

Risk Management: l' ISO ha emesso le nuove norme ISO /IEC 31000 - ISO/IEC 31010 - ISO Guide 73

La gestione del rischio (Risk Management) è il processo mediante il quale si misura o si stima il rischio e successivamente si sviluppano delle strategie per governarlo.

Si occupano di gestione del rischio sia le grandi imprese che hanno dei team appositi dedicati alla identificazione, analisi e valutazione dei rischi, sia le piccole imprese che invece approcciano informalmente alla gestione del rischio, sia le persone che inconsciamente lo valutano quotidianamente e decidono di conseguenza.

Alcuni esempi:

“Oggi le previsioni del tempo non sono buone e c'è il rischio di pioggia, sfortunatamente non ho con me l'ombrello.. pazienza esco comunque correndo il rischio di bagnarmi”

“Sono in una strada molto trafficata e ho la necessità di andare dall'altra parte , il semaforo con l'attraversamento pedonale è a 300 metri di distanza... e' più sicuro fare 300 metri a piedi passando dall'altra parte al semaforo che attraversare qui e rischiare di essere investito da una macchina”.

Noi abbiamo a che fare con la gestione del rischio ogni giorno della nostra vita e dobbiamo prendere delle decisioni basandoci sulle valutazioni che facciamo di ogni singola situazione. Queste valutazioni vengono fatte generalmente attraverso una analisi delle probabilità che un evento possa accadere (es. la possibilità di pioggia), le potenziali conseguenze che un evento si porta dietro (il bagnarsi) e i modi che posso usare per mitigare il rischio (guardo se le nubi sono minacciose prima di incamminarmi, considero se sono comunque in grado di chiamare un taxi etc.)

In alcuni casi la valutazione del rischio potrebbe essere altamente soggettiva mentre in altre circostanze una analisi più quantitativa, fatta utilizzando tecniche complesse e modelli matematici, potrebbe essere più appropriata (es. stimare scientificamente il rischio associato alla emissione di una polizza di assicurazione sulla vita, basata sulla conoscenza dell'età dell'assicurato, il suo peso, il suo lavoro, il suo stile di vita e le sue abitudini)

L'ISO e l'IEC (International Electrotechnical Commission) hanno recentemente emesso 3 importanti norme che sono utili alle organizzazioni interessate ad adottare un approccio alla gestione del rischio più sistematico e disciplinato .

ISO Guide 73:2009 - Risk Management -Vocabulary

Questa norma definisce il rischio come “l'effetto dell'incertezza sugli obiettivi” e va a spiegare che il rischio è spesso caratterizzato dal riferimento a potenziali eventi e alle relative conseguenze con associato la probabilità del loro accadimento.

Ogni organizzazione ha un suo particolare approccio al rischio e infatti molte organizzazioni di successo si sono affermate grazie alla loro capacità di assumersi dei rischi che altri avevano considerato inaccettabili.

L'attitudine al rischio di una organizzazione è definita dalla norma ISO Guide 73:2009 come "l'approccio dell'organizzazione a valutare ed eventualmente ricercare, farsi carico, affrontare o sfuggire dai rischi".

Il processo di gestione dei rischi include, secondo tale norma, l'applicazione sistematica delle politiche di gestione, delle procedure e delle prassi operative relative alle attività di comunicazione, consultazione, definizione del contesto, identificazione, analisi, valutazione, trattamento, monitoraggio e revisione del rischio.

ISO/IEC 31000:2009 - Risk Management - Principles and guidelines

Questa norma stabilisce una serie di principi che necessitano di essere soddisfatti per rendere efficace la gestione dei rischi.

Essa raccomanda che le organizzazioni sviluppino, implementino e continuamente migliorino il contesto in cui avviene la gestione del rischio con lo scopo di integrare tale processo all'interno della governance globale dell'organizzazione, in congruenza quindi con la strategia e la politica, la pianificazione e la gestione dei processi, i valori e la cultura.

ISO/IEC 31010:2009 - Risk Management - Risk assessment techniques

Questa norma ribadisce che tutte le organizzazioni, di qualsiasi tipo e dimensione, si trovano a gestire una gamma di rischi che possono influenzare la loro capacità di raggiungere gli obiettivi. Questi obiettivi possono essere relativi ad una vasta gamma di attività in funzione delle varie organizzazioni e possono andare dalle iniziative strategiche alle iniziative più operative, dai processi ai progetti, con riflessi sociali, ambientali, tecnologici, di sicurezza dei prodotti/servizi, commerciali, finanziari economici, politici e di immagine.

La norma enfatizza il fatto che tutte le attività di una organizzazione includono dei rischi che devono essere opportunamente gestiti.

Il processo di gestione del rischio è di fondamentale supporto al processo decisionale prendendo in considerazione, con un determinato grado di incertezza, la possibilità di accadimento eventi futuri o di circostanze particolari (previste e non previste) e dei loro effetti sugli obiettivi fissati. E' quindi di fondamentale importanza l'adozione di adeguate tecniche per la valutazione dei rischi che permettano un alto grado di oggettività di questa attività.

CISQCERT è da sempre attento alla evoluzione della materia avendo seguito l'evoluzione della normativa ISO sin dalla prime fasi di predisposizione dei vari "draft" delle norme.

CISQCERT ha predisposto un corso introduttivo sul tema del "Risk Management" volto a presentare il contenuto del pacchetto di norme prima citato alle organizzazioni, manager, auditor e consulenti interessati.

Tale corso di una giornata è per ora a disposizione su richiesta e verrà messo a catalogo nel secondo semestre dell'anno.

Per qualunque ulteriore informazione prego contattarci al n. **02.661543.26** oppure all'indirizzo corsi@cisqcert.com