ferma

FEDERATION OF
EUROPEAN RISK
MANAGEMENT
ASSOCIATIONS

STANDARD DI RISK MANAGEMENT

Introduzione

Lo Standard di Risk Management è il risultato del lavoro di un team creato dalle più importanti organizzazioni di risk management del Regno Unito - The Institute of Risk Management (IRM), The Association of Insurance and Risk Managers (AIRMIC) e ALARM, The National Forum for Risk Management in the Public Sector.

Il team si è avvalso inoltre del contributo di un'ampia gamma di altri organismi professionali operanti nel risk management per un lungo periodo di tempo.

Il risk management è una disciplina in rapida evoluzione ed esistono molte concezioni e definizioni diverse dei suoi contenuti, delle sue modalità di gestione e delle sue finalità. È necessario attenersi ad uno standard, ad un quadro di riferimento comune, per esser certi di condividere:

- *la terminologia relativa utilizzata*
- *il processo di attuazione del risk management*
- *la struttura organizzativa del risk management*
- *le finalità del risk management*

È importante che lo standard comune tenga conto degli aspetti positivi e negativi del rischio.

Il risk management non riguarda soltanto le imprese o gli enti pubblici, ma qualsiasi attività a breve o lungo termine. I vantaggi e le opportunità offerte non andrebbero valutate semplicemente nel contesto dell'attività in sé, ma in relazione ai molti diversi soggetti interessati sui quali può influire.

Ci sono molti modi di raggiungere gli obiettivi del risk management e sarebbe impossibile tentare di analizzarli tutti in un unico documento. L'intenzione, quindi, non è mai stata di produrre uno standard normativo che avrebbe spinto verso l'approccio basato sulle caselle a scelta multipla, né di stabilire un processo certificabile. Attenendosi alle varie fasi che compongono questo standard, le organizzazioni potranno dimostrare - sebbene in modi diversi - la loro conformità a esso. Lo standard rappresenta la miglior procedura con la quale le organizzazioni possono misurarsi.
Lo standard ha sempre utilizzato, laddove possibile, la terminologia del rischio recentemente indicata dall'Organizzazione internazionale di normalizzazione (ISO) nel suo documento Guida ISO/IEC 73 Risk management – Vocabolario – Linee guida in uso negli standard.

Tenendo conto della rapida evoluzione di questo settore, gli autori saranno grati alle organizzazioni che vorranno fornire il proprio feedback sullo standard dopo averlo utilizzato (l'elenco degli indirizzi è consultabile alla fine della presente Guida).
Si prevede infatti di modificare regolarmente lo standard in base alle pratiche migliori.

1. Il rischio

Il rischio può esser definito come la combinazione delle probabilità di un evento e delle sue conseguenze (Guida ISO/IEC 73).

Qualunque tipo di iniziativa implica potenzialmente eventi e conseguenze che rappresentano possibili benefici (elementi positivi) o minacce al successo (elementi negativi).

La concezione del risk management come attività legata sia agli aspetti positivi sia a quelli negativi del rischio è sempre più diffusa. Di conseguenza, questo standard valuta il rischio da entrambe le prospettive.

Nel campo della sicurezza, si ammette in genere che le conseguenze sono esclusivamente negative e quindi la gestione di questo tipo di rischio si concentra sulla prevenzione e sulla riduzione del danno.

2. Il risk management

Il risk management fa parte integrante del management strategico di ogni organizzazione. È il processo attraverso il quale le organizzazioni affrontano i rischi legati alle loro attività con lo scopo di ottenere benefici durevoli nell'ambito di ogni attività, in generale e in particolare.

La base di un buon risk management consiste nell'identificazione e nel trattamento di questi rischi. Il suo scopo è di conferire il massimo valore sostenibile ad ogni attività dell'organizzazione. Esso permette la comprensione dei potenziali aspetti positivi e negativi di tutti i fattori che possono influenzare l'organizzazione. Incrementa le probabilità di successo, mentre riduce sia le probabilità di fallimento sia l'incertezza sul raggiungimento degli obiettivi generali dell'organizzazione.

Il risk management deve essere un processo continuo e graduale che coinvolge tutta la strategia dell'organizzazione e la sua implementazione. Deve affrontare sistematicamente tutti i rischi che circondano le attività dell'organizzazione nel passato, nel presente e, soprattutto, nel futuro.

Deve essere integrato nella cultura dell'organizzazione attraverso una politica efficace e un progetto gestito dai massimi dirigenti.

Deve trasformare la strategia in obiettivi tattici e operativi, assegnare responsabilità a ogni livello dell'organizzazione rendendo ogni manager e ogni impiegato responsabile della gestione del rischio come parte stessa dei doveri professionali.

Favorisce le responsabilità, misura e premia le performance, promuovendo in tal modo l'efficienza operativa a tutti i livelli.

