AICQ per U&C

Gestione del Rischio nelle norme della famiglia ISO 9000

Soddisfare i requisiti UNI EN ISO 9001:2008 applicando i principi e le metodologie del Risk Management, quale processo fondamentale per una gestione consapevole e responsabile di un'organizzazione.

Si assiste a un proliferare di norme e linee guida internazionali sui Sistemi di Gestione (SG), che affrontano singolarmente i diversi aspetti delle attività fornendo requisiti legati a qualità, ambiente, salute e sicurezza sul luogo di lavoro, responsabilità sociale e altro. È opportuno non lasciarsi trarre in inganno da tutti questi "Sistemi di Gestione", ma tenere ben presente che, contrariamente a quanto affermato nella nota alla definizione[1] 3.2.2 dell'ISO 9000, esiste un solo e indivisibile SG complessivo di un'organizzazione, volto a un suo governo "consapevole" e "responsabile" ed all'eccellenza nelle prestazioni a vantaggio di tutte le parti interessate. Tale "SG" dovrebbe *definire, attuare e soddisfare in modo coerente e armonico la politica e gli obiettivi legati a tutti gli aspetti dell'attività di un'organizzazione, con lo scopo di guidarla, tenerla sotto controllo, aiutarla a cogliere le opportunità e difenderla dagli eventi indesiderati, ponendo l'accento sulla prevenzione di tali eventi e la minimizzazione delle loro conseguenze negative.*

La definizione, del tutto personale, di "SG", prima riportata, è derivata dalle varie definizioni di SG e integrata con quella di "Risk Management" che la norma AS/NZS 4360:2004 indica come "*la cultura, i processi e le strutture volte a concretizzare le opportunità potenziali mentre gestiscono gli effetti negativi*". Se sposiamo questa filosofia, vorrà dire che ci saremo convinti che le metodologie legate a questa disciplina potrebbero aiutare le nostre organizzazioni ad essere sempre più competitive, in linea con la visione "bilaterale" dei rischi illustrata nella Figura 1 e confermata dalla guida ISO 31000:2009 (Risk Management - Principi e linee guida). D'altra parte anche ISO 14001 e Regolamento EMAS definiscono l'impatto ambientale come "qualunque modifica dell'ambiente, negativa o positiva".

L'ISO 9001:2008, pur non introducendo nuovi requisiti, mette in atto un primo timido tentativo di parlare più esplicitamente di rischi associati al business (punto 0.1 Introduzione – Generalità) che influenzano la progettazione e l'attuazione del Sistema di Gestione per la Qualità (SGQ).

L'ISO 9001:2000 non citava mai esplicitamente i rischi, ma li trattava in modo indiretto: le non conformità, in particolare potenziali, come rischi e le azioni correttive/preventive per il loro trattamento. Ritengo, però, che solo una piccolissima percentuale di SGQ certificati consideri e attui tale visione. Inoltre l'accento è posto soprattutto sui rischi con conseguenze negative e occorre arrampicarsi sui vetri per vedere nel concetto di "miglioramento continuo" un vago suggerimento circa la possibilità di cogliere le opportunità. D'altra parte si parla soltanto di azioni correttive e/o preventive, mentre i riferimenti alle azioni di miglioramento sono soltanto indiretti.

Per contro le ISO 9001 e 14001, nelle rispettive introduzioni, a proposito di "Compatibilità con altri SG", accennano al Risk Management come un ulteriore SG. In entrambe le norme il senso della frase è:

La presente norma non include requisiti specifici di altri SG, come quelli particolari per ...omissis... o per la gestione dei rischi, sebbene i suoi elementi possano essere allineati o integrati con quelli di altri SG.

La prima osservazione è che il Risk Management non è un ulteriore "Sistema di Gestione", come si deduce chiaramente dalla ISO 31000. Nonostante il parere di alcuni, infatti, la maggioranza dei membri ISO partecipanti al GdL "Risk Management", tra cui l'Italia, si era espressa nel senso di considerarlo un insieme di processi (macro-processo - Figura 2), con una "struttura di Riferimento" (framework) che, permeando tutti i processi, risulta uno strumento per il governo efficace, efficiente, responsabile e consapevole dell'organizzazione.

