Titolo breve	**Risk management nelle Norme della famiglia ISO 9000**
Sotto-titolo	***Soddisfare i requisiti della 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***

Autore: Ing. Gennaro Bacile di Castiglione

Consulente, Referente dei Registri SICEP di AICQ SICEV, membro del GdL UNI "Terminologia della Gestione del Rischio" e dell'ISO/TMB/WG "Risk Management"

ABSTRACT:

Dopo una breve introduzione che inquadra il Risk Management nell'ambito del sistema di gestione di un'organizzazione e che confronta i principi alla base delle ISO 9000 con i principi del Risk Management contenuti nella ISO 31000, si passa a considerare nel dettaglio tutti quei punti della ISO 9001:2008 nei quali gli aspetti legati alla gestione del rischio sono parte integrante dei requisiti della norma stessa e che, quindi, possono essere soddisfatti più agevolmente applicando i principi e le metodologie del Risk Management.

Si vuole mettere in evidenza che tutto questo non è esplicitato in modo sufficientemente chiaro nel testo della ISO 9001, ma è comunque presente tra le righe.

INTRODUZIONE

Si assiste ad 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 ed altro. Naturalmente è necessario 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 della ISO 9000:2005, esiste un solo ed indivisibile SG complessivo di un'organizzazione, volto ad un suo governo "consapevole" e "responsabile" ed all'eccellenza nelle prestazioni a vantaggio di tutte le parti interessate. Tale "Sistema" dovrebbe *definire, attuare e soddisfare in modo coerente ed armonico la politica e gli obiettivi relativi 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.*

Le varie norme sui Sistemi di Gestione (SG) in realtà descrivono ciascuna una parte del sistema complessivo (vedere ad esempio la definizione[2] del "*sistema di gestione ambientale*" della ISO 14001:2004).

La definizione, del tutto personale, di "Sistema", prima riportata, è derivata dalle varie definizioni sui SG ed integrata con quella di "Risk Management" definito dalla norma AS/NZS 4360:2004 come "*la cultura, i processi e le strutture che sono indirizzate 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 a essere sempre più competitive, in linea con la visione "bilaterale" dei rischi illustrata nella Figura 1 e confermata dalla guida ISO 31000:2009. D'altra parte anche nella ISO 14001:2004 si definisce l'impatto ambientale come "*qualunque modificazione dell'ambiente, **negativa** o **benefica***".

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

[1] La nota alla definizione 3.2.2 della 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] La definizione 3.8 della ISO 14001:2004, recita:

"***Sistema di gestione ambientale (SGA)**: Parte del sistema di gestione di un'organizzazione utilizzata per sviluppare ed attuare la propria politica ambientale e gestire i propri aspetti ambientali*".

A mio modo di vedere, nel titolo della ISO 9001:2000/2008 c'è un'imprecisione:

"*Sistemi di gestione per la qualità – Requisiti*", manca l'aggettivo "Minimi". Infatti si tratta proprio dei Requisiti "minimi" di un Sistema di Gestione per la Qualità (SGQ), volti ad ottenere esclusivamente l'efficacia dei processi, anche quando si impone il "miglioramento continuo"; nessun accenno all'efficienza che aiuterebbe ad aumentare la soddisfazione di tutte le parti interessate, non solo del cliente.

I rischi legati all'attività di un'organizzazione sono numerosi e riguardano tutti i processi aziendali: dai rischi finanziari a quelli legati al mercato, ai paesi in cui si opera, alla concorrenza, al prodotto, alla capacità produttiva, alla sicurezza e salute dei lavoratori, dei clienti e della collettività, rischi ambientali, ecc..

Le metodologie legate al Risk Management consentono di identificare i rischi, analizzarli e prendere delle decisioni "consapevoli" per trattarli in modo adeguato. Dovrebbero mettere in grado le organizzazioni di valutare, attraverso una approfondita analisi costi-benefici, la possibilità di utilizzare le migliori tecnologie disponibili, al di là di quanto richiesto dalla normativa cogente in merito.

La 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. Sono sicuro di non sbagliare affermando che solo una piccolissima percentuale di sistemi certificati ISO 9001 abbiano preso in considerazione ed attuato questa visione. Inoltre l'accento è posto soprattutto sui rischi con conseguenze, effetti, impatti negativi ed occorre arrampicarsi sui vetri per vedere nel concetto di "miglioramento continuo" un vago suggerimento circa la possibilità di cogliere le opportunità. Peraltro si parla solo di azioni correttive e/o preventive, mentre non sono espressamente citate le azioni di miglioramento.

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

Per contro, al paragrafo 0.4 (*Compatibility with other management systems*), entrambe le ISO 9001:2000/2008, accennano al Risk Management come ad un ulteriore SG. L'accenno è presente anche nella ISO 14001:2004; in tutti e tre i documenti il senso della frase è:

La presente norma internazionale 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" e questo è chiaramente definito nella ISO 31000. Nonostante il parere di alcuni, infatti, la maggioranza dei membri ISO partecipanti al GdL "Risk Management", tra cui l'Italia, si è espressa nel senso di considerarlo un insieme di processi (macro-processo, vedere più avanti la Figura 1), con una "struttura di Riferimento" (framework) che permea tutti i processi di un'organizzazione e che risulta essere uno strumento per un governo efficace, efficiente, responsabile e, soprattutto, consapevole dell'organizzazione stessa.

