Rischio e *"Risk Based Thinking"* nella futura ISO 9001

L'ISO ha sviluppato e imposto, dal 2012, una struttura comune per tutti i futuri Management Systems Standard (MSS). Si tratta dell'ormai famosa *High Level Structure* (HLS), che include, oltre al titolo dei vari punti principali per i futuri MS ISO, molte definizioni e parti consistenti di testo. La sua applicazione è obbligatoria (per lo meno a livello ISO, come spiegato in un altro articolo dedicato nel presente dossier) sia per tutte le nuove norme sia per la revisione di quelle attualmente in vigore.
È stata sviluppata dall'ISO/TMB/JTCG "Joint technical Coordination Group on MSS", inizialmente come ISO Guide 83, poi inserita all'interno di un "Annex SL" alle ISO/IEC Directives, Part 1 Consolidated ISO Supplement del 2012, aggiornato nel 2013.
Con la nuova struttura sono già uscite alcune norme, tra cui ISO 22301:2012 (Business Continuity MS) e ISO/IEC 27001:2013 (Information Security MS); nuove norme sono in fase di sviluppo più o meno avanzata, per altre, come le più conosciute ISO 9001 e ISO 14001, è iniziata la revisione periodica e si prevede una pubblicazione quasi contemporanea nel corso del 2015.
HLS ha il pregio di sottolineare che il MS di un'organizzazione è unico e i sempre più numerosi MSS sono dedicati a stabilire i requisiti per una o più "discipline", evidenziando tutti gli elementi comuni, i punti di forza del MS Generale, già illustrati nella ISO Guide 72:2001[1] .
Nella nuova struttura si ritrovano, anche se ordinati in modo parzialmente diverso, tutti gli elementi chiave comuni delle ISO 9001:2008 e 14001:2004, che nelle future edizioni saranno allineati come numerazione e articolazione dei punti. Tra gli scopi di questo approccio comune per tutti i MSS è di aumentarne la coerenza e il valore per gli utilizzatori, facilitandone l'utilizzo contemporaneo con lo sviluppo e l'attuazione di un unico MS, che soddisfi contemporaneamente più MSS (talvolta chiamato "Sistema di Gestione Integrato").
I nuovi requisiti che fanno riferimento al rischio e alla sua gestione sono tra le novità più significative introdotte della HLS. In realtà si tratta solo di aver reso esplicito qualcosa che era già ampiamente sottinteso nella gestione di un'organizzazione, da qualsiasi punto di vista la si affrontasse, a partire dalla qualità secondo la ISO 9001. Nel seguito cercheremo, tra l'altro, di chiarire meglio tale asserzione. Le considerazioni, anche se attraverso esempi riferiti al CD della futura revisione della ISO 9001 e, in parte, alla sua edizione attuale (2008), sono applicabili a qualsiasi MSS.

Rischio e sistemi di gestione

Era già apparso chiaro da tempo che, nelle intenzioni di ISO, i futuri MSS sarebbero stati sempre più *"risk-based"*. Con questa motivazione, nel 2008, si invitavano gli esperti del *Working Group* (WG) ISO sul *Risk Management* a dichiarare la propria disponibilità a partecipare al processo di revisione della ISO 19011 riguardante gli audit di MS, giustificando la richiesta con la considerazione che la allora futura ISO 31000:2009[2] avrebbe potuto avere influenza sulle future edizioni dei MSS. Per inciso, nella 19011:2011 il termine "risk" è presente per oltre 50 volte con riferimento prevalente ai rischi relativi al processo di audit.
Nell'immaginario comune il rischio è visto come qualcosa che può portare esclusivamente a conseguenze negative. Questo è anche dovuto ad una imprecisione che si fa comunemente di considerare pericolo e rischio come sinonimi (errore avvalorato dai dizionari nelle varie lingue), mentre si tratta di due concetti distinti anche se correlati. Ad esempio, anche considerando solo le conseguenze negative, si assicura un rischio, non certamente un pericolo. Ovvero l'assicurazione, a fronte di un "premio", risarcirà, in tutto o in parte, i danni (conseguenze) che presumibilmente si possono avere per l'accadimento di un evento peri-

Note

[1] ISO Guide 72:2001 - Guidelines for the justification and development of management system standards - ritirata a maggio 2012, in concomitanza con la prima pubblicazione dell'HLS

