Il risk management secondo il «Modello» ex D.Lgs. 231/2001

di Alberto Pesenato (*) e Elisa Pesenato (**)

La gestione del rischio (risk management) conseguente alla valutazione dello stesso (risk assessment) è necessaria nell'analisi delle attività sensibili e nella determinazione delle aree di rischio. Tali concetti sono richiamati dal documento CoSO II e dalla circolare 83607/2012 della Guardia di Finanza. Questo primo contributo ne illustra le linee essenziali e le modalità applicative.

Introduzione

Recentemente la Circolare della Guardia di Finanza n. 83607/2012 ha trattato diffusamente la composizione del Modello di organizzazione, gestione e controllo dedicando alla stessa il Volume III, che così recita a pag. 76 «*Ai fini dell'elaborazione dei modelli, che devono essere costruiti secondo uno schema che riprenda i processi* di risk assessment e risk management normalmente *attuati nelle imprese, la relazione illustrativa evidenzia come la normativa preveda una maggiore tipizzazione dei modelli validi per i vertici, come risulta dal disposto dell'art. 6, comma 2, che tratteggia un modello ben strutturato, con un contenuto minimo obbligatorio e non derogabile*».

Risk management o gestione del rischio (CoSO Report II)

L'aspetto più significativo introdotto e richiamato espressamente dalla Circolare della GdF 83607/2012 è la definizione di un modello di riferimento che detta i principi generali al Management per il «governo» dell'azienda e che si basa sui seguenti elementi principali:
a. obiettivi;
b. rischi;
c. controlli.

Obiettivi

La finalità principale del sistema di controllo interno è quella di fornire una ragionevole assicurazione sul raggiungimento degli obiettivi aziendali;quindi è di fondamentale importanza che tali obiettivi siano individuati e ben specificati nonché condivisi all'interno di tutta l'organizzazione. Il vertice aziendale oltre a definire gli obiettivi strategici prioritari (ad esempio ottenimento di vantaggi competitivi, sviluppo del *core business*, soddisfacimento delle aspettative degli *stakeholders*, ecc..), dovrebbe prevedere modalità per la loro specificazione a livello di obiettivi operativi e per la loro diffusione all'interno della organizzazione (1).

Rischi

Ogni azienda è chiamata a fronteggiare rischi di diversa natura a tutti i livelli della organizzazione, per ogni attività o processo. In questo contesto il rischio è considerato come un qualsiasi evento «sfavorevole» che può pregiudicare il raggiungimento degli obiettivi aziendali. I rischi possono «minacciare» la sopravvivenza della azienda, la sua capacità competitiva, la situazione finanziaria, compromettere l'immagine aziendale sul mercato e la qualità dei prodotti e dei servizi. Non esiste nella pratica aziendale alcun mo-

Note:
(*) Revisore legale, Consulente Area D. Lgs. 231/2001 (Presidente OdV Karrell Srl - Trentino trasporti esercizio SpA)
(**) Auditor (SCI) Sistema di Controllo Interno - Consulente Area 231/2001
(1) Si veda *Il modello di organizzazione gestione e controllo ex D. Lgs. n. 231/2001 e l'Organo di Vigilanza* WKI - IPSOA IV Edizione 2013 e contributi in www.albertopesenato.net.

do per eliminare totalmente il rischio, tuttavia il rischio può essere «gestito» in maniera tale da non compromettere l'operatività aziendale.
Il management deve essere consapevole di quali sono i rischi che minacciano il proprio processo e determinare di conseguenza il livello di rischio considerato «accettabile» impegnandosi a mantenerlo entro tale livello attraverso azioni mirate di risk management (2).
Gli elementi che caratterizzano il rischio sono la «probabilità» del verificarsi dell'evento e il relativo «gravità/impatto» che l'evento dannoso può avere sulla organizzazione. Tali elementi consentono di identificare quali rischi sono «significativi» per l'azienda e perciò devono essere attentamente presi in considerazione e quali, invece, hanno una rilevanza minore e possono essere trascurati.
I rischi aziendali (3) traggono origine da una serie di rischi strategici che minacciano la realizzazione del piano strategico; i rischi strategici sono indirizzati dai fattori di rischio (ad es.: complessità delle operazioni, attenzione e competenza manageriale, liquidità del patrimonio, pressione del vertice per il raggiungimento degli obiettivi, ecc.) e devono essere tradotti in micro rischi classificabili in livelli o categorie. Un esempio di catalogazione dei rischi è il seguente come esposti nel CoSO Report II.