La seconda osservazione è che quell'affermazione appare in forte contrasto con lo spirito stesso delle norme sui sistemi di gestione, visto che per la qualità è necessario tenere sotto controllo almeno i rischi legati al prodotto ed al mercato e nell'ambito ISO 14001 almeno quelli per l'ambiente. Non cade in tale contraddizione la OHSAS 18001:2007 (*Occupational health and safety management system – Requirements*).

IL FUTURO DELLE NORME SUI SISTEMI DI GESTIONE ED IL RISK MANAGEMENT

È significativo il fatto che, per la revisione della ISO 19011 (Linee guida per gli audit qualità e ambiente), si invitavano i partecipanti al GdL ISO sul Risk Management ad indicare la propria disponibilità ad essere coinvolti in tale revisione, giustificando la richiesta con la considerazione che la allora futura ISO 31000 (*Risk management — Principles and guidelines on implementation* – poi pubblicata il 15/11/2009) potrebbe avere influenza sulle future edizioni delle norme riguardanti i sistemi di gestione, in quanto questi ultimi sono destinati a divenire sempre più "risk based".

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 mette in evidenza il ciclo PDCA, in linea con la filosofia del miglioramento continuo.

Il Risk Management è un macro-processo iterativo di direzione, trasversale, che interagisce, in misura più o meno profonda in relazione al settore di attività, con tutti gli altri processi operativi, gestionali e di supporto. Per questo dovrebbe essere attuato attraverso una cultura diffusa in tutti i settori dell'organizzazione ed a tutti i livelli, secondo quanto necessario; una filosofia ed un elemento

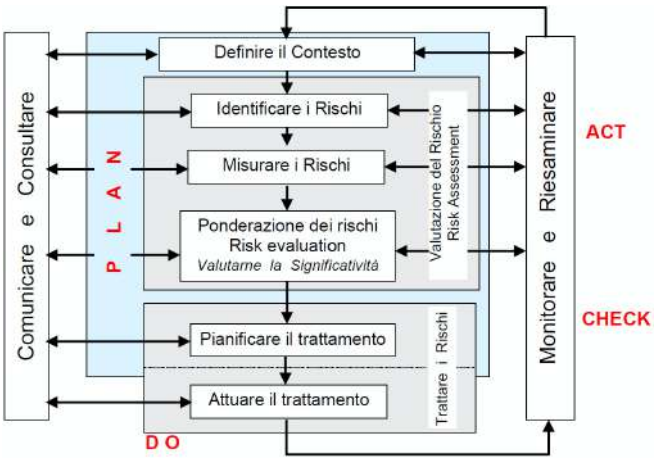

Figura 2.Macro-processo di gestione del rischio

portante del governo di un'organizzazione. A tale proposito svolgono un ruolo di primaria importanza i requisiti relativi alla "competenza, formazione/addestramento e consapevolezza", comuni a tutte le norme sui SG.

L'integrazione di tutti gli aspetti legati all'attività di un'organizzazione in un unico SG, che includa come macro-processo fondamentale la gestione coordinata di tutti i rischi, risponde ad un principio di tipo olistico, soprattutto se immaginiamo l'organizzazione stessa come un organismo vivente: un organismo complesso, all'interno del quale individui, coordinati secondo uno schema ben strutturato, operano utilizzando risorse, infrastrutture e competenze al fine di realizzare quello che è lo scopo di ogni organismo vivente: sopravvivere e crescere. Alla luce di queste considerazioni potremmo immaginare il Risk Management come un

Processo Biologico Vitale di un'Organizzazione

Potrebbe sembrare solo una frase ad effetto, ma riflettendoci il paragone è perfettamente calzante: Risk Management come il "sistema immunitario" dell'organismo vivente che è l'organizzazione; le consente di difendersi dagli eventi indesiderati e, quindi, di continuare ad operare e svilupparsi. Un "sistema immunitario" che non si limita a reagire alle infezioni (eventi indesiderati), ma effettua azione di prevenzione (una sorta di "vaccinazione"). Questo è particolarmente vero se consideriamo i danni legati ad un incidente ambientale, i cui costi possono essere tali da mettere in seria difficoltà anche le organizzazioni finanziariamente più solide.

D'altra parte potremmo anche affermare che il Rischio, se lo conosci, lo eviti o cerchi di ridurlo per gli aspetti che possono portare a conseguenze negative, mentre lo affronti per cogliere le opportunità ed ottenere benefici. In altre parole se lo conosci puoi tenerlo sotto controllo. Tutto questo risponde anche ad uno degli otto "Principi di gestione per la qualità": ***Decisioni basate su dati di fatto***.