[2] Irecapita in Italia come UNI ISO 31000:201, gestione del rischio - principi e linee guida

coloso. In questo esempio si evidenziano le componenti di un rischio "negativo": le sue "fonti" (pericolo, minaccia ed evento potenziale), le conseguenze e l'incertezza collegata alla probabilità dell'evento ed all'entità delle conseguenze.
Nell'immaginario comune, quindi, l'espressione *"Risk Based Thinking"* potrebbe essere intesa come manifestazione del più profondo pessimismo!
In realtà le cose stanno diversamente: basta pensare al mercato borsistico dove rischio elevato corrisponde alla possibilità di forti guadagni o perdite; per contro, il rischio basso consente guadagni modesti, ma anche una certa fiducia di non incorrere in perdite del capitale investito. In entrambi gli esempi vediamo che l'incertezza (del mercato, in questo caso) gioca un ruolo fondamentale.
Nell'ambito di un QMS, così come per ogni altro MS, il rischio è correlato alla volontà di concretizzare un'opportunità e riguarda tutto ciò che può agevolare o impedire il raggiungimento degli obiettivi relativi a quell'opportunità. Il *risk management* è uno strumento fondamentale per consentire delle decisioni "consapevoli" e, per questo, risponde perfettamente a uno dei principi di gestione per la qualità (QMPs), che nella versione aggiornata dell'ISO/CD 9001 - Annex A (QMP6 - Processo decisionale basato su evidenze) recita tra l'altro: *"Le decisioni basate sull'analisi e sulla valutazione di dati e informazioni hanno più probabilità di produrre i risultati desiderati. Il processo decisionale può essere complesso e spesso comporta qualche incertezza. È importante comprendere le relazioni di causa ed effetto e le conseguenze potenziali"*.
L'incertezza, le relazioni causa-effetto e le possibili conseguenze sono tra le componenti tipiche del rischio.

Nel prospetto 1 sono evidenziate le correlazioni tra i QMPs e i principi per una efficace gestione del rischio riportati al punto 3 della UNI ISO 31000:2010.
Il *"Risk Based Thinking"* è un atteggiamento mentale spontaneo di ogni essere vivente. Qualsiasi decisione umana, ma non solo, dalla più banale alla più critica, è il risultato di una valutazione del rischio per lo più inconsapevole. Gli esempi possono essere pressoché infiniti: scegliere come investire i propri risparmi, come vestirvi al mattino, le motivazioni per cui si prepara la lista della spesa prima di andare al supermercato, la decisione se prendere un medicinale dopo aver letto il "bugiardino" o se sottoporsi a un intervento chirurgico (ad esempio un intervento di plastica). In tutti questi esempi ci sono delle opportunità da cogliere, ma, al tempo stesso, occorre considerare potenziali effetti collaterali indesiderati. Siamo di fronte, inoltre, a un concetto relativo, per cui lo stesso rischio può avere conseguenze positive per alcuni soggetti e negative per altri. Rimanendo nel campo di atteggiamenti legalmente e moralmente corretti, la concorrenza (leale) è uno di tali rischi: il rapporto qualità-prezzo può fare guadagnare o perdere quote di mercato.