La seconda osservazione è che quell'affermazione appare in forte contrasto con lo spirito stesso delle norme sui SG: infatti, per la qualità è necessario tenere sotto controllo almeno i rischi legati al prodotto e al mercato e in ambito ISO 14001 almeno quelli legati agli aspetti ambientali delle proprie attività e prodotti.

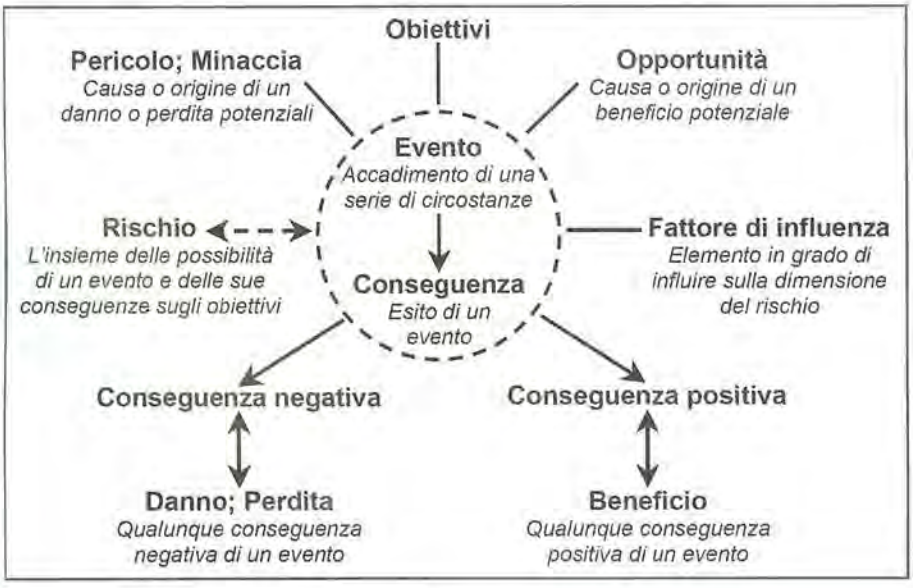

Figura 1 - Concetti relativi al Rischio (da UNI 11230:2007)

Il futuro delle norme sui sistemi di gestione e il risk management

È significativo il fatto che, per la revisione della norma ISO 19011 (Linee guida per gli audit qualità e ambiente), s'invitassero i membri del GdL ISO sul Risk Management a parteciparvi, motivando la richiesta con la considerazione che la nuova ISO 31000 avrebbe avuto influenza sulle future edizioni delle norme riguardanti i SG, destinati a divenire sempre più "basati sul rischio".

Il macro-processo di risk management

La figura 2 si ritrova, nella sostanza, in molte pubblicazioni, compresa la più recente ISO

31000, e fornisce una visione di assieme del macro-processo di gestione del rischio applicabile a tutti gli aspetti dell'attività di un'organizzazione.
Questo schema evidenzia il ciclo PDCA, in linea con la filosofia del miglioramento continuo.
Il risk management è un macro-processo iterativo di direzione, trasversale, che interagisce con tutti gli altri processi operativi, gestionali e di supporto. Per questo dovrebbe essere attuato attraverso una cultura opportunamente diffusa in tutti i settori e livelli: una filosofia ed un elemento portante del governo di un'organizzazione. A tale proposito svolgono un ruolo di primaria importanza i requisiti di "competenza, formazione/addestramento e consapevolezza", comuni a tutte le norme sui SG.
Si può affermare che la conoscenza dei rischi aiuta a prendere decisioni consapevoli e responsabili, in linea con uno degli otto "Principi di gestione per la qualità": *Decisioni basate su dati di fatto.* Se conosci il rischio puoi tenerlo sotto controllo, minimizzando i possibili eventi indesiderati ed aumentando gli sforzi per cogliere le opportunità ed ottenere benefici.

ISO 9001:2008 e la gestione del rischio

Sono numerosi i requisiti nel corpo della norma che richiamano, direttamente o indirettamente (anche se non sempre in maniera esplicita), concetti e principi della gestione dei rischi. Spesso tali richiami erano già presenti nell'edizione 2000 e nelle precedenti, ma in qualche caso sono stati evidenziati maggiormente nei chiarimenti e nelle note del 2008. Pur essendo possibile un esame puntuale e dettagliato dell'intera norma, nel seguito riportiamo e commentiamo soltanto gli aspetti di alcuni punti, ritenuti particolarmente efficaci per evidenziare come sia possibile e, soprattutto, opportuno riesaminare l'applicazione ai propri processi di tutti i requisiti ISO 9001 alla luce del Risk Management.
Nel testo si è utilizzata la numerazione dei punti ISO 9001:2008 e, tra virgolette e in corsivo, si riportano frasi integrali tratte dalla norma. A volte si riportano frasi da altre norme: in tali casi è indicato il riferimento puntuale della citazione.