In appendice sono presenti le due tabelle seguenti:

Tabella A mette a confronto puntualmente gli otto principi di gestione per la qualità con gli undici principi per un'efficace gestione del rischio;

Tabella B riporta le principali definizioni di Rischio e di alcuni termini correlati

GESTIONE EMERGENZE

La ISO 9001:2000/2008 non contengono alcun requisito relative alla gestione delle emergenze, né suggerimenti in proposito, ad esempio inseriti nelle note, che, come tutti sappiamo, non fanno parte dei requisiti. Eppure nell'edizione 2008 avrebbero forse dovuto inserire qualcosa sull'argomento, tenendo conto del fatto che la ISO GUIDE 72:2001 (Linea guida interna all'ISO per la giustificazione e lo sviluppo delle norme sui Sistemi di Gestione), in Appendice B, dove elenca i "Requisiti Comuni" dei SG, prevede (punto B.2.7) una "*Contingency preparedness for foreseeable events*", ovvero la preparazione alle emergenze per eventi prevedibili. La ISO 9004:2009 fa esplicito riferimento ai piani di emegenza, così come, tra le norme per la certificazione, la ISO 14001:2004 e la 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, per dirla con il linguaggio dell'edizione 2008, la capacità dell'organizzazione di soddisfare i requisiti del prodotto.

Riporto solo un esempio tra i tanti che si potrebbero citare: un'esplosione, un incendio, un terremoto, 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; al di là dei costi relativi, l'organizzazione potrebbe non essere in grado di soddisfare alcuni requisiti contrattuali legati ad esempio ai termini di consegna.

Inoltre si dovrebbero considerare non solo 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 ed il Comitato Tecnico ISO-TC223 Societal Security sta preparando numerose norme sull'argomento, tra cui la ISO/DIS 22301 (Preparedness and continuity management systems – Requirements) prevista per la certificazione, oltre alle seguenti guide:

ISO/DIS 22300 Societal Security – Vocabulary.
ISO/CD 22313 Societal Security -- Business Continuity Management Systems – Guidance.
ISO/FDIS 22320 Societal Security -- Emergency Management -- Requirements For Command And Control.

LA ISO 9001:2008 ED IL RISK MANAGEMENT

Sono numerosi i requisiti nel corpo della Norma ISO 9001:2008 che richiamano, direttamente o indirettamente (anche se non sempre in maniera esplicita), concetti e principi strettamente legati alla gestione dei rischi. Spesso tali richiami erano già presenti nell'edizione 2000 e nelle precedenti edizioni della norma, ma in qualche caso sono stati evidenziati maggiormente nei chiarimenti e nelle note dell'edizione 2008. Nel seguito riportiamo e commentiamo gli aspetti significativi di ogni requisito da questo punto di vista utilizzando la numerazione dei punti della ISO 9001:2008. Nel testo, tra virgolette ed in corsivo, sono riportate frasi integrali tratte dalla ISO 9001:2008. Alcune volte, sempre tra virgolette ed in corsivo, possono essere riportate frasi da altre norme, ad esempio dalla ISO 31000:2009: in questi casi è indicato il riferimento puntuale prima o dopo la citazione.

4 SISTEMA DI GESTIONE PER LA QUALITÀ

4.1 Requisiti Generali

Questo punto della norma ha due parti strettamente legate tra loro e per le quali le metodologie del Risk management possono aiutare a determinare ed a migliorare i processi del SGQ.

La prima parte è quella che riguarda la cosiddetta "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 mettere in evidenza quali siano i punti e gli aspetti critici dei processi stessi e delle loro interazioni, ovvero i rischi, intesi come opportunità da sfruttare, pericoli, minacce, non conformità potenziali da evitare o comunque fronteggiare. D'altronde 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 solo riferimento a quelli in outsourcing, è pressoché automatico pensare che tale concetto dovrebbe essere applicato a tutti i processi del SGQ.

Per ciascun processo (interno o esterno) si tratta di identificare ***l'impatto potenziale*** sui processi a valle e sul prodotto finale, impatto che può essere positivo o negativo: i controlli, i monitoraggi, le 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 1 vista sopra), 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 consultazione" in parallelo al "risk assessment" e proseguendo con il "trattamento" e la "misurazione/riesame", per poi ripetere il ciclo PDCA, in ottica di miglioramento continuo.

D'altra parte, nella ISO 9000:2005, al punto 2.3 definisce un approccio per sviluppare ed attuare un SGQ del tutto simile a quello indicato al 4.1 della 9001, ma con l'aggiunta del primo bullet:

"*a) determinare le esigenze e le aspettative dei clienti e delle altre parti interessate;*"

che corrisponde 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 altri parti interessate interne ed esterne (in ottica ISO 9004, TQM, modelli di eccellenza): mette in grado di definire i criteri di valutazione dei rischi (loro livello di significatività e di accettabilità) e permette di agevolare l'operatività di un'organizzazione creando un clima favorevole alla sua attività con 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 ed il mercato finanziario in genere.

