La gestione del rischio è parte integrante della governance di un'organizzazione

di Gennaro Bacile di Castiglione

Sin dalla sua prima edizione del 2009 la ISO 31000[1] ha avuto una grande diffusione ed è stata da subito tra le dieci norme ISO più popolari, adottata da almeno 39 Paesi come norma nazionale (tra cui l'Italia e tutti gli altri Paesi OCSE). Inizialmente era stata sviluppata da un gruppo di lavoro ad-hoc, direttamente costituito in seno all'ISO/TMB *(Technical Management Board)*. Preso atto dell'interesse crescente per l'argomento, pochi anni dopo la pubblicazione della prima edizione era stato creato un *Project Committee* trasformato nel *Technical Committee* ISO/TC 262 *Risk Management* nell'agosto 2012. Inizialmente i Paesi membri effettivi erano 18, oltre a 7 Paesi osservatori. Attualmente conta 59 Paesi membri effettivi e 20 osservatori, con 11 gruppi di lavoro attivi e 6 documenti in fase di elaborazione.
L'edizione 2018 nasce dalla necessità di far sì che tale norma sia uno strumento in linea con lo stato dell'arte e con le necessità di tutti coloro che desiderino contribuire a creare e proteggere il valore per l'organizzazione per cui operano e per tutte le sue parti interessate rilevanti. Aiuta i *leader* a tutti i livelli nello stabilire e nel raggiungere gli obiettivi strategici e operativi, attraverso una gestione efficace ed efficiente dei relativi rischi e in grado di supportare il processo decisionale, allo scopo di migliorare le prestazioni dell'organizzazione.
Tra gli obiettivi di questa seconda edizione della linea guida sulla gestione del rischio vi erano quelli di:

- aumentare la comprensibilità del testo e la facilità di utilizzo;
- mettere in evidenza l'importanza di rendere il *risk management* parte integrante del sistema di gestione dell'organizzazione, dei suoi processi, della strategia e delle attività operative, allo scopo di consentire un processo decisionale informato e, soprattutto, consapevole;
- insistere sull'impegno e sul coinvolgimento attivo di tutte le parti interessate rilevanti esterne e interne, a partire dall'alta direzione e dai *leader* a tutti i livelli.

Lo sviluppo della nuova edizione ha creato delle aspettative che sembrano essere state in buona parte soddisfatte. L'interesse per la ISO 31000 è cresciuto in maniera esponenziale per l'introduzione da parte ISO della HLS (Struttura di Alto Livello), che ha come caratteristica peculiare quella di richiedere un approccio basato sul rischio alla gestione dell'organizzazione e che è stata imposta per tutte le norme sui sistemi di gestione a partire dal 2012.
Il nuovo testo si presenta più conciso e comprende alcuni cambiamenti sostanziali come, ad esempio, l'importanza data ai fattori umani e culturali nel raggiungimento degli obiettivi di un'organizzazione e una maggiore enfasi su una più solida integrazione del *risk management* con il processo decisionale e, più in generale, con tutti i processi del sistema di gestione a livello sia strategico sia operativo.
La ISO 31000 e tutti gli altri documenti elaborati nell'ambito dell'ISO/TC 262 hanno assunto una valenza culturale decisamente importante per lo sviluppo di nuove norme ISO e potenzialmente, sia pure in maniera indiretta, per l'intero mondo della normazione. Infatti l'Annex SP delle Direttive ISO[2] stabilisce che un *Technical Committee* ISO, che desideri sviluppare norme per settori specifici che includano requisiti, linee guida e aspetti terminologici relativi alla gestione del rischio, ha l'obbligo di fare riferimento alla ISO 31000 e all'ISO/TC 262. Lo stesso Annex SP impone riferimenti obbligatori simili su argomenti chiave per la gestione nelle organizzazioni[3].
Per questo l'ISO/TC 262 e tutti i corrispondenti gruppi di lavoro nazionali hanno una grande responsabilità e un obbligo di chiarezza nei confronti sia di chi vuole sviluppare nuove norme destinate ad affrontare anche la gestione dei rischi, sia degli utilizzatori di quei documenti.

