PUBBLICATA LA NORMA ISO PER LA COMPLIANCE DELLE ORGANIZZAZIONI

Il 14 aprile 2021 l' UNI ha pubblicato la norma ISO 37301:2021 che rappresenta un passaggio chiave nell'assetto normativo per la governance delle organizzazioni perchè delinea taluni requisiti peculiari, tra i quali: l'analisi e l'identificazione dei fattori interni ed esterni, con espresso riferimento tra gli altri anche al quadro di riferimento legale e regolatorio; la valutazione dei rischi di compliance (documented information); una funzione compliance, con specifici requisiti ed attribuzione di compiti e poteri necessari per supervisionare e assicurare la conformità del sistema di controllo e relazionare al top management sull'attuazione del sistema; l'approvazione di una Compliance Policy, che incoraggi anche il "raising concerns", ossia le segnalazioni di sospetti di violazioni e vieti ritorsioni.

Davide PIERATTONI è ingegnere gestionale e dottore di ricerca in ingegneria industriale e dell'informazione. Già ricercatore di ruolo in sistemi di elaborazione all'Università di Udine, è responsabile della sicurezza delle informazioni di Innova S.p.A. Con oltre 20 anni di esperienza nell'Information Technology, si occupa di sicurezza, privacy e compliance di settore.

1. Principi e contenuti della norma ISO 37301

Il 14 aprile 2021 l' UNI ha pubblicato la norma ISO 37301:2021 "*Compliance Management Systems – Requirements with guidance for use*" che rappresenta un passaggio chiave nell'assetto normativo per la governance delle organizzazioni.
La norma è in vigore dal 1° luglio 2021 e rappresenta l'evoluzione della linea guida conosciuta in Italia come **UNI ISO 19600:2016** "*Compliance Management Systems – Guidelines*". Essa è applicabile alle piccole, medie e grandi organizzazioni in tutti i settori - pubblico, privato e no-profit - e indipendentemente dalla natura delle attività, ma l'aspetto più **innovativo** riguarda la **certificabilità** del nuovo *standard*.

Il nuovo CMS (Compliance Management System) si fonda su alcuni principi: buona *Governance*, proporzionalità, integrità, trasparenza, *accountability* e sostenibilità. Da essi discendono le *Compliance Obligations*, cioè i requisiti ai quali un'organizzazione deve obbligatoriamente adeguarsi (leggi, regolamenti, permessi, licenze, convenzioni, protocolli e anche sentenze delle Corti di Giustizia o dei Tribunali o provvedimenti delle Autorità garanti) e quelli ai quali decide di conformarsi volontariamente (accordi, politiche, procedure, codice etico, regolamenti interni, codici di condotta delle associazioni di categoria). La norma ISO 37301 introduce finalmente il concetto di **cultura della** *compliance* **aziendale**: l'idea che ci siano dei principi, dei valori e dei comportamenti aziendali strutturati, espressi e partecipati non tanto attraverso la formazione e la condivisione a tutti i livelli, quanto soprattutto con l'esempio di chi sta al vertice dell'organizzazione.
Il processo di valutazione dei rischi di *compliance* costituisce un pilastro per l'attuazione del CMS e per la scelta di risorse e processi di gestione del rischio coerenti, e va definito con un **approccio integrato e normato dalla ISO 31000. Su questo viene in aiuto la Circolare Tecnica DC n. 29/2021 di Accredia [1] che, lungi dal rappresentare una metodologia di valutazione formale del rischio, consente di anticiparne l'impatto e l'entità delle iniziative di misura e contenimento necessarie.**

Tra i requisiti della ISO 37301 vi è l'istituzione di una *funzione* aziendale dedicata alla *compliance*, che presidii le Compliance Obligations e i conseguenti rischi (*Compliance Risk*). La *funzione compliance* deve avere indipendenza dalle strutture decisionali ed esecutive, accesso diretto all'alta direzione e un livello di autorità e di competenza adeguato e commisurato al contesto.
A concretizzare l'esercizio del CMS sono richieste attività operative particolari che riguardano la chiara attribuzione dei ruoli e delle responsabilità nel contesto, la definizione di **controlli,** la pianificazione di **procedure**, la capacità di far emergere preoccupazioni e stimolare azioni correttive, la regolamentazione dei processi di indagine, e il monitoraggio sull'attuazione del sistema mediante *audit* interni. La norma invita anche ad attivare un sistema di *whistleblowing* conforme alla ISO 37002, per assicurare l'anonimato e la riservatezza al soggetto che volesse riferire sospetti di violazioni senza temere o subire ritorsioni.