4.2 Requisiti relativi alla documentazione

La norma, tra le altre cose, richiede che la documentazione del SGQ includa:

"*d) documenti, comprese 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 espressamente 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 e del tipo di attività, della complessità dei processi e delle loro interazioni, della competenza del personale, le domande da porsi potrebbero essere sostanzialmente due:

- quali **impatti negativi si potrebbero generare,** in una certa area, per la mancanza di una procedura, un'istruzione, una registrazione o un loro scarso grado di dettaglio?
- quali **impatti positivi si potrebbero generare,** in una certa area, 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 potremmo trovare legami con la gestione del rischio. D'altronde il secondo principio della ISO 31000:2009 ci dice che "*la gestione del rischio fa parte delle responsabilità della direzione ed è parte integrante di tutti i processi dell'organizzazione, inclusi la pianificazione strategica e tutti i processi di gestione dei progetti e del cambiamento*".

Il punto 5.4 (obiettivi e pianificazione del SGQ) è probabilmente quello più interessato, considerando che nella definizione di Rischio è insito il concetto di influenza che questo ha sulla capacità/possibilità di raggiungere gli obiettivi.

Il punto 5.5.3, come i successivi 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 della ISO 31000:2009); vedere anche figura 2.

È anche possibile evidenziare il collegamento che c'è tra "*le modifiche che potrebbero avere effetti sul SGQ*" (punto 5.6.2.f) ed il "contesto" in cui opera l'organizzazione. Inoltre non è possibile dubitare che vi sia una stretta correlazione tra il Riesame di Direzione della ISO 9001 ed il Riesame che fa parte del macro-processo di Gestione del Rischio.

6 GESTIONE DELLE RISORSE

Anche il punto 6, pur non contenendo riferimenti espliciti al Risk Management, può e dovrebbe essere interpretato in questi termini:

6.1: mettere a disposizione le risorse che consentano all'organizzazione di cogliere al meglio le opportunità e di tenere a distanza gli eventi indesiderati, in altre parole di raggiungere l'obiettivo principale di soddisfare sempre più e sempre meglio i clienti.

6.2: il personale deve avere la competenza necessaria a tenere sotto controllo i rischi legati alla propria attività (naturalmente non stiamo parlando solo di quelli relativi a salute e sicurezza sul lavoro) e deve essere reso consapevole del proprio contributo al raggiungimento degli obiettivi per la qualità, che come abbiamo visto è influenzato dai rischi.

6.3: possiamo limitarci anche ad una sola considerazione, anche se tutto ciò che ha a che fare con le infrastrutture è influenzato dai rischi: come definire un programma di manutenzione adeguato? La risposta è una sola, ma con i soliti due aspetti: in funzione degli impatti potenziali negativi che la mancata manutenzione potrebbe avere sul rispetto dei requisiti dei prodotti, anche in termini di tempi di consegna, o dei potenziali impatti positivi di un incremento della manutenzione…la manutenzione potrebbe contemplare una sostituzione di un impianto o di una macchina.

6.4: forse qui il legame con i rischi può apparire più evidente e non solo con impatti negativi dovuti ad esempio ad incidenti sul lavoro ed alla possibilità di un fermo impianto da parte delle autorità. L'ambiente di lavoro può anche incidere fortemente sulla produttività e sulla qualità dei prodotti stessi.

7 REALIZZAZIONE DEL PRODOTTO

7.1 Pianificazione della realizzazione del prodotto

Valgono qui le considerazioni fatte per il punto 4.1, considerando i rischi legati al prodotto ed ai processi di realizzazione.

7.2 Processi relativi al cliente

7.2.1 nel determinare i requisiti del prodotto è estremamente importante identificare i rischi legati al prodotto stesso: spesso la valutazione dei rischi per la sicurezza fa parte dei requisiti cogenti, ma vi possono essere altri rischi, legati al mercato alla concorrenza al tipo di clienti cui il prodotto è destinato, intermedi o finali. In quelli che la norma chiama "*i requisiti non stabiliti dal cliente, ma necessari per l'uso specificato o per quello previsto, ove conosciuto*" (punto b) o "*ogni ulteriore requisito ritenuto necessario dall'organizzazione stessa*" (punto d), potranno essere inseriti i requisiti che consentono di ridurre rischi "negativi" e/o "positivi".

7.2.2 il riesame dei requisiti del prodotto è anche un riesame dei rischi legati al prodotto e tra l'altro permette di gestire i rischi relativi a incomprensioni con il cliente, evitando la possibilità di contenziosi e/o di costi aggiuntivi se non si è valutata adeguatamente la propria capacità di soddisfare i requisiti, anche in termini di tempi di consegna.

7.2.3 la comunicazione con il cliente, come già accennato, ha una stretta correlazione con l'attività di comunicazione e consultazione prevista nel macro-processo di gestione del rischio (figura 2).

7.3 Progettazione e sviluppo

La progettazione è l'attività con la quale si può maggiormente incidere sui rischi legati al prodotto, al di là degli aspetti cogenti già richiamati per il punto 7.2.1 (ad esempio Marcatura CE). A parte il riferimento ai "*requisiti cogenti applicabili*" tra gli elementi in ingresso, non è però presente alcun richiamo puntuale alla gestione dei rischi, se non al punto 7.3.7 dove si richiede che il riesame delle modifiche della progettazione comprenda la valutazione dell'**effetto** di tali modifiche sulle parti componenti e sul prodotto già consegnato.