CoSO II La gestione del rischio aziendale (ERM Entreprise Risk Management)
Si fa riferimento ai rischi strategici della gestione aziendale, gli obiettivi aziendali possono essere così individuati: (4)
– strategici: sono espressi in termini generali e devono essere allineati alla *mission* aziendale e la devono supportare. Riflettono la scelta del management di come l'azienda si adopera per creare valore per i suoi *stakeholders*;
– operativi: riguardano l'efficacia e l'efficienza delle operazioni aziendali. È necessario che riflettano l'ambiente micro - macro economico nel quale l'azienda opera. Il management deve assicurarsi che gli obiettivi siano reali, riflettano le esigenze del mercato e siano espressi nei giusti
termini al fine di consentire un'attendibile valutazione della *performance*;
– di reporting: riguardano le informazioni, che devono essere accurate, complete e coerenti con i fini perseguiti;
– di conformità (5): le aziende devono condurre le loro attività (e spesso assumere provvedimenti particolari) in conformità alle leggi e ai regolamenti in vigore.
Lo studio (ERM) ha identificato otto componenti del sistema di controllo tra loro interconnessi. Questi componenti sono:
– ambiente interno: il management formula la filosofia di base e determina il livello di accettabilità del rischio. Determina, in termini generali, i modi in cui il rischio è considerato e affrontato dalle persone che operano in azienda;
– definizione degli obiettivi: gli obiettivi devono essere fissati prima di procedere all'identificazione degli eventi che possono pregiudicare il loro conseguimento;
– identificazione degli eventi: devono essere identificati gli eventi che possono avere un impatto sull'attività aziendale. Comporta l'identificazione di fatti potenziali di origine interna e esterna che possono pregiudicare il conseguimento degli obiettivi. È necessario distinguere gli eventi che rappresentano rischi da quelli che rappresentano opportunità;
– valutazione del rischio: i rischi identificati (rischi di gestione) sono analizzati al fine di determinare come devono essere gestiti. I rischi sono collegati agli obiettivi e possono pregiudicarne il raggiungimento. I rischi sono valutati sia in termini di rischio inerente (6)

Note:
(2) «*Risk management has emerged more or less independently in a number of areas including: safety, insurance, banking, investment, medicine, artificial intelligence, mathematics, public policy analysis, and internal control.*» (M. Leitch, *Intelligent internal control and Risk Management*).
(3) Si ricorda al lettore che il documento CoSO II (ERM) si riferisce alla molteplicità dei rischi aziendali dei quali quelli riferiti alle leggi e regolamenti (ex 231/2001) sono solo una parte.
(4) *La gestione del rischio aziendale ERM Enterprise Risk Management (CoSO II)* Il Sole 24Ore - Pagg. 3, 4, 22, 23
(5) Si ricorda qui, come in altre parti, che lo studio ERM non si riferisce al Rischio di compimento di reati od illeciti ma in generale al Rischio di gestione aziendale e delle sue componenti tra le quali il rischio suddetto.
(6) Si fa notare come nella pratica professionale per la determinazione del «Rischio di Infrazione» il Rischio Inerente o Intrinseco abbia come significato che i fatti aziendali ovvero le operazioni registrate possano contenere operazioni cosiddette «sensibili».