HLS, ISO/CD 9001 e rischio: le possibili criticità

L'ISO/TMB/JTCG ha sviluppato la HLS ispirandosi, per quanto riguarda il rischio alla ISO 31000:2009, ma, non volendo imporre la sua adozione come vincolante per tutti i MSS, ha cercato di rendere i concetti relativi ancora più generali di quanto già non fossero nella ISO 31000 stessa e nelle (identiche) definizioni della ISO Guide 73:2009 *(Risk management - Vocabulary)*.
La definizione di rischio della ISO 31000 è "effetto dell'incertezza sugli obiettivi", da intendersi come "influenza dell'incertezza sul raggiungimento degli obiettivi", in linea con le considerazioni fatte nel paragrafo precedente. Nella HLS, invece, è stato eliminato il riferimento agli obiettivi, probabilmente nel tentativo di darle un'accezione più ampia. Questo però ha fatto perdere di significato la definizione stessa che appare troppo vaga e senza correlazione con un qualsiasi MS. Infatti, la definizione di MS riportata nella HLS, ripresa da ISO/CD 9001 e 9000, ci dice che è un "*insieme di elementi correlati o interagenti di un'organizzazione finalizzato a stabilire politiche, obiettivi e processi per conseguire tali obiettivi*". Inoltre al punto 6.1 (HLS e ISO/CD 9001) si stabilisce che "*l'organizzazione deve determinare i rischi e le opportunità che è necessario affrontare per assicurare che il QMS possa conseguire gli esiti previsti*". Va da se che gli "esiti previsti" si raggiungono attraverso obiettivi e traguardi.
Nella definizione di rischio, la nota 1, ripresa anche in HLS, ISO/CD 9000 e 9001, precisa che *"un effetto è uno scostamento da quanto atteso - positivo e/o negativo"*. È chiaro quindi per tutti che in quest'ambito il rischio può avere conseguenze sia positive sia negative [3]. Da qui un altro aspetto critico si riscontra nell'espressione "rischi e opportunità" prima citata, che porterebbe a pensare ai rischi come qualcosa di legato esclusivamente a potenziali conseguenze negative e alle opportunità come sinonimo di "rischio positivo". Invece, anche in linea con la UNI 11230:2007 (Gestione del Rischio – Vocabolario), un'opportunità è una "fonte di rischio" (*"risk source"* definita nelle ISO 31000 e Guide 73) che può portare a benefici/guadagni, mentre le minacce o i pericoli sono fonti di rischio negativo. In alcuni ambiti si usano anche le espressioni *"upside risk"* (rischio positivo) e *"downside risk"* (rischio negativo).
L'analisi SWOT *(Strengths, Weaknesses, Opportunities, and Threats)* è una tecnica ben conosciuta nell'ambito del project management ed è usata anche per la valutazione di un'iniziativa imprenditoriale. Si tratta di identificare i punti di forza e di debolezza (fattori interni), opportunità e minacce (fattori esterni) che possono favorire o contrastare il raggiungimento degli obiettivi. I fattori interni possono essere visti come "minacce e opportunità" interne all'organizzazione. Questi elementi derivano dalla determinazione del "Contesto dell'Organizzazione", punto 4 della HLS e ISO/CD 9001: in particolare il punto 4.1 *(L'organizzazione deve determinare i fattori esterni ed interni pertinenti alle sue finalità e che influenzano la sua capacità di conseguire gli esiti previsti per il proprio QMS)*. La "Definizione del Contesto" è la prima fase del processo di *risk management* secondo la ISO 31000:2009 (5.3).
L'ISO/TMB/JTCG, nel documento N360 del 03/12/2013 (Annex SL Concepts), afferma che il riferimento a "Rischi e Opportunità" *è inteso a descrivere in modo ampio qualcosa che costituisce una minaccia che può avere effetto danno-*

Principi di gestione per la qualità (ISO/CD 9001 – Annex A)	Principi per la gestione del rischio (ISO 31000:2009 - punto 3) La gestione del rischio:
QMP 1 - Orientamento al cliente per il successo durevole di un'organizzazione. QMP 3 - Partecipazione attiva delle persone nel conseguire gli obiettivi dell'organizzazione. QMP 7 - Gestione delle relazioni con le parti interessate.	a) crea e protegge il valore h) tiene conto dei fattori umani e culturali i) è trasparente e "inclusiva" (globale - complessiva) contribuisce in maniera dimostrabile al raggiungimento degli obiettivi e al miglioramento della prestazione.
QMP 2 - Leadership - I leader creano le condizioni in cui le persone si impegnano nel conseguire gli obiettivi per la qualità dell'organizzazione QMP 4 - Approcci per Processi - Il QMS è composto di processi correlati. Comprendere come i risultati siano realizzati dal sistema, consente all'organizzazione di ottimizzare le proprie prestazioni.	b) è parte integrante di tutti i processi dell'organizzazione e fa parte delle responsabilità della direzione. e) è sistematica, strutturata e tempestiva. Un tale approccio alla gestione del rischio contribuisce all'efficienza ed a risultati coerenti, confrontabili ed affidabili.
QMP 5 - Miglioramento - è essenziale per un'organizzazione per mantenere l'attuale livello di prestazione, reagire ai cambiamenti del contesto interno ed esterno e per creare nuove opportunità.	g) è "su misura" e in linea con il contesto esterno ed interno. j) è dinamica, iterativa e reattiva al cambiamento. k) favorisce il miglioramento continuo dell'organizzazione.
QMP 6- Processo decisionale basato su evidenze: comporta qualche incertezza ed è importante comprendere le relazioni di causa-effetto e le conseguenze potenziali.	c) è parte del processo decisionale. d) affronta esplicitamente l'incertezza. f) si basa sulle migliori informazioni disponibili.