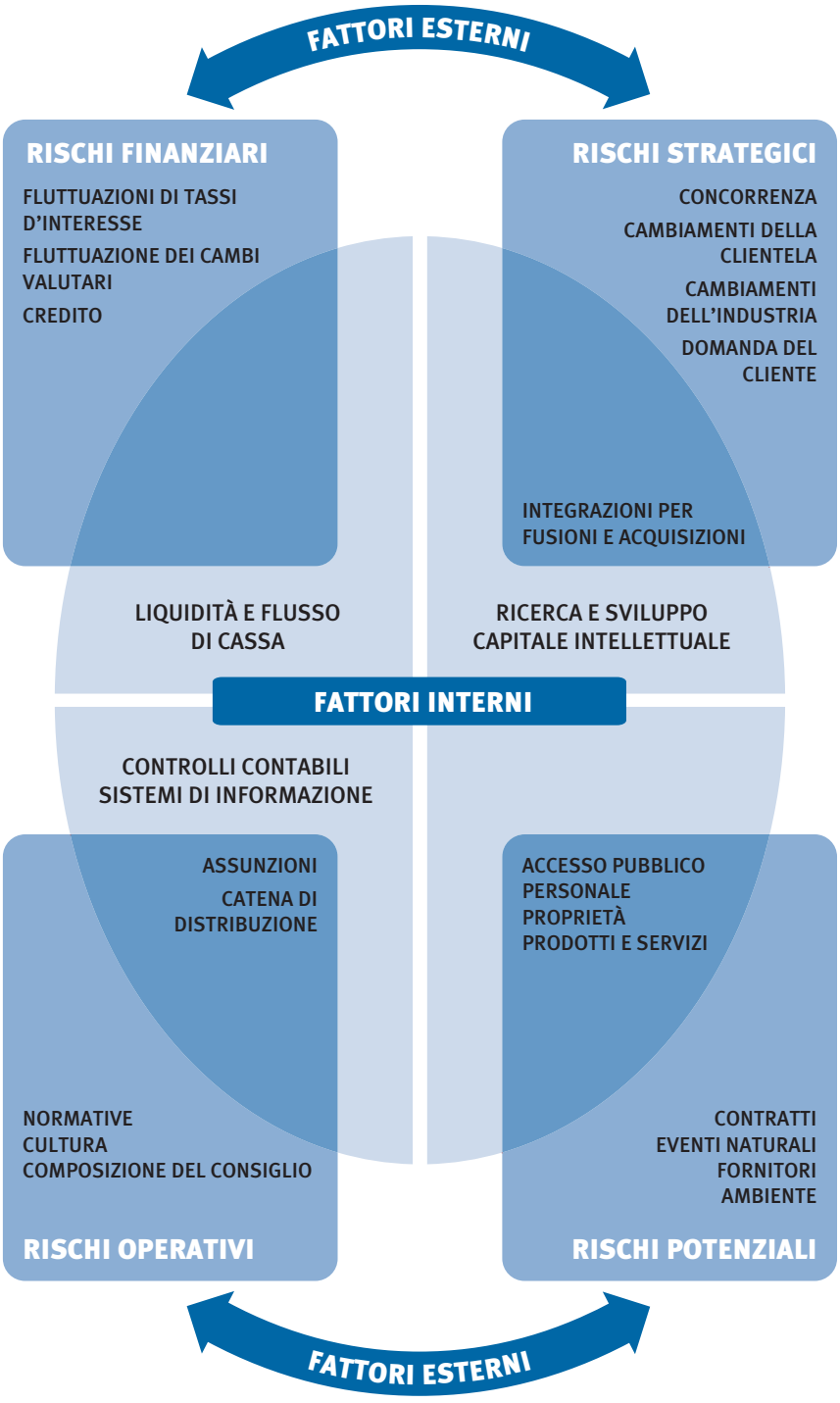
2.1 Fattori esterni e interni

I rischi che minacciano un'organizzazione e la sua gestione possono aver origine da fattori sia esterni sia interni a essa.

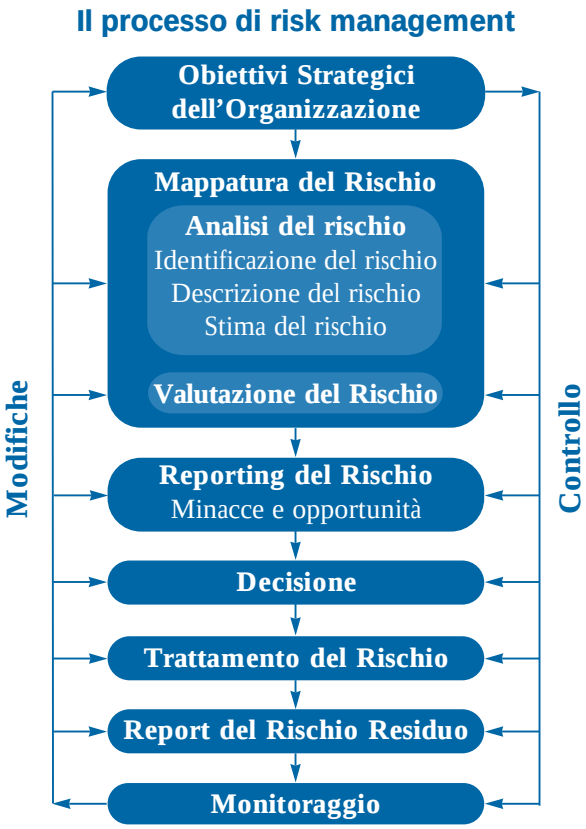
Il diagramma a tergo riassume esempi di rischi chiave presenti in queste aree e mostra come alcuni tipi rischi possano avere fattori di stimolo sia esterni sia interni e quindi occupare entrambe le aree.