2. Obiettivi e opportunità di integrazione con la norma ISO 37001

È vantaggioso per un'organizzazione ottimizzare il modo in cui opera per ottenere sia la conformità ai requisiti specificati nella ISO 37001, norma certificabile e di riferimento in tema di anticorruzione, sia a quelli propri della ISO 37301, e quindi apportare i miglioramenti affinché le due norme possano integrarsi.
Un'organizzazione già certificata ISO 37001 può soddisfare più facilmente i requisiti specificati nella ISO 37301, poiché gli ambiti sono complementari ed entrambi gli schemi normativi si basano sull'Annex SL, che armonizza la struttura di alto livello di tutti gli standard ISO [2].
Occorre tuttavia comprendere le differenze di obiettivi tra le norme ISO 37301 e ISO 37001:

- l'adozione della ISO 37301 punta a stabilire una buona *governance*, con elementi come integrità, cultura, conformità, reputazione, valori ed etica, identificando e gestendo gli obblighi di conformità dell'organizzazione al fine di soddisfare un ampio spettro di vincoli normativi;
- l'adozione della ISO 37001 è motivata dal dimostrare alle parti interessate che l'organizzazione applica misure tangibili per prevenire, rilevare e rispondere alla corruzione, con l'obiettivo di sottrarsi a fenomeni avversi sul piano economico, di mercato e sociale che sussistono se atti di corruzione sono o sono stati commessi nella sua sfera di attività.

3. Integrazione tra la norma ISO 37301 e il MOGC ex D.Lgs. 231/01

La disponibilità di uno standard certificabile invita a un raffronto anche con i Modelli di Organizzazione, Gestione e Controllo adottati ai sensi del D.Lgs. 231/2001.

In prima istanza può accadere di confondere i due sistemi. Tuttavia i presidi e i protocolli elaborati nell'ambito del MOGC 231 hanno la finalità di prevenire una serie ben delimitata di illeciti penali, detti *reati presupposto* (art. 24 e ss. D.Lgs. 231/2001). Pur interessando in maniera trasversale tutti i processi, il D.Lgs. 231/2001 non è che una delle leggi di cui la *funzione compliance* secondo la ISO 37301 deve curare la corretta applicazione.

Come accade per tutti i modelli organizzativi, anche l'efficacia del MOGC 231 si riduce quando esso è avulso dal reale sistema di compliance aziendale o non viene promosso a tutti i livelli dell'organizzazione come requisito di sostenibilità del business, oltreché come opportunità di miglioramento tangibile e continuativo. La concreta attuazione di un MOGC 231, nonché il suo stato di aggiornamento e adeguatezza, è pertanto uno degli obiettivi di sistema che la ISO 37301 si propone di disciplinare e certificare. Tutte le attività di controllo e verifica, gli sforzi aziendali nel dimostrare il proprio impegno e la propria *accountability* con la ISO 37301 vengono così spinti verso un unico schema organizzato e strutturato, eliminando l'approccio a compartimenti stagni.

Nella norma ISO 37301 si evidenzia il collegamento tra la certificazione e la prova dell'effettivo impegno societario a una corretta gestione della *compliance*, aspetto che potrebbe essere valorizzato anche in sede giurisdizionale in merito alla responsabilità da reato dell'ente o dell'impresa.

