RISK MANAGEMENT

Generalità e metodologia operativa

Raffaella Rospetti - Alessandro Orlandini

Rev. 00 - 06 2020

SOMMARIO

PREMESSA

Nel corso degli anni hanno assunto sempre maggiore attenzione corpi di regole a base del governo dell'impresa che ne indirizzano strategie ed azioni anche a tutela degli interessi dei vari portatori di interesse: la "***Corporate Governance".***

In tale ambito, più di recente, ha assunto rilievo crescente il tema della ***gestione dei rischi.***

A partire dalla metà degli anni 90 i contenuti di ***Risk Management*** e ***Corporate Governance*** si sono intrecciati sempre di più: attualmente avere una "buona" gestione dell'azienda è divenuto sinonimo di essere dotati di un adeguato e formalizzato sistema di gestione dei rischi.

Nel contempo, le tecniche di *risk analysis*, tradizionalmente limitate all'individuazione dei rischi assicurabili - e quindi da trasferire contrattualmente - sono state sostituite da processi più pervasivi con responsabilità diffuse a vari livelli dell'organizzazione e non perimetrati solo su alcune funzioni.

Nei settori soggetti a vigilanza (Banche, SIM, Assicurazioni) il quadro di riferimento per la gestione dei rischi è ampiamente regolato da normative europee, leggi nazionali e delibere.

Per le società quotate, la tendenza è confermata anche dalla recente edizione del Codice di Autodisciplina emesso da Borsa Italiana Spa, normativa facoltativa per le società con azioni quotate nei mercati regolamentati ma, in ogni caso, valido riferimento di Governance per tutte le aziende. Orbene, il Codice pone il processo di Gestione dei Rischi come assolutamente fondamentale per una corretta Governance, attribuendo la responsabilità dello stesso direttamente al Consiglio di Amministrazione, quindi ai massimi livelli apicali.

IL RISK MANAGEMENT: LA SITUAZIONE ITALIANA

In Italia, funzioni di risk management sono presenti in aziende operanti nei settori regolamentati dove questa è obbligatoria oppure nelle realtà di grandi o grandissime dimensioni.

Nelle PMI il tema del risk management non è ancora adeguatamente diffuso, pur essendo presenti comunque processi di gestione del rischio laddove previsto da normative cogenti o volontarie.

Lo si nota, in particolare, nell'imposizione fatta dal legislatore in alcuni settori particolarmente sentiti:

- nell'ambito della **sicurezza sul lavoro** la normativa vigente (D.Lgs. 81/2008) prevede la redazione di un Documento di Valutazione dei Rischi, da redigere secondo tecniche tipiche di *risk management*;

- nell'ambito della disciplina sulla **responsabilità amministrativa delle imprese da reato (D. Lgs. 231/2001)**, la norma prevede la predisposizione di modelli di organizzazione e gestione sulla base di preliminari attività di individuazione delle "aree a rischio"; attività che vanno effettuate secondo un tipico approccio da *risk management;*

- la recente normativa europea sul **trattamento dei dati personali "Privacy"** (Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016) è pervasa da aspetti di gestione con approccio di risk analysis: ad esempio prevede l'adozione di approcci e politiche che tengano conto costantemente del rischio che un determinato trattamento di dati personali può comportare. O ancora, nella valutazione dell'impatto di determinate potenziali conseguenze nella prospettiva di definire adeguate misure di sicurezza nel trattamento dei dati (anche in questo caso con il ricorso a tecniche tipiche di *risk management);*

- 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

- L'art. **2428 del Codice Civile** stabilisce che il bilancio debba "essere corredato da una relazione degli amministratori contenente [...] una descrizione dei **principali rischi** e incertezze cui la società è esposta";

- Il **D.Lgs. 39/2010,** intervenuto sul Codice Civile, prevede che il collegio sindacale vigili sull'efficacia dei sistemi di controllo interno e di **gestione del rischio.**

Soprattutto nelle realtà di media grandezza, fortemente orientate al business, il risultato di questa frammentazione è spesso nella non omogeneità delle valutazioni e nella dispersione dei risultati delle analisi nei rivoli dell'organizzazione.

La responsabilità risulta normalmente concentrata nella direzione aziendale, che vive le varie *risk analysis* di settore come meri obblighi normativi, distribuendo la competenza "per materia" con pochi punti di contatto, perdendo di vista da un lato la possibilità di sinergie fra i vari processi di valutazione e, di conseguenza, la possibilità di razionalizzazione di costi; dall'altro l'opportunità di utilizzare il risk management come preziosa risorsa e opportunità di gestione orientata al business.