7.4 Approvvigionamento

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 gli outsourced processes di cui al 4.1 e molto chiaro (almeno alla luce dell'edizione 2008 – non lo era altrettanto nei primi anni di applicazione della Vision 2000 per la quale si erano avute le interpretazioni più fantasiose, come la presunta contrapposizione tra i processi in outsourcing e l'approvvigionamento).

"*Il tipo e l'estensione del controllo applicato sul fornitore e sul prodotto approvvigionato devono dipendere dall'**effetto** del prodotto approvvigionato sulla successiva realizzazione del prodotto o sul prodotto finale*".

7.5 Produzione ed erogazione del servizio

7.5.1 le condizioni controllate per le attività di produzione e di erogazione del servizio saranno in relazione alla criticità delle attività stesse e sull'impatto che l'assenza o la presenza di informazioni sulle caratteristiche del prodotto, istruzioni di lavoro, apparecchiature idonee di lavoro e di monitoraggio e misurazione, ecc., può avere sulla capacità di realizzare un prodotto ed erogare un servizio che risponda ai requisiti.

7.5.2 "*L'organizzazione deve validare tutti i processi di produzione e di erogazione del servizio, nel caso in cui il risultato non può essere verificato da successive attività di monitoraggio o misurazione **e, di conseguenza, le carenze possono evidenziarsi solo** quando il prodotto è già in uso o il servizio è stato erogato*". È evidente che la validazione sarà tanto più estesa ed i criteri per il riesame e l'approvazione dei processi tanto più stringenti, in relazione alla gravità delle carenze potenziali. La ISO 9001 non contempla aspetti legati alle opportunità da cogliere, ma è ovvio che a parità di risultati per il prodotto, la validazione potrebbe essere effettuata con criteri più stringenti se questo consentisse di rendere il processo, oltre che efficace, anche più efficiente.

7.5.3 la rintracciabilità, oltre ai casi in cui sia un requisito contrattuale o cogente, può aiutare a ridurre le conseguenze di eventuali difetti riscontrati su lotti già consegnati (campagne di richiamo più mirate). È evidente che anche in questo caso il grado di approfondimento/dettaglio dipende dagli impatti potenziali. Allo stesso modo il grado di dettaglio e le modalità dell'identificazione del prodotto e del suo stato "*lungo tutta la sua realizzazione*", dipenderà dall'impatto potenziale della mancata identificazione sui processi a valle.

Le decisioni circa le modalità di trattamento della "*Proprietà del Cliente*" (7.5.4) e di "*Conservazione del Prodotto*" (7.5.5), saranno influenzate dagli impatti potenziali delle regole definite in proposito.

7.6 Tenuta sotto controllo delle apparecchiature di monitoraggio e di misurazione

A questo punto forse non è più necessario approfondire tanto l'argomento. Da quanto detto in precedenza sarà naturale pensare che la determinazione delle attività di monitoraggio e di misurazione, la scelta delle apparecchiature necessarie, delle loro caratteristiche metrologiche, degli intervalli di taratura, ecc., andranno effettuate in relazione ai rischi correlati risultati delle attività di monitoraggio e di misurazione stesse, tenendo conto non solo delle minacce e dei pericoli, ma anche delle opportunità da cogliere.

8 MISURAZIONE, ANALISI E MIGLIORAMENTO

8.1 Generalità

Valgono qui molte delle considerazioni fatte per il punto 4.1, considerando i rischi legati al prodotto ed ai processi di realizzazione. Tutto il punto 8 della ISO 9001, insieme con il 5.6 (Riesame di Direzione) dovrebbe essere affrontato considerando le attività di "Monitoraggio e Riesame" suggerite al punto 5.6 della ISO 31000:2009 di cui riportiamo quanto segue:

> *I processi di monitoraggio e riesame dell'organizzazione dovrebbero comprendere tutti gli aspetti del processo di gestione del rischio allo scopo di:*
> - *assicurare che i controlli siano efficaci ed efficienti sia nella progettazione sia nell'operatività;*
> - *ottenere ulteriori informazioni per migliorare la valutazione del rischio;*
> - *analizzare ed apprendere dagli eventi (compresi i near-miss), cambiamenti, tendenze, successi e fallimenti;*
> - *rilevare i cambiamenti nel contesto esterno ed interno, comprese le modifiche ai criteri di rischio e al rischio stesso, che possano richiedere revisioni dei trattamenti del rischio e delle priorità; e*
> - *identificare i rischi emergenti.*
>
> *I progressi nell'attuazione dei piani di trattamento del rischio forniscono una misura della prestazione. I risultati possono essere incorporati all'interno della gestione della prestazione complessiva dell'organizzazione, nelle misurazioni e nelle attività di reporting esterne ed interne.*
>
> *I risultati del monitoraggio e riesame dovrebbero essere registrati e riferiti esternamente ed internamente, come appropriato, e dovrebbero anche essere utilizzati come dati in ingresso al riesame della struttura di riferimento per la gestione del rischio.*