4 Sistema di Gestione per la Qualità

4.1 Requisiti Generali

Questo punto della norma ha due parti strettamente legate tra loro, per le quali le metodologie del Risk Management possono aiutare a definire e a migliorare il controllo dei processi del SGQ.
La prima riguarda la "Mappatura dei Processi": "*determinare i processi necessari per il SGQ e la loro applicazione nell'ambito di tutta l'organizzazione*", aggiungerei indipendentemente dal fatto che tali processi siano realizzati all'interno o affidati all'esterno (outsourced processes, seconda parte del punto 4.1). L'analisi che è necessario fare per "determinare" tutto ciò che serve per governare al meglio tali processi, monitorarli, misurarli, migliorarli ecc., include il riuscire a identificare quali siano i punti e gli aspetti critici dei processi stessi e delle loro interazioni, in altre parole i rischi, intesi come opportunità da sfruttare, pericoli, minacce, non conformità potenziali da evitare o comunque fronteggiare. Infatti la nota 3, aggiunta nell'edizione 2008, chiarisce in modo inequivocabile che "*il tipo e l'estensione del controllo da applicare al processo affidato all'esterno possono essere influenzati da fattori quali l'impatto potenziale del processo affidato all'esterno sulla capacità dell'organizzazione di fornire un prodotto conforme ai requisiti*". Anche se la nota fa riferimento soltanto a quelli in outsourcing, è pressoché automatico pensare che tale concetto dovrebbe essere applicato a tutti i processi del SGQ.
Per ogni processo, interno o esterno, si tratta di identificare l'*impatto potenziale* sui quelli a valle e sul prodotto finale, impatto che può essere positivo o negativo: controlli, monitoraggi e misurazioni dovrebbero essere tali da riuscire a massimizzare gli impatti positivi (cogliere le opportunità di miglioramento) e minimizzare quelli negativi (evitare gli eventi indesiderati, le non conformità).
Il ciclo insito nel macro-processo di gestione del rischio (figura 2), contiene quanto necessario per un'analisi dei processi del SGQ effettuata proprio in quest'ottica a partire dalla definizione del contesto, proseguendo con la "comunicazione e consultazione" in parallelo alla "valutazione del rischio", poi con il "trattamento", infine con la "misurazione/riesame", per poi ripetere il ciclo PDCA, in ottica di miglioramento continuo.
D'altra parte l'ISO 9000, al punto 2.3 definisce un approccio per sviluppare e attuare un SGQ del tutto simile a quello indicato al 4.1 della 9001, aggiungendo che occorre "*determinare le esigenze e le aspettative dei clienti e delle altre parti interessate*", corrispondente al "*definire il contesto*" nel ciclo del Risk Management, con l'aiuto della "*comunicazione e consultazione*".
È un passo di fondamentale importanza per capire cosa si aspettano i clienti (in ottica ISO 9001) e le altre parti interessate interne ed esterne (in ottica ISO 9004, TQM, modelli di eccellenza): mette in grado di definire i criteri di valutazione dei rischi (il loro livello di significatività e di accettabilità) e permette di agevolare l'operatività di un'organizzazione creando un clima favorevole alla sua attività grazie a relazioni non conflittuali con chi abita nelle vicinanze del sito produttivo, con i media, con l'opinione pubblica e con le autorità, oltre a migliorare i rapporti con le banche e il mercato finanziario in genere.
I punti 5.5.3 (Comunicazione interna), 7.2.3 (Comunicazione con il Cliente) e 8.2.1 (Soddisfazione del Cliente) hanno un collegamento stretto con "*la Comunicazione e la Consultazione con i portatori d'interesse esterni e interni*" che "*dovrebbe aver luogo durante tutte le fasi del processo di gestione del rischio*" (punto 5.2 - ISO 31000:2009).