Ad esempio, di regola le analisi dei rischi in materia di sicurezza sul lavoro, quando non presente un'articolazione specifica, sono concentrate presso le funzioni tecnico-operative; quelle in materia di privacy normalmente presso le risorse umane o l'IT, quelle in materia di responsabilità ammnistrativa presso la funzione legale come d'altronde quelle per l'individuazione dei rischi assicurabili; quelle inerenti il bilancio d'esercizio nelle funzioni amministrative.

IL RISK MANAGEMENT NELL'AMBITO DEI SISTEMI DI GESTIONE

L'ISO ha pubblicato nel 2012 un documento prescrittivo (denominato Annex SL) che pone la gestione del rischio al centro di qualsiasi Sistema di Gestione. Ogni norma inerente i requisiti di un sistema di gestione dovrà adeguarsi alla struttura dello standard costituita da 10 macro requisiti, comuni a tutte le normative gestionali certificabili da parte di un ente terzo indipendente.

Il requisito n. 4 impone la determinazione dei fattori di rischio che possono impedire ai suoi processi di business di essere efficaci, l'analisi cause-effetto, una pianificazione di trattamento del rischio al manifestarsi degli effetti, la verifica di efficacia, sia del sistema di gestione in sé, sia del piano di gestione del rischio che deriva dal campo di applicazione del Sistema di Gestione.

A seguito di di tale prescrizione, le nuove norme ISO 9001:2015 (Sistemi di Gestione per la Qualità), ISO 14001:2015 (Sistemi di Gestione Ambientale), ISO 45001: 2016 (Sistemi di gestione Sicurezza sul Lavoro) hanno tutte reso esplicito e hanno incorporato il **concetto di rischio e l'esigenza di una sua gestione** in un approccio di sistema.

Ci si attende, ovviamente, che via via tutti i sistemi certificabili prevedano sempre più una centralità del Risk Management.

QUALI SOLUZIONI?

Ovviamente la costituzione di una funzione specifica di risk management in alcune realtà medie o medio-piccole prevedrebbe un costo probabilmente non sostenibile.

Una soluzione adeguata potrebbe essere quella *dell'outsourcing* del completo processo di risk management che consenta di soddisfare tutte le esigenze:

- di conformità alle normative;
- di individuazione dei rischi da trasferire sul mer cato assicurativo.

Ciò consentirebbe da un lato di evitare l'impegno economico di una funzione specificamente dedicata, dall'altro di definire comunque una "cabina di regia" unica dei rischi globali che, con approccio professionale, consenta una corretta gestione dell'individuazione, della valutazione e del trattamento dei rischi con approcci coerenti e metodologia unica.

I RIFERIMENTI

L'approccio che viene proposto tiene in considerazione i due principali riferimenti internazionali in tema di risk management:

- l'E.R.M. - Enterprise Risk Management (o CoSO II) ;
- la norma UNI ISO 31.000 "Risk Management".

L'Enterprise Risk Management è un modello definito dalla *Treadway Commission* (USA) nel 2004 e deriva dall'evoluzione di Sistemi di Controllo Interno definiti a partire dalla fine degli anni '80 per contrastare i fenomeni di frode finanziaria che hanno contraddistinto quel periodo., Il framework, che enfatizza la fase di identificazione e gestione dei rischi visti non solo in senso negativo ma anche come eventi incerti ma potenzialmente forieri di opportunità, considera, la globalità dei rischi e specificamente quelli afferenti alle business unit operative e commerciali

L**a norma ISO 31000 del 2009 "Risk Management – Principles and guidelines"** è stata redatta dall'ISO (International Organization for Standardization). Nel 2010 è stata pubblicata la traduzione in italiano della norma 31000:2010 "Gestione del Rischio".

Scopo della norma tecnica è quello di rendere disponibili a tutti i principi e le linee guida generali sulla gestione del rischio e di renderla adattabile a qualsiasi tipo di organizzazione (impresa pubblica o privata, o sociale, associazione gruppo o individuo) e lungo tutto il periodo di operatività dell'organizzazione stessa.

Nella ISO 31000 viene evidenziata la necessità di sviluppo, attuazione e miglioramento continuo di un modello di riferimento di Risk Management, il cui scopo consiste nell'integrazione del processo di gestione del rischio nella governance complessiva dell'organizzazione, nella strategia e nella pianificazione, nei processi di reporting, nelle politiche, nei valori e nella cultura, al fine di assicurare un'efficace gestione del rischio coerente in tutta l'organizzazione.