Prospetto 1 – Correlazione tra i QMPs ed i principi della gestione del rischio

Note

[3] In linea per altro con la definizione di "impatto ambientale" (conseguenza potenziale di un rischio per l'ambiente) della ISO 14001 e del regolamento EMAS: " qualunque modificazione dell'ambiente, negativa o benefica..."

so o negativo o, alternativamente, qualcosa che ha il potenziale per un effetto benefico o positivo. Non è inteso essere un'interpretazione tecnica, statistica o scientifica del termine "rischio". Aggiunge, inoltre, che la determinazione di minacce e opportunità può essere effettuata in modo informale oppure formale attraverso metodologie qualitative o quantitative.

La figura 1 è un'elaborazione del diagramma concettuale A.1 della UNI 11230:2007 e illustra i concetti relativi al rischio. Oltre al diverso aspetto grafico, sono stati aggiunti i due concetti di *Downside e Upside Risk* e l'indicazione dell'influenza che può avere l'incertezza. Quest'ultima influenza, o può influenzare in misura più o meno elevata, qualsiasi elemento del Rischio, anche se, a volte, alcuni elementi potrebbero essere certi con un adeguato grado di confidenza (mi riferisco, ad esempio, ai punti di forza e di debolezza, minacce e opportunità identificate a seguito di un'analisi SWOT ben condotta). Gli elementi più incerti sono legati a eventi e conseguenze, in particolare alla loro probabilità ed entità.

Azioni preventive, trattamento del rischio e controlli

HLS e ISO/CD 9001 non contengono più un requisito specifico relativo alle "Azioni Preventive". Questo viene giustificato dal fatto che uno degli scopi chiave di un MS formale è quello di operare come uno strumento di prevenzione: basta vedere le frasi già citate dei punti 4.1 e 6.1. Ma, in accordo a questi punti sarebbe di notevole aiuto introdurre un concetto tipico del *risk management:* "trattamento del rischio", definito come "Processo per modificare il rischio". Il trattamento può comportare attività speculari come "assumere o aumentare l'esposizione al rischio al fine di cogliere un'opportunità" o mitigare la parte negativa di un rischio. Modificare la probabilità di un evento sia nel senso di aumentarla perché può portare benefici, sia nel senso di ridurla per gli eventi sfavorevoli. Intraprendere azioni per modificare le conseguenze cercando di incrementare quelle positive e di limitare le negative. Nel momento in cui saremo entrati pienamente nella cultura del *"Risk Based Thinking"* saremo in grado di interpretare le non conformità (NC) come conseguenze negative di un rischio da "trattare". Come ben sappiamo si devono identificare le cause della NC (fonti di rischio: minacce ed eventi indesiderati) ed eliminarle o comunque ridurne la probabilità. Se siamo di fronte ad una NC potenziale vorrà dire che abbiamo effettuato un *risk assessment* (valutazione del rischio), identificando ed assegnando una priorità al rischio relativo alla NC ed il trattamento coinciderà con una Azione Preventiva. Se la NC si fosse già concretizzata, il trattamento coinciderebbe con un'azione correttiva. In questo caso potremmo dire che la NC è duplice: oltre al problema riscontrato, la NC metterebbe in evidenza una carenza nel processo di *Risk Assessment* che non ci aveva consentito di identificare il rischio relativo a quella specifica NC, ovvero nel processo di trattamento del rischio che non era stato efficace. Inoltre, tutte le azioni tese a conseguire i risultati desiderati, incluso il miglioramento continuo, possono essere interpretate come "trattamento del rischio".