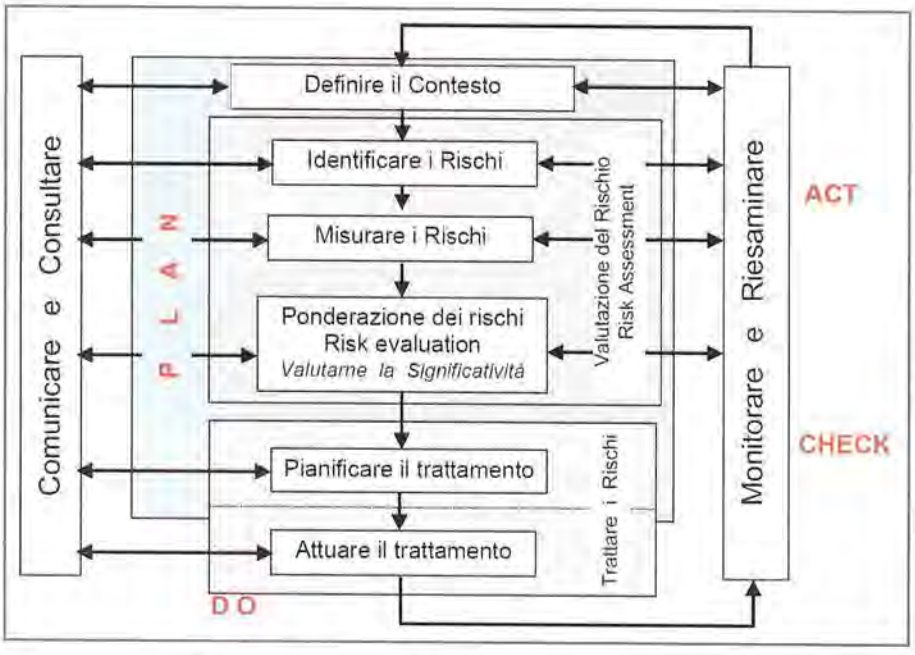

Figura 2 - Macro-processo di gestione del rischio

4 Sistema di Gestione per la Qualità

4.2 Requisiti relativi alla documentazione

La norma, tra le altre cose, richiede che la documentazione del SGQ includa i "*documenti, comprese le registrazioni, che l'organizzazione ritiene necessari per assicurare l'efficace pianificazione, funzionamento e tenuta sotto controllo dei propri processi.*"

Come fare a definire quali documenti, oltre a quelli richiesti dalla norma, siano necessari e quale debba essere il loro grado di dettaglio? Oltre a tener conto, come suggerito dalla nota 2, della dimensione dell'organizzazione, del tipo di attività, della complessità dei processi, delle loro interazioni e della competenza del personale, le domande da porsi potrebbero essere in sostanza due, per ogni area/processo:

- Quali impatti negativi potrebbe generare la mancanza di una procedura, un'istruzione, una registrazione o un loro scarso grado di dettaglio?
- Quali impatti positivi si potrebbero generare inserendo una nuova procedura, un'istruzione, una registrazione o migliorando il grado di dettaglio di quelle esistenti?

5 Responsabilità della Direzione

In tutto il capitolo 5 troviamo legami con il Risk Management. D'altronde il secondo principio dell'ISO 31000:2009 ci dice che "*la gestione del rischio fa parte delle responsabilità di direzione ed è parte integrante di tutti i processi dell'organizzazione, inclusi la pianificazione strategica e la gestione dei progetti e del cambiamento*".

Note

[1] La nota alla definizione 3.2.2 - ISO 9000:2005, recita: "*Un sistema di gestione di un'organizzazione può includere sistemi di gestione differenti, quali un sistema di gestione per la qualità, un sistema di gestione finanziaria o un sistema di gestione ambientale*".

[2] Esiste una correlazione stretta tra gli otto principi di gestione per la qualità (ISO 9000:2005) e gli undici principi per un'efficace gestione del rischio (ISO 31000:2009).

[3] Vedere in proposito la guida ISO/IEC 31010:2009 (Risk management - Risk assessment techniques).

Probabilmente il punto 5.4 (obiettivi e pianificazione del SGQ) è quello più chiaramente coinvolto, se si considera la definizione di Rischio in cui è insito il concetto di influenza che questo ha sulla capacità/possibilità di raggiungere gli obiettivi.