I vantaggi riconosciuti ad un'implementazione di un sistema di gestione dei rischi conforme alla norma sono i seguenti:

- incremento delle possibilità di raggiungere gli obiettivi;
- la promozione di una gestione "proattiva" volta a favorire le opportunità, a migliorare la prevenzione delle minacce e la gestione degli incidenti e alla minimizzazione dei danni;
- il miglioramento dell'identificazione delle minacce ma anche delle opportunità;
- il miglioramento del reporting, della governance, dell'efficacia ed efficienza operativa e dei controlli;
- il censimento e la costruzione di una base affidabile dei rischi/opportunità, fondamentali per la pianificazione e il processo decisionale;
- l'incremento della fiducia da parte degli stakeholder.

La norma è distinta in

- **Principi;**
- **Framework;**
- **Processo.**

I Principi definiscono i valori e la "filosofia" del processo, supportano una chiara e coordinata visione del rischio all'interno di tutta l'organizzazione, collegano la struttura di riferimento e la pratica di risk management agli obiettivi strategici e aiutano ad allineare il risk management alle attività dell'azienda.

La struttura (**Framework**) suggerita dalla norma dovrà essere adattabile alle caratteristiche specifiche dell'organizzazione anche al fine di rendere la gestione dei rischi pienamente integrata all'interno della stessa.

Gli steps previsti sono i seguenti:

- DEFINIZIONE DEL "MANDATO" E DELL'IMPEGNO: LA POLITICA DI GESTIONE DEL RISCHIO

L'implementazione di un adeguato processo di gestione del rischio richiede un impegno forte e formalizzato da parte della Direzione aziendale. La definizione di una adeguata "politica" di gestione del rischio è un momento fondamentale; andrà poi adeguatamente diffusa e conosciuta ad ogni livello.

- PROGETTAZIONE DELLA STRUTTURA DI RIFERIMENTO PER LA GESTIONE DEL RISCHIO

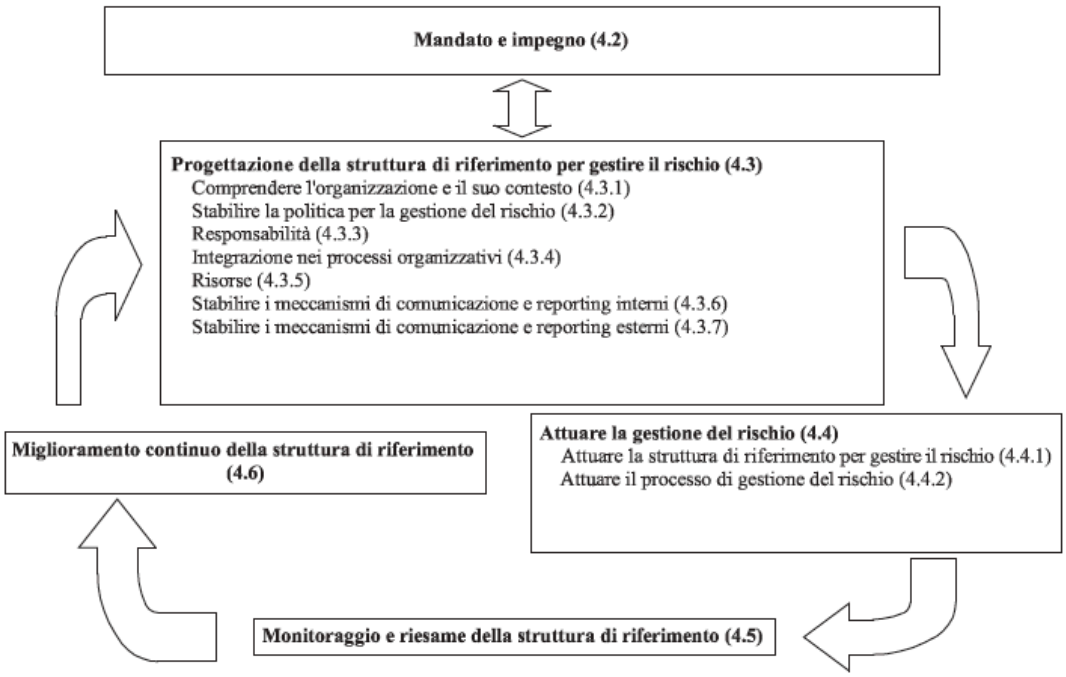
Sulla base della politica di gestione del rischio formalizzata, dovranno essere definiti:

- le varie responsabilità in seno all'organizzazione,
- l'integrazione del processo di risk management nell'ambito dei processi organizzativi aziendali,
- la quantificazione dei fabbisogni in termini di risorse umane, tecniche e finanziarie necessarie per la corretta gestione dei rischi e le correlate attività formative;
- i meccanismi di comunicazione e reporting sia interni che esterni;

- ATTUAZIONE DELLA GESTIONE DEL RISCHIO

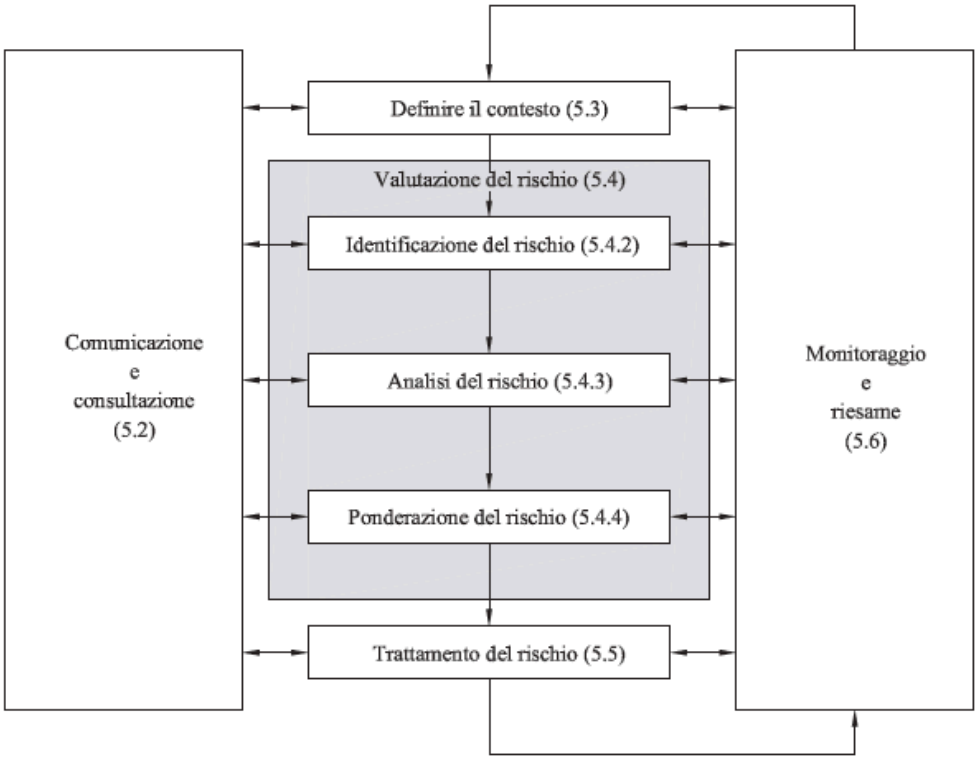
Sulla base del progetto approvato, si darà ausilio alla Direzione nell'attuare sia la struttura di riferimento nella gestione del rischio che il processo vero e proprio di risk management con la definizione di un "piano di gestione del rischio".

- MONITORAGGIO E RIESAME DELLA STRUTTURA DI RIFERIMENTO


Mandato e impegno (4.2)
Progettazione della struttura di riferimento per gestire il rischio (4.3)
Comprendere l'organizzazione e il suo contesto (4.3.1)
Stabilire la politica per la gestione del rischio (4.3.2)
Responsabilità (4.3.3)
Integrazione nei processi organizzativi (4.3.4)
Risorse (4.3.5)
Stabilire i meccanismi di comunicazione e reporting interni (4.3.6)
Stabilire i meccanismi di comunicazione e reporting esterni (4.3.7)
Attuare la gestione del rischio (4.4)
Attuare la struttura di riferimento per gestire il rischio (4.4.1)
Attuare il processo di gestione del rischio (4.4.2)
Monitoraggio e riesame della struttura di riferimento (4.5)
Miglioramento continuo della struttura di riferimento (4.6)

IL PROCESSO DI GESTIONE DEL RISCHIO

La norma UNI ISO 31.000, prevede che per l'implementazione di un corretto processo di gestione del rischio debba essere osservato il seguente schema:



Particolarmente significativa è la parte prettamente valutativa del rischio, che si compone dei seguenti fondamentali steps:

- L'IDENTIFICAZIONE DEI RISCHI
- L'ANALISI DEI RISCHI IDENTIFICATI
- LA LORO PONDERAZIONE

La fase di **IDENTIFICAZIONE DEI RISCHI** è di fondamentale importanza. In stretta collaborazione con la Direzione e con i vari titolari di processo, si procede ad una attenta elencazione dei rischi, suddivisi in categorie omogenee.

Una suddivisione tradizionale prevede le seguenti macro-categorie:

- **Rischi "esterni"** (ad es.: concorrenza, esigenze dei consumatori, andamento macroeconomico, inadempienze dei fornitori, politica, regolamenti/normative, calamità naturali);
- **Rischi "interni"** a loro volta suddivisibili in :

  - **Rischi strategici** (ad es.: reputazione, partnership/alleanze, pricing, capacità di produzione)
  - **Rischi operativi** (connessi tipicamente ai processi operativi aziendali, sia delle gestione caratteristica che dei processi "corporate" di supporto. Ad es. per quanto riguarda il processo "Risorse Umane" possono prevedersi i rischi di inserimenti di nuove professionalità non adeguate, livelli retributivi non coerenti con la professionalità acquisita, errori nella definizione e contabilizzazione paghe e contributi, ecc. Per il processo Approvvigionamenti" possono prevedersi i rischi di non adeguata pianificazione acquisti, acquisizione di risorse a prezzi non adeguati, non corretta gestione delle scorte di merce deperibili, fornitori inadempienti ecc.) Per il processo di "conformità normativa" (compliance) possono prevedersi i rischi di mancata conformità nel trattamento dei dati personali (privacy), incidenti sul lavoro per non ottemperanza ai dettami delle norma sulla *safety* sui luoghi di lavoro, non conformità alla normativa antiriciclaggio, ecc..

  - **Rischi finanziari**, ad esempio i rischi di cambio, di liquidità, tassi di interesse ecc.

Ovviamente questa è una mera elencazione accademica.

La corretta individuazione dei rischi va contestualizzata sulla specifica realtà aziendale oggetto analisi. Potranno così aggiungersi rischi specifiuci di settore (industriale, commerciale, di servizi, agricola) o di collocazione geografica.

In sintesi, la fase di individuazione dei rischi andrà "cucita addosso" alla singola realtà aziendale.

L'ANALISI DEL RISCHIO è la fase a maggior valore aggiunto, dove è di fondamentale importanza una specifica conoscenza del mondo aziendale e le dinamiche relative.

La tradizionale metodologia prevede i seguenti momenti :

- la valutazione del rischio "inerente" (o rischio "lordo") ;
- la valutazione del relativo sistema di controllo;
- la valutazione del rischio residuo (o rischio "netto").

La valutazione tanto del rischio inerente che di quello residuo avviene sulla base di una metrica "severità di impatto – frequenza di accadimento" su una scala 1-5.

Il rischio "inerente" è un concetto di rischio puramente teorico che incomberebbe sull'organizzazione se la stessa non fosse dotata di alcun sistema di controllo.

Quindi si procede all'autovalutazione del sistema di controllo in grado di mitigare quello specifico rischio.

La differenza di valutazione fra il rischio inerente e il relativo sistema di controllo darà come risultato il rischio "residuo" (o rischio "netto").

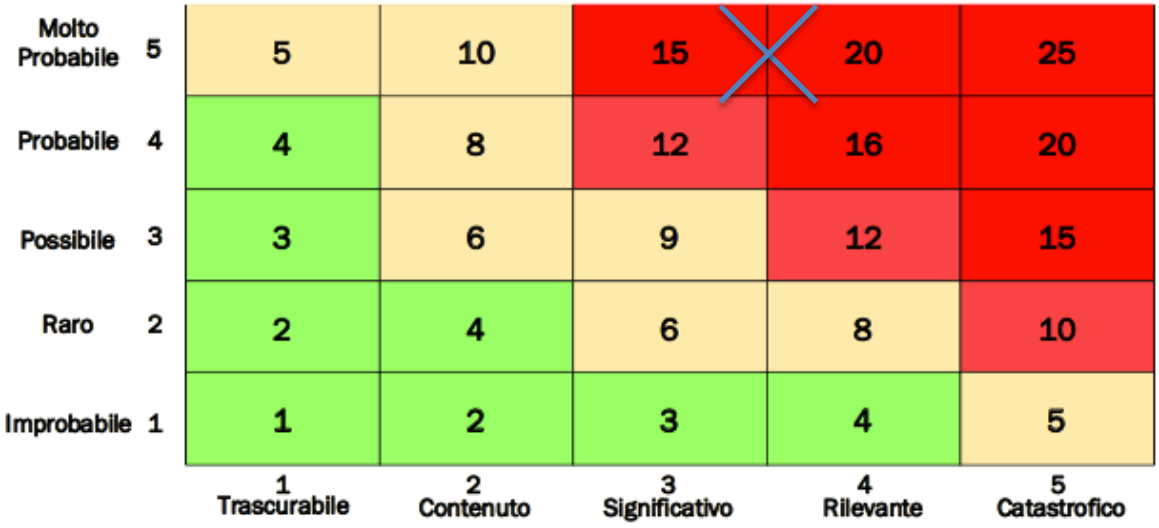
Un esempio concreto:

Nell'ambito dei rischi operativi/compliance, è stato individuato il rischio di infortunio sul lavoro.

Si procede a valutare il rischio inerente (lordo), quindi come se non ci fosse alcun presidio di controllo. La valutazione effettuata della severità di impatto e della frequenza di accadimento , è molto seria:

- severità di impatto pari a 4 (rilevante)
- frequenza di accadimento pari a 5 (molto probabile)

VALUTAZIONE RISCHIO INERENTE



Si procede quindi alla valutazione del sistema di controllo interno dello specifico rischio analizzato, costituito da:

- Sistema di Gestione per la sicurezza sul lavoro in linea con le migliori prassi internazionali;
- procedure operative estremamente precise ed esaurienti e effettivamente applicate;
- formazione continua del personale;
- sistema di deleghe appropriate.

Viene quindi valutato con un punteggio di 4: "adeguato".

Il rischio residuo che risulta è quindi pari a 1 per quanto riguarda la frequenza di accadimento (remoto). Mentre la gravità di impatto resta di 4. Ciò in quanto il sistema di gestione e gli altri presidi organizzativi sono idonei ad incidere sulla variabile frequenza ma non sull'eventuale impatto .

VALUTAZIONE RISCHIO RESIDUO

Come si nota dal grafico, tuttavia, ora il rischio (residuo) è posizionato in un'area "verde" di accettabilità.

La **PONDERAZIONE** del rischio consente, sulla base degli esiti della valutazione, di definire le attività da intraprendere in relazione ad ogni singolo rischio.

Le opzioni sono ovviamente molteplici.

- **Non assunzione**: tale strategia consiste nell'evitare, ove possibile, di assumersi un dato rischio; una decisione simile viene applicata nel momento in cui le altre misure non risultino idonee, sia dal punto di vista gestionale che da quello prettamente economico, a ridurre il contenuto di rischio al di sotto delle soglia di accettabilità;

- **Riduzione:** questo metodo consiste nell'adozione di tecniche di prevenzione e protezione, ai fini di una riduzione sostanziale delle probabilità di accadimento e del livello degli impatti. Questo tipo di prevenzione impatta sulla componente probabilistica, mentre la protezione è indirizzata a contenere gli effetti dannosi;

- **Trasferimento**: il trasferimento dei rischi implica l'assunzione di una posizione diametralmente opposta a quella da gestire; si considera idonea questa modalità nel momento in cui i rischi da trattare siano finanziari e legati all'uso di contratti derivati oppure

siano mappati nell'ambito dei rischi da trasferire tramite polizze ad hoc sul mercato assicurativo.

- **Condivisione**: la suddivisione del rischio tra diversi soggetti è considerabile una modalità efficace, nel momento in cui i terzi siano competenti disposti a condividere il rischio responsabilmente, in genere grazie alla promessa di un premio o come contropartita in sede contrattuale con partner d'affari;

- **Accettazione**: consiste nell'assunzione di un rischio, ma non nell'adozione di tecniche di trasferimento/riduzione dello stesso; si utilizza questa metodologia quando l'assunzione di quel rischio non è ritenuta preoccupante per l'incolumità dell'organizzazione, o quando le strategie di contenimento siano giudicate eccessivamente onerose. È comunque possibile adottare, in questo caso, una forma di autoassicurazione, tramite l'accantonamento di un ammontare di denaro tale da coprire le potenziali perdite, stimato mediante tecniche probabilistiche (fondo rischi).