(qui inteso come rischio in assenza di qualsiasi intervento) sia di rischio residuo (rischio dopo aver attivato interventi per ridurlo), determinando la probabilità che il rischio si verifichi e il relativo impatto;
– risposta al rischio: il *management* identifica e valuta le risposte possibili al rischio, che potrebbero essere: evitare, accettare, ridurre e compartecipare il rischio. Seleziona una serie di azioni per allineare i rischi emersi con la tolleranza al rischio e al rischio accettabile;
– attività di controllo: devono essere definite e realizzate politiche e procedure per assicurare che le risposte al rischio siano efficacemente eseguite;
– informazioni e comunicazione: le informazioni pertinenti devono essere identificate, raccolte e diffuse nella forma e nei tempi che consentano alle persone di adempiere alle proprie responsabilità. Si devono attivare comunicazioni efficaci in modo che queste fluiscano per l'intera struttura organizzativa: verso il basso, verso l'alto e trasversalmente;
– monitoraggio: l'intero processo deve essere monitorato e modificato se necessario. Il monitoraggio si concretizza in interventi continui, integrati nella normale attività operativa aziendale, in valutazioni oppure in una combinazione dei due metodi.
I vantaggi connessi possono essere molteplici.
In definitiva si determinano gli obiettivi, si identificano gli eventi e si affronta l'eventuale rischio aziendale che è essenzialmente un «rischio di gestione» che dipende dalla strategia adottata dal CdA.
In effetti gli eventi che si devono analizzare a dai quali discendono i possibili rischi derivano dai fattori esposti nel proseguo (7).
• Fattori esterni (Esogeni)
– economia;
– ambiente;
– politica;
– sociale;
– tecnologia.
• Fattori interni (Endogeni)
– infrastrutture;
– personale;
– processi;
– tecnologia.
Con questa metodologia si analizzano i fattori e conseguentemente si identificano gli eventi che possono pregiudicare il conseguimento degli obiettivi aziendali.
Le tecniche per la identificazione degli eventi sono state esposte nella Tavola 1 del numero di luglio della presente rivista a cui si rimanda. Come si può notare questo approccio si basa sul «rischio di gestione» che dipende dalla strategia aziendale e che ben poco ha a che vedere con uno specifico diretto ed univoco rischio di commissione degli illeciti o reati previsti dal D. Lgs. 231/2001 se non nei fattori interni riguardanti il personale ed i processi.
Nell'ambito di questo «rischio di gestione» vengono definite le aree e le procedure da monitorare ed inseguito i protocolli da consigliare per impedire la commissione dell'illecito o reato.
Esempi di cause che scaturiscono dal «rischio» includono:
• decisioni errate dovute all'utilizzo di informazioni non corrette o per scarsa comunicazione;
• *reporting* inaccurato;
• perdite economico-finanziarie;
• inadeguata salvaguardia del patrimonio aziendale;
• uso inefficiente delle risorse;
• piani di investimento inadeguati;
• inadeguata esecuzione dei piani aziendali;
• inefficienza e inefficacia delle attività operative;
• non aderenza a procedure interne, regolamentazioni e leggi in vigore;
• dispute legali e insoddisfazione degli utenti/clienti;
• discredito dell'immagine aziendale;
• attività fraudolente.
Il processo di valutazione dei rischi è stato trattato nei paragrafi precedenti e verrà ripreso successivamente al momento di analizzare le componenti del sistema di controllo interno. In questo contesto è opportuno sottolineare come le attività di individuazione, misurazione e classificazione dei rischi siano strettamente integrate nel processo di pianificazione degli obiettivi strategici ed operati-

Nota:
(7) *La gestione del rischio aziendale ERM Enterprise Risk Management (CoSO II)* PricewaterhouseCoopers - Il Sole 24 Ore II edizione 2008, Pagg. 48, 49 e 53.