È possibile distinguere ulteriormente le tipologie di rischio, per esempio strategico, finanziario, operativo, potenziale e via dicendo.

2.1 Esempio di fattori di stimolo dei rischi principali



2.2 Il processo di risk management



Il risk management protegge e dà valore all'organizzazione e ai suoi stakeholder, sostenendo gli obiettivi dell'organizzazione con:

- *la predisposizione di un quadro metodologico che consente uno svolgimento coerente e controllato di ogni futura attività*
- *il miglioramento del processo decisionale, della pianificazione e della creazione di priorità attraverso una comprensione esauriente e strutturata dell'attività commerciale, della volatilità e degli elementi positivi /negativi del progetto*
- *il contributo ad un utilizzo/allocazione più efficace del capitale e delle risorse all'interno dell'organizzazione*
- *la riduzione della volatilità nelle aree non essenziali dell'attività*
- *la protezione e il potenziamento del patrimonio e dell'immagine aziendale*
- *lo sviluppo e il sostegno delle persone e della base di conoscenza dell'organizzazione*
- *l'ottimizzazione dell'efficienza operativa*

3. Verifica del rischio

La verifica del rischio è definita dalla Guida ISO/IEC 73 come il processo generale di analisi e valutazione del rischio.
(Vedi appendice)

4. Analisi del rischio

4.1 Identificazione del rischio

L'identificazione del rischio si propone di misurare l'esposizione di un'organizzazione all'incertezza. Ciò richiede una conoscenza approfondita dell'organizzazione stessa, del mercato nel quale opera, dell'ambiente legale, sociale, politico e culturale di riferimento, nonché lo sviluppo di un'adeguata comprensione dei suoi obiettivi strategici e operativi, dei fattori critici di successo e delle minacce e opportunità ad essi connessi.

L'identificazione del rischio va affrontata con metodo per garantire che tutte le attività significative all'interno dell'organizzazione siano state individuate e che tutti i rischi derivanti da tali attività siano stati determinati. Vanno infine individuate e classificate tutte le volatilità che sono legate a queste attività.

Le attività e le decisioni aziendali possono essere classificate in vari modi, per esempio:

- *Strategiche – Riguardano gli obiettivi strategici di lungo periodo. Possono essere influenzate da aspetti quali la disponibilità di capitale, rischi derivanti da decisioni di enti governativi o rischi politici, modifiche di leggi e regolamenti, rischi di reputazione, mutamenti dell'ambiente naturale.*
- *Operative – Riguardano i problemi quotidiani che l'organizzazione affronta nello sforzo di raggiungere i suoi obiettivi strategici.*
- *Finanziarie – Riguardano l'efficace gestione e controllo delle finanze dell'organizzazione e gli effetti dei fattori esterni, per esempio la disponibilità di credito, i tassi di cambio, l'oscillazione dei tassi d'interesse e altri valori di mercato.*
- *Gestione della conoscenza – Riguardano l'efficacia nella gestione e nel controllo delle risorse della conoscenza, la loro produzione, protezione e diffusione. Tra i fattori esterni possono esserci l'uso o l'abuso non autorizzato della proprietà intellettuale, guasti alle linee di fornitura di energia, tecnologia concorrente. Tra i fattori interni vi sono malfunzionamenti del sistema o la perdita di personale avente un ruolo chiave.*
- *Conformità – Riguardano temi quali la salute e la sicurezza, l'ambiente, le denominazioni commerciali, la protezione del consumatore, la protezione dei dati, le procedure di assunzione e questioni normative.*
- *Malgrado l'identificazione del rischio possa essere eseguita da consulenti esterni, è probabile che un approccio interno con processi e strumenti coerenti e coordinati (vedi Appendice, pag. XX) sia più efficace. La "proprietà" interna del processo di risk management è essenziale.*

4.2 Descrizione del rischio

La descrizione del rischio si propone di mostrare i rischi identificati in forma strutturata, per esempio attraverso l'utilizzo di una tabella. La tabella di descrizione del rischio a tergo può essere usata per favorire la descrizione e la valutazione dei rischi. L'uso di una struttura progettata con cura è necessario per garantire un processo esauriente di identificazione, descrizione e valutazione del rischio. Lo studio delle conseguenze e della probabilità di ogni rischio indicato nella tabella dovrebbe permettere di dare la priorità ai rischi chiave che richiedono un'analisi più dettagliata. I rischi identificati nell'ambito delle attività commerciali e del processo decisionale possono essere classificati come strategici, progettuali/tattici, operativi. È importante inserire il risk management nella fase concettuale di un progetto nonché nel corso della vita del progetto stesso.