4. Prospettive aperte

Le organizzazioni debbono affrontare e gestire la complessità con efficienza ed efficacia: la norma ISO 37301 appare oggi una proposta promettente poiché aiuta a inquadrare in modo sistematico i propri requisiti di conformità – obbligatori e volontari – e assicurarne il dovuto presidio, a supporto delle strategie e degli impegni futuri.

La scelta di certificarsi ISO 37301 conduce necessariamente a una seria revisione delle proprie capacità di formazione, di comunicazione e di gestione delle competenze, con impegno da parte di tutta la struttura e avvalendosi di figure professionali di riferimento da dedicare costantemente allo scopo. Lo sforzo richiede investimenti importanti, non solo per il raggiungimento dell'obiettivo di certificazione

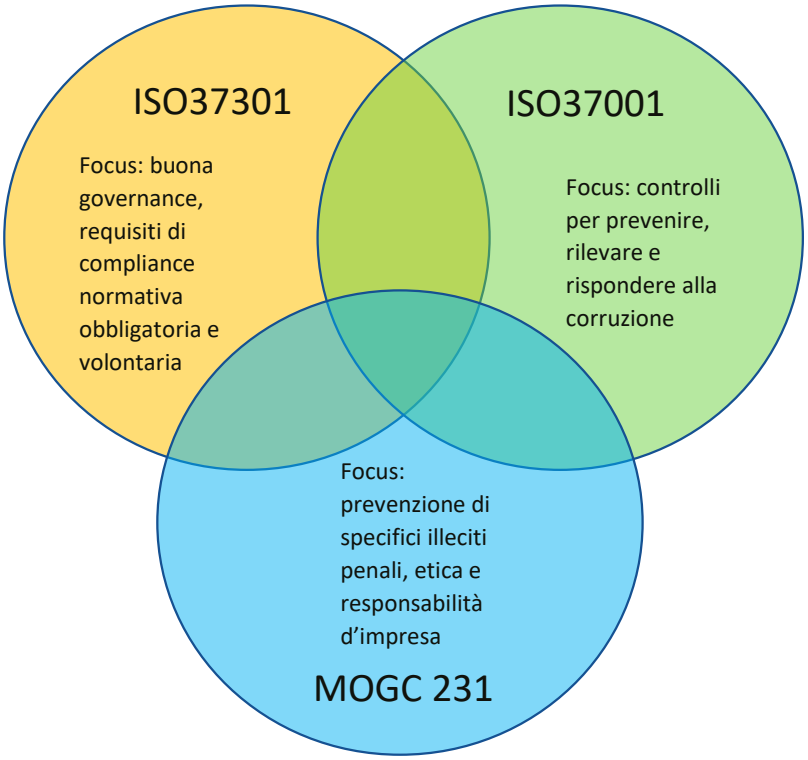

Figura 1 - ISO 37031 come norma ponte tra sistemi di gestione, modelli organizzativi e compliance

ma anche e soprattutto per il suo mantenimento.
Se per altre certificazioni e modelli organizzativi ciò non fosse già evidente, nel caso della norma ISO 37301 la ricaduta positiva di tali investimenti è manifesta anche sul piano della collettività. Oltre al vantaggio che, in termini finanziari, discende dalla sostenibilità del business nel tempo, l'evidenza della *compliance* di un'impresa soddisfa infatti aspettative molto alte: a partire dalle garanzie di qualità e affidabilità dei rapporti tra imprese e Pubblica Amministrazione, in primis quelle che contribuiscono all'esercizio delle funzioni essenziali dello Stato, fino allo sviluppo più armonioso e virtuoso del tessuto economico e sociale di una nazione. ©

RIFERIMENTI

[1] Accredia, Circolare Tecnica DC n. 29/2021 "Disposizioni in merito all'accreditamento per lo schema CMS, ai fini del rilascio di certificazioni ISO 37301:2021", 5 luglio 2021; disponibile su https://www.accredia.it/documenti/
[2] ISO/IEC Directives, Part 1 - Consolidated ISO Supplement - Procedures for the technical work - Procedures specific to ISO; disponibile su https://www.iso.org ◊