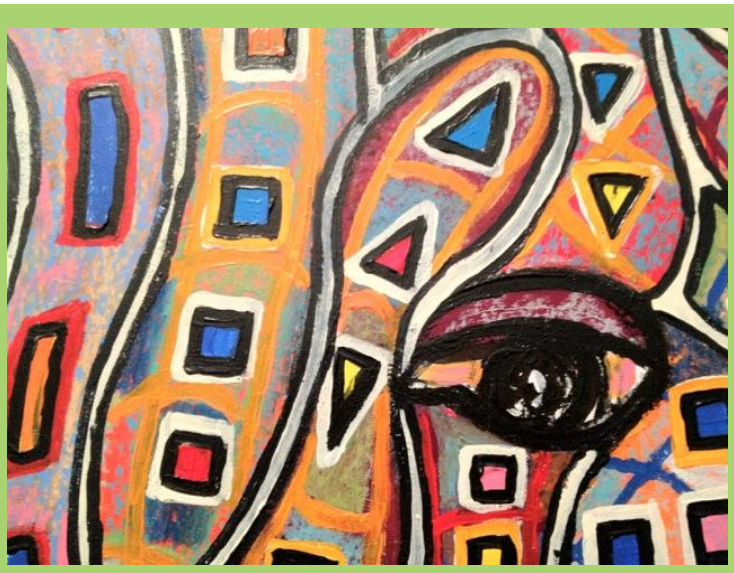
consultia srl
consultia@consultia.it

La norma UNI ISO 31000:2010 “Gestione del rischio”

Principi e linee guida



Giuseppe Bifulco – *“In ogni direzione”* – Milano, collezione privata (particolare)

La gestione del rischio è un obiettivo a cui ogni impresa attenta agli aspetti preventivi dovrebbe tendere e che ogni cliente dovrebbe pretendere, in particolare in settori caratterizzati da alta variabilità.

La Linea Guida ISO 31000 ci propone un modello di gestione del rischio e di integrazione dello stesso nel sistema di gestione aziendale. Essa è applicabile a tutte le tipologie di rischio (da quelli strategici a quelli operativi, valutari, di mercato, di compliance, di paese, ecc.)

Nel novembre del 2010 è stata pubblicata la norma UNI ISO 31000:2010 “Gestione del rischio”, traduzione italiana della corrispondente norma internazionale ISO 31000 del novembre 2009.

Come tutte le Linee Guida, di recente pubblicazione, la sua struttura presenta:

- Un’introduzione - fondamentale per la comprensione dei successivi capitoli
- Lo scopo ed il campo di applicazione (1)
- I termini e le definizioni - molto articolati e completi (2).
- Il paragrafo relativo ai principi (3)
- La struttura di riferimento per la gestione del rischio (4)
- Il processo di gestione del rischio (5)
- Un’appendice dedicata alla “Gestione del rischio robusta” (Appendice A)

via morgantini, 14
I • 20148 milano
P.IVA 03763740960
tel. +39 02.36.50.94.57

La Linea Guida, ancora una volta – e non poteva essere altrimenti- si basa sul modello PDCA (Plan – Do – Check - Act), considerato la base di riferimento sia del paragrafo 4 che del 5.

Introduzione

L'introduzione delinea la struttura della norma e pone particolare attenzione sui vantaggi di una corretta ed attiva gestione del rischio. Tra i vantaggi[1]:

- aumentare la probabilità di raggiungere gli obiettivi[2];
- incoraggiare la gestione proattiva;
- migliorare il reporting cogente e volontario;
- costruire una base affidabile per il processo decisionale e la pianificazione;
- accrescere le prestazioni in ambito salute e sicurezza - protezione ambientale;
- migliorare l'apprendimento organizzativo.

L'introduzione indica anche la gamma dei portatori di interesse a cui la Linea Guida è destinata. Tra questi sono citati anche gli "estensori di norme, guide, procedure e codici di comportamento".

Scopo e campo di applicazione

Il campo di applicazione, descritto nel capitolo 1, specifica che la linea guida è adattabile a qualsiasi tipo di organizzazione (impresa pubblica, privata o sociale, associazione, gruppo o individuo) e lungo l'intera vita dell'organizzazione medesima.

La linea guida è stata strutturata, inoltre, per fornire un modello indipendente dal tipo di rischio considerato, che abbia conseguenze negative oppure positive.

Termini e definizioni[3]

Il capitolo 2, dedicato alla terminologia, è particolarmente interessante e da solo vale la lettura del documento. Non è possibile, in questa breve sintesi, soffermarsi su tutte o anche solo su una parte delle definizioni. Però, dato che la Linea Guida rimarca più volte l'importanza del contesto, sia esterno che interno, vorrei approfondire solo le relative definizioni.

[1] La lista non è esaustiva
[2] Una corretta gestione del rischio non è volta solo a ridurre la probabilità che accada un evento negativo, ma anche che accada un evento positivo
[3] Si veda anche UNI 11230:2007 "Gestione del rischio – Vocabolario"

Il **Contesto Esterno**, definito come "L'ambiente esterno nel quale l'organizzazione cerca di conseguire i propri obiettivi[4]. Gli esempi riportati individuano come fattori caratteristici:

- l'ambiente culturale, sociale, politico, cogente, finanziario, tecnologico, economico, naturale e competitivo, sia internazionale, nazionale, regionale o locale, le relazioni con i portatori di interesse esterni;gli elementi determinanti e le tendenze fondamentali che hanno un impatto sugli obiettivi dell'organizzazione.

Il **Contesto Interno,** definito come "L'ambiente interno nel quale l'organizzazione cerca di conseguire i propri obiettivi"[5]. Esso può comprendere:

- la Governance, la struttura organizzativa, i ruoli e le responsabilità; le politiche, gli obiettivi e le strategie che sono in atto per conseguirli; le capacità, intese in termini di risorse e conoscenza (per esempio, capitale, tempo, persone, processi, sistemi e tecnologie); i sistemi informativi, il flusso di informazioni e i processi decisionali (sia formali, sia informali); le relazioni con i portatori d'interesse interni, le loro percezioni e valori; la cultura dell'organizzazione; le norme, le Linee Guida e i modelli adottati dall'organizzazione; la forma e l' estensione delle relazioni contrattuali.

Giuseppe Bifulco – *"In ogni direzione"* – Milano, collezione privata (particolare)

In termini generali possono essere identificati, a titolo di esempio e non in termini esaustivi, i seguenti rischi:

[4] UNI ISO 31000:2010 paragrafo 2.10
[5] UNI ISO 31000:2010 paragrafo 2.11

Rischi esterni:

- Concorrenti
- Bisogni dei clienti
- Progresso tecnologico
- Normative di legge nei mercati di riferimento
- Costi materie prime e delle utility
- Oscillazioni cambi e tassi
- Fornitori

Rischi interni:

- Strategici:
- Ciclo di vita del prodotto
- Proprietà intellettuale
- Penali dei clienti
- Finanziari
- Liquidità
- Capitale proprio
- Operazionali
- Processo
- Qualità del prodotto
- Catena dei fornitori
- Frode da parte dei collaboratori /terzi
- Errori non intenzionali
- Salute e sicurezza dei lavoratori
- infrastrutture

Rischi specifici per il settore

Alcuni esempi:

- Nel settore della catena di produzione di alimentari, cosmetici, farmaci (o imballi destinati a questi settori), i rischi specifici possono essere connessi alla contaminazione batterica o alla deperibilità delle materie prime;

- In una fonderia, alcuni rischi riguardano difetti occulti, che non è possibile evidenziare se non (e comunque non sempre), con sofisticati strumenti di controllo.
- In una web farm dei rischi specifici possono riguardare gli attacchi dall'esterno, la manomissione dei sistemi, il furto di credenziali.

I due capitoli fondanti della Linea Guida riguardano:

- La struttura gestionale di riferimento (capitolo 4)
- Il processo di gestione del rischio (capitolo 5)

I principi

I principi, riportati nel capitolo 3, evidenziano una serie di caratteristiche della gestione del rischio. In particolare, essa crea e protegge il valore dell'impresa; si vuole in tal modo evidenziare la creazione del valore, accanto a quello della protezione del valore come finalità della gestione del rischio. Conseguentemente, essa è una "parte integrante di tutti i processi dell'organizzazione", anche se poi solo per alcuni di essi, sulla base dei risultati della ponderazione del rischio, si procederà con l'attività di trattamento del rischio stesso. Quindi, proprio in virtù di una decisione da prendere, la gestione del rischio è "parte del processo decisionale", e necessariamente deve "trattare esplicitamente dell'incertezza", essendo questa una caratteristica intrinseca alla gestione del rischio".

Giuseppe Bifulco – *"In ogni direzione"* – Milano, collezione privata (particolare)

Quali sono gli strumenti per ridurre tale incertezza, o, per lo meno, per tenerla sotto controllo? Ecco che ci vengono incontro altri principi che elencano le specifiche caratteristiche che deve possedere la gestione del rischio, la quale deve essere: "sistematica, strutturata, tempestiva, basata sulle migliori informazioni possibili", "su misura"; ed ancora "tiene conto dei fattori umani e

culturali", "trasparente ed inclusiva", "dinamica, iterativa e reattiva al cambiamento".

Insomma, dichiara l'ultimo principio: "La gestione del rischio favorisce il miglioramento continuo dell'organizzazione" Come poteva essere altrimenti?

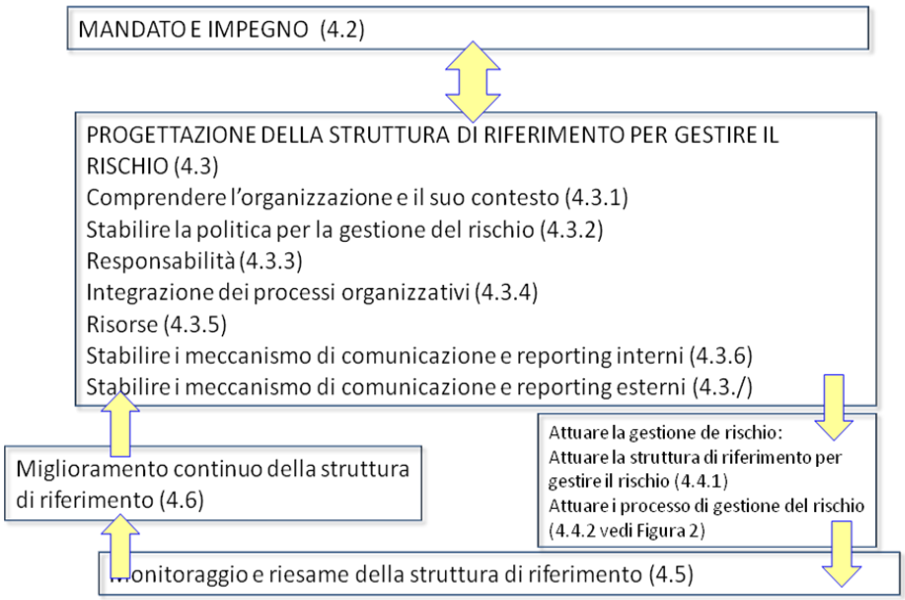
La strutture gestionale di riferimento

Il capitolo 4 tratta della struttura gestionale di riferimento e fornisce le indicazioni per la sua progettazione, sviluppo e miglioramento con riguardo ai componenti e alle loro modalità di relazione. L'iter di gestione è il consolidato modello PDCA, che prevede, a valle della definizione da parte della Direzione del "Mandato e Impegno", le fasi di:

- Progettazione della struttura di riferimento per la gestione del rischio
- Attuazione della gestione del rischio
- Monitoraggio e riesame della struttura di riferimento
- Miglioramento continuo della struttura di riferimento

La figura 1 illustra i componenti della struttura e la loro relazione. Lo schema è riportato nella Linea Guida[6]; i numeri indicano i paragrafi in cui i concetti sono sviluppati.

Figura 1 - La relazione tra i componenti della struttura di riferimento per gestire il rischio



[6] UNI ISO 31000:2010 capitolo 4

Come tutte i documenti che forniscono indicazioni sui sistemi di gestione, anche la Linea Guida UNI ISO 31000:2010 fornisce il quadro di riferimento riguardante la politica per la gestione del rischio, la quale deve contemplare gli obiettivi e gli impegni necessari per il loro conseguimento. La politica, oggetto di comunicazione all'interno ed all'esterno dell'organizzazione, dovrebbe trattare i seguenti punti[7]:

- il fondamento logico dell'organizzazione per gestire il rischio
- i legami tra gli obiettivi dell'organizzazione, le sue politiche e la politica per la gestione del rischio;
- i vari gradi di responsabilità;
- il modo in cui sono trattati i conflitti d'interesse;
- l'impegno a rendere disponibili le risorse necessarie per supportare coloro che hanno i vari gradi di responsabilità;
- il modo in cui viene misurata e riferita la prestazione relativa alla gestione del rischio;
- l'impegno a riesaminare e migliorare periodicamente, nonché in risposta ad un evento o ad un cambiamento di circostanze, la politica per la gestione del rischio e la struttura di riferimento.

Di fatto, attraverso una politica strutturata e completa si pongono le basi per tutti gli elementi che concorrono alla definizione della struttura di riferimento.

I passi operativi susseguenti alla definizione della politica, prevedono quindi che l'organizzazione[8]:

- definisca tempistica e strategia appropriate per attuare la struttura di riferimento;
- applichi la politica ed il processo di gestione del rischio ai processi organizzativi;
- rispetti i requisiti cogenti;

Giuseppe Bifulco – *"In ogni direzione"* – Milano, collezione privata (particolare)

[7] UNI ISO 31000:2010 paragrafo 4.3.2
[88] UNI ISO 31000:2010 paragrafo 4.4.1

- si assicuri che il processo decisionale, compresi lo sviluppo e la definizione degli obiettivi, sia in linea con gli esiti dei processi di gestione del rischio;
- svolga sessioni di informazione e formazione-addestramento;
- comunichi e si consulti con i portatori di interesse, per assicurare che la propria struttura di riferimento rimanga adeguata.

Il processo di gestione del rischio

Il capitolo 5 fornisce le Linee Guida affinché il processo diventi parte essenziale dell'organizzazione e quindi integri il sistema di gestione aziendale; quest'ultimo si completa quindi con un ulteriore tassello, che affianca le componenti tradizionali, ormai consolidate (ambiente, sicurezza, qualità, ecc.).

Gli elementi del processo considerato sono:

- Definizione del contesto
- Valutazione del rischio (Identificazione, Analisi, Ponderazione)
- Trattamento del rischio

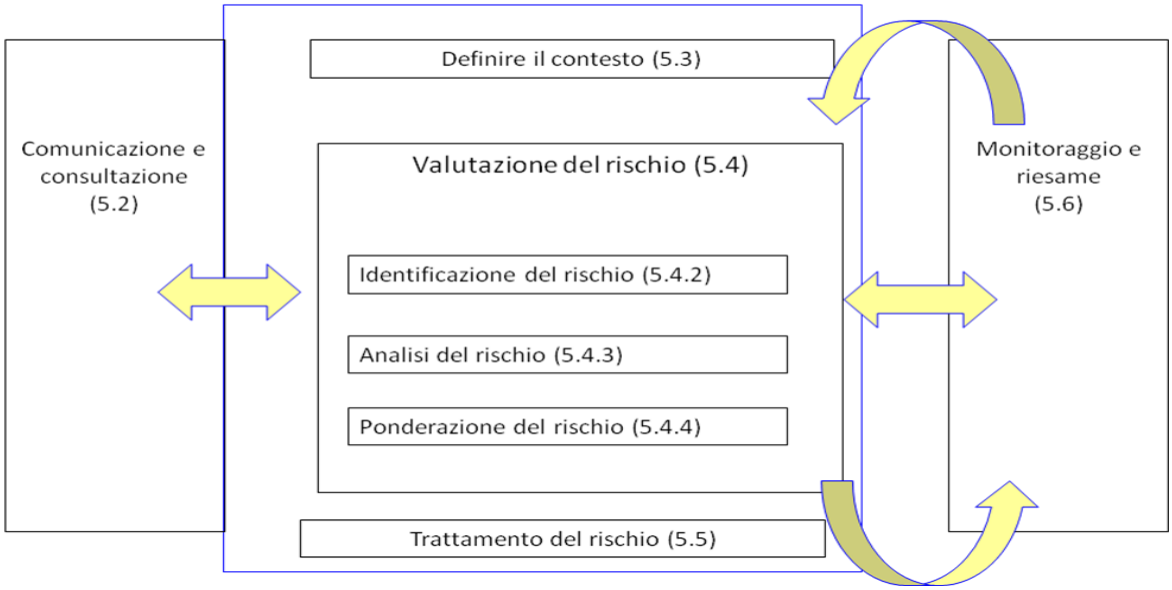
Trasversalmente si evidenziano le attività di: comunicazione e consultazione, monitoraggio e riesame.

Il processo deve essere ripetuto per ogni ambito di potenziale rischio, in ogni "area e livello, così come nelle specifiche funzioni, progetti ed attività"[9]; peraltro, dato che "ogni specifico settore od applicazione della gestione del rischio comporta particolari necessità, interlocutori, percezioni e criteri" è fondamentale "definire il contesto" come attività iniziale del processo, da un punto di vista generale, non specifico[10].Da ciò discende il principio che la gestione del rischio è un "abito su misura"; per essere veramente efficace, ogni situazione va studiata ed analizzata nella sua specificità e la Linea Guida, in sintesi, ci insegna proprio come fare questo, nel migliore dei modi.

La figura 2 mette in evidenza, secondo uno schema riportato dalla Linea Guida[11], gli elementi che concorrono al processo. I numeri indicano i paragrafi della Linea Guida in cui i concetti sono sviluppati.

[9] UNI ISO 31000:2010 capitolo Introduzione
[10] UNI ISO 31000:2010 capitolo Introduzione
[11] UNI ISO 31000:2010 capitolo 5

Figura 2 - Il processo di gestione del rischio

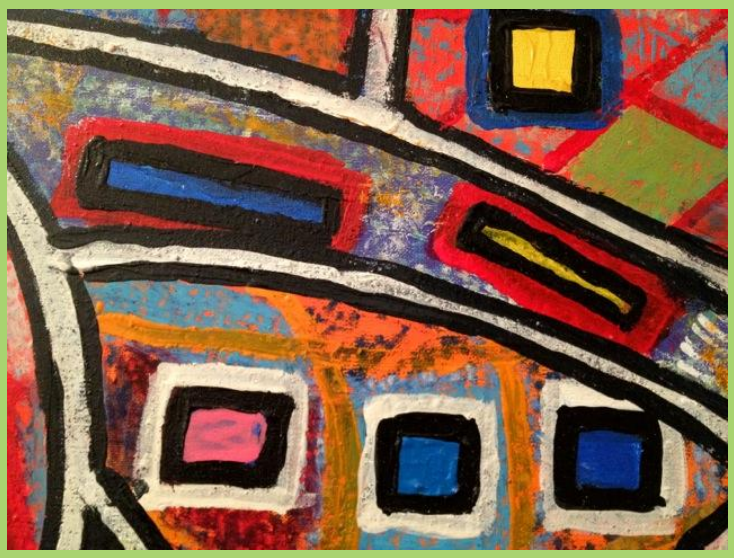


La gestione del rischio robusta

Completa la Linea Guida l'appendice A, dedicata alle caratteristiche che deve possedere una gestione del rischio robusta; si tratta di ulteriori elementi per integrare la struttura di riferimento; per ogni elemento (attributo) sono forniti esempi di indicatori:

ATTRIBUTO	ESEMPIO DI INDICATORE
Miglioramento continuo	Misura delle prestazioni dell'organizzazione
Completa responsabilità dei rischi	Consapevolezza, da parte di tutti i membri dell'organizzazione, dei rischi, dei sistemi di controllo, dei compiti assegnati
Applicazione della gestione del rischio nell'intero processo decisionale	Documentazione delle decisioni assunte e della motivazioni che hanno portato a tali decisioni

ATTRIBUTO	ESEMPIO DI INDICATORE
Comunicazione continua	Evidenza della comunicazione per i portati di interesse
Piena integrazione nella struttura di Governance dell'organizzazione	Dichiarazione nella politica dell'organizzazione, evidenze delle dichiarazioni ed azioni dei responsabili



Giuseppe Bifulco – *"In ogni direzione"* – Milano, collezione privata (particolare)

Conclusioni

La Linea Guida sono uno strumento complesso che deve essere letto, riletto ed applicato per poterne comprendere appieno le potenzialità ed implicazioni. Peraltro, non sono forniti esempi applicativi; se da un lato ciò ha il pregio di rendere assolutamente asettico il contenuto del documento, dall'altro ne risultano più difficili la lettura e la comprensione. Gli "Aiuti pratici", cui ci aveva abituati ad esempio la ISO 19011, relativa agli audit, avrebbero facilitato, senza interferire nell'impianto complessivo, l'analisi del documento.

Infine è da evidenziare che la complessità dell'approccio fa sì che la Linea Guida sia destinata ad imprese di dimensioni medio - grandi; solo queste hanno, infatti, la forza organizzativa per poter sostenere l'impatto che essa comporta; nonostante ciò, anche realtà di minori dimensioni possono trovare in questo documento spunti di riflessione che, sia pure per applicazioni parziali, forniscano preziose indicazioni per una consapevole e matura gestione del rischio.

		APPLICAZIONE	
		ADEGUATA	**NON ADEGUATA**
PROCEDURA	**NON ADEGUATA**	**NON CONFORMITA' MINORE PROCEDURALE**	**NON CONFORMITA' GRAVE**
	ADEGUATA	**CONFORMITÀ**	**NON CONFORMITA' MINORE APPLICATIVA**

Tabella 1

Esempi di scrittura di Non Conformità applicativa

La non conformità applicativa può essere scritta in forma testuale o schematica, in ogni caso maggiori sono le informazioni riportate (ed il modello schematico riduce la possibilità di dimenticare delle parti) maggiore è la possibilità di ricostruire, e quindi di oggettivare, il caso specifico che si è verificato.

In forma testuale:

- Nell'Ufficio Approvvigionamenti gli ordini di acquisto 23/2010 e 67/2009 (pari al 30% dei contratti esaminati) non riportavano le condizioni di pagamento, contrariamente a quanto specificato nella procedura PR. ACQ/01.

In forma schematica:

- **Area**: Ufficio Approvvigionamenti
- **Evidenza**: Ordini di acquisto 23/2010 e 67/2009
- **Campionamento**: 6 contratti dal marzo 2009 al febbraio 2010
- **Non conformità**: non riportano le condizioni di pagamento
- **Riferimenti**: procedura PR.ACQ/01

Esempio di cosa esprime una Non Conformità

- Dove concentrare l'attenzione - **Area**: Ufficio Approvvigionamenti
- In quali casi si è verificata - **Evidenza**: Ordini di acquisto 23/2010 e 67/2009
- Entità/estensione del fenomeno - **Campionamento**: 6 contratti dal marzo 2009 al febbraio 2010
- Problema riscontrato - **Non conformità**: non riportano le condizioni di pagamento

- Dove viene spiegato - **Riferimenti**: procedura PR.ACQ/01

Non Conformità procedurale

Le modalità di registrazione delle non conformità procedurali possono essere descrittive in fatti, di norma registrano un evento e non sono il risultato di uno specifico caso di campionamento.