4.2.1 Tabella – Descrizione del rischio

1. Denominazione del rischio	
2. Estensione del rischio	Descrizione qualitativa degli eventi, loro dimensioni, tipologia, numero e fattori correlati
3. Natura del rischio	Per esempio: strategico, operativo, finanziario, cognitivo o di conformità
4. Stakeholder	Le parti in causa e le loro aspettative
5. Quantificazione del rischio	Rilevanza e probabilità
6. Tolleranza/propensione al rischio	Potenziale di perdita e di impatto finanziario del rischio Valore a rischio Probabilità e dimensioni di perdite/guadagni potenziali Obiettivo/i di controllo del rischio e livello atteso di performance
7. Trattamento e meccanismi di controllo del rischio	Strumenti primari attraverso i quali si gestisce attualmente il rischio Livelli di fiducia nei controlli esistenti Identificazione dei protocolli di controllo e revisione
8. Potenziali azioni di miglioramento	Raccomandazione per la riduzione del rischio
9. Sviluppi della strategia e della politica aziendale	Identificazione della funzione responsabile dello sviluppo della strategia

4.3 Stima del rischio

La stima del rischio può essere quantitativa, semi-quantitativa o qualitativa in termini di probabilità dell'evento e di possibili conseguenze.

Per esempio, le conseguenze in termini sia di minacce (rischi negativi) sia di opportunità (rischi positivi) possono essere alte, medie o basse (vedi Tabella 4.3.1). Il diverso grado di probabilità richiede definizioni distinte in quanto a minacce e opportunità (vedi Tabella 4.3.2 e 4.3.3).

Nella tabella a tergo vi sono alcuni esempi. Le organizzazioni potranno scegliere quale fra i diversi gradi di conseguenze e probabilità soddisfa maggiormente le esigenze specifiche.

Per esempio, molte organizzazioni ritengono che una valutazione alta, media o bassa delle conseguenze e delle probabilità sia sufficientemente adeguata alle loro caratteristiche e possa essere rappresentata con una matrice 3 x 3.

Altre organizzazioni giudicano più positivamente la valutazione delle conseguenze e delle probabilità ottenuta con una matrice di 5 x 5.

Tabella 4.3.1 Conseguenze – Minacce ed opportunità

Alte	Impatto finanziario sull'organizzazione probabilmente superiore a €x Notevole impatto sulla strategia o sulle attività operative dell'organizzazione Notevole preoccupazione degli stakeholder
Medie	Impatto finanziario sull'organizzazione probabilmente compreso fra €x e €y Discreto impatto sulla strategia o sulle attività operative dell'organizzazione Discreta preoccupazione degli stakeholder
Basse	Impatto finanziario sull'organizzazione probabilmente inferiore a €y Modesto impatto sulla strategia o sulle attività operative dell'organizzazione Modesta preoccupazione degli stakeholder

Tabella 4.3.2 Probabilità dell'evento – Minacce

Stima	Description	Indicators
Alta (Probabile)	Evento probabile ogni anno o in più del 25% dei casi.	Possibile verificarsi dell'evento diverse volte nel corso del periodo (per esempio, dieci anni). Si è verificato recentemente.
Media (Possibile)	Evento probabile nell'arco di dieci anni o in meno del 25% dei casi.	Possibile verificarsi dell'evento più di una volta nel corso del periodo (per esempio, dieci anni). Possibili difficoltà di controllo dovute a influenze esterne. Esistono dati sugli eventi passati?
Bassa(Remota)	Evento improbabile nell'arco di dieci anni o in meno del 2% dei casi.	Non si è verificato. È improbabile che si verifichi.

Tabella 4.3.3 Probabilità dell'evento – Opportunità

Stima	Descrizione	Indicatori
Alta (Probabile)	Probabile esito favorevole nell'arco di un anno o in più del 75% dei casi.	Chiara opportunità su cui si può fare affidamento con ragionevole certezza, da realizzare nel breve periodo sulla base degli attuali processi gestionali.
Media (Possibile)	Prospettive ragionevoli di esito favorevole nell'arco di un anno o con una probabilità compresa fra il 25 e il 75% dei casi.	Opportunità realizzabili ma che richiedono un'attenta gestione. Opportunità che possono presentarsi al di là di quanto programmato.
Bassa (Remota)	Alcune probabilità di esito favorevole nel medio termine o in meno del 25% dei casi.	Possibile opportunità che deve ancora essere esaminata a fondo dal management. Opportunità le cui probabilità di successo è bassa sulla base delle risorse gestionali attualmente impiegate.

4.4 Metodi e tecniche di analisi del rischio
L'analisi dei rischi può svolgersi attraverso una serie di tecniche. Ci sono tecniche specifiche per i rischi positivi o negativi e altre applicabili a entrambe le tipologie di rischio. ***(Vedi gli esempi in Appendice, pag. 14)***.

4.5 Profilo di rischio
Il processo di analisi del rischio genera un profilo di rischio che assegna un voto di significatività ad ogni rischio e fornisce uno strumento per dare la priorità alle attività di trattamento del rischio. Ogni rischio identificato viene così classificato al fine di determinarne l'importanza relativa.

Questo processo consente la mappatura del rischio nell'area produttiva interessata, definisce le procedure primarie di controllo esistenti e indica le aree nelle quali il volume degli investimenti per il controllo del rischio andrebbe aumentato, diminuito o riequilibrato.