8.2 Monitoraggio e Misurazione

8.2.1 il monitoraggio della soddisfazione del cliente, come già accennato, ha uno stretto collegamento con "la Comunicazione e la Consultazione con i portatori d'interesse esterni e interni". "Le informazioni relative alla percezione del cliente sul fatto che l'organizzazione abbia o no soddisfatto i suoi requisiti", che la ISO 9001 richiede di raccogliere ed analizzare, dovrebbero essere volte a capire anche quali sono le esigenze e le aspettative del cliente relative al prodotto fornito e quindi a comprendere ed evidenziare le opportunità e le minacce/pericoli correlati a quei prodotti (in altre parole i rischi). L'importanza che il cliente dà a ciascun aspetto della fornitura aiuta a definire i criteri per la valutazione della significatività (ponderazione) del rischio correlato alle forniture. "*L'obiettivo della*

ponderazione del rischio è di agevolare, sulla base degli esiti dell'analisi del rischio, i processi decisionali riguardo a quali rischi necessitano un trattamento e le relative priorità di attuazione" (da ISO 31000:2009 – punto 5.4.4).

8.2.2 la norma richiede, tra l'altro, che il programma degli audit interni "*prenda in considerazione lo stato e l'importanza dei processi e delle aree da sottoporre ad audit, così come i risultati di audit precedenti. Devono essere definiti i criteri, il campo di applicazione, la frequenza ed i metodi dell'audit*…" Gli audit interni dovrebbero essere più frequenti per le aree/processi più critici ovvero quelli con rischi dal livello di significatività più elevato e aiutare a mettere in evidenza la necessità di rivedere i relativi risk assessment e trattamento.

8.2.3 per il monitoraggio e la misurazione dei processi una nota suggerisce che "*il tipo e l'estensione del monitoraggio o della misurazione siano appropriati per ciascuno dei propri processi in relazione al loro* ***impatto*** *sulla conformità ai requisiti del prodotto e sull'efficacia del sistema di gestione per la qualità*". È evidente che il monitoraggio e la misurazione dei processi dovrebbe comprendere il monitoraggio e la misurazione dei rischi relativi.

8.2.4 la pianificazione del monitoraggio e della misurazione del prodotto dovrebbe tenere conto dei rischi (pericoli/minacce ed opportunità) legati al prodotto stesso ed alle caratteristiche da monitorare e misurare.

8.3 Tenuta sotto controllo del prodotto non conforme

Tra i modi con cui trattare il prodotto non conforme la norma prevede "*azioni appropriate agli* ***effetti****, o agli* ***effetti potenziali****, della non conformità quando il prodotto non conforme venga rilevato dopo la consegna o dopo che ne sia iniziata l'utilizzazione*".

8.4 Analisi dei dati

"*L'organizzazione deve determinare, raccogliere ed analizzare i dati appropriati per dimostrare l'adeguatezza e l'efficacia del sistema di gestione per la qualità e per valutare dove possa essere realizzato il miglioramento continuo dell'efficacia del sistema stesso*". L'analisi dei dati e delle informazioni dovrebbe comprendere quelli relativi ai rischi: vedere quanto riportato in precedenza al punto 8.1, a proposito del punto 5.6 della ISO 31000:2009 (Monitoraggio e Riesame nella Gestione del Rischio).

8.5 Miglioramento

Il punto 8.5 è forse quello più esplicitamente correlato a processi di Risk Management in particolare al "trattamento" del rischio. Il collegamento è chiaro per quanto riguarda i trattamento dei rischi con conseguenze/impatti negativi attraverso le azioni correttive e/o preventive per l'eliminazione delle cause di non conformità rispettivamente reali e/o potenziali. Inoltre la norma chiarisce anche che le azioni "*devono essere appropriate agli* ***effetti*** *delle non conformità riscontrate e/o dei problemi potenziali*".

Le connessioni non si limitano agli aspetti negativi, ma coinvolgono anche il miglioramento continuo: quali possono essere gli impatti positivi se accade un certo evento, ovvero se si mette in atto un approccio diverso rispetto a quello attuale, un approccio che consenta di ottenere prestazioni più elevate in termini di minore difettosità, maggiore produttività, minori costi, tempi di attraversamento più rapidi, minore inquinamento, risparmio di risorse naturali, riduzione di pericoli per salute e sicurezza, ecc., ecc.

CONSIDERAZIONI FINALI

Utilizzando i principi e, almeno in parte, le metodologie del Risk Management, potremmo riuscire a migliorare l'efficacia del SGQ e, iterando il ciclo del processo di gestione del rischio ed 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, raccogliendo 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".

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

Appendice - Tabella A: confronto e correlazione tra gli otto principi di gestione per la qualità e gli undici principi per un'efficace gestione del rischio.