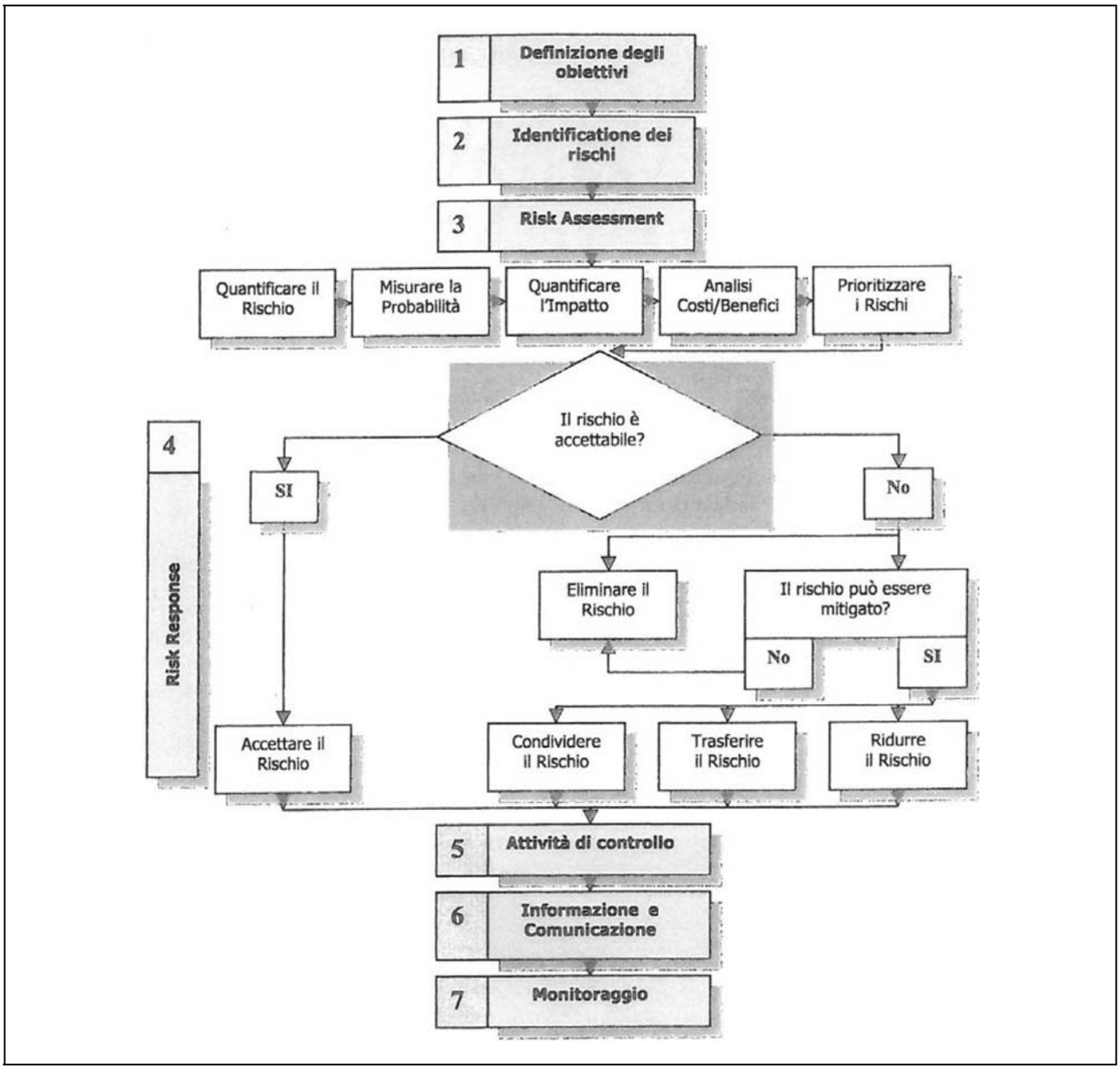
vi. Il vertice aziendale, nella fase di specificazione degli obiettivi, deve tener conto di quali sono i rischi che ne minacciano il raggiungimento. È opportuno perciò adottare una metodologia sistematica di valutazione del rischio (risk assessment) (8) che produca una mappatura dei rischi aziendali individuando le attività maggiormente minacciate e per le quali è necessaria la presenza di meccanismi di controllo adeguati.

Controlli

Il termine controllo è inteso come capacità di orientare o «guidare» l'attività di un settore aziendale o di un'intera azienda, allo scopo di avanzare verso gli obiettivi attesi. Il controllo è pertanto strumentale al raggiungi-

Nota:
(8) L'argomento sarà trattato nel prossimo contributo.

Tavola 1 - Risk management flow chart



Fonte: Epstein,J., Rejc, A., (CMA Canada), 2006, *Identifying, measuring and managing organizational risk for improved performances*, Risk Management Accounting Guideline.

mento del risultato prefissato e consiste nel porre in essere azioni dirette a circoscrivere il rischio di mancato raggiungimento dell'obiettivo stesso.
Il controllo riduce/elimina le conseguenze del rischio, rileva il rischio e segnala l'esigenza di un'azione correttiva. Il controllo può essere svolto in due momenti:
– prima di porre in essere l'azione: è il cosidetto controllo preventivo;
– dopo aver posto in essere l'azione: questo è il controllo rivelatore.
I controlli possono esemplificarsi nelle attività più svariate.

Conclusione

In conclusione il risk management consente di:
1) poter disporre di strumento utile per approfondire le conoscenze sull'ambiente e sull'impresa;
2) poter disporre di un valido supporto per le decisioni strategiche;
3) poter disporre di un potente veicolo di comunicazione con gli *stakeholders*;
4) coinvolgere della maggior parte delle persone chiave presenti in azienda;
5) utilizzare le risorse in modo efficace ed efficiente.