La responsabilità aiuta a garantire l'accertamento della "proprietà" del rischio e lo stanziamento della risorsa di gestione adeguata.

5. Valutazione del rischio

Una volta completato il processo di analisi del rischio, è necessario confrontare i rischi stimati e i criteri di rischio fissati dall'organizzazione. Essi possono comprendere costi e benefici associati, requisiti legali, fattori socioeconomici ed ambientali, questioni riguardanti gli stakeholder, ecc. La valutazione del rischio serve quindi a definire la rilevanza dei rischi per l'organizzazione e l'accettazione o meno di ogni rischio specifico.

6. Trattamento del rischio

Il trattamento del rischio è il processo di selezione e di attuazione di misure che modificano il rischio. Questo processo ha come elemento principale il controllo e la mitigazione del rischio, ma si estende fino a comprendere, per esempio, l'eliminazione del rischio, il trasferimento del rischio, il finanziamento del rischio ecc.

NOTA: In questo standard, il finanziamento del rischio si riferisce ai meccanismi (per esempio, programmi assicurativi) di finanziamento delle conseguenze del rischio. In genere, il finanziamento del rischio non viene inteso come l'accantonamento di fondi destinati a coprire il costo di attuazione del trattamento del rischio (come definito dalla Guida ISO/IEC 73; vedi pagina 17).

Qualsiasi sistema di trattamento del rischio deve consentire quanto meno:

- *il funzionamento efficace ed efficiente dell'organizzazione*
- *efficaci controlli interni*
- *la conformità alle leggi e ai regolamenti.*

Il processo di analisi del rischio contribuisce al funzionamento efficace ed efficiente dell'organizzazione, identificando quei rischi che richiedono attenzione da parte dell'amministrazione. Essa dovrà dare la priorità alle azioni di controllo del rischio in base al beneficio potenziale derivante per l'organizzazione.

L'efficacia del controllo interno è legata al grado di eliminazione o di riduzione del rischio derivante dalle misure di controllo proposte.

La convenienza del controllo interno dipende dal rapporto fra il costo di implementazione del controllo e i benefici attesi di riduzione del rischio.

I controlli proposti devono essere valutati in termini di effetto economico potenziale in assenza di iniziative e in termini di costo della/e azione/i proposta/e e richiedono in ogni caso informazioni più dettagliate e ipotesi immediatamente disponibili.

Innanzitutto è necessario determinare il costo di attuazione. Il calcolo deve essere accurato poiché questo costo assume rapidamente la funzione di linea di riferimento rispetto alla quale si misura il costo efficacia. Poi bisogna calcolare la perdita attesa in caso di assenza di iniziative dopodiché, confrontando i risultati, il management può decidere se attuare o meno le misure di controllo del rischio.

La conformità alle leggi e ai regolamenti non è facoltativa. Un'organizzazione deve comprendere le norme applicabili e attuare un sistema di controlli per conformarsi alle disposizioni di legge. Solo occasionalmente vi può essere una qualche flessibilità, quando il costo di riduzione di un rischio è del tutto sproporzionato rispetto al rischio stesso.
Un metodo di protezione finanziaria dall'impatto del rischio consiste nel suo finanziamento, per esempio attraverso l'assicurazione. Bisogna però riconoscere che alcuni danni o parti di essi non sono assicurabili, ad esempio i costi non assicurati associati alla salute, alla sicurezza e agli incidenti ambientali sul luogo di lavoro, che possono includere danni morali ai dipendenti e danni alla reputazione dell'organizzazione.

7. Reporting e comunicazione del rischio

7.1 Reporting interno

Livelli differenti all'interno di un'organizzazione necessitano di informazioni differenti sul processo di risk management.

Il consiglio di amministrazione deve:

- *conoscere i rischi più significativi affrontati dall'organizzazione*
- *conoscere i possibili effetti sul valore degli azionisti dovuti agli scostamenti rispetto alla gamma attesa di performance*
- *garantire livelli adeguati di consapevolezza in ogni parte dell'organizzazione*
- *sapere in che modo l'organizzazione intende affrontare una crisi*
- *essere consapevole dell'importanza della fiducia degli stakeholder nei confronti dell'organizzazione*
- *sapere come gestire le comunicazioni con la comunità degli investitori laddove necessario*
- *esser certo che il processo di risk management funzioni efficacemente*
- *diffondere una chiara politica di risk management che specifichi le linee direttive e le responsabilità di risk management*

Le Unità operative devono:

- *be aware of risks which fall into their area of responsibility, the possible impacts these may have on other areas and the consequences other areas may have on them*
- *have performance indicators which allow them to monitor the key business and financial activities, progress towards objectives and identify developments which require intervention (e.g. forecasts and budgets)*
- *have systems which communicate variances in budgets and forecasts at appropriate frequency to allow action to be taken*
- *report systematically and promptly to senior management any perceived new risks or failures of existing control measures*

Gli individui devono:

- *comprendere le loro responsabilità nei singoli rischi*
- *comprendere come consentire un costante miglioramento dei risultati di risk management*
- *comprendere che il risk management e la consapevolezza del rischio sono una parte fondamentale della cultura di un'organizzazione*
- *riferire sistematicamente e puntualmente ai massimi dirigenti qualsiasi sospetto di nuovo rischio o malfunzionamento nelle misure di controllo esistenti.*

7.2 Reporting esterno

Una società deve informare regolarmente i propri stakeholder, illustrando le sue politiche di risk management e l'efficacia nel raggiungimento degli obiettivi.

Gli stakeholder prestano attenzione sempre maggiore affinché le organizzazioni diano prova di una gestione efficace delle loro attività non finanziarie in aree quali, per esempio, le relazioni comunitarie, i diritti dell'uomo, le procedure di assunzione, la salute e la sicurezza e l'ambiente.

Una buona corporate governance richiede che le società adottino un approccio metodico al risk management che:

- *protegga gli interessi dei loro stakeholder*
- *garantisca che il Consiglio di amministrazione assolva i suoi doveri, definendo una strategia, sviluppando valore e monitorando la performance dell'organizzazione*
- *garantisca l'esistenza dei controlli di gestione e il loro funzionamento adeguato.*

Le disposizioni per il reporting ufficiale del risk management vanno indicate chiaramente e messe a disposizione degli stakeholder.

Il reporting ufficiale deve indicare:

- *i metodi di controllo – in particolare le responsabilità della direzione aziendale nel risk management*
- *i processi utilizzati per identificare i rischi e il modo in cui vengono affrontati dai sistemi di risk management*
- *i sistemi primari di controllo esistenti per la gestione di rischi significativi*
- *i sistemi di controllo e di revisione esistenti*

Ogni carenza rilevata dal sistema, o all'interno del sistema stesso, va riportata insieme alle azioni intraprese per affrontarla.

8. La struttura e l'amministrazione del risk management

8.1 La politica di risk management

La politica di gestione del rischio di un'organizzazione deve definire il suo approccio e la sua propensione al rischio, nonché indicare le responsabilità di risk management a ogni livello dell'organizzazione.

La sua politica ufficiale deve inoltre attenersi alle eventuali norme di legge, per esempio su salute e sicurezza nell'ambiente di lavoro.

Il processo di risk management fa parte di un insieme integrato di strumenti e tecniche da utilizzare nelle sue varie fasi. Per essere efficace, il processo di risk management richiede:

- *l'impegno da parte del direttore generale e dei dirigenti dell'organizzazione*
- *l'assegnazione di responsabilità all'interno dell'organizzazione*
- *la distribuzione di risorse adeguate per la formazione e lo sviluppo di una maggior consapevolezza al rischio da parte di tutti i compartecipanti.*

8.2 Ruolo del Consiglio

Il Consiglio ha il compito di stabilire gli obiettivi strategici dell'organizzazione e di creare l'ambiente e le strutture che permettano il corretto funzionamento della gestione del rischio.

Ciò può avvenire attraverso un gruppo esecutivo, un comitato non esecutivo, un collegio di revisori o altra funzione analoga, che sia conforme alle modalità operative dell'organizzazione e possa svolgere il ruolo di "garante" del risk management.

Il Consiglio deve considerare come minimo, nella valutazione del suo sistema di controllo interno:

- *la natura e l'estensione dei rischi negativi accettabili per la società nell'ambito della sua specifica attività*
- *le probabilità che si verifichino tali rischi*
- *le modalità di gestione dei rischi non accettabili*
- *la capacità della società di minimizzare le probabilità e l'impatto sull'attività*

- *costi e benefici del rischio e dell'attività di controllo intrapresa*
- *l'efficacia del processo di gestione del rischio*
- *le implicazioni sul rischio delle decisioni del consiglio.*

8.3 Ruolo delle Unità operative
Comprende i punti seguenti:

- *le Unità operative hanno una responsabilità primaria nella gestione quotidiana del rischio*
- *i responsabili delle Unità hanno il compito di promuovere la consapevolezza al rischio nell'ambito del suo esercizio; essi devono inserire obiettivi di risk management nell'attività dell'Unità*
- *il risk management deve essere argomento regolarmente discusso nelle riunioni di direzione per consentire l'esame delle esposizioni e modificare le priorità alla luce di un'efficace analisi del rischio*
- *i responsabili delle Unità devono accertarsi che il risk management venga incluso tanto nella fase concettuale dei progetti quanto in ogni fase successiva dei progetti stessi.*

8.4 Ruolo della funzione di risk management
A seconda delle dimensioni dell'organizzazione, la funzione di risk management può essere svolta da un unico responsabile, da un risk manager part-time o da un intero reparto dedicato.

L'esercizio della funzione di risk management deve prevedere:

- *la determinazione di una politica e di una strategia di risk management*
- *un responsabile generale di risk management a livello strategico e operativo*
- *lo sviluppo di una cultura consapevole del rischio nell'ambito dell'organizzazione che preveda un'adeguata formazione*
- *la creazione di una politica e di strutture interne di rischio nelle imprese*
- *la progettazione e la revisione di processi di risk management*
- *il coordinamento delle diverse attività funzionali di consulenza sul risk management all'interno dell'organizzazione*
- *lo sviluppo di processi di risposta al rischio, quali programmi d'emergenza e di continuità aziendale*
- *la preparazione di report sul rischio per il consiglio e gli stakeholder*

8.5 Ruolo dell'audit interno
È probabile che il ruolo di internal audit cambi a seconda dell'organizzazione.

In pratica, questo ruolo può comprendere una parte o la totalità dei seguenti punti:

- ***concentrare il lavoro di audit interno sui rischi significativi, così come identificati dal management, e verificare i processi di risk management all'interno di un'organizzazione.***
- ***fornire garanzie sulla gestione del rischio***
- ***fornire sostegno e partecipazione attiva nel processo di risk management***
- ***facilitare l'identificazione/la verifica del rischio e formare lo staff di linea al risk management e al controllo interno***
- ***coordinare i reporting sul rischio al consiglio, al collegio di revisori, ecc.***

Nella scelta del ruolo più adeguato di una particolare organizzazione, l'audit interno deve garantire il rispetto dei requisiti professionali di indipendenza e oggettività.

8.6 Risorse e attuazione
Le risorse necessarie ad attuare la politica di risk management dell'organizzazione vanno stabilite chiaramente a ogni livello decisionale e all'interno di ogni unità aziendale.

Oltre a ricoprire altre eventuali funzioni operative, il personale addetto alla gestione del rischio deve conoscere con chiarezza il suo ruolo di coordinamento della politica e della strategia di risk management. La stessa precisione è necessaria anche per coloro che si occupano dell'audit e della revisione dei controlli interni, nonché di agevolare il processo di risk management.

Il risk management va integrato nell'organizzazione attraverso le attività strategiche e di bilancio. Ciò deve essere espresso chiaramente nell'ambito della formazione del personale e in ogni altra attività di preparazione e di sviluppo, nonché all'interno dei processi operativi, per esempio nei progetti di sviluppo di prodotti e servizi.

9. Controllo e revisione del processo di risk management

Un'efficace gestione del rischio richiede una struttura di reporting e revisione che assicuri l'efficace identificazione e valutazione dei rischi e l'esistenza di controlli e di risposte adeguate.

È necessario eseguire controlli regolari di conformità alla politica aziendale e agli standard, nonché rivedere costantemente i risultati degli standard per identificare opportunità di miglioramento. Bisogna ricordare che le organizzazioni sono dinamiche e operano in ambienti dinamici. È necessario identificare i cambiamenti interni all'organizzazione e al suo ambiente ed effettuare le opportune modifiche ai sistemi.

Il processo di controllo deve garantire l'esistenza di un monitoraggio adeguato delle attività dell'organizzazione, nonché la comprensione e il rispetto delle procedure. È necessario identificare i cambiamenti interni all'organizzazione e al suo ambiente ed effettuare le opportune modifiche ai sistemi.

Qualsiasi processo di controllo e di revisione deve inoltre stabilire se:

- *le misure adottate hanno prodotto i risultati sperati*
- *le procedure adottate e le informazioni raccolte per intraprendere la verifica erano adeguate*
- *maggiori conoscenze avrebbero contribuito a prendere decisioni migliori e a trarre insegnamenti utili per future verifiche e gestioni dei rischi.*

10. Appendice

Tecniche di identificazione del rischio - esempi

- *Brainstorming*
- *Questionari*
- *Studi di amministrazione aziendale che analizzano ogni processo aziendale e descrivono sia i processi interni sia i fattori esterni che li possono influenzare*
- *Analisi comparative di settore (benchmarking)*
- *Analisi di scenario*
- *Workshop di verifica del rischio*
- *Indagini su incidenti avvenuti*
- *Attività di auditing e ispezioni*
- *HAZOP (studi di Hazard & Operability)*

Metodi e tecniche di analisi del rischio – esempi

Rischio positivo

- *Indagini di mercato*
- *Prospezioni*
- *Test marketing*
- *Ricerca e sviluppo*
- *Analisi di impatto commerciale*

Entrambi

- *Modelli di interdipendenza*
- *Analisi SWOT (forze, debolezze, opportunità, minacce)*
- *Analisi dell'albero degli eventi*
- *Pianificazione della continuità dell'attività*
- *Analisi BPEST (commerciale, politica, economica, sociale, tecnologica)*
- *Modellizzazione di opzioni reali*
- *Scelte decisionali in condizioni di rischio e incertezza*
- *Inferenza statistica*
- *Misurazione delle medie e della varianza*
- *Analisi PESTLE (politica, economica, sociale, tecnica, legale, ambientale)*

Rischi negativi

- *Analisi delle minacce*
- *Analisi dell'albero dei guasti*
- *Analisi FMEA (analisi dei modi e degli effetti dei guasti)*

FOR LOCAL INFORMATION, PLEASE CONTACT THE OFFICE OF THE NATIONAL ASSOCIATION

AGERS - Asociacion Española de Gerencia de Riesgos y Seguros
Príncipe de Vergara, 86 - 1ª Esc., 2º Izda.– 28006 Madrid - SPAIN
Tel: + 34 91 562 84 25 – Fax: + 34 91 590 07 80 – Email: gerencia@agers.es – www.agers.es

AIRMIC - The association of Insurance and Risk Managers
Lloyd's Avenue, 6 – London EC3N3AX - UK
Tel: + 44 207 480 76 10 – Fax: + 44 207 702 37 52 – Email: enquiries@airmic.co.uk – www.airmic.com

AMRAE - Association pour le Management des Risques et des Assurances de l'Entreprise
Avenue Franklin Roosevelt, 9-11 – 75008 Paris - FRANCE
Tel: + 33 1 42 89 33 16 – Fax: + 33 1 42 89 33 14 – Email: amrae@amrae.fr – www.amrae.fr

ANRA - Associazione Nazionale dei Risk Manager e Responsabili Assicurazioni Aziendali
Via del Gonfalone 3, I-20123 Milano - ITALY
Tel: + 39 02 58 10 33 00 – Fax: + 39 02 58 10 32 33 – Email: anra@betam.it – www.anra.it

APOGERIS - Associação Portuguesa de Gestão de Riscos e Seguros
Avenida da Boavista, 1245, 3a Esq. – 4100-130 Porto – PORTUGAL
Tel: + 351 22 608 24 62 – Fax: + 351 22 608 24 73 – E-mail: anfernandes@sonae.pt – www.apogeris.pt

ASPAR CR - Association of Insurance and Risk Management of the Czech Republic o.s.
Nad Ohradou 7 – 13000 Praha 3 – Tel: + 420 602 384 256 – Email: asparcr@volny.cz

BELRIM - Belgian Risk Management Association
Rue Gatti de Gamond, 254 – 1180 Bruxelles - BELGIUM
Tel: + 32 2 389 23 95 – Fax: + 32 2 389 22 72 – Email: info@belrim.com – www.belrim.com

BfV - Bundesverband firmenverbundener Versicherungsvermittler und -Gesellschaften e.V.
c/o Mr Hans-Otto GEIGER – Postfach 1916 – D-67209 Frankenthal – GERMANY
Tel: + 49 6233 86 2507 - Fax: + 49 6233 86 2507 - Email: hans-otto.geiger@ksb.com – www.bfv-fvv.de

BRIMA - Bulgarian Risk Management Association
101, Tzarigradsko chausse, floor 4 – Sofia 1113 – BULGARIA
Tel: + 359 878 100292 – Fax: + 359 2 971 0702 – Email: office@brima.biz – www.brima.biz

DARIM - DI's Risk Management Forening
DK-1787 Copenhagen – DENMARK
Tel: + 45 33 77 33 77 – Fax: + 45 33 77 33 00 – Email: darim@di.dk – www.di.dk

DVS - Deutscher Versicherungs-Schutzverband e.V.
Breite Strasse 98 - D 53111 Bonn - GERMANY
Tel: + 49 228 98 22 30 - Fax: + 49 228 63 16 51- Email: dvs@dvs-schutzverband.de – www.dvs-schutzverband.de

FINNRIMA - Finnish Risk Management Association
Talvikkitie 40 A 33, 01300 Vantaa – FINLAND
Tel: + 358 9 5607 5361 – Fax: + 358 9 5607 5365 – Email: srhy@hennax.fi – www.srhy.fi

NARIM - Nederlandse Associatie van Risk en Insurance Managers
P.O. Box 65707 - 2506 EA Den Haag – THE NETHERLANDS
Tel: + 31 70 345 7426 – Fax: + 31 70 427 3263 – Email: ielsdewild@imfo.nl – www.narim.com

POLRISK - Polish Risk Management Association
ul. Rzymowskiego 30 lok. 424 - 02-697 Warszawa - POLAND
Tel: + 48 22 331 8121 – Fax: + 48 22 331 81 22 – Email: info@polrisk.pl – www.polrisk.pl

RUSRISK - Russian Risk Management Society
Address Expert Institute, Staraya Ploshchad 10/4, Moscow, 103070 – RUSSIA
Tel: + 7 495 231 53 56 - Fax: + 7 495 231 53 56 - Email: info@rrms.ru – www.rrms.ru

SIRM - Swiss Association of Insurance and Risk Managers
Gutenbergstrasse 1, Postfach 5464, CH-3001 Bern - SWITZERLAND
Tel: + 41 31 388 87 89 – Fax: + 41 31 388 87 88 – Email: info@sirm.ch – www.sirm.ch

SWERMA - Swedish Risk Management Association
Gränsvägen 15 - SE-135 47 Tyresö - SWEDEN
Tel: + 468 742 13 07 - Fax: + 468 798 83 11- E-mail: info@swerma.se – www.swerma.se

ALARM - The National Forum for Risk Management in the Public Sector
Queens Drive, Exmouth - Devon, EX8 2AY
Tel: + 44 1395 223399 - Fax: + 44 1395 223304 - Email: admin@alarm.uk.com - www.alarm-uk.com

IRM - The Institute of Risk Management
6 Lloyd's Avenue - London EC3N 3AX
Tel: + 44 20 7709 9808 - Facsimile + 44 20 7709 0716 - Email: enquiries@theirm.org - www.theirm.org

FERMA – Avenue Louis Gribaumont, 1 / B.4 – 1150 BRUSSELS - BELGIUM
TEL: +32 2 761 94 32 – FAX: +32 2 771 87 20 – EMAIL: info@ferma.eu – WEBSITE: www.ferma.eu