carattere generale, la nuova ISO 37301 è verificabile, riportante, dunque, i requisiti prescrittivi compatibili con una vera e propria certificazione dello *standard* ISO, peculiare delle norme *Type A*.

Anche il CMS, come tutte le norme introdotte dal 2012, nasce sotto il *framework* del HLS - *High Level Structure*, permettendo la sua facile integrazione con altri sistemi di gestione nel costituire un singolo sistema integrato che permette di soddisfare contemporaneamente i requisiti di più MMS.
Il Comitato Tecnico internazionale ISO/TC 309 "*Governance of Organizations*", 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. 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*.
Interessanti sono i principi base su cui si fonda il nuovo *Compliance Management System* che possiamo riassumere in: buona *Governance*, proporzionalità, integrità, trasparenza, *accountability* e sostenibilità e sui quali 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.
Viene introdotto 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. Questo punto della norma interagisce con i capitoli

relativi al *recruiting*, all'inserimento dei nuovi assunti, e alla formazione, sezione molto espansa rispetto agli *standard* precedenti.
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 e livello di autorità e competenza complessivo adeguato a una funzione così rilevante.
Inoltre, nel punto 4.6 del sistema, è esplicitamente richiesto un processo di *Compliance Risk Assessment*, ovviamente in linea con la ISO 31000, il *framework* di gestione del rischio secondo ISO, la cui ultima edizione risale al 2018. 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.

Nel capitolo 8 della norma ci sono una serie di attività operative peculiari che riguardano la pianificazione e la definizione di controlli e procedure, il far emergere preoccupazioni e i processi di indagine. Elemento di base dell'*Operational Control* risulta essere il codice di condotta che promuove, in maniera proattiva, la *Compliance Culture*: viene definito di "vitale" importanza che l'organismo di governo e l'alta direzione dimostrino 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. Si invita, infine, a sviluppare un meccanismo *Whistleblowing*, che, come abbiamo detto, presto sarà normato dalla ISO 37002, 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.
In uno scenario normativo in continua evoluzione, caratterizzato da mercati instabili e incerti, ora le organizzazioni hanno l'opportunità di orientarsi e conformarsi a uno *standard* univoco e riconosciuto, che rappresenta una linea guida di *best practice* internazionale. La ISO 37301 è senza dubbio un'opportunità di miglioramento delle prestazioni e della sostenibilità aziendale.

Cindy Martine Grasso
Membro UNI/CT 016/GL 09 "Governance delle Organizzazioni Technical Team Member"
Compliance Manager Senior

THE EVOLUTION OF THE COMPLIANCE MANAGEMENT SYSTEM (CMS)

On April 13, 2021 the new ISO 37301: 2021 "Compliance Management Systems - Requirements with user guide" was published. It is a very important standard.
Although technically it is a first edition, ISO 37301 represents the evolution of the standard UNI ISO 19600: 2016 "Compliance Management Systems - Guidelines".
The most innovative aspect and of priority importance is the certifiability of the new standard.
Even the CMS, like all the rules introduced since 2012, was born under the framework of the HLS - High Level Structure, allowing its easy integration with other management systems.
In a constantly evolving regulatory world, characterized by unstable and uncertain markets, the organizations have the opportunity to orient themselves and conform to a unique and recognized standard now, which represents a guideline of international best practice. ISO 37301 is undoubtedly an opportunity to improve performance and corporate sustainability. More details in this article.