La ISO 31000 attuale risulta essere un documento introduttivo alla gestione del rischio più semplice e più snello dell'edizione precedente, una guida utile e con un'ampia applicabilità a qualsivoglia caso specifico e a ogni tipo di rischio, un documento generico ma rilevante per tutte le organizzazioni di qualunque dimensione e settore, indipendentemente dal o dai Paesi in cui opera. Per la sua essenzialità, però, presenta ancora alcuni aspetti che sarebbe opportuno approfondire e chiarire in modo esaustivo e privo di ambiguità, quali ad esempio la relazione tra i concetti di opportunità, minacce/pericoli e rischi, oltre alla differenza tra il significato di "effetti" come si trova nella definizione di rischio e quello di "conseguenze" di un evento che hanno influenza sugli obiettivi. La futura IEC/ISO 31010[4] in fase di pubblicazione (revisione della IEC/ISO 31010:2009) fornirà già una serie di approfondimenti in grado di chiarire numerosi aspetti della valutazione dei rischi e, più in generale, sul r*isk management* e sui suoi concetti fondamentali.
Inoltre l'ISO/TC 262 ha in preparazione, tra gli altri, due documenti che potranno risultare preziosi a tale scopo: un Handbook sull'applicazione della ISO 31000 e la norma terminologica ISO 31073, che sostituirà il precedente vocabolario sulla gestione del rischio, la ISO Guide 73. In particolare nelle intenzioni dell'ISO/TC 262/TC G1[5], la struttura della futura ISO 31073 sarà simile a quella dei documenti sulla terminologia delle famiglie di norme sui sistemi di gestione, quale ad esempio la ISO 9000 che è suddivisa in tre sezioni fondamentali:

1. concetti fondamentali e principi di gestione per la qualità;
2. termini e definizioni;
3. appendice con la rappresentazione grafica delle relazioni tra i concetti.

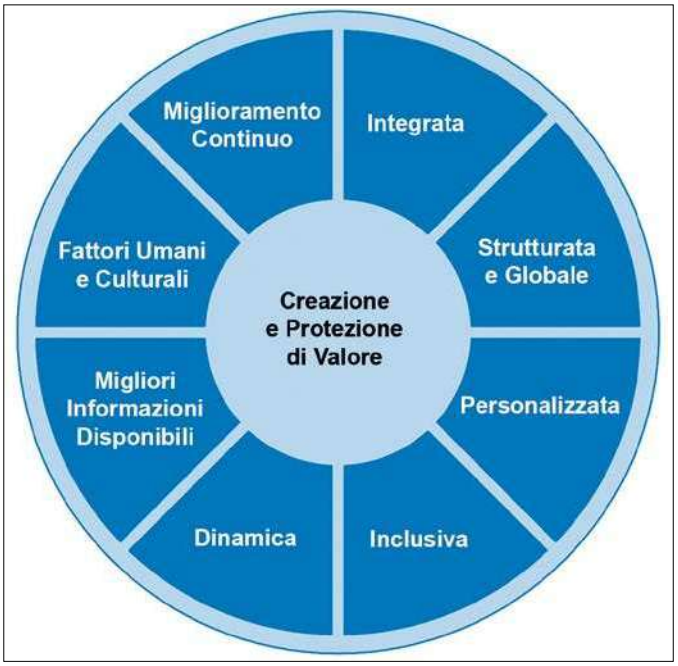

Figura 1 - Principi per la gestione del rischio (da UNI ISO 31000)

Struttura sulla quale il gruppo di lavoro UNI sulla gestione del rischio si trova particolarmente d'accordo. Infatti già oltre 10 anni fa, in occasione della preparazione dei documenti pubblicati da ISO nel 2009, aveva suggerito una simile impostazione, soprattutto in relazione ai diagrammi concettuali.
La ISO 31000 ribadisce che il rischio è un concetto neutro e che le sue potenziali conseguenze in relazione agli obiettivi possono essere sia positive, sia negative o contemporaneamente positive e negative. Può essere comunque utilizzata anche da coloro i quali ritengano che il rischio

Note

[1] La nuova ISO 31000 è stata pubblicata il 14/02/2018, recepita in Italia come UNI ISO 31000 il 17/05/2018 e pubblicata in italiano il 20/11/2018
[2] ISO/IEC Directives, Part 1, Consolidated ISO Supplement, 2018 (9th edition) - può essere scaricato liberamente da https://www.iso.org/directives-and-policies.html
[3] Annex SP, che era nato prescrivendo solo il riferimento alla ISO 14001, ai documenti correlati e al TC 207 per aspetti legati alla gestione ambientale, è stato esteso anche alla famiglia ISO 9000 (gestione per la qualità), alla famiglia ISO 55000 (asset management) e alla ISO 26000 per la responsabilità sociale, oltre che alla ISO 31000 come detto
[4] La IEC/ISO 31010:20XX, di cui è prevista la pubblicazione nel corso del 2019, è stata elaborata da un gruppo di lavoro misto, costituito da esperti dell'ISO/TC 262 *Risk management* e dal IEC/TC 56 *Dependability*, ai cui lavori l'Italia ha contribuito con esperti UNI e CEI
[5] Terminology Coordination Group

possa avere potenziali conseguenze esclusivamente negative, anche se costoro perdono una buona parte dei benefici che si possono ottenere applicando le linee guida e i principi in essa contenuti. Infatti il principio "zero" ci dice che lo scopo della gestione del rischio è la creazione e la protezione di valore per l'organizzazione e per le sue parti interessate. La gestione del rischio è *"cultura, processi e strutture volti a realizzare le opportunità potenziali mentre si tengono sotto controllo gli effetti indesiderati* [6]".

D'altra parte anche la ISO 9001 al punto 0.3.1 ci dice che il *risk-based thinking* è *"volto a cogliere le opportunità e a prevenire risultati indesiderati"*.

Il *risk-based thinking* rappresenta un atteggiamento mentale che si configura come una cultura diffusa e ben radicata nell'organizzazione (parte integrante della "conoscenza organizzativa"), un modo di pensare per poter prendere decisioni consapevoli, senza richiedere metodologie formali per la valutazione e il trattamento del rischio. Una gestione del rischio "formale", invece, si configura come un processo strutturato e sistematico quale quello che ritroviamo descritto nella ISO 31000.

Il *risk-based thinking* dovrebbe essere diffuso a tutti i livelli dell'organizzazione per far sì che anche chi non abbia alcuna delega di responsabilità sia in grado di identificare e segnalare ai responsabili opportunità e minacce: tutto ciò è anche in linea con quanto suggerito dalla ISO 31000 dove si dice che, nell'ambito di assegnate *"autorità, responsabilità e obbligo di rendere conto ai livelli appropriati all'interno dell'organizzazione", "ognuno ha la responsabilità di gestire il rischio"*.

Il rischio è l'effetto dell'incertezza in relazione agli obiettivi: in altre parole può essere considerato come la percezione che noi umani abbiamo nei riguardi del potenziale comportamento di un sistema, derivante dall'incertezza sulla conoscenza e/o sulla comprensione di un evento futuro, delle sue conseguenze sugli obiettivi, così come delle variabili coinvolte, inclusa la possibilità e la probabilità di accadimento. L'incertezza non riguarda soltanto il raggiungimento o meno degli obiettivi, ma interviene anche nel processo con cui si stabiliscono gli obiettivi stessi (vedere anche la figura 2).

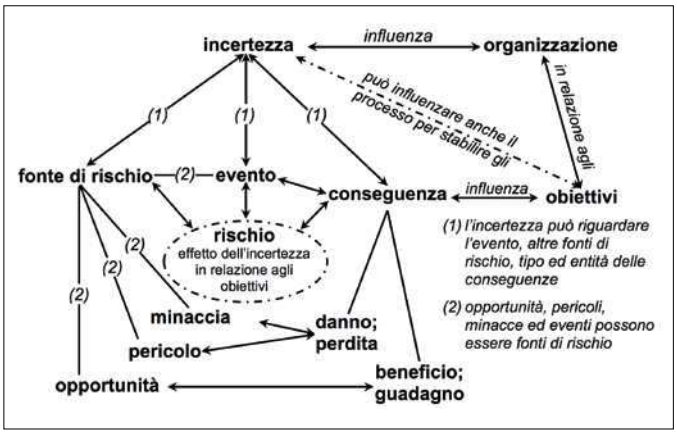

Figura 2 - Incertezza, rischio e concetti correlati

Il gruppo di lavoro UNI sulla gestione del rischio ha richiesto la collaborazione di altri organi tecnici nazionali, che seguono le più diffuse norme ISO sui sistemi di gestione, per portare avanti la stesura di una linea guida italiana dal titolo provvisorio: *Gestione del Rischio - Linea guida per l'integrazione della gestione del rischio nella governance e nelle attività operative di un'organizzazione in accordo alla UNI ISO 31000, con particolare riferimento ai sistemi di gestione basati sulle norme ISO che seguono la struttura di alto livello (HLS).*

