6128/01

Edizione italiana a cura di
Associazione Italiana Internal Auditors
e PRICEWATERHOUSECOOPERS

La gestione del rischio aziendale

ERM - *Enterprise Risk Management*:
modello di riferimento
e alcune tecniche applicative

CoSO
Committee of Sponsoring Organizations
of the Treadway Commission

Negli ultimi anni è cresciuto notevolmente l'interesse per le tematiche della gestione del rischio ed è diventata sempre più evidente la necessità di disporre di un valido modello di riferimento per identificare, valutare e gestire i rischi in modo efficace.
La sopravvivenza di un'azienda è assicurata dalla sua capacità di creare valore per i suoi stakeholder. Questo enunciato costituisce la filosofia di fondo della "gestione del rischio aziendale". Tutte le aziende devono affrontare eventi incerti e la sfida del management è di determinare il *quantum* di incertezza accettabile per creare valore. L'incertezza rappresenta sia un rischio che un'opportunità e può potenzialmente ridurre o accrescere il valore dell'azienda.
Il modello ERM (*Enterprise Risk Management*) esposto in questo volume consente al management di affrontare efficacemente le incertezze e i conseguenti rischi e opportunità, accrescendo così le capacità dell'azienda di generare valore.
Il volume si articola in due parti. La prima parte illustra il modello dell'ERM: il modello fornisce una definizione della gestione del rischio aziendale e ne descrive i principi e i concetti, fornisce inoltre una guida per tutti i livelli del management, che operano sia nelle imprese che in altre organizzazioni, per valutare e accrescere l'efficacia del processo di gestione del rischio. La seconda parte, intitolata "Tecniche applicative", illustra le tecniche utili per applicare in concreto i principi del modello. L'*Executive Summary* iniziale offre un'ampia panoramica sulla strutturazione del modello ed è destinata al CEO, all'alta direzione, agli amministratori, ai legislatori e alle autorità di vigilanza.

La gestione del rischio aziendale

6128/01

ISBN 88-324-6128-5

€ 32,00

Il Sole 24 ORE

Edizione italiana a cura di
Associazione Italiana Internal Auditors
e PRICEWATERHOUSECOOPERS

LA GESTIONE DEL RISCHIO AZIENDALE

ERM - Enterprise Risk Management: un modello di riferimento e alcune tecniche applicative

CoSO
Committee of Sponsoring Organizations
of the Treadway Commission

Il Sole 24 ORE

Titolo originale: *Enterprise Risk Management – Integrated Framework: Executive Summary and Framework*, *Enterprise Risk Management – Integrated Framework: Application Techniques*, 2 vol.

Traduzione dall'inglese a cura di Associazione Italiana Internal Auditors e PricewaterhouseCoopers

Questa edizione è stata chiusa in redazione il 5 aprile 2006

ISBN 88-324-6128-5

Sede legale - Direzione e redazione: via Monte Rosa, 91 - 20149 Milano
Servizio Clienti: tel. 3022.5680 (prefisso 02 oppure 06)
fax: 3022.5400 (prefisso 02 oppure 06)

Prima edizione: maggio 2006

Committee of Sponsoring Organizations of the Treadway Commission (CoSO)

Oversight	Representative
CoSO Chair	John J. Flaherty
American Accounting Association	Larry E. Rittenberg
American Institute of Certified Public Accountants	Alan W. Anderson
Financial Executives International	John P. Jessup Nicholas S. Cyprus
Institute of Management Accountants	Frank C. Minter Dennis L. Neider
The Institute of Internal Auditors	William G. Bishop, III David A. Richards

---

Project Advisory Council to CoSO

Guidance

Tony Maki, Chair
Partner
Moss Adams LLP

Mark S. Beasley
Professor
North Carolina State University

Jerry W. DeFoor
Vice President and Controller
Protective Life Corporation

James W. DeLoach
Managing Director
Protiviti Inc.

Andrew J. Jackson
Senior Vice President of Enterprise Risk Assurance Services
American Express Company

Steven E. Jameson
Executive Vice President, Chief Internal Audit & Risk Officer
Community Trust Bancorp, Inc.

John P. Jessup
Vice President and Treasurer
E. I. duPont de Nemours and Company

Tony M. Knapp
Senior Vice President and Controller
Motorola, Inc.

Douglas F. Prawitt
Professor
Brigham Young University

PricewaterhouseCoopers LLP

Author

Principal Contributors

Richard M. Steinberg
Former Partner and Corporate Governance Leader (Presently Steinberg Governance Advisors)

Miles E.A. Everson
Partner and Financial Services Finance, Operations, Risk and Compliance Leader
New York

Frank J. Martens
Senior Manager, Client Services
Vancouver, Canada

Lucy E. Nottingham
Manager, Internal Firm Services
Boston

Sommario

Appendici

Executive Summary

La sopravvivenza di un'azienda è assicurata dalla sua capacità di creare valore per i suoi stakeholder. Questo enunciato costituisce la filosofia di fondo della "gestione del rischio aziendale". Tutte le aziende devono affrontare eventi incerti e la sfida del management è di determinare il *quantum* di incertezza accettabile per creare valore. L'incertezza rappresenta sia un rischio che un'opportunità e può potenzialmente ridurre o accrescere il valore dell'azienda. L'ERM consente al management di affrontare efficacemente le incertezze e i conseguenti rischi e opportunità, accrescendo così le capacità dell'azienda di generare valore.

Il management massimizza il valore quando formula strategie e obiettivi al fine di conseguire un equilibrio ottimale tra target di crescita e di redditività e rischi conseguenti, e quando impiega in modo efficiente e efficace le risorse nel perseguire gli obiettivi aziendali. L'ERM, il cui modello è illustrato nella prima parte del presente volume, ha le seguenti caratteristiche.

- *L'allineamento della strategia al rischio accettabile* - Il management stabilisce il livello di rischio accettabile per valutare le alternative strategiche, fissare i corrispondenti obiettivi e sviluppare i meccanismi per gestire i rischi che ne derivano.
- *Il miglioramento della risposta al rischio individuato* - L'ERM fornisce una metodologia rigorosa per identificare e selezionare tra più risposte alternative al rischio quella più adeguata (evitare, ridurre, condividere, accettare il rischio).
- *La riduzione degli imprevisti e delle perdite conseguenti* - Le aziende, accrescendo la loro capacità di identificare eventi potenziali, di valutare i relativi rischi e di formulare risposte adeguate, riducono la frequenza degli imprevisti come pure i costi e le perdite conseguenti.
- *L'identificazione e la gestione dei rischi correlati e multipli* - Ogni azienda deve affrontare una miriade di rischi che interessano diverse aree dell'organizzazione, e l'ERM facilita la formulazione di un'efficace risposta ai rischi con impatti correlati e risposte univoche a rischi multipli.
- *L'identificazione delle opportunità* - Analizzando tutti gli eventi potenziali, il management è in grado di identificare e cogliere proattivamente le opportunità che emergono.

- *Il miglioramento dell'impiego di capitale* - L'acquisizione di informazioni affidabili sui rischi consente al management di valutare efficacemente il fabbisogno finanziario complessivo e di migliorare, così, l'allocazione del capitale.

Queste caratteristiche proprie dell'ERM aiutano il management a conseguire i propri obiettivi di performance e di redditività e di evitare perdite di risorse. Inoltre, contribuiscono ad assicurare l'efficacia del reporting e la conformità alle leggi e ai regolamenti, e costituiscono un ausilio per evitare danni all'immagine aziendale e le conseguenze che ne derivano. In sintesi, l'ERM supporta l'organizzazione nel raggiungimento delle mete desiderate evitando insidie e imprevisti di percorso.

Eventi – rischi e opportunità

Un evento può avere un impatto negativo, un impatto positivo, o entrambi. Eventi con impatti negativi costituiscono "rischi", che possono ostacolare la creazione di valore o erodere quello esistente. Eventi con un impatto positivo possono compensare impatti negativi o possono costituire "opportunità". Le opportunità sono possibilità che un evento si verifichi e influisca positivamente per il conseguimento degli obiettivi, contribuendo, così, alla creazione di valore oppure preservando quello esistente. Il management valuta le opportunità emerse, riconsiderando le strategie formulate in precedenza o i processi di definizione degli obiettivi in atto ed elaborando nuovi piani per cogliere i vantaggi che ne derivano.

Definizione dell'ERM

L'ERM, che tratta dei rischi e delle opportunità che influenzano la creazione o la preservazione di valore, è definito come segue:

> *La gestione del rischio aziendale è un processo, posto in essere dal consiglio di amministrazione, dal management e da altri operatori della struttura aziendale; utilizzato per la formulazione delle strategie in tutta l'organizzazione; progettato per individuare eventi potenziali che possono influire sull'attività aziendale, per gestire il rischio entro i limiti del rischio accettabile e per fornire una ragionevole sicurezza sul conseguimento degli obiettivi aziendali.*

Questa definizione riflette alcuni concetti fondamentali. L'ERM è:

- un processo continuo e pervasivo che interessa tutta l'organizzazione;
- svolto da persone che occupano posizioni a tutti i livelli della struttura aziendale;
- utilizzato per la formulazione delle strategie;

- utilizzato in tutta l'organizzazione: sia nelle sue singole attività (in ogni livello e in ogni unità della struttura), che nella sua attività complessiva. Esso include una visione del rischio che considera l'azienda nel suo complesso;
- progettato per identificare eventi potenziali che potrebbero influire sull'attività aziendale e per gestire il rischio entro i limiti del rischio accettabile;
- in grado di fornire una ragionevole sicurezza al consiglio di amministrazione e al management;
- in grado di conseguire obiettivi relativi a una o più categorie distinte, ma che si possono sovrapporre.

Questa definizione è intenzionalmente estensiva e racchiude i concetti chiave, fondamentali per capire come le aziende devono gestire il rischio; fornisce i criteri di base da applicare in tutte le organizzazioni, quale che sia la loro natura. Si focalizza direttamente sul raggiungimento degli obiettivi di una specifica organizzazione e fornisce i criteri per valutare l'efficacia dell'ERM.

Conseguimento degli obiettivi

Nell'ambito della missione e della visione aziendale, il management definisce gli obiettivi strategici, sceglie la strategia e fissa gli obiettivi specifici, coerenti con la strategia, e li assegna a vari livelli della struttura organizzativa. L'ERM è finalizzato al conseguimento degli obiettivi aziendali rientranti nelle seguenti categorie:

- *strategici* - sono di natura generale e definiti ai livelli più elevati della struttura organizzativa, allineati e a supporto della missione aziendale;
- *operativi* - riguardano l'impiego efficace ed efficiente delle risorse aziendali;
- *di reporting* - riguardano l'affidabilità delle informazioni fornite dal reporting;
- *di conformità* - riguardano l'osservanza delle leggi e dei regolamenti in vigore.

Questa classificazione degli obiettivi aziendali consente di approfondire differenti aspetti della gestione del rischio. Queste categorie distinte, ma connesse o sovrapponibili (un determinato obiettivo può rientrare in più di una categoria) riguardano esigenze diverse dell'azienda e possono essere di competenza diretta di più manager. Questa classificazione consente inoltre di distinguere quanto ci si può attendere da ciascuna categoria di obiettivi. Un'altra categoria che riguarda la "salvaguardia delle risorse", adottata da qualche azienda, è descritta nel prosieguo di questo studio.

Poiché gli obiettivi riguardanti l'affidabilità del reporting e la conformità alle leggi e ai regolamenti sono sotto il diretto controllo dell'azienda, l'ERM è in grado di fornire una ragionevole sicurezza per il conseguimento di questa tipologia di obiettivi. Il conseguimento degli obiettivi strategici e operativi è soggetto a eventi esterni che non sempre rientrano nella sfera di controllo dell'azienda; di conseguenza, la gestione del rischio può solo fornire una ragionevole sicurezza che il management e il consiglio di amministrazione, nel suo ruolo di vigilanza, siano tempestivamente informati della misura in cui si stanno realizzando detti obiettivi.

I componenti dell'ERM

L'ERM è costituito da otto componenti interconnessi. Essi derivano dal modo in cui il management gestisce l'azienda e sono integrati con i processi operativi. Questi componenti sono:

- *Ambiente interno* - L'ambiente interno, che costituisce l'identità essenziale di un'organizzazione, determina i modi in cui il rischio è considerato e affrontato dalle persone che operano in azienda, come pure la filosofia della gestione del rischio, i livelli di accettabilità del rischio, l'integrità e i valori etici e l'ambiente di lavoro in generale.
- *Definizione degli obiettivi* - Gli obiettivi devono essere fissati prima di procedere all'identificazione degli eventi che possono potenzialmente pregiudicare il loro conseguimento. L'ERM assicura che il management abbia attivato un adeguato processo di definizione degli obiettivi e che gli obiettivi scelti supportino e siano coerenti con la missione aziendale e siano in linea con i livelli di rischio accettabile.
- *Identificazione degli eventi* - Gli eventi esterni e interni, che influiscono sul conseguimento degli obiettivi aziendali, devono essere identificati distinguendoli tra "rischi" e "opportunità". Le opportunità devono essere valutate riconsiderando la strategia definita in precedenza o il processo di formulazione degli obiettivi in atto.
- *Valutazione del rischio* - I rischi sono analizzati, determinando la probabilità che si verifichino in futuro e il loro impatto, al fine di stabilire come devono essere gestiti. I rischi sono valutati in termini di rischio inerente (rischio in assenza di qualsiasi intervento) e di rischio residuo (rischio residuo dopo aver attuato interventi per ridurlo).
- *Risposta al rischio* - Il management seleziona le risposte al rischio emerso (evitarlo, accettarlo, ridurlo, comparteciparlo) sviluppando interventi per allineare i rischi emersi con i livelli di tolleranza al rischio e di 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 esse-

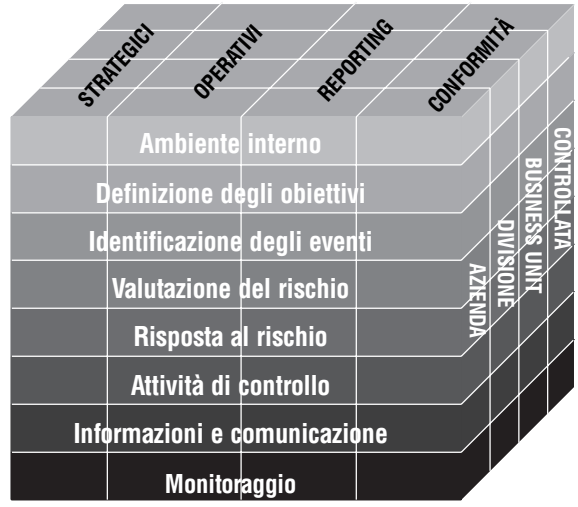
re identificate, raccolte e diffuse nella forma e nei tempi che consentano alle persone di adempiere correttamente le proprie responsabilità. In linea generale, si devono attivare comunicazioni efficaci, in modo che queste fluiscano per l'intera struttura organizzativa: verso il basso, verso l'alto e trasversalmente.

- *Monitoraggio* - L'intero processo dell'ERM deve essere monitorato e modificato ove necessario. Il monitoraggio si concretizza in interventi continui integrati nella normale attività operativa aziendale o in valutazioni separate, oppure in una combinazione dei due metodi.

L'ERM non è un procedimento strettamente sequenziale, nel quale un componente influisce solo sul successivo. Si tratta, invece, di un processo interattivo e multidirezionale in cui ogni componente può influire o influisce su un altro componente, indipendentemente dalla sequenza del processo.

Legami tra obiettivi e componenti

Esiste un rapporto diretto tra obiettivi, ossia ciò che un'azienda si sforza di conseguire, e i componenti dell'ERM, ovvero ciò che occorre per conseguire gli obiettivi. Questo rapporto è schematizzato in una matrice tridimensionale a forma di cubo.



Le quattro categorie di obiettivi – strategici, operativi, di reporting e di conformità – sono rappresentate nelle colonne verticali del cubo, gli otto componenti sono invece rappresentati nelle righe orizzontali del cubo, e le unità operative dell'organizzazione sono rappresentate dalla terza dimensione della matrice. Questo schema fa capire l'estrema flessibilità del modello, che qui si illustra: esso può essere applicato, sia all'intero processo di gestione del rischio aziendale, sia distintamente alle singole categorie di obiettivi, ai componenti, alle singole unità operative e alle singole sub unità di queste ultime.

Efficacia

La valutazione dell'efficacia del processo di gestione del rischio aziendale è un giudizio soggettivo, fondato sulla presenza degli otto componenti e sul loro corretto funzionamento. Pertanto, i componenti costituiscono anche dei criteri di efficacia. Così, se in un processo tutti gli otto componenti sono presenti e funzionano correttamente, ciò rappresenta una prova dell'assenza di debolezze significative e che i rischi che si vogliono affrontare sono al di sotto del livello di rischio ritenuto accettabile.

Quando un processo di gestione del rischio aziendale è giudicato efficace per ciascuna delle quattro categorie di obiettivi, ciò significa che il consiglio di amministrazione e il management hanno una ragionevole sicurezza di venire a conoscenza della misura in cui gli obiettivi strategici e operativi si stanno conseguendo, che i report sono affidabili e che le leggi e i regolamenti in vigore sono osservati.

Gli otto componenti non funzionano in modo identico in ogni azienda. L'applicazione del modello, in aziende medio-piccole, per esempio, potrebbe essere meno formale e meno strutturata. Ciò nondimeno, le piccole aziende possono avere un efficace processo di gestione del rischio, purché ciascun componente sia presente e funzioni correttamente.

Limiti

Sebbene l'ERM procuri importanti benefici, tuttavia, esistono dei limiti. Oltre ai fattori illustrati in precedenza esistono dei limiti dovuti a possibili errori di giudizio quando si prendono decisioni gestionali, all'impossibilità di proteggersi da tutti i rischi anche perché il rapporto costo-benefici diverrebbe gravoso, a errori umani che possono procurare danni involontari, alla possibilità che i controlli siano aggirati da parte di due o più persone in collusione e al management che può eludere le decisioni sulla gestione dei rischi. Queste limitazioni non consentono al consiglio di amministrazione e al management di ottenere una sicurezza assoluta sul conseguimento degli obiettivi aziendali.

Il controllo interno e l'ERM

Il controllo interno è parte integrante dell'ERM, che qui si presenta. Pertanto, il modello di gestione del rischio aziendale incorpora il controllo interno fornendo un più completo strumento per il management. Il controllo interno è definito e descritto nella pubblicazione intitolata "*Il sistema di controllo interno*". Poiché questa pubblicazione ha superato bene la "prova del tempo" e ha costituito la base per regolamenti e leggi attualmente in vigore, essa rimane ancora valida come pure la definizione e il modello di controllo interno. Sebbene solo una parte della pubblicazione "*Il sistema di controllo in-*

terno" sia riprodotta in questo studio, ciò nondimeno questa pubblicazione è da considerarsi virtualmente parte integrante del presente volume.

Ruoli e responsabilità

Ogni persona, che opera in un'organizzazione, ha una certa responsabilità nell'ERM. Il CEO ne ha la responsabilità ultima e ne assume la paternità. Il management promuove la filosofia di gestione del rischio e l'osservanza del livello di rischio accettabile, e gestisce i rischi nella sua sfera di responsabilità in coerenza con i livelli di "tolleranza al rischio". Generalmente, il risk officer, il direttore finanziario, l'internal auditor assolvono compiti chiave di supporto alla gestione del rischio, altre persone svolgono invece compiti puramente esecutivi nella gestione del rischio in conformità alle direttive e ai protocolli. Il consiglio di amministrazione svolge un ruolo importante di supervisione del processo di gestione del rischio aziendale e contribuisce alla determinazione del livello di rischio accettabile. Un certo numero di soggetti esterni, come i clienti, i fornitori, partner, revisori esterni e analisti finanziari spesso forniscono informazioni utili per il buon funzionamento del processo di gestione del rischio aziendale, ma essi non rispondono della sua efficacia, né fanno parte del processo medesimo.

Com'è strutturato questo studio

Questo studio si articola in due sezioni. Prima delle due sezioni vi è il presente "Executive Summary". L'Executive Summary offre un'ampia panoramica sulla strutturazione del modello ed è destinato al Ceo, all'alta direzione, agli amministratori, ai legislatori e alle autorità di vigilanza.

La prima sezione illustra il modello dell'ERM. Il modello fornisce una definizione della gestione del rischio aziendale e ne descrive i principi e i concetti, fornisce inoltre una guida per tutti i livelli del management, che operano sia nelle imprese che in altre organizzazioni, per valutare e accrescere l'efficacia del processo di gestione del rischio.

La seconda sezione, intitolata "Tecniche applicative", illustra le tecniche utili per applicare in concreto i principi del modello.

I destinatari di questo studio

Le azioni che si raccomanda di intraprendere a seguito di questo studio dipendono dalla posizione e dal ruolo delle parti interessate:

- *Il consiglio di amministrazione* - Il consiglio deve discutere con l'alta direzione dello stato del processo di gestione del rischio aziendale e, ove necessario, supervisionare il processo stesso. Il consiglio deve assicurarsi di essere stato ben informato sui rischi più rilevanti e delle relative azioni che il management sta attivando e di come il management sta operando

per rendere il sistema efficace. Il consiglio può attingere notizie a tal fine, contattando gli internal auditor, i revisori esterni e altri soggetti.

- *L'alta direzione* - Questo studio raccomanda che il CEO valuti l'adeguatezza del processo di gestione del rischio adottato dalla sua organizzazione. Un possibile approccio potrebbe consistere nel riunire i responsabili delle unità operative e personale con compiti chiave per predisporre una valutazione preliminare dell'adeguatezza e efficacia del processo in essere. Qualunque sia la forma, una valutazione preliminare dovrà stabilire se sussista la necessità di procedere a una successiva valutazione più ampia e più approfondita e, in tal caso, dovrà stabilire come effettuarla.
- *Altro personale* - I manager e altro personale della struttura dovranno accertare, alla luce del presente modello, come le loro responsabilità si concretizzano nella realtà aziendale e studiare, con personale di livello gerarchico più elevato, le proposte per rafforzare il processo di gestione del rischio. Gli internal auditor devono considerare la portata dei loro interventi riguardanti l'ERM.
- *Il legislatore e le autorità di vigilanza* - Il presente modello intende contribuire a una visione univoca e condivisa dell'ERM, inclusi i suoi limiti e i suoi vantaggi. Il legislatore o le autorità di vigilanza possono fare riferimento a questo modello nel definire i limiti della gestione del rischio per non creare false aspettative quando sono promulgati leggi, regolamenti o raccomandazioni o quando attivano ispezioni sui soggetti sui quali esercitano la loro autorità di vigilanza.
- *Le organizzazioni professionali* - Le organizzazioni professionali, che emettono raccomandazioni in materia di gestione finanziaria, di revisione contabile e argomenti affini devono valutare i propri standard di lavoro e le raccomandazioni alla luce del presente studio. L'eliminazione delle divergenze sui concetti e sulla terminologia e quindi l'utilizzo di un linguaggio univoco, avvantaggia tutte le parti interessate.
- *I docenti e i ricercatori* - Il presente studio o modello può essere oggetto di ricerca e analisi in sede accademica al fine di proporre possibili miglioramenti. Una volta che questo studio è accettato come punto di riferimento comune, i suoi concetti e termini devono essere recepiti dai programmi di studio universitario.

Avendo creato con questo modello una base per una mutua comprensione, tutte le parti interessate potranno parlare lo stesso linguaggio e comunicare in modo più efficace. Il management sarà in grado di valutare il processo di gestione del rischio, comparandolo con gli standard, qui definiti, di migliorare l'efficacia del processo in essere e di indirizzare la loro organizzazione verso gli obiettivi definiti. Le ricerche future potranno beneficiare del presente studio come base di riferimento o di partenza. Il legislatore e le autorità di vigilanza potranno meglio comprendere il concetto di ERM, inclusi i suoi vantