ANRA

Associazione Nazionale dei Risk Manager
e Responsabili Assicurazioni Aziendali

Gli standard di Risk Management e l'ISO 31000

Adottare processi coerenti all'interno di una struttura di riferimento generale per contribuire ad assicurare che il rischio sia gestito efficacemente, con efficienza e in maniera coerente in tutta l'organizzazione.

Gli standard di Risk Management e l'ISO 31000

Position Paper ANRA

9 novembre 2011

In collaborazione e con il supporto di Strategica Group

Paolo Rubini

Presidente ANRA

In un contesto macroeconomico in cui la vulnerabilità delle imprese aumenta, il Risk Management è sempre più al centro dell'attenzione di molti amministratori e dirigenti, che si interrogano sulle modalità di individuazione, misurazione e trattamento dei rischi aziendali in un'ottica sistematica.

ANRA risponde a tale esigenza pubblicando un documento che descrive il processo di Risk Management, come definito dalle Linee Guida di ISO 31000: esse sono il risultato delle best practices internazionali, nate in Australia ed in Inghilterra, recepite da FERMA, la Federazione Europea delle Associazioni di Risk Management e finalmente trasferite in un modello generale che costituisce la nuova frontiera della professione.

Enrico Guarnerio

Presidente Comitato Tecnico Scientifico ANRA

L'agire in un contesto economico globalizzato ha portato alla consapevolezza di doversi adeguare a situazioni che comportano la gestione di rischi sempre più articolati e complessi.

I requisiti di sempre maggiore trasparenza, la volontà di gestire il rischio secondo modalità scientificamente strutturate attraverso l'adozione di metodologie condivise e riconosciute internazionalmente, non potranno che favorire lo sviluppo della professionalità e dell'importanza del ruolo del Risk Manager.

Indice

1. Obiettivi del Position Paper

Le organizzazioni in generale, siano esse piccole/medie imprese o grandi gruppi societari, si trovano, oggi più che in passato, ad affrontare tematiche connesse alla probabilità del verificarsi di eventi che rendono incerto il raggiungimento dei propri obiettivi.

L'effetto dell'incertezza sul raggiungimento degli obiettivi aziendali è definito "rischio"[1].

Tutti noi siamo consapevoli che lo svolgimento di qualsiasi tipo di attività economica comporta dei rischi. Tuttavia oggi, grazie alla crescita della cultura e della disciplina manageriale, agli studi ed alle ricerche in tema di gestione dei rischi, ai suggerimenti delle associazioni di settore e agli effetti dei provvedimenti dello stesso legislatore finalizzati a garantire un'informativa sempre più trasparente al mercato, si assiste ad un interesse sempre maggiore verso i vantaggi offerti dall'attività di Risk Management.

ANRA, nel 1972, nasce proprio con lo scopo di diffondere la cultura della gestione del rischio in azienda.

La pubblicazione dello standard ISO 31000 ad opera del Comitato Tecnico ISO/TMB "*Risk Management*", ha portato ANRA alla creazione di un Gruppo di studio composto da professionisti del settore e risk manager di importanti aziende, con l'intento di analizzarne e approfondirne i contenuti.

Il presente documento ha come principale obiettivo la divulgazione dello standard ISO 31000, scelto da ANRA quale modello di riferimento per l'esercizio dell'attività di Risk Management, fornendo al lettore una sintetica descrizione e una chiave di lettura dei principali contenuti.

Il Position Paper termina con una descrizione delle possibili interdipendenze degli attori che intervengono nelle attività di Risk Management.

1. Il termine rischio è stato tradotto in lingua italiana come "Insieme delle possibilità di un evento e delle sue conseguenze sugli obiettivi" UNI/ISO 11230:2007 Gestione del rischio – Vocabolario.

2. Contesto di riferimento

La funzione di Risk Management, proprio in quanto inserita all'interno della corporate governance segue la disciplina che regolamenta il sistema organizzativo aziendale[2].

Come emerge dalla lettura dei provvedimenti di legge emanati in questo ultimo decennio, il sistema organizzativo aziendale che si sta affermando è finalizzato ad assicurare una sana e prudente gestione aziendale e il perseguimento della stabilità finanziaria e patrimoniale attraverso il contenimento del rischio, oltre che la correttezza e la trasparenza dei comportamenti dei soggetti coinvolti nella produzione di beni e/o nella prestazione di servizi. Le disposizioni che regolamentano la funzione di Risk Management rientrano tra i principi che sottendono la generale disciplina in tema di corporate governance.

La richiesta in capo alle organizzazioni di disporre di solidi strumenti di governo societario, ha portato il legislatore, comunitario e italiano, alla introduzione negli ordinamenti, seppur inizialmente per settori specifici, di dettagliati obblighi inerenti la prevenzione di determinati rischi, a partire dalla tutela della integrità fisica del soggetto 'lavoratore', fino alla nuova concezione della attività di prevenzione dei rischi in capo al soggetto "impresa", necessaria anche in quanto elemento oggetto di *disclosure* a generale tutela del soggetto "mercato"[3].

Connessa al tema della gestione dei rischi risulta essere la configurazione delle responsabilità del management aziendale nei confronti del mercato (stakeholder, autorità di vigilanza). Responsabilità riconducibili all'interno della più ampia funzione attribuita all'iniziativa economica, che, secondo il nostro Legislatore "*Non può svolgersi in contrasto con l'utilità sociale o in modo da recare danno alla sicurezza, alla libertà, alla dignità umana.*" (Art. 41 Costituzione).

Facendo riferimento anche a questo principio contenuto nella nostra Carta fondamentale, negli ultimi anni alcuni settori, in particolare quello bancario, assicurativo

2. La pubblicazione nel 1999 del Codice di Autodisciplina, cd. Codice Preda, da parte del Comitato per la *Corporate Governance* delle Società Quotate, istituito da Borsa Italiana S.p.A., rappresenta un termine di riferimento fondamentale nella definizione dei criteri di *Corporate Governance*. Il codice, più volte aggiornato, contiene raccomandazioni di indirizzo, tali da costituire il modello di "*best practice*" per l'organizzazione ed il corretto funzionamento delle società quotate italiane.

3. Si vedano, a conferma di tale indirizzo: la direttiva n. 2003/51/CE relativa ai conti annuali e ai conti consolidati di taluni tipi di società, delle banche e altri istituti finanziari e delle imprese di assicurazione; la direttiva n. 2004/109/CE, sull'armonizzazione degli obblighi di trasparenza riguardanti le informazioni sugli emittenti i cui valori mobiliari sono ammessi alle negoziazioni in un mercato regolamentato; la direttiva 20101/76/EU, in tema di requisiti patrimoniali per il portafoglio di negoziazione e le ricartolarizzazioni e il riesame delle politiche remunerative da parte delle autorità di vigilanza. Con questi provvedimenti si è introdotto, fra gli altri, l'obbligo di disclosure sui principali rischi delle società i cui valori mobiliari sono ammessi alla negoziazione in un mercato regolamentato e operante all'interno di uno Stato membro e dell'insieme delle società, anche non quotate, incluse nel consolidamento.

e finanziario sono stati oggetto di una dettagliata regolamentazione mirata alla creazione di funzioni di vigilanza e controllo, interno ed esterno all'impresa, nonché di nuove forme di responsabilità, al fine di garantire una maggiore stabilità dell'impresa a tutto vantaggio dell'affidabilità del mercato.

In una prospettiva di Corporate Governance, dunque, il tema della valutazione dei rischi si intreccia con quello della progettazione e implementazione del sistema di controllo interno, a garanzia dell'efficienza ed efficacia aziendale, della salvaguardia dei beni aziendali e della conformità alle leggi e regolamenti.

La funzione di gestione dei rischi è, inoltre, coerente e riconducibile alle disposizioni dell'imprescindibile d.lgs. n.231/2001, in tema di responsabilità amministrativa delle persone giuridiche[4].

Come sappiamo, alcuni "delicati" settori sono già oggi tenuti a prevedere all'interno delle organizzazioni interessate la funzione di Risk Management. In particolare, i settori bancario e assicurativo e della sanità, oltre che le società quotate, in osservanza agli obblighi che derivano dalla disciplina che coinvolge la redazione del bilancio.

Analogamente le società quotate sono destinatarie di obblighi similari, in osservanza delle disposizioni aventi ad oggetto la disciplina relativa alla redazione del bilancio.

Tuttavia anche per molti altri settori osserviamo una crescente numerosità di norme che, in modo più o meno diretto, richiamano la necessità della presenza, all'interno dell'organizzazione aziendale, di una attività di Risk Management.

Si vedano, ad esempio, il Testo unico per la sicurezza sul lavoro e il Codice dell'ambiente a tutela della salute della collettività[5].

Nel settore della grande distribuzione e dei servizi ai consumatori ed utenti, il Codice del Consumo include fra gli obblighi del produttore e del distributore, a tutela dell'acquirente, l'adozione di misure proporzionate, in funzione delle caratteristiche del prodotto fornito, che comprendano "*le iniziative opportune per evitare il verificarsi di rischi*" legati ad un ampio concetto di difettosità del prodotto (Art. 104 comma 3 del Codice del Consumo).

Le aspettative circa la predisposizione di una figura o di un protocollo finalizzati alla gestione dei rischi in azienda hanno avuto pieno riconoscimento nelle decisioni delle

4. D.lgs. n.231/2001, *Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica.* Il provvedimento "invita" qualsiasi tipologia di società all'adozione di modelli organizzativi adeguati alla prevenzione del verificarsi dei reati elencati nel decreto stesso, attraverso la predisposizione di un'adeguata ed efficiente organizzazione amministrativa e contabile societaria. Il d.lgs. n.231/2001 non contiene norme prescrittive, tuttavia l'adozione di un modello organizzativo aziendale predisposto in maniera 'adeguata' legittima il giudice, nel caso si verifichi uno dei reati previsti nel provvedimento ad una esenzione di responsabilità da parte della società.

5. Si vedano: il D.lgs 81/2008 e succ. modifiche Testo Unico in materia di tutela della salute e della sicurezza nei luoghi di lavoro) e il D.lgs. n. 152 del 3 aprile 2006 Codice dell'ambiente.

corti di giustizia, che hanno statuito in tema di mancata adozione di modelli organizzativi adeguati ai sensi del d.lgs.231/01 e di misure di sicurezza a tutela dei consumatori (es. i rischi di richiamo del prodotto).

2.1. Le società quotate

Il legislatore ha emanato dettagliate disposizioni rivolte alle società quotate volte a favorire un'adeguata analisi e gestione dei rischi aziendali.

Il Testo Unico della Finanza che disciplina il settore prevede, fra gli altri, l'obbligo per gli organi amministrativi delegati e i dirigenti che provvedono alla redazione dei documenti contabili societari di attestare con apposita relazione allegata al bilancio d'esercizio e quello consolidato la predisposizione di adeguate procedure amministrative e contabili finalizzate alla formazione del bilancio e di ogni altra comunicazione di carattere finanziario.

La relazione sulla gestione comprende un'analisi attendibile dell'andamento e del risultato della gestione, nonché della situazione dell'emittente e dell'insieme delle imprese incluse nel consolidamento, unitamente alla descrizione dei "principali rischi e incertezze cui sono esposti"[6].

Si tenga presente, inoltre, la disposizione del codice civile che, in tema di bilancio destinato alla pubblicazione, relativamente al regime delle deroghe previsto all'art. 2423 c.c. stabilisce che "*Se le informazioni richieste da specifiche disposizioni di legge non sono sufficienti a dare una rappresentazione veritiera e corretta, si devono fornire le informazioni complementari necessarie allo scopo*". Si noti che la deroga non è intesa quale facoltà, bensì come obbligo previsto al fine di salvaguardare la clausola della rappresentazione veritiera e corretta. Mentre l'Art. 2423-bis c.c. "Princìpi di redazione del bilancio" impone nella redazione del bilancio l'osservanza dei seguenti princìpi: valutazione delle voci secondo prudenza e nella prospettiva della continuazione dell'attività; [...] 4) e che tenga conto dei rischi e delle perdite di competenza dell'esercizio, anche se conosciuti dopo la chiusura di questo; [...].

Si consideri, inoltre a riguardo, l'art.19 comma 1, lett.b) del D.lgs. n.39/2010 che nel dettare le regole in tema di revisioni legali dei conti annuali e dei conti consolidati, impone agli enti di interesse pubblico che il comitato di controllo interno e la revisione contabile "vigili sull'efficacia dei sistemi di controllo interno, di revisione interna, se applicabile, e di gestione del rischio".

L'interesse generale e l'importanza che il legislatore attribuisce alla funzione di Risk Management è ulteriormente dimostrata dal fatto che, il Ministero dell'Economia e delle Finanze richiede specifiche competenze in materia di "gestione del rischio e controllo interno" in capo a coloro che desiderano sostenere l'esame di idoneità professionale per

6. Vedi art. 154 *bis* lett. e) del d.lgs. n. 58/1998 così come modificato nel 2005 dalla legge n.262 a tutela del risparmio. Quest'ultima previsione era già contenuta all'art.4 della direttiva n. 2004/109/CE cd. transparency.

acquisire il titolo di revisore contabile (art. 4 D.lgs. n.39/2010)[7]. Quest'ultima previsione è contenuta anche nella direttiva 2004/109/CE, cd. "Transparency".

2.2. Il settore bancario

Per quanto riguarda il settore bancario, si consideri il regolamento congiunto della Banca d'Italia e della Consob, emanato nel 2007, in cui si indica il sistema di gestione del rischio dell'impresa, per Banche, SIM e Intermediari finanziari, come composto da: "*le strategie, le politiche, i processi e i meccanismi riguardanti l'individuazione, l'assunzione, la gestione, la sorveglianza e l'attenuazione dei rischi a cui l'intermediario è o potrebbe essere esposto (tra cui il rischio di credito, di mercato, operativo, reputazionale e strategico) e per determinare e controllare il livello di rischio tollerato*" (Regolamento congiunto Banca d'Italia e Consob, Art.2 Definizioni).

Regole armonizzate in materia di politiche e prassi di remunerazione rivolte a banche e imprese di investimento – introdotte con la direttiva europea n. 2010/76/UE in armonia con i principi internazionalmente concordati e approvati dal Financial Stability Board impongono al consiglio di amministrazione degli enti creditizi il coinvolgimento delle funzioni di controllo interno (Internal Audit, Risk Management e Compliance) e risorse umane, nella definizione delle politiche retributive[8]. Secondo la direttiva n. 2010/76/UE, i regimi remunerativi dovranno essere "adeguati", cioè posti in grado di evitare "l'assunzione di rischi eccessivi e imprudenti" che, purtroppo in passato hanno portato in alcuni Stati al verificarsi di rischi sistemici oltre che al fallimento di numerosi istituti di credito.

2.3. Il settore assicurativo

Anche nel settore assicurativo, come nel settore bancario, è stato introdotto il nuovo sistema di vigilanza di solvibilità "risk based"[9].
In particolare, abbiamo la direttiva 2009/138/CE, cd. Solvency II. La direttiva definisce un nuovo regime di solvibilità che conferisce, rispetto al regime vigente, maggiore rilevanza alla qualità della gestione dei rischi e alla solidità dei controlli interni. A tal proposito la direttiva Solvency II stabilisce che le imprese di assicurazioni devono condurre, nell'ambito del proprio sistema di gestione dei rischi, la valutazione interna del rischio e della solvibilità (cd. ORSA, *Own Risk and Solvency Assessment*). Tale valutazione riguarda il fabbisogno di solvibilità globale tenuto conto del profilo di rischio specifico, dei limiti di tolleranza del rischio approvati dal consiglio di amministrazione e della strategia operativa dell'impresa.

7. D.lgs. n. 39/2010, Attuazione della direttiva 2006/43/CE relativa alle revisioni legali dei conti annuali e dei conti consolidati, modifica delle direttive n.78/660/CEE e 83/349/CEE, e abrogazione della direttiva 84/253/CEE.

8. Direttiva n. 2010/76/UE attuata con provvedimento della Banca d'Italia, il 30 marzo 2011. La direttiva elabora principi e standard concordati in ambito internazionale e si inserisce nel più ampio novero di misure volte a garantire la stabilita' e il buon funzionamento del sistema bancario e finanziario in risposta alla crisi. Per assicurarne un'applicazione e un'interpretazione corretta e omogenea all'interno dell'Unione Europea, alla direttiva si accompagnano le Linee Guida del CEBS (Autorità bancaria europea dal 1° gennaio 2011).

9. Direttiva 2009/138/CE in materia di accesso ed esercizio delle attività di assicurazione e di riassicurazione, cd.Solvency II. Nel settore assicurativo, come nel settore bancario, sono state emanate una serie di direttive europee che, di fatto, hanno esteso i principi contenuti nella normativa di Basilea II al settore assicurativo.

Già nel 2008, l'autorità di vigilanza nazionale di settore, ISVAP, aveva introdotto con regolamento n.20/2008, l'obbligo in capo alle imprese di assicurazione di creare al proprio interno una funzione di Risk Management appropriata alla natura, dimensione e complessità dell'attività. Tale funzione risponde all'organo amministrativo e la sua collocazione organizzativa deve essere tale da non dipendere da funzioni operative; in osservanza all'art. 21 dello stesso regolamento, la funzione di Risk Management:

a) *concorre alla definizione delle metodologie di misurazione dei rischi;*
b) *concorre alla definizione dei limiti operativi assegnati alle strutture operative e definisce le procedure per la tempestiva verifica dei limiti medesimi;*
c) *valida i flussi informativi necessari ad assicurare il tempestivo controllo delle esposizioni ai rischi e l'immediata rilevazione delle anomalie riscontrate nell'operatività;*
d) *predispone la reportistica nei confronti dell'organo amministrativo, dell'alta direzione e dei responsabili delle strutture operative circa l'evoluzione dei rischi e la violazione dei limiti operativi fissati;*
e) *verifica la coerenza dei modelli di misurazione dei rischi con l'operatività svolta dalla impresa;*
f) *concorre all'effettuazione delle prove di stress test.*

È invece recente la pubblicazione del regolamento ISVAP n.39/2011 relativo alle politiche di remunerazione delle imprese di assicurazione che, in linea con gli indirizzi internazionali, devono risultare coerenti con la sana e prudente gestione del rischio e in linea con gli obiettivi strategici [...] (art.4 regolamento n.39/2011)[10]. Il regolamento attribuisce al Consiglio di Amministrazione l'obbligo di coinvolgere le funzioni di controllo interno (Internal Audit, Risk Management e Compliance) e Risorse Umane nella definizione delle politiche retributive, unitamente alla creazione di meccanismi di incentivazione che tengano conto, "*ove appropriato, anche di obiettivi di carattere non economico, quali la compliance e l'efficienza della gestione del servizio alla clientela*" (art.12. comma 2, lett. a e b)[11].

Anche le disposizioni regolamentari dell'Autorità di vigilanza del settore assicurativo sono volte alla implementazione di un sistema efficiente di gestione che coinvolga in prima persona le imprese di assicurazione attraverso la richiesta di procedere ad un'autovalutazione della rispondenza dei sistemi di remunerazione in essere alle disposizioni regolamentari[12].

10. Regolamento ISVAP n.39/2011, art. 4 Principi generali. *Le imprese adottano politiche di remunerazione coerenti con la sana e prudente gestione del rischio e in linea con gli obiettivi strategici, la redditività e l'equilibrio dell'impresa nel lungo termine. 2. Le imprese evitano politiche di remunerazione basate in modo esclusivo o prevalente sui risultati di breve termine, tali da incentivare una eccessiva esposizione al rischio.*

11. Le imprese di assicurazione sono tenute all'assunzione di politiche di remunerazione che misurino le *performances* degli amministratori sulla base di indicatori che tengano conto dei rischi associati e dei correlati oneri, in un orizzonte temporale non breve [...] e che creino meccanismi di incentivazione che tengano conto, "*ove appropriato, anche di obiettivi di carattere non economico, quali la compliance e l'efficienza della gestione del servizio alla clientela*" (Regolamento Isvap n.39/2011, art.12)

12. Sono operative dal 1° gennaio 2011, le nuove Autorità di vigilanza sul settore finanziario europeo, a livello macro e microprudenziale; l'EIOPA sovrintende al comparto assicurativo.

2.4. Il settore sanitario

Il settore che più di ogni altro, è già da anni orientato a definire le funzioni del Risk Management è sicuramente il settore sanitario. L'importanza dell'individuazione e gestione dei rischi e dei cd. eventi sentinella, ai fini della tutela della salute dei cittadini è apparsa di basilare importanza nell'offerta di prestazioni sanitarie.

I principali provvedimenti in materia di gestione del rischio in sanità sono stati redatti dal Ministero della Salute. Già nel 2004 era stato realizzato il documento titolato "*Risk Management in sanità. Il problema degli errori*". Nel 2006, è stato creato il Glossario in tema di sicurezza dei pazienti e di gestione del rischio clinico. L'anno successivo, il *Protocollo per gli eventi sentinella oltre alla Raccomandazione per prevenire gli atti di violenza a danno degli operatori sanitari*.

Nel 2009 è seguita la Raccomandazione per la prevenzione degli eventi avversi conseguenti al malfunzionamento dei dispositivi medici/apparecchi elettromedicali.

La rilevanza del ruolo del Risk Manager, oggi presente all'interno delle strutture sanitarie è fondamentale per definire i protocolli di gestione dei rischi di ciascuna unità operativa. L'osservanza dei protocolli è oramai un comportamento consolidato nello svolgimento dell'attività professionale degli operatori del settore.

Alcune regioni hanno fatto seguire l'introduzione della funzione di Risk Management ad una periodica mappatura dei rischi di tutte le Aziende Ospedaliere, Sanitarie Locali e Fondazioni a partecipazione pubblica facenti capo al Servizio Sanitario Regionale[13].

13. Si veda il documento della regione Lombardia, Direzione Generale Sanità, Mappatura dei rischi del Sistema Sanitario regionale, anno 2011.

3. Gli standard di Risk Management

Le aziende hanno la necessità di comprendere il livello complessivo di rischio insito nei loro processi e nelle loro attività. Ciò implica il riconoscere e dare priorità ai rischi più significativi, individuare le criticità, riconoscere le debolezze dei controlli, arrivando ad attuare un efficace processo di Risk Management.

La progettazione, l'attuazione di piani di gestione del rischio e la definizione delle relative strutture di riferimento, richiedono di prendere in considerazione le differenti esigenze di una specifica organizzazione, i suoi obiettivi, il contesto, la struttura, le operazioni, i processi, le funzioni, i progetti, i prodotti, i servizi e le specifiche prassi adottate.

Negli ultimi anni si è assistito ad una costante crescita del bisogno di gestire il rischio in modo sempre più efficace e rigoroso, integrato nella governance complessiva, nella strategia, nella pianificazione, nella gestione, nei processi di reporting, nelle politiche, nei valori e nella cultura dell'impresa.

Tale esigenza ha portato alla ricerca e all'adozione di processi sempre più strutturati, in grado di contribuire ad assicurare che il rischio sia gestito efficacemente e in maniera coerente rispetto all'organizzazione nel suo complesso.

Gli standard di riferimento

La formalizzazione di un processo di Risk Management, dei suoi contenuti, degli attori coinvolti, delle modalità di valutazione e delle strategie di gestione dei rischi, ha coinvolto numerose associazioni nell'implementazione di studi di documenti atti a evidenziare le caratteristiche del modello di Risk Management. La realizzazione di linee guida di standard di processo ha consentito alle aziende di adottare il modello più congruo alle proprie esigenze, nel rispetto delle regole nazionali e internazionali che devono seguire le singole organizzazioni.

Gli standard maggiormente conosciuti sono:

- AIRMIC, ALARM, IRM, 2002. Standard elaborato dalle maggiori organizzazioni di Risk Management del Regno Unito, ripreso successivamente anche dalla Federazione Europea delle Associazioni di Risk Management – FERMA -.
- Co.So. II, 2004. Pubblicato dal *Committee of Sponsoring Organizations of the Treadway Commission* (organismo privato USA che si occupa di controlli interni e Corporate Governance), il documento descrive i principi, le componenti ed i concetti più rilevanti della gestione del rischio aziendale, con particolare attenzione ai ruoli e ai compiti delle diverse funzioni in ottica Corporate Governance[14].

14. Il Co.So. Report (*Committee of Sponsoring Organizations of the Treadway Commission*) è uno tra i modelli più utilizzati nel mondo per l'implementazione di piani e programmi di Risk Management. Esso è utilizzato per la gestione di rischi integrati (ERM: Enterprise Risk Management) e offre una ricca sezione di tecniche alternative a supporto dell'applicazione del modello.

- AS/NZS 4360:2004. Primo standard elaborato in Australia/Nuova Zelanda che fornisce le linee guida generiche del processo di Risk Management.
- AS/NZS - ISO 31000:2009. Evoluzione del precedente standard Australiano, sviluppato in Europa come standard ISO e adottato sia in Europa sia successivamente in Australia/Nuova Zelanda.
- ISO Guide 73:2009 - Vocabulary, 2009. Guida che uniforma il significato della terminologia tecnica relativa al processo di Risk Management, in lingua inglese.
- ISO 31000, 2009. Il documento titolato "Risk Management. Principles and guidelines" contiene le linee guida applicative dell'art.41 secondo comma lett.b della direttiva 2006/43 relativa ai conti annuali e consolidati (attuata in Italia con il d.lgs. N.39/2010).
- ISO 31010, 2009. Il documento titolato "Risk Management Techniques" che supporta lo standard ISO 31000 fornendo indicazioni su apposite tecniche di assessment dei rischi.
- UNI ISO 11230, 2007. Risk Management. Vocabolario, in lingua italiana.
- UNI ISO 31000, 2010. Il documento titolato "Risk Management. Principi e linee guida" è una traduzione in lingua italiana delle linee guida ISO 31000.

I vantaggi dell'applicazione di uno standard

L'adozione di uno standard di Risk Management riconosciuto a livello internazionale consente, in generale, di aumentare il grado di consapevolezza della necessità di gestire il rischio, di migliorare l'efficacia e l'efficienza della gestione del rischio e del sistema dei controlli, di rendere maggiormente affidabile il processo decisionale, di migliorare la qualità dei rischi e di incrementare la confidenza e la fiducia dei portatori d'interesse interni ed esterni all'impresa.

4. Lo standard ISO 31000

Lo standard ISO 31000 è stato redatto nel 2009 dal Comitato Tecnico ISO/TMB "*Risk Management*"[15].

Lo standard ISO 31000 fornisce i principi e linee guida per la gestione di qualsiasi forma di rischio in un modo sistematico, trasparente e credibile ed all'interno di qualunque campo di applicazione e contesto.

Lo standard ISO 31000 promuove l'armonizzazione dei processi di gestione del rischio, senza per questo prescindere dalle esigenze di specifiche considerazioni connesse a ciascuna azienda, fornendo un approccio comune a supporto di norme che riguardano rischi e/o settori specifici, senza peraltro sostituirsi a tali norme.

La peculiarità dello standard ISO 31000 è data dalla sua applicabilità a **qualsiasi tipologia di impresa** (indipendentemente dallo specifico settore di competenza), in relazione ai suoi **vari ambiti di attività** (inclusi le strategie, i processi operativi, lo sviluppo dei progetti), così come a **qualsiasi tipo di rischio** a cui è esposta (quale sia la sua natura o le conseguenze, positive o negative che può generare).

Lo standard ISO 31000 stabilisce alcuni principi che devono essere soddisfatti per rendere efficace la gestione del rischio e raccomanda che le organizzazioni sviluppino, attuino e migliorino in continuo una struttura di riferimento, il cui lo scopo è integrare il processo per gestire il rischio all'interno della governance complessiva dell'impresa. L'applicazione dello standard ISO 31000 consente di definire e uniformare i processi di gestione del rischio, replicandoli all'interno dell'organizzazione.

Lo standard ISO 31000 intende soddisfare le esigenze di una vasta gamma di portatori d'interesse, tra i quali in particolare: i responsabili dello sviluppo della politica di gestione del rischio all'interno dell'organizzazione, coloro che devono garantire che il rischio sia gestito efficacemente e coloro che hanno l'esigenza di valutare l'efficacia dell'organizzazione nel gestire il rischio.

La struttura dello standard ISO 31000 si fonda sulla relazione fra i **Principi** che devono essere osservati per gestire efficacemente il rischio, la **Struttura di riferimento** in cui si attua la gestione del rischio[16] ed il **Processo di gestione del rischio**[17].

Nei capitoli che seguono vengono illustrate le singole componenti dello standard.

15. Lo stesso standard ISO 31000 è stato successivamente recepito, in lingua italiana, sotto la competenza della Commissione Tecnica UNI "Sicurezza della società e del cittadino" ed ha avuto definitiva approvazione in data 25 novembre 2010.

16. Figura 1 rappresentata nei capitoli che seguono

17. Figura 1 rappresentata nei capitoli che seguono

5. I princìpi

Lo standard ISO 31000 indica una serie di principi a cui un'organizzazione dovrebbe ispirarsi per conseguire un'efficace gestione del rischio.

Secondo i principi forniti dall'ISO 31000, la gestione del rischio:

a) crea e protegge il valore;
b) è parte integrante di tutti i processi dell'organizzazione;
c) è parte del processo decisionale;
d) tratta esplicitamente l'incertezza;
e) è sistematica, strutturata e tempestiva;
f) si basa sulle migliori informazioni disponibili;
g) è "su misura";
h) tiene conto dei fattori umani e culturali;
i) è trasparente e inclusiva;
j) è dinamica, iterativa e reattiva al cambiamento;
k) favorisce il miglioramento continuo dell'organizzazione.

La gestione del rischio, effettuata con un approccio sistematico, tempestivo e strutturato:

- contribuisce in maniera dimostrabile al raggiungimento degli obiettivi e al miglioramento della prestazione;
- non è un'attività indipendente, separata dalle attività e dai processi principali dell'organizzazione;
- aiuta a effettuare scelte consapevoli, determinare la scala di priorità delle azioni e distinguere tra linee di azione alternative;
- contribuisce all'efficienza ed a risultati coerenti, confrontabili ed affidabili;
- favorisce il coinvolgimento appropriato e tempestivo dei portatori d'interesse e, in particolare, dei responsabili delle decisioni, a tutti i livelli dell'organizzazione.

Le organizzazioni dovrebbero sviluppare ed attuare strategie per migliorare la maturità dei propri sistemi di gestione del rischio unitamente a tutti gli altri aspetti della propria organizzazione.

6. La struttura di riferimento

Tutte le organizzazioni dovrebbero puntare ad un appropriato livello di prestazioni della propria struttura di riferimento per la gestione del rischio in linea con la criticità delle decisioni da prendere.

Tenuto conto che i rischi sono considerati in termini di "*effetto dell'incertezza sugli obiettivi*", la loro gestione è considerata come centrale per i processi di gestione dell'organizzazione e essenziale per il raggiungimento degli stessi obiettivi.

Il successo della gestione del rischio dipende pertanto dall'efficacia della struttura gestionale di riferimento che fornisce le fondamenta e gli assetti per integrare la stessa gestione del rischio nell'intera organizzazione a tutti i livelli.

La struttura di riferimento ha il compito di garantire che le informazioni relative al rischio, ottenute dal processo di gestione, siano riferite nel rispetto dei programmi di comunicazione e reporting agli organi decisionali pertinenti per materia.

Figura 1:
Relazioni tra i componenti della struttura di riferimento per gestire il rischio.
Fonte:
UNI ISO 31000

La struttura gestionale di riferimento deve essere strutturata al fine di supportare l'attività di gestione dei rischi attraverso l'applicazione del processo di gestione del rischio ai diversi livelli aziendali, integrando la gestione del rischio all'interno del sistema gestionale complessivo, arrivando ad adattare i componenti della struttura di riferimento alle specifiche esigenze aziendali.

L'impegno forte e costante da parte della direzione dell'organizzazione, unitamente ad una pianificazione strategica rigorosa, è fattore imprescindibile per una efficace gestione del rischio e del suo perdurare.