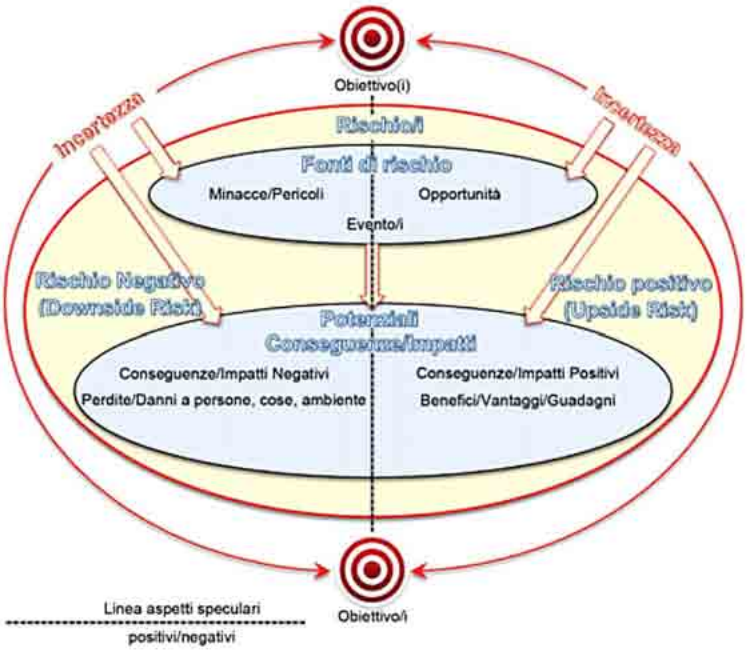

Figura 1 - Rischio e concetti correlati

Conclusioni

Esistono evidenti e significative similitudini tra ISO 31000 e ISO/CD 9001 in molti punti, come illustrato nel Prospetto 2:

È stata inoltre pubblicata la ISO/IEC 31010:2009 *(Risk Assessment Techniques)* che fornisce una guida nella scelta dei metodi per effettuare la valutazione del rischio e, in appendice, una descrizione di molti di tali metodi. È significativo e interessante notare che alcuni di questi sono già ampiamente conosciuti come tecniche e/o metodologie specifiche per la qualità, di applicazione pressoché universale o per settori specifici (Brainstorming, Interviste, Check-list, Delphi, HACCP, Root cause analysis, FMEA, Ishikawa, ecc).

ISO/CD 9001	ISO 31000:2009 (UNI ISO 31000:2010)
Contesto dell'organizzazione (4)	Definire il contesto (5.3)
Leadership e impegno (5.1)	Mandato e impegno (4.2)
Politica per la qualità (5.2)	Stabilire la politica per la gestione del rischio (4.3.2)
Ruoli organizzativi, responsabilità e autorità (5.3)	Responsabilità (4.3.3)
Risorse, competenza e consapevolezza (7.1, 7.2 e 7.3)	Risorse (4.3.5)
Pianificazione (6)	Valutazione del rischio (5.4)
Pianificazione, attività operative e miglioramento (6, 8 e 10)	Trattamento del rischio (5.5)
Comunicazione (7.4)	Comunicazione e consultazione (5.2)
Valutazione delle prestazioni (9)	Monitoraggio e riesame (5.6)

Prospetto 2- Similitudini strutturali tra ISO/CD 9001 ed ISO 31000:2009

L'utilizzo della ISO 31000, così come della ISO/IEC 31010, non sarà certamente un requisito, ma senza alcun dubbio può risultare utile.

È responsabilità dell'organizzazione decidere in che misura approfondire il risk management nell'ambito del proprio QMS, tenendo conto della complessità e criticità dei suoi prodotti, servizi, processi, contesto in cui opera e livello di maturità del QMS stesso.

L'approccio al rischio della HLS, pur dettato dalla volontà di rendere il concetto più ampio possibile, sta mettendo in difficoltà gli estensori delle norme, in particolare in quei ambiti dove il *"Risk Based Thinking"* non è ancora consolidato come per ISO/CD 9001 e ISO/CD 14001. Potrebbe accadere che nei vari MSS il rischio sia affrontato in maniera diversa, mentre il processo potrebbe essere assolutamente simile e allineato, pur considerando le ovvie diversità tra le tipologie di rischio nelle varie discipline. Le differenze nell'approccio al rischio, se dovessero divenire più evidenti, farebbero perdere buona parte dei vantaggi che erano tra gli scopi della HLS, creando confusione e disorientamento in chi intende sviluppare un MS integrato per più discipline. Un risultato non in linea con gli obbiettivi iniziali ed i principi della normazione.

Alla luce di ciò, sarebbe auspicabile un maggior coordinamento inter-settoriale tra i diversi comitati tecnici impegnati nell'elaborazione di MSS. Ciò consentirebbe di mettere a fattor comune le diverse culture e i diversi approcci alla gestione del rischio, un "*management tool*" di sicura rilevanza per l'evoluzione della normazione tecnica nel cruciale ambito dei MS.

Gennaro Bacile di Castiglione
Coordinatore GL UNI Gestione del Rischio
Membro della CT UNI Gestione per la qualità e metodi statistici