Esempio di scrittura di Non Conformità procedurale

- La registrazione dell'attività di formazione è effettuata tramite un Database di recente introduzione non menzionato nella procedura PR.RUM/01, nella quale si fa riferimento al modulo cartaceo M. RUM/01, non più utilizzato

In molte situazioni di fatto si riscontra una situazione la cui gravità è minore rispetto alla non conformità; si tratta, in questo caso della formulazione di commenti. Esempi di commenti, con un taglio procedurale sono i seguenti:
È evidente che la nuova soluzione adottata con il Database è soddisfacente, ma deve essere aggiornata la procedura
La procedura PR. ACQ/01 non è rispettata sia pure per un numero limitato di casi

Le cause dell'origine delle Non Conformità

Un Sistema per funzionare correttamente deve essere:

NOTO, cioè il personale deve conoscerne l'esistenza, per poterlo utilizzare;

DISPONIBILE, cioè le informazioni in esso contenute, e necessarie per la sua applicazione/gestione, devono essere accessibili al personale;

Giuseppe Bifulco – *"In ogni direzione"* – Milano, collezione privata (particolare)

APPLICATO, cioè deve essere utilizzato in modo continuo così come previsto e/o specificato;

APPLICABILE, cioè il suo contenuto deve riferirsi alle attività realmente svolte in azienda, essere scritto in una lingua comprensibile al personale che lo utilizza ed essere utilizzabile in tutti i casi per i quali esso è stato concepito.
Per questo le cause di Non Conformità, cioè mancata applicazione di quanto predisposto (piani, procedure, contratti, ecc.), sono dovute soprattutto a:

- carenze formative (il Sistema non è noto oppure non è disponibile al personale)
- carenza di risorse (umane ed infrastrutture)
- mancanza di tempo (non è applicato oppure non è applicabile)
- attività non efficace (mancanza di valore aggiunto al processo)
- mix delle cause precedenti

Infine, per la ricerca della causa della Non Conformità può essere utilizzata la tecnica del campionamento, andando alla ricerca dell'origine del problema, tramite un campionamento selettivo e mirato.

Le Osservazioni invece non evidenziano una carenza rispetto al criterio, ma sono orientate al miglioramento, offrendo la possibilità di essere più efficienti.
Sono sempre formulate in positivo e sono possibiliste (valutare, considerare, …); devono essere valutate nel loro rapporto costo-benefici prima di poter essere messe in pratica.
Nella formulazione delle osservazioni è importante, quando possibile, mettere in evidenza le motivazioni che inducono a segnalarla.

Esempio di scrittura di osservazioni

- Considerare, al fine di una maggiore garanzia di tutela dei dati, Back-up giornalieri piuttosto che settimanali, come attualmente eseguito. Considerare anche Back-up in luogo remoto.
- Valutare di integrare le registrazioni relative all'applicazione delle MACCP con il sistema qualità, al fine di eliminare registrazioni ridondanti (es. pulizia e controllo merce in entrata).
- Considerare una sola procedura relativa alla formazione alla sicurezza del personale, rispetto alle due attualmente in vigore, al fine di semplificare l'impianto documentale e le registrazioni ad esso connesse.

In sintesi

È fondamentale l'atteggiamento mentale con cui si affronta un audit: un auditore, all'inizio di un audit deve essere certo che il processo, il contratto, la funzione che dovrà verificare rispetta i requisiti posti. Nel proseguo dell'audit confermerà questa sua posizione oppure diminuirà la sua fiducia nella capacità dell'attività oggetto di audit di rispettare i requisiti. la sua posizione è quindi aperta, di fronte ad una domanda che gli auditati non comprendono non si chiede "forse questo processo non è regolamentato" ma piuttosto "forse non sono stato chiaro nel formulare il quesito".

Giuseppe Bifulco – *"In ogni direzione"*- Milano, collezione privata (particolare)

Ecco, ci sarebbe molto altro da dire per migliorare il processo di audit ed innovarlo, ma in sintesi, per fare un audit in modo efficace il primo, che deve porsi in gioco e rivedere la propria posizione, i propri metodi è proprio l'auditore.

Fonti: per la stesura del'articolo è stata fondamentale la decennale esperienza come auditor, rispetto a diversa sistemi di gestione maturata in più di vent'anni, oltre a numerose attività di docenza sul tema. Sono stati utilizzati anche spunti di riflessione ed articoli presenti sul WEB per il quali non è stato possibile rintracciare, a distanza di tempo, la fonte esatta

Dicembre 2011

A cura di Monica Perego

AIATI S.r.l. docente di TUV Italia