6 Gestione delle Risorse

Anche il punto 6, pur non contenendo riferimenti espliciti al Risk Management, dovrebbe essere interpretato in quest'ottica per mettere a disposizione risorse (personale, infrastrutture e ambiente di lavoro) tali da consentire di cogliere al meglio le opportunità e di evitare gli eventi indesiderati, perseguendo l'obiettivo principale di soddisfare sempre più i clienti.

7 Realizzazione del Prodotto

In tutto il punto 7, compreso il 7.6 (apparecchiature di monitoraggio e di misurazione), valgono le riflessioni fatte per il punto 4.1, considerando i rischi legati a prodotto e processi del SGQ.

In aggiunta possiamo ricordare che i rischi legati alla catena di fornitura sono uno degli argomenti maggiormente trattati nella letteratura e sono un aspetto particolarmente critico nelle aziende moderne dove l'esternalizzazione è sempre più frequente, così come la tendenza a ridurre sempre più le giacenze di magazzino. Il collegamento con i processi affidati all'esterno, di cui al 4.1, è molto chiaro (almeno alla luce dell'edizione 2008).

8 Misurazione, Analisi e Miglioramento

Valgono anche qui molte delle considerazioni riportate per il punto 4.1. L'intero punto 8, insieme con il 5.6 (Riesame di Direzione) dovrebbe essere affrontato tenendo presenti le attività di "Monitoraggio e Riesame" suggerite al punto 5.6 della ISO 31000:2009.

Gestione emergenze

L'ISO 9001 non contiene alcun requisito relativo alla gestione delle emergenze, né suggerimenti nelle note. Eppure nell'edizione 2008 si sarebbe potuto inserire qualche indicazione sull'argomento, tenendo conto che l'ISO GUIDE 72:2001 (Linea guida interna ISO per la giustificazione e lo sviluppo delle norme sui SG), in Appendice B, dove elenca i "Requisiti Comuni" dei SG, prevede (punto B.2.7) una "*preparazione alle emergenze per eventi prevedibili*". La guida ISO 9004:2009 fa esplicito riferimento ai piani di emergenza, così come, tra le norme per la certificazione di SG, ISO 14001:2004 e OHSAS 18001:2007 hanno un requisito specifico (in entrambe al punto 4.4.7 – Preparazione e risposta alle emergenze). Questa appare una carenza macroscopica della ISO 9001:2008, in quanto le emergenze di qualsiasi tipo possono influenzare la qualità o la capacità dell'organizzazione di soddisfare i requisiti del prodotto e altre aspettative dei clienti.

Riporto un solo esempio tra i tanti che si potrebbero citare: un'esplosione, un incendio, un terremoto o un'inondazione potrebbero avere conseguenze anche sulla qualità, oltre che sull'ambiente, sulla salute e sicurezza dei lavoratori e/o dei vicini. Materie prime, componenti, prodotti finiti, potrebbero danneggiarsi; oltre ai costi relativi, l'organizzazione potrebbe non essere in grado di soddisfare alcuni requisiti contrattuali legati, ad esempio, ai termini di consegna. Si dovrebbero considerare non soltanto le emergenze dirette, ma anche quelle indirette che potrebbero coinvolgere i propri fornitori.

Esiste già la norma inglese BS 25999-2:2007 "Business continuity Management: specification", prevista per la certificazione; il Comitato Tecnico ISO/TC223 (Societal Security) sta preparando norme sull'argomento, tra cui l'ISO/DIS 22301 (Preparedness and continuity management systems – Requirements) prevista per la certificazione, oltre ad alcune guide sull'argomento.

Considerazioni finali

Utilizzando i principi[2] e, almeno in parte, le metodologie del Risk Management, potremmo riuscire a migliorare l'efficacia del SGQ. Iterando il ciclo del processo di gestione del rischio e incrementando l'uso degli strumenti messi a disposizione[3], saremo in grado di avere un quadro sempre più preciso dei rischi correlati alla nostra attività, attraverso dati e informazioni utili a stabilire nuovi traguardi ed obiettivi, anche in termini economico-finanziari.

Sarà quindi possibile attuare una gestione sempre più consapevole dell'organizzazione in accordo con il principio delle "decisioni basate su dati di fatto". ■

Gennaro Bacile di Castiglione
Membro del SC UNI Gestione del Rischio e dell'ISO/TC 262 Risk Management
Consulente, Referente dei Registri SICEP di AICQ SICEV