Gli obiettivi di gestione del rischio dovranno ovviamente essere coerenti con gli obiettivi e le strategie dell'organizzazione e con la sua cultura. Prima ancora di iniziare la fase di progettazione e di attuazione della struttura di riferimento per gestire il rischio, la direzione dovrà valutare e comprendere il contesto dell'organizzazione, sia interno sia esterno, poiché le peculiarità dei diversi contesti possono influenzare significativamente la progettazione della struttura medesima.

La comunicazione e la condivisione delle informazioni di pertinenza da parte della struttura di riferimento all'interno della azienda favoriscono una maggiore responsabilizzazione a tutti i livelli dell'organizzazione, mentre sarà onere della direzione comunicare ai portatori d'interesse i benefici dell'attività di gestione del rischio intrapresa, data la delicatezza delle informazioni.

Tuttavia, effetti positivi dall'attività di gestione del rischio si avranno solo se ciascuna organizzazione avrà la capacità di cercare o riconoscere al proprio interno le persone che, per la loro esperienza e competenza, siano in grado di realizzare la struttura di riferimento che meglio si adatta a svolgere tale compito.

I vari gradi di responsabilità ai diversi livelli all'interno dell'organizzazione dovranno essere assegnati verificandone periodicamente la loro appropriatezza e garantendo alla struttura le adeguate risorse per poter svolgere correttamente l'attività. Può risultare opportuno, a tale riguardo, assegnare specifici obiettivi e determinare chiari indicatori di prestazione allo scopo di favorire un miglioramento continuo della gestione del rischio.

7. Il processo di Risk Management secondo lo standard ISO 31000

Il processo di gestione del rischio può essere rappresentato come un elenco di attività coordinate e con una sequenzialità ciclica.

Lo standard ISO 31000 ha concepito il processo di Risk Management prevedendo alcune fasi principali – identificazione, analisi, ponderazione e trattamento del rischio – evidenziando altresì come la preventiva definizione del contesto, il monitoraggio e la comunicazione siano comunque degli elementi basilari per attuare correttamente le attività di Risk Management (cfr. Figura 2).

È importante evidenziare come il processo di gestione del rischio debba essere non solo parte integrante della strategia e della gestione d'impresa, ma anche strumento gestionale incorporato nella cultura e nelle prassi dell'organizzazione.

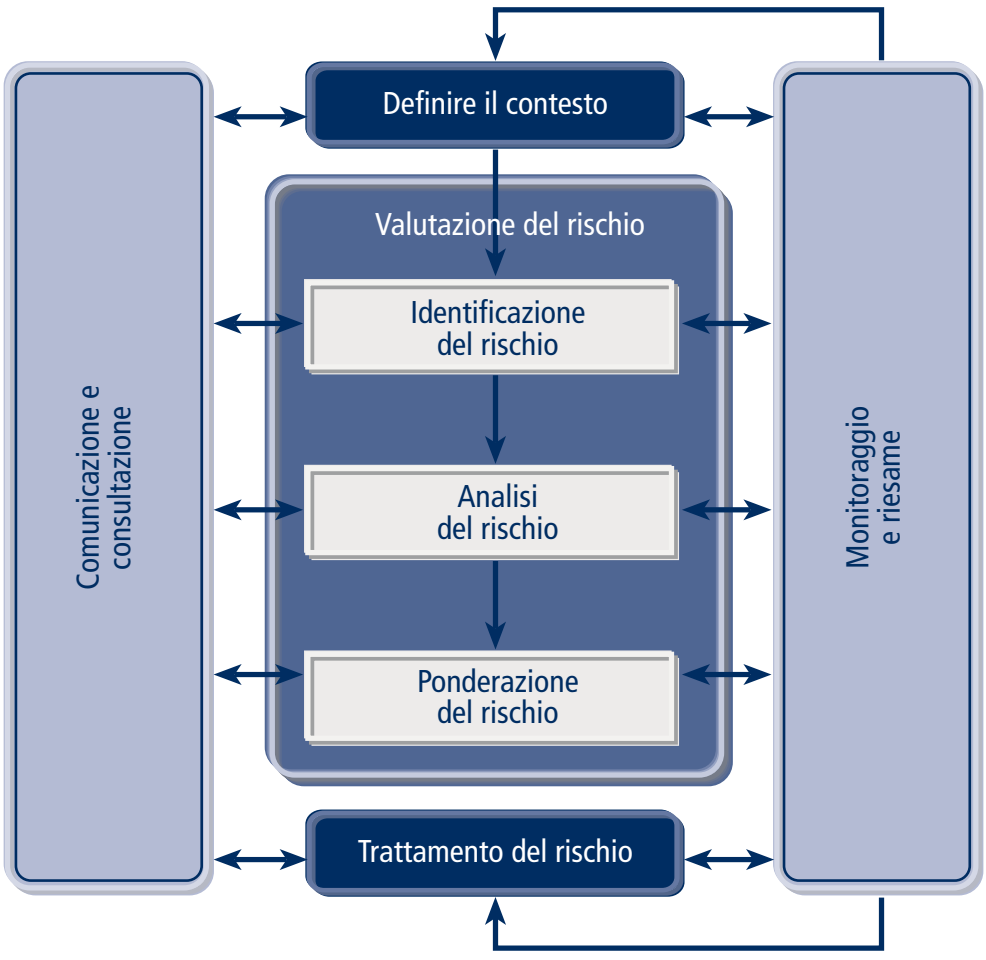

Figura 2:
Processo di gestione del rischio.
Fonte:
UNI ISO 31000

Nella rappresentazione del processo secondo lo standard ISO 31000, la comunicazione e la consultazione, così come il monitoraggio e il riesame, dovrebbero essere attuate all'interno di ogni fase del processo e non solo come elemento finale, in quanto essenziali per il buon andamento del processo stesso.

Le fasi tipiche della gestione del rischio vengono migliorate grazie a procedure chiare e condivise, oltre che mediante la continua interdipendenza tra attori e funzioni.

7.1. Comunicazione e consultazione

I piani per la comunicazione e la consultazione riguardano il rischio in sé, le sue cause, le conseguenze e le misure prese per il relativo trattamento. I piani di comunicazione devono essere impostati in modo tale da mettere in condizione i portatori di interesse di valutare le circostanze e prendere determinate decisioni.

Le attività di comunicazione e consultazione, pur tenendo conto degli aspetti di integrità personale e di riservatezza, dovrebbero aver luogo durante tutte le fasi del processo di gestione del rischio, in quanto indispensabili per l'efficacia e i risultati dell'intero processo.

L'approccio migliore per massimizzare gli effetti della consultazione è quello del "lavoro di squadra": il management deve definire il contesto in modo appropriato, assicurarsi che i rischi siano adeguatamente identificati e che le esigenze degli stakeholder siano comprese e considerate. Deve, inoltre, essere in grado di creare analisi specifiche unendo diverse aree di competenza, prendendo in considerazione in misura appropriata differenti punti di vista nella definizione dei criteri di rischio e nella ponderazione dei rischi stessi.

La comprensibilità e l'accuratezza nella redazione delle informazioni risulta inoltre essere fondamentale sia per comunicare adeguatamente un piano di trattamento del rischio, sia per intensificare e far comprendere agli stakeholders la necessaria azione di change management in atto per lo sviluppo del processo di Risk Management.

7.2. Definizione del contesto

Una caratteristica importante dello standard ISO 31000 riguarda l'introduzione della "definizione del contesto" quale attività preliminare del processo di gestione del rischio.

La gestione del rischio è un processo continuo che sostiene lo sviluppo e l'attuazione della strategia di un'organizzazione e che deve affrontare metodicamente tutti i rischi associati a qualsiasi attività dell'organizzazione. Questo implica la conoscenza dei fattori critici di successo, delle minacce e delle opportunità legate al raggiungimento degli obiettivi.

La definizione del contesto consente di cogliere gli obiettivi dell'organizzazione, l'ambiente in cui essa persegue tali obiettivi, i relativi portatori d'interesse e la diversità dei criteri di rischio, elementi che contribuiscono tutti a rivelare e valutare la natura e la complessità dei rischi.

Per poter far fronte a una corretta analisi dei rischi, le organizzazioni devono, innanzitutto, definire il contesto in cui opera l'azienda in relazione ai propri obiettivi, identificandone i parametri esterni ed interni, e selezionando i criteri di rischio che andranno considerati nell'implementazione del processo.

Il contesto esterno

La comprensione del **contesto esterno**, rappresentato dall'ambiente dove l'azienda cerca di perseguire i propri obiettivi, è importante al fine di assicurare che le finalità e le preoccupazioni dei portatori d'interesse esterni siano adeguatamente e correttamente considerati nello sviluppo dei criteri di rischio.

Il contesto esterno è costituito dagli elementi determinanti e le tendenze fondamentali che influenzano gli obiettivi dell'organizzazione, quali l'ambiente sociale, politico, finanziario, tecnologico, economico, naturale e competitivo, le relazioni con i portatori d'interesse esterni.

Il contesto interno

Il **contesto interno** è rappresentato dall'ambiente interno nel quale l'organizzazione cerca di conseguire i propri obiettivi ed è caratterizzato da qualsiasi cosa, all'interno della stessa organizzazione, che può influenzare il modo in cui un'organizzazione intende gestire il rischio.

Il processo di gestione del rischio non può prescindere dalla comprensione del contesto interno, dovendo necessariamente integrarsi con la cultura, i processi, la struttura, la strategia e gli obiettivi dell'organizzazione. Ciò implica conoscere e comprendere a fondo gli aspetti di governance, i ruoli e le responsabilità attribuiti nell'organizzazione nonché le loro relazioni con i processi, le risorse a disposizione, le caratteristiche delle relazioni con gli stakeholder, i sistemi, i flussi informativi, i processi decisionali, le norme, le linee guida e i modelli adottati dall'azienda.

Il contesto del processo di gestione del rischio

La gestione del rischio dovrebbe essere intrapresa in funzione degli obiettivi e degli ambiti di applicazione all'interno dell'organizzazione aziendale, ciò anche al fine di allocare correttamente le risorse necessarie per il conseguimento dei risultati attesi.

La definizione del contesto del processo di gestione del rischio dovrebbe aiutare ad assicurare che l'approccio alla gestione del rischio adottato sia appropriato alle circostanze, all'organizzazione ed ai rischi che influenzano la realizzazione dei propri obiettivi. Ciò implica, a titolo esemplificativo, la definizione delle responsabilità, delle attività, degli obiettivi, delle funzioni, dei progetti, delle metodologie di valutazione del rischio, dei criteri di valutazione delle prestazioni e l'efficacia della gestione del rischio.

Definire i criteri di rischio

Nell'ambito della fase di definizione del contesto, l'organizzazione dovrebbe inoltre definire i criteri da utilizzare per valutare la significatività del rischio.
Tali criteri dovrebbero riflettere i valori, gli obiettivi e le risorse dell'organizzazione, essere coerenti con la politica per la gestione del rischio stabilita ed essere poi riesaminati continuamente.

I principali criteri da prendere in considerazione riguardano: l'individuazione delle fonti di rischio, la definizione delle modalità di misurazione del livello di rischio, la definizione del livello di rischio che l'organizzazione è disposta a sopportare (risk appetite e/o risk tollerance), le correlazioni tra i rischi, l'orizzonte temporale e i metodi di misurazione delle cause e conseguenze degli eventi.

7.3. Valutazione del rischio

La fase di valutazione del rischio è complessivamente rappresentata dalle attività di identificazione, analisi e ponderazione del rischio.

7.3.1. Identificazione

La fase di identificazione dei rischi consiste nel selezionare ed evidenziare le fonti di rischio, gli eventi, le cause e i potenziali effetti degli avvenimenti che possono avere un impatto sui fattori critici di successo e sul raggiungimento degli obiettivi dell'organizzazione.

L'obiettivo di tale fase è quello di generare un elenco completo dei rischi, evitando di tralasciare eventi che necessariamente non verrebbero considerati nelle analisi successive.

L'identificazione deve comprendere l'esame degli effetti indiretti di particolari conseguenze, inclusi gli effetti a cascata o cumulativi, e considerare un'ampia gamma di conseguenze, significative o meno, anche se la fonte o causa di rischio può non essere manifesta.

L'azienda deve applicare strumenti e tecniche d'identificazione adatti ai propri obiettivi e capacità ed ai rischi cui far fronte; in questa fase è importante che le informazioni siano pertinenti ed aggiornate e derivanti anche da conoscenze ed esperienze pregresse.

Nell'identificazione dei rischi dovrebbero essere coinvolte persone con appropriate conoscenze.

7.3.2. Analisi del rischio

L'analisi del rischio implica lo sviluppo di una conoscenza del rischio ed è caratterizzata dalla valutazione delle conseguenze positive o negative (impatto) e della verosimiglianza (probabilità) derivanti dall'accadimento dei rischi individuati nella fase di Identificazione.

I risultati dell'analisi e le modalità con le quali vengono espresse, forniscono i dati e gli elementi necessari per procedere al processo decisionale, caratterizzato dalle successive fasi di ponderazione e trattamento del rischio. I report dovrebbero evidenziare eventuali fattori critici, quali divergenze di opinioni, disponibilità e qualità delle informazioni o limiti nella modellazione.

Per conoscere il profilo di rischio dell'impresa, è necessaria un'approfondita analisi delle sue componenti. L'analisi del rischio può essere intrapresa con vari livelli di dettaglio, in funzione del rischio, dello scopo dell'analisi e delle dei dati e delle risorse disponibili e dovrebbe considerare il livello di efficacia ed efficienza dei sistemi di controlli esistenti, nonché la coerenza delle valutazioni con i criteri di rischio definiti durante l'esame del contesto.

L'analisi può essere condotta mediante la modellazione in forma qualitativa, semi-quantitativa o quantitativa dei dati disponibili, che possono essere a loro volta rappresentati dagli eventi registrati o estratti da studi sperimentali. Un elemento di particolare rilevanza che deve essere considerato è rappresentato dall'interdipendenza tra differenti rischi e relative fonti.

I risultati dell'analisi possono essere espressi in termini di impatti tangibili e intangibili e, in funzione dei casi, possono esprimere più di un valore numerico o di un termine descrittivo.

La combinazione tra impatto e probabilità, le modalità in cui vengono espresse le informazioni disponibili, lo scopo per cui vengono utilizzati i dati in uscita, l'interdipendenza tra differenti rischi e le relative fonti, riflettono il livello e la tipologia di rischio dell'organizzazione.

7.3.3. Ponderazione del rischio

La fase di ponderazione considera i criteri di rischio stabiliti durante l'esame del contesto e i risultati delle analisi dei rischi e mira a definire quali rischi necessitano un trattamento e le relative priorità di attuazione.

Tenuto conto della propensione al rischio dell'organizzazione e dei criteri di rischio stabiliti, le decisioni possono limitarsi a mantenere attivi i controlli esistenti senza procedere ad una ulteriore fase trattamento del rischio o, in alternativa, procedere ad una ulteriore fase di analisi.

7.4. Trattamento del rischio

A seguito delle decisioni prese nella fase di ponderazione, il processo di Risk Management prevede il passaggio alla fase di trattamento del rischio, caratterizzato dalla valutazioni delle opzioni più opportune per modificare il profilo dei rischi e l'implementazione dei piani attuativi.

Il trattamento del rischio è contraddistinto da un processo ciclico che prevede la valutazione delle opzioni di trattamento del rischio, la valutazione dell'efficacia delle opzioni prescelte e la considerazione della tollerabilità o meno dei livelli di rischio residuo a valle del trattamento.

Il trattamento del rischio prevede normalmente l'attuazione di diverse possibili soluzioni, quali: l'eliminazione della fonte di rischio (anche attraverso la rinuncia a svolgere l'attività che lo sottende), l'assunzione del rischio al fine di perseguire una opportunità, la modifica della probabilità di accadimento e/o dell'impatto delle conseguenze, la condivisione del rischio con altri soggetti (trasferimento), la ritenzione del rischio in modo consapevole.
La scelta dell'opzione di trattamento del rischio più appropriata implica l'ottenimento del miglior rapporto tra costi di attuazione e benefici derivanti, tenendo in considerazione eventuali requisiti di obbligatorietà.

Il trattamento del rischio richiede il coinvolgimento di diversi portatori d'interesse, dai quali il livello di rischio potrebbe essere percepito in modo differente fra loro.

Il trattamento dei rischi deve basarsi su un piano strutturato in funzione delle priorità di intervento e deve essere monitorato ai fini della verifica dell'efficacia delle misure adottate.

Il piano di trattamento dei rischi deve essere ben integrato all'interno dell'organizzazione e adeguatamente documentato, indicando: i soggetti coinvolti sia in fase di approvazione che di attuazione, i criteri di scelta delle opzioni di trattamento, le aspettative in termini di risultato, i piani di azione, i requisiti relativi alle risorse, i parametri di misurazione delle prestazioni, i requisiti di reporting e la programmazione degli interventi.

A valle del processo di trattamento attuato, il rischio residuo dovrebbe essere riesaminato con il coinvolgimento dei responsabili delle decisioni e degli altri portatori d'interesse, al fine, se opportuno, di essere assoggettato a ulteriore trattamento.

7.5. Monitoraggio e riesame

Il processo di gestione del rischio prevede la pianificazione di attività di monitoraggio e riesame pianificate, che comportano verifiche regolari di tutti gli aspetti che lo compongono.

Le attività di monitoraggio e riesame servono a assicurare l'efficacia e l'efficienza dei controlli, garantire il flusso delle informazioni necessarie per l'analisi del rischio, analizzare gli eventi, rilevare i cambiamenti nel contesto (interno, esterno e relativo alla definizione dei criteri di rischio) che possono influenzare il livello di rischio e richiedere eventuali revisioni dei trattamenti e delle priorità.

I risultati del monitoraggio devono essere registrati e riferiti nel modo più appropriato e forniscono gli elementi necessari al riesame della struttura di riferimento per la gestione del rischio.

Oltre a monitorare l'efficacia dei controlli esistenti, l'efficienza globale delle attività e la realizzazione di ulteriori controlli, il monitoraggio deve accertare il rapporto costo-benefici dei controlli già esistenti.

Infine, il monitoraggio e la misurazione includono la valutazione sulla diffusione della cultura del rischio, delle performance e della preparazione dell'organizzazione, la conoscenza della struttura di riferimento, nonché la valutazione della misura in cui i compiti di gestione del rischio sono allineati con le altre attività aziendali e il monitoraggio di routine degli indicatori di performance.

8. Ruoli e attori del processo di Risk Management

La definizione di ruoli e mansioni che i diversi soggetti devono ricoprire all'interno della Corporate Governance è stata stabilita anche grazie alla determinazione dei Sistemi di Controllo Interno (SCI): i soggetti e le funzioni che contribuiscono alla gestione dell'impresa in modo sano, corretto e coerente con gli obiettivi aziendali e di Risk Management sono stati attentamente e congiuntamente identificati da organizzazioni internazionali, il cui obiettivo è stato quello di delineare con chiarezza i punti cardine del sistema di governo d'impresa in ottica di efficienza e di aderenza ai principi normativi, senza sovrapposizioni di attività.
Sono state quindi definite tre linee di difesa, o livelli di controllo, che hanno l'obiettivo di individuare responsabilità, ruoli e compiti delle diverse funzioni coinvolte nel controllo e nella gestione dei rischi aziendali.

Il Risk Management è una disciplina che fa parte di tali livelli di controllo.

In base alla natura e alla dimensione dell'organizzazione, il Risk Management può essere gestito da un consulente che svolge, limitatamente nel tempo e per singole categorie di rischio, l'implementazione di analisi e di processi di Risk Management, oppure può essere creata una funzione all'interno dell'azienda volta allo sviluppo di piani di Risk Management atti a durare nel tempo.
Le diverse responsabilità riguardo alla gestione dei rischi che devono essere riportate nei documenti di policy aziendale, sono ampie ed estese. E' importante a tale riguardo evitare possibili sovrapposizioni di ruoli, attribuendo una funzione chiara e ben definita al Risk Manager che dovrà essere affiancato agli altri responsabili aziendali.

Per diffondere la cultura del rischio e avviare piani di gestione del rischio, il Risk Manager, insieme al suo team, deve possedere competenze trasversali, dall'ambito assicurativo alla gestione d'impresa e dalla compliance alla conoscenza del settore merceologico in cui opera l'azienda. Egli non dovrà sostituirsi ai risk owner o diventare owner di rischi che non gli competono, per non violare il principio della accountability. Tuttavia, per coordinare efficacemente tutti gli attori che prendono parte al processo di gestione del rischio, egli dovrà conoscere gli impianti, i cicli di produzione, i margini di contribuzione, le caratteristiche dei prodotti da vendere o dei servizi da erogare; dovrà conoscere e saper implementare le metodologie per disegnare piani specifici di gestione del rischio, non solo considerando le attività e i processi che l'azienda ha in essere, ma anche facendo un'attenta analisi del contesto in cui opera e delle prospettive di sviluppo dell'organizzazione.

8.1. La figura del Risk Manager

L'obiettivo del Risk Manager è quello di promuovere, a tutti i livelli, l'attività di gestione del rischio, facendo crescere la responsabilizzazione di tutto il personale riguardo specifiche politiche di presidio del rischio.

Il Risk Manager ha una forte predisposizione a motivare le persone, alla pianificazione e al controllo e la capacità di tradurre le esigenze del Consiglio di Amministrazione in azioni strategiche volte a mitigare i rischi con accezione negativa e favorire lo sfruttamento delle opportunità alimentate da un insieme di rischi.

Il Consiglio di Amministrazione ha la generale responsabilità di determinare la direzione strategica dell'organizzazione e la propensione al rischio, creare il contesto e la struttura per la gestione del rischio, comprendere i rischi più significativi e gestire l'azienda nel momento di crisi.

In questo contesto, il Risk Manager affiancherà i responsabili di tutte le funzioni aziendali e li supporterà nelle loro decisioni sui rischi specifici della funzione, svolgendo un ruolo di coordinamento nelle decisioni sui rischi trasversali a più funzioni. Egli deve saper porre le condizioni per mettere in atto dei meccanismi adeguati per ottenere il miglioramento continuo delle prestazioni, dialogare con i manager di funzione affinché venga garantita l'attuazione delle raccomandazioni per il miglioramento del livello di rischio e per assicurare che nuovi rischi e circostanze vengano individuate e correttamente segnalate.

Inoltre, il Risk Manager deve essere in grado di far comprendere, accettare e implementare il processo di Risk Management, per arrivare alla realizzazione di report che contengano anche la segnalazione di eventi che avrebbero potuto configurarsi quali eventi negativi/perdite e che evidenziano l'esistenza di una potenziale situazione di rischio (cd. eventi sentinella).

Le responsabilità dirette del Risk Manager – in quanto owner del processo di Risk Management – sono invece basate sullo sviluppo e l'aggiornamento di una politica del rischio, sull'aggiornamento continuo riguardo le attività specialistiche del settore, sul coordinamento della funzione di gestione del rischio e delle sue attività, sulla compilazione dei report informativi riguardanti i rischi preponderanti e sullo sviluppo di piani di emergenza e di recupero e sul supporto delle indagini. Il Risk Manager deve essere in grado di controllare il processo di Risk Management all'interno della globale attività aziendale, ricevere e fornire garanzie sulla gestione del rischio, relazionare sull'efficienza e l'efficacia dei controlli interni.

In particolare, il Risk Manager dovrà supportare il Management nell'individuare i rischi e, in quanto responsabile del funzionamento del processo, dovrà fornire ai responsabili di funzione o divisione gli strumenti necessari per identificare e valutare i singoli rischi aziendali. Poiché l'attività da svolgere deve essere continuativa all'interno di ogni organizzazione, le sue decisioni devono essere supportate da un adeguato sistema informativo che raccolga tutte le informazioni sui rischi consentendo una più semplice fase di consolidamento dei risultati.

Dopo la stesura del piano di Risk Management il Risk Manager deve avere l'approvazione dai vertici aziendali per l'attuazione dei programmi relativi e delle singole attività da svolgere. Insieme ai più alti livelli dell'organizzazione si dovranno identificare gli obiettivi

strategici, tattici e operativi che saranno indispensabili per ottenere risultati economico-finanziari dai processi messi in atto dall'azienda. Il Risk Manager dovrà assegnare specifiche responsabilità ad ogni livello dell'organizzazione e comunicare le informazioni rilevanti, le procedure e gli obiettivi specifici al fine di diffondere la cultura del rischio e ottenere dei feedback riguardo i processi essenziali per l'attività di impresa.