Principi di gestione per la qualità (UNI EN ISO 9000:2005 – punto 0.2)	**Principi per un'efficace gestione del rischio** (UNI ISO 31000:2010 – punto 3) **La Gestione del Rischio…**
a) **Orientamento al cliente.** Le organizzazioni dipendono dai propri clienti e dovrebbero pertanto capire le loro esigenze presenti e future, soddisfare i loro requisiti e mirare a superare le loro stesse aspettative. c) **Coinvolgimento delle persone.** Le persone, a tutti i livelli, costituiscono l'essenza dell'organizzazione ed il loro pieno coinvolgimento permette di porre le loro capacità al servizio dell'organizzazione. h) **Rapporti di reciproco beneficio con i fornitori.** Un'organizzazione ed i suoi fornitori sono interdipendenti ed un rapporto di reciproco beneficio migliora, per entrambi, la capacità di creare valore.	h) **… tiene conto dei fattori umani e culturali**. Nell'ambito della gestione del rischio si individuano capacità, percezioni e aspettative delle persone esterne ed interne che possono facilitare o impedire il raggiungimento degli obiettivi dell'organizzazione. i) **… è trasparente e "inclusiva" (globale - complessiva).** Il coinvolgimento appropriato e tempestivo dei portatori d'interesse e, in particolare, dei responsabili delle decisioni, a tutti i livelli dell'organizzazione, assicura che la gestione del rischio rimanga pertinente ed aggiornata. Il coinvolgimento, inoltre, permette che i portatori d'interesse siano opportunamente rappresentati e che i loro punti di vista siano presi in considerazione nel definire i criteri di rischio.
d) **Approccio per processi.** Un risultato desiderato si ottiene con maggiore efficienza quando le attività e le relative risorse sono gestite come un processo. b) **Leadership.** I leader stabiliscono unità di intenti e di indirizzo dell'organizzazione. Essi dovrebbero creare e mantenere un ambiente interno che coinvolga pienamente le persone nel conseguimento degli obiettivi dell'organizzazione.	b) … **è parte integrante di tutti i processi dell'organizzazione**. … non è un'attività indipendente, separata dalle attività e dai processi principali dell'organizzazione.… fa parte delle responsabilità della direzione ed è parte integrante di tutti i processi dell'organizzazione, inclusi la pianificazione strategica e tutti i processi di gestione dei progetti e del cambiamento.
e) **Approccio sistemico alla gestione.** Identificare, comprendere e gestire, come fossero un sistema, processi tra loro correlati contribuisce all'efficacia e all'efficienza dell'organizzazione nel conseguire i propri obiettivi.	e) … **è sistematica, strutturata e tempestiva**. Un approccio sistematico, tempestivo e strutturato alla gestione del rischio contribuisce all'efficienza ed a risultati coerenti, confrontabili ed affidabili.
f) **Miglioramento continuo.** Il miglioramento continuo delle proprie prestazioni complessive dovrebbe essere un obiettivo permanente dell'organizzazione.	a) …..**crea e protegge il valore**. La gestione del rischio contribuisce in maniera dimostrabile al raggiungimento degli obiettivi ed al miglioramento della prestazione, per esempio in termini di salute e sicurezza delle persone, security, rispetto dei requisiti cogenti, consenso presso l'opinione pubblica, protezione dell'ambiente, qualità del prodotto, gestione dei progetti, efficienza nelle operazioni, governance e reputazione k) **… favorisce il miglioramento continuo dell'organizzazione**. Le organizzazioni dovrebbero sviluppare ed attuare strategie per migliorare la maturità della propria gestione del rischio insieme a tutti gli altri aspetti della propria organizzazione.
g) **Decisioni basate su dati di fatto.** Le decisioni efficaci si basano sull'analisi di dati e di informazioni.	c) … **è parte del processo decisionale**. … aiuta i responsabili delle decisioni ad effettuare scelte consapevoli, determinare la scala di priorità delle azioni e distinguere tra linee di azione alternative. d) … **affronta esplicitamente l'incertezza**. … tiene conto esplicitamente dell'incertezza, della natura di tale incertezza e di come può essere affrontata. f) … **si basa sulle migliori informazioni disponibili**. Gli elementi in ingresso al processo per gestire il rischio si basano su fonti di informazione quali dati storici, esperienza, informazioni di ritorno dai portatori d'interesse, osservazioni, previsioni e parere di specialisti. Tuttavia, i responsabili delle decisioni dovrebbero informarsi, e tenerne conto, di qualsiasi limitazione dei dati o del modello utilizzati o della possibilità di divergenza di opinione tra gli specialisti.

(*UNI EN ISO 9001:2008 – Introduzione – 0.1 Generalità*) L'adozione di un sistema di gestione per la qualità dovrebbe essere una decisione strategica di un'organizzazione. La progettazione e l'attuazione del sistema di gestione per la qualità di un'organizzazione sono influenzate: a) dal contesto nel quale essa opera, dai cambiamenti in tale contesto e dai rischi ad esso associati; b) dalle sue mutevoli esigenze; c) dai suoi particolari obiettivi; d) dai prodotti che fornisce; e) dai processi che adotta; f) dalla sua dimensione e dalla sua struttura organizzativa.	g) … è "su misura". La gestione del rischio è in linea con il contesto esterno ed interno e con il profilo di rischio dell'organizzazione. j) … è dinamica, iterativa e reattiva al cambiamento. … è sensibile e risponde al cambiamento continuamente. Ogni qual volta accadono eventi esterni ed interni, cambiano il contesto e la conoscenza, si attuano il monitoraggio ed il riesame, emergono nuovi rischi, alcuni rischi si modificano ed altri scompaiono.

