Gestione dei rischi legali: opportunità di successo e sostenibilità

di Emilia Catto e Gennaro Bacile di Castiglione

Le organizzazioni operano in un ambiente complesso nel quale i requisiti legali e normativi possono variare tra le diverse nazioni: sono tenute a rispettare le leggi di tutti i Paesi in cui operano e questo intensifica la necessità di comprendere il contesto e avere fiducia nei propri processi.
Le organizzazioni devono tenere il passo con i cambiamenti del contesto legale e normativo e rivedere i propri obblighi man mano che vengono sviluppate nuove attività e processi: in un contesto caratterizzato da una notevole incertezza, devono prendere decisioni e intraprendere azioni che possono avere conseguenze legali significative. La gestione del rischio legale le aiuta a proteggere e aumentare il loro valore. La possibilità di dare evidenza di essere affidabili sotto tutti i punti di vista ha delle positive ricadute su molti aspetti dell'organizzazione, che vanno dalla rivalutazione patrimoniale di un sito che, con ragionevole certezza, non ha problemi di mancato rispetto dei requisiti e delle aspettative delle parti interessate, all'apprezzamento da parte degli investitori per titoli che si dimostrano affidabili nel tempo, fino alla riduzione dei premi per le assicurazioni a fronte di rischi ben definiti e governati.
Essere affidabili significa quindi:

- mantenere delle buone relazioni con tutte le parti interessate e soddisfarne le aspettative
- essere sostenibili nel tempo.

Il pieno soddisfacimento dei requisiti, derivanti dalle prescrizioni delle norme cogenti applicabili e di quelli derivanti dagli accordi che l'organizzazione ha sottoscritto volontariamente a vario titolo, comporta un impegno rilevante che passa attraverso più fasi, tra le quali si evidenziano:

- identificazione (normativa cogente nazionale e internazionale, relativa a prodotti e servizi, ambiente, salute e sicurezza sul lavoro, ecc.);
- interpretazione (confronto con esperti);
- adeguata applicazione (in termini di risorse e competenze);
- monitoraggio (del rispetto degli obblighi con adeguati controlli).

Nell'ambito della famiglia ISO 31000 per la gestione del rischio, la UNI ISO 31022:2021[1]- Linee guida per la gestione del rischio legale si propone di fornire suggerimenti e raccomandazioni per la gestione delle sfide specifiche relative al rischio legale, come documento complementare alla ISO 31000, la cui applicazione può essere personalizzata per ogni organizzazione e il suo contesto, non essendo dedicato a un particolare settore o industria.
Il documento:

- fornisce linee guida per una gestione del rischio legale che sia allineata alla politica per il rispetto degli obblighi ed è in grado di stimolare un'adeguata fiducia sulla capacità di soddisfare tali obblighi e gli obiettivi dell'organizzazione;
- può essere utilizzato da organizzazioni di tutti i tipi e dimensioni per fornire un approccio più strutturato e coerente alla gestione del rischio legale a vantaggio dell'organizzazione e delle sue parti interessate in tutti i processi;
- offre un approccio gestionale integrato all'identificazione, analisi e ponderazione del rischio legale;
- sostiene e integra gli approcci esistenti, li rende più robusti fornendo migliori informazioni e approfondimenti sui potenziali problemi che l'organizzazione potrebbe affrontare;
- supporta qualsiasi processo di rispetto degli obblighi che le organizzazioni potrebbero avere in atto, come un sistema di gestione per la *compliance* o di altro tipo;
- supporta la funzione *Compliance*[2] identificando in modo più ampio i diritti e gli obblighi legali e contrattuali dell'organizzazione.

La norma non è destinata a sostituire le necessarie consulenze legali (interne o esterne) richieste dai "*risk owners*" (titolari del rischio), né a essere applicata al processo legislativo o a un processo volto a sollecitare l'elaborazione di nuove leggi o modifiche a quelle esistenti. Lo scopo del documento, invece, è quello di sviluppare una migliore comprensione della gestione del rischio legale affrontato da un'organizzazione che applica i principi della ISO 31000, incoraggiando un approccio più sistematico e coerente per aiutare il vertice a raggiungere i risultati strategici con un comportamento consapevole, etico e sostenibile.
Questo documento risulta essere un utile complemento, oltre che della UNI ISO 31000:2018, di tutte quelle norme sui sistemi di gestione in cui il rispetto degli obblighi di legge sia uno degli aspetti preponderanti (vedere anche Tabella 1).

Che cos'è il rischio legale?

È il rischio relativo a questioni legali, regolamentari e contrattuali, nonché derivante da diritti e obblighi extracontrattuali.
Può nascere da:

- contesto esterno (fattori esterni al controllo da parte dell'organizzazione);
- contesto interno (sotto il controllo dell'organizzazione).

Il mancato rispetto dei requisiti e delle aspettative delle parti interessate può avere conseguenze negative immediate e considerevoli, che potrebbero influenzare le prestazioni e la reputazione di un'organizzazione e portare a procedimenti penali nei confronti dell'alta direzione.
Occorre però saper prevenire anche le conseguenze del non rispetto dei requisiti e delle aspettative dell'organizzazione da parte di controparti che interagiscono a diverso titolo con l'organizzazione stessa, sviluppandone la consapevolezza dei doveri, ma anche dei propri diritti.
Tale rischio risulta particolarmente elevato in contesti internazionali.

Principi

La gestione efficace del rischio legale si basa sui valori e i principi di cui alla Figura 1. Questi otto elementi sono stati rivisitati per essere applicati nell'ambito della gestione del rischio legale, con l'aggiunta del principio di "equità", di cui non esiste una definizione, ma si chiarisce che tale termine incorpora idee e concetti diversi, tra cui giustizia, correttezza e uguaglianza.

Figura 1 - Principi per la gestione del rischio [Fonte: UNI ISO 31000:2018]

Processo di gestione del rischio legale

Il processo di gestione del rischio legale (paragrafo 5 della norma - Figura 2) viene poi analizzato sulla base dei suggerimenti della ISO 31000:2018, integrandoli con considerazioni relative alle specificità di tale rischio. Si tratta di un processo iterativo che dovrebbe essere integrato in tutte le attività dell'organizzazione.

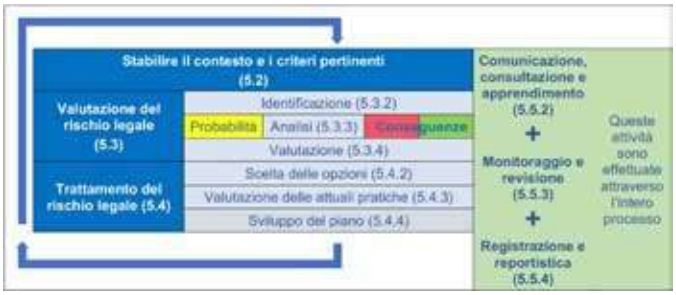

Figura 2 - Fasi del processo di gestione del rischio legale in relazione ai punti della UNI ISO 31022

Attuazione della gestione del rischio legale

L'ultimo punto della linea guida, il 6, definisce i passaggi per arrivare a una corretta attuazione della gestione del rischio legale. Questo punto risulta essere complementare a quanto la UNI ISO 31000 suggerisce come struttura di riferimento (*framework*) per assistere un'organizzazione nell'integrare la gestione del rischio. Tale gestione dovrebbe essere parte integrante della *governance* e delle attività operative dell'organizzazione per assicurare un processo decisionale consapevole. Dovrebbe essere pienamente allineata con la strategia, gli obiettivi e il sistema di gestione. Tutto questo include:

- la definizione di una politica per la gestione del rischio legale;
- l'identificazione delle funzioni organizzative responsabili, assegnando autorità, responsabilità e obbligo di rendere conto della sua corretta realizzazione a figure dotate di competenza e capacità adeguate, fornite del necessario supporto di una consulenza legale interna o esterna;
- tra gli altri strumenti di gestione, lo sviluppo di adeguate procedure per l'integrazione del processo di gestione del rischio legale negli altri processi, l'allocazione delle risorse e l'attivazione di un processo di comunicazione;
- la promozione della consapevolezza del rischio legale da parte di un'alta direzione che agisce da esempio, attiva un sistematico programma di formazione e stimola la partecipazione di tutti i dipendenti anche attraverso gruppi di lavoro multidisciplinari.

Appendici

La linea guida riporta 5 esempi che risultano particolarmente utili per impostare e attuare la gestione del rischio legale:

- Appendice A (informativa): Un esempio di metodo per l'identificazione del rischio legale - Matrice di identificazione del rischio legale (LRIM). Riporta uno schema per una tabella con 6 categorie di rischio da identificare e attribuire per le varie attività dell'organizzazione;
- Appendice B (informativa): Un esempio di registro dei rischi legali. Suggerisce tre possibili tabelle a supporto di un efficace registro dei rischi legali:
  Tabella 1: si basa su una raccolta di potenziali eventi di rischio legale con le leggi applicabili, le possibili conseguenze, casi passati, opinioni legali, soluzioni consigliate;
  Tabella 2: utilizzata per riassumere gli argomenti consulenza legale ricevuta, analisi quantitativa e/o qualitativa e decisione sui rischi legali identificati;
  Tabella 3: riporta una serie di domande per interviste strutturate che consentano di ottenere *input* dai responsabili dei processi per esaminare sia l'esposizione sia l'efficacia dell'ambiente di controllo e consentire di costruire e tenere aggiornato il registro.
- Appendice C (informativa): Un esempio per stimare la probabilità di eventi correlati al rischio legale. Contiene lo schema per una tabella strutturata su 5 livelli di adeguatezza relativi a 5 indicatori, corrispondenti a parametri rilevanti per l'analisi dello stato dei processi di gestione del rischio legale: aiuta a identificare dove si annidano le criticità;
- Appendice D (informativa): Un esempio per stimare le conseguenze di eventi legati al rischio legale. Contiene lo schema per una tabella strutturata su 5 livelli di entità di danno derivante da 4 diversi tipi di conseguenze, a seguito di eventi relativi a parametri diversi (monetari e non);
- Appendice E (informativa): Aspetti chiave da considerare nel riesame dei contratti. Elenco di 28 aspetti chiave da valutare per un esauriente riesame di un contratto allo scopo di ridurre al minimo il rischio legale. L'organizzazione dovrebbe esaminare ciascun aspetto nella corretta prospettiva distinguendo tra contratti con fornitori oppure con clienti di prodotti o servizi.

Conclusioni

Uno degli obiettivi della UNI ISO 31022 è aiutare le organizzazioni a sviluppare e diffondere una cultura positiva del rispetto degli obblighi, considerando che una gestione efficace e corretta dei rischi legali dovrebbe essere considerata come un'opportunità da cogliere, a causa dei numerosi vantaggi che offre, quali ad esempio:

- migliorare le opportunità di *business* e la sostenibilità;
- proteggere e migliorare la reputazione e la credibilità;
- tenere conto delle aspettative delle parti interessate;
- dimostrare di essere socialmente responsabile attraverso l'impegno a gestire i propri rischi legali in modo efficace ed efficiente;
- aumentare la fiducia di terze parti nella capacità di raggiungere un successo duraturo;
- minimizzare il rischio che si verifichi un'infrazione con i relativi costi e danni alla reputazione.

La maggior parte delle organizzazioni, inoltre, considerano l'evoluzione legislativa come una minaccia capace di generare nuovi onerosi requisiti. Non si può negare che questo sia in buona parte vero, ma un'organizzazione eccellente dovrebbe considerare che una tale evoluzione potrebbe configurarsi come un'interessante opportunità per risultare competitiva, anticipando l'adeguamento legislativo rispetto ai concorrenti.

TABELLA 1 - ESEMPI DI NORME SUI SISTEMI DI GESTIONE PER L'APPLICAZIONE DELLE QUALI LA UNI ISO 31022:2021 POTREBBE RISULTARE UNA GUIDA MOLTO UTILE (ELENCO NON ESAUSTIVO)

- UNI EN ISO 9001:2015, Sistemi di gestione per la qualità - Requisiti
- UNI EN ISO 14001:2015, Sistemi di gestione ambientale - Requisiti e guida per l'uso
- UNI EN ISO 22301:2019, Sicurezza e resilienza - Sistemi di gestione per la continuità operativa - Requisiti
- UNI CEI EN ISO/IEC 27001:2017, Tecnologie Informatiche - Tecniche di sicurezza - Sistemi di gestione della sicurezza dell'informazione - Requisiti
- UNI ISO 37001:2016, Sistemi di gestione per la prevenzione della corruzione - Requisiti e guida all'utilizzo
- ISO 37301:2021, Sistemi di gestione per il rispetto degli obblighi (*compliance*) - Requisiti e guida per l'uso (pubblicata il 13/04/2021, sostituisce la UNI ISO 19600:2016)
- UNI ISO 45001:2018, Sistemi di gestione per la salute e sicurezza sul lavoro - Requisiti e guida per l'uso

Nota: l'ordine è dato dal numero di ciascuna norma

Gennaro Bacile di Castiglione
Coordinatore UNI/CT 043/GL 02 "Gestione del Rischio"

Emilia Giovanna Catto
Membro UNI/CT 004/GL 01 "Sistemi di Gestione Ambientale"

GUIDELINES FOR THE MANAGEMENT OF LEGAL RISK

UNI ISO 31022 assists organizations in managing legal risk efficiently and cost effectively in order to meet the expectations of a wide range of stakeholders. By developing an improved understanding of the external and internal legal context, organizations may be able to develop new opportunities or improve operational performance. One of the objectives is to help organizations to develop and spread a positive culture of compliance, considering that an effective and sound management of legal risks should be considered as an opportunity to be pursued and seized, due to the numerous advantages that it offers. More details in this article.

Note

[1] La norma è identica alla ISO 31022, pubblicata nel maggio 2020 e adottata da UNI nel febbraio 2021.
[2] La funzione di *Compliance* è, in generale, una funzione di controllo indipendente la cui missione consiste nel presidiare il rischio di mancato rispetto degli obblighi.