8.2. Interdipendenza con le altre principali figure amministrative e di controllo

La configurazione delle interdipendenze e delle interrelazioni tra il Risk Manager, o la funzione a cui fa riferimento, e le altre figure aziendali è differente a seconda della dimensione, della visione e dell'approccio aziendale. Nella visione allargata della Corporate Governance le relazioni tra le funzioni sono determinate dai sistemi di controllo interno che hanno come obiettivo quello di garantire l'adeguatezza delle modalità di controllo rispetto ai rischi da presidiare.

La "*Guidance for Boards and Audit Committees*", documento pubblicato il 21 settembre 2010 e redatto congiuntamente da FERMA (Federazione Europea delle Associazioni di Risk Management) e da ECIIA (Confederazione Europea degli Istituti di Internal Auditing), definisce tre livelli di difesa col fine di garantire l'adeguatezza delle modalità di controllo rispetto alle esigenze poste dai rischi da presidiare.

Alla prima linea di difesa appartiene il Management Operativo, ovvero l'insieme di persone che hanno la ownership, la responsabilità e la accountability per valutare, controllare e mitigare i rischi e mantenere efficaci controlli interni.

La seconda linea di difesa include la funzione di Risk Management. Tale funzione definisce il framework di risk management, facilita e controlla l'attuazione di efficaci pratiche di gestione del rischio da parte dei manager operativi, assiste i risk owner nella definizione della esposizione al rischio e riporta le informazioni connesse ai rischi all'interno dell'organizzazione. Oltre alla funzione di Risk Management, come parte di questa seconda linea di difesa, alcune organizzazioni hanno previsto una funzione distinta di Compliance, per monitorare i rischi di inadempienza, i rischi cioè di non conformità alle leggi e ai regolamenti, anche interni. In tale veste, la funzione di Compliance riferisce direttamente all'alta direzione.

Altre funzioni di controllo specifiche possono essere rivolte alla salute e alla sicurezza del personale, alla catena di approvvigionamento, agli aspetti di tutela dell'ambiente e/o della qualità.

Alla terza linea di difesa appartiene la funzione di revisione interna (Internal Audit). Tale funzione, attraverso un approccio basato sul rischio, fornisce garanzia (assurance) al Board dell'organizzazione e al Senior Management, su come l'azienda valuta e gestisce i propri rischi, compresa la descrizione delle modalità attraverso le quali la prima e la seconda linea di difesa operano.
L'attività di controllo effettuata dall'Internal Audit contribuisce a identificare, gestire e tenere sotto controllo possibili eventi negativi, al fine di fornire una ragionevole certezza in merito al raggiungimento degli obiettivi dell'organizzazione.

Tutte le attività svolte, all'interno dei tre livelli di controllo, sono dirette al Senior Management e al Consiglio di Amministrazione, che hanno il pieno potere decisionale riguardo alla gestione ultima dei rischi individuati.

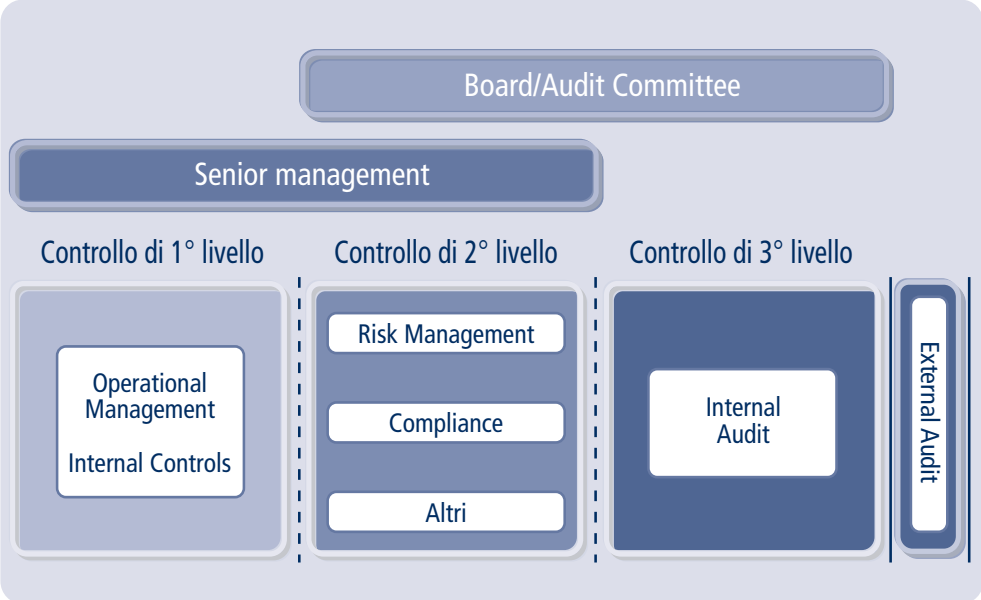

Figura 3:
I tre livelli dei Sistemi di Controllo Interno. Fonte: FERMA/ECIIA

Il Consiglio di Amministrazione supervisiona e conferisce le linee guida al management definendo il 'risk appetite', è consapevole dei rischi più significativi per l'organizzazione e ha come obiettivo ultimo quello di verificare se la dirigenza sta rispondendo in modo appropriato alle richieste del consiglio e alle esigenze aziendali.

Definendo le proprie aspettative in termini di integrità e di valori etici, il Consiglio di Amministrazione fornisce gli obiettivi generali al management e stabilisce le indicazioni riguardanti l'allocazione delle risorse. Uno dei compiti principali, nell'ambito di gestione del rischio, è quello di supervisionare il processo di Risk Management acquisendo conoscenza della misura in cui il management ha attivato un efficace processo di gestione del rischio aziendale. Il Consiglio di Amministrazione deve definire il livello di rischio accettabile dall'azienda, ma anche esaminare il rischio effettivo.

L'internal Audit deve invece svolgere una funzione di assurance sull'efficacia del processo implementato. L'obiettivo è quello di garantire l'adeguata gestione dei principali rischi aziendali e la corretta ed efficace implementazione del processo all'interno del sistema aziendale.

La complementarità delle figure del Risk Manager e dell'Internal Auditor deriva dalla volontà di entrambi di supportare il management nella gestione del rischio.

ANRA

ANRA è l'associazione che dal 1972 riunisce i Risk Manager e i Responsabili delle Assicurazioni Aziendali.

ANRA annovera tra i propri iscritti i Risk Manager delle maggiori imprese italiane.

ANRA svolge un ruolo centrale per la creazione e lo sviluppo in Italia di una cultura della gestione dei rischi ed è un interlocutore imprescindibile per le problematiche relative al Risk Management.

ANRA è il referente istituzionale per la diffusione delle best practices internazionali, in coordinamento con FERMA (la Federazione delle Associazioni Europee di Risk Management) e IFRIMA (la Federazione Internazionale delle Associazioni di Risk Management), delle quali è membro fondatore.

Hanno contribuito alla realizzazione del documento

Paolo Rubini
Presidente ANRA
Responsabile Risk Management Telecom Italia SpA

Enrico Guarnerio
Presidente Comitato Tecnico Scientifico ANRA
Presidente e Amministratore Delegato Strategica Group Srl

Marco Terzago
Vice-Presidente ANRA
Group Risk Engineering Manager
Risk/Insurance Manager South-Europe SKF Industrie SpA

Roberto Bosco
Consigliere ANRA
Corporate Risk Manager Mediaset SpA

Alessandro De Felice
Consigliere ANRA
Group Risk Manager
Prysmian SpA

Domenico Fumai
Risk Management Telecom Italia SpA

Rita Crocitto
Ph.D. - Docente a contratto Università L. Bocconi-Milano
Responsabile Scientifico Divisione studi e ricerche Strategica Group Srl

In collaborazione e con il supporto di

Strategica Group

PARTNER IN RISK MANAGEMENT

www.strategicagroup.com