Appendice – Tabella B: Principali definizioni di Rischio e di alcuni termini correlati

Termine	Definizione
Rischio *ISO 31000:2009* *Tutte le definizioni della ISO 31000:2009 sono riprese dalla ISO/IEC Guide 73:2009*	Effetto dell'incertezza sugli obiettivi. Nota 1 Un effetto è uno scostamento da quanto atteso - positivo e/o negativo. Nota 2 Gli obiettivi possono presentare aspetti differenti (come scopi finanziari, di salute e sicurezza, ambientali) e possono intervenire a livelli differenti (come progetti, prodotti e processi strategici, riguardanti l'intera organizzazione). Nota 3 Il rischio è spesso caratterizzato dal riferimento a eventi potenziali e conseguenze, o una combinazione di questi. Nota 4 Il rischio è spesso espresso in termini di combinazione delle conseguenze di un evento (compresi cambiamenti nelle circostanze) e della verosimiglianza del suo verificarsi. Nota 5 L'incertezza è lo stato, anche parziale, di assenza di informazioni relative alla comprensione o conoscenza di un evento, delle sue conseguenze o della loro verosimiglianza.
Rischio *UNI 11230:2007*	L'insieme della possibilità di un evento e delle sue conseguenze sugli obiettivi. Nota 1 Il termine "rischio" viene più frequentemente usato quando vi è la possibilità di conseguenze negative. Nota 2 Il concetto di rischio implica la sua dimensione e cioè la "combinazione della probabilità di un evento e della entità delle sue conseguenze". Nota 3 Talora viene definito come "possibilità di un accadimento che Impatta sui risultati". Nota 4 In alcuni settori, per esempio in quello finanziario, al concetto di rischio viene associato anche quello di "conseguenza positive". Più in generale, si fa riferimento al binomio rischio-rendimento, nel senso che maggiore è la dimensione del rischio a cui ci si espone e maggiore dovrebbe essere il rendimento.
Rischio *AS/NZS 4360:2004*	La possibilità che accada qualcosa che avrà un impatto sugli obiettivi. Nota 1 Un Rischio è spesso specificato in termini di un evento o circostanze e delle conseguenze che ne possono derivare. Nota 2 Il Rischio è misurato in termini di combinazione tra le conseguenze di un evento e la loro probabilità/frequenza (likelihood). Nota 3 Il Rischio può avere un impatto positivo o negativo.
Fonte di rischio *ISO 31000:2009*	Elemento che da solo o in combinazione con altri possiede il potenziale intrinseco di originare il rischio. Nota Una fonte di rischio può essere tangibile o intangibile.
Evento *ISO 31000:2009*	Il verificarsi o il modificarsi di un particolare insieme di circostanze. Nota 1 Un evento può consistere in una o più episodi e può avere diverse cause. Nota 2 Un evento può consistere nel non verificarsi di qualcosa. Nota 3 A volte di ci si può riferire ad un evento come un "incidente" o "evento sfavorevole". Nota 4 Ad un evento senza conseguenze (2.18) ci si può anche riferire come un "near miss", "incidente", "near hit" o "close call".
Conseguenza *ISO 31000:2009*	Esito di un evento che influenza gli obiettivi. Nota 1 Un evento può portare ad una gamma di conseguenze. Nota 2 Una conseguenza può essere certa o incerta e può avere effetti positivi o negativi sugli obiettivi. Nota 3 Le conseguenze possono essere espresse in modo quantitativo o qualitativo. Nota 4 Le conseguenze iniziali possono aggravarsi attraverso effetti indiretti (per esempio "effetto domino").

Commento personale:

la definizione base di Rischio delle ISO/IEC Guide 73:2009 ed ISO 31000:2009 non appare troppo felice. Da una parte tende a far confondere il rischio con le sue conseguenze ("effetto"), dall'altra potrebbe far pensare che l'incertezza sia riferita a quali siano gli obiettivi. Dovrebbe essere letta come "*effetto dell'incertezza in relazione agli obiettivi".* Fortunatamente le note chiariscono a sufficienza i concetti che ci sono dietro al termine "Rischio". Si riportano anche le definizioni di altre due norme che, pur nella formulazione alquanto diversa, non solo non sono in contrasto, ma contribuiscono a chiarire meglio il concetto di rischio e ad evitare gli errori che normalmente si commettono nel linguaggio comune, dove, sia in italiano che in inglese, si tende ad utilizzare come sinonimi i termini di rischio e di pericolo ed a considerare il rischio soltanto come qualcosa che può avere conseguenze esclusivamente negative. In parte cade in questo errore anche la ISO 9004:2009 che in più punti accenna a "*rischi ed opportunità*", quando abbiamo visto che le opportunità fanno parte del rischio insieme ai pericoli ed alle minacce. Questo nonostante la stessa ISO 9004:2009 citi espressamente la ISO 31000.