Nell'introduzione si afferma, tra l'altro, che: *la struttura di alto livello (HLS) ha molte correlazioni con ISO 31000 e alcune parti derivano direttamente da quest'ultima, sia pure con semplificazioni che, in alcuni casi, necessitano di chiarimenti. Un'applicazione maggiormente strutturata e organica della gestione del rischio in accordo alle linee guida offerte dalla UNI ISO 31000, costituisce esempio di applicazione di un approccio olistico, che consente di cogliere i vantaggi dalla sinergia che si crea attraverso l'integrazione dei principi, della struttura di riferimento e del processo per la gestione del rischio con i requisiti delle norme sui sistemi di gestione basate sulla struttura di alto livello (HLS), in modo tale da creare un sistema unico di gestione integrata efficace ed efficiente.*

Per applicare con efficacia ed efficienza le raccomandazioni della ISO 31000 occorre:

- approfondire e assimilare i principi di cui al punto 4 della norma (vedere figura 1);
- stabilire la "struttura di riferimento" *(framework)*, ovvero quell'insieme di elementi organizzativi che consentono di progettare, mettere in atto, monitorare, riesaminare, registrare, informare e migliorare continuamente la gestione del rischio in tutta l'organizzazione;
- integrare tali elementi nel sistema di *governance* dell'organizzazione e in tutti i suoi processi gestionali e operativi;
- progettare un processo di *risk management* (figura 3) in modo che sia personalizzato e adattato al proprio contesto interno ed esterno;
- mettere in atto tale processo per consentire di rafforzare, attraverso decisioni consapevoli, la creazione e la protezione del valore, per l'organizzazione e per le sue parti interessate;
- assicurarsi che la gestione del rischio sia integrata in modo tale da consentire, per tutti i processi dell'organizzazione, di cogliere le opportunità sfruttando i propri punti di forza e prevenire possibili effetti negativi, derivanti da minacce, da pericoli e da punti di debolezza.

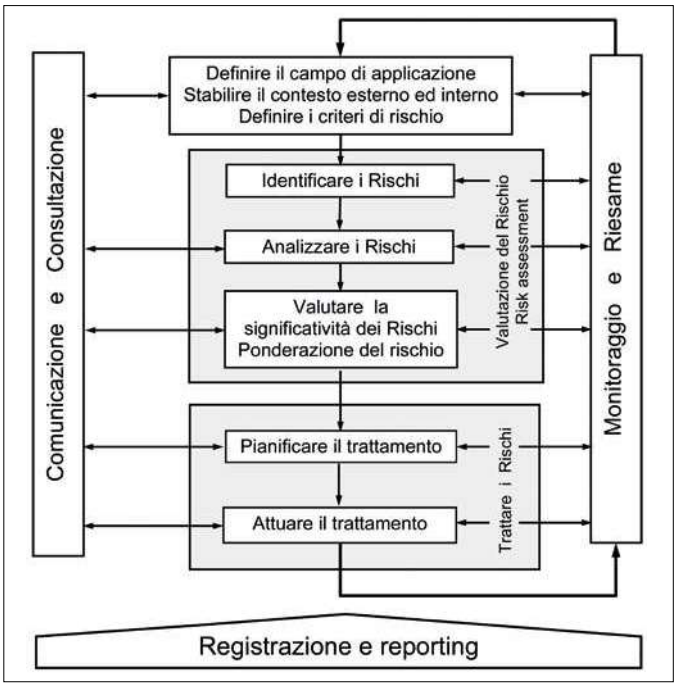

Figura 3 - Processo di Gestione del Rischio

Gennaro Bacile di Castiglione
Coordinatore UNI/CT 043/GL 02 "Gestione del Rischio"
Membro di Organi Tecnici UNI su designazione dell'Ordine degli Ingegneri di Monza e Brianza e del Consiglio Nazionale degli Ingegneri

Note

[6] Definizione di *risk management* da AS/NZS 4360:2004, la norma, emessa da Australia e Nuova Zelanda, che è stata il punto di partenza della ISO 31000.

RISK MANAGEMENT IS AN INTEGRAL PART OF ORGANIZATION'S GOVERNANCE

The new ISO 31000 provides guidelines for all those people whose goal is to create and protect value for organizations and for all relevant interested parties by setting and achieving objectives, managing related risks and making decisions in order to improve performance. The second edition of the standard was developed in order to improve usability and make the new document clearer and easier to implement. The new document highlights the importance of making risk management part of the organization management system structure, processes, objectives, strategy, and activities in order to enable a informed and aware decision-making. It places a greater focus on the involvement of top management and leaders at all levels, as well as of other internal and external interested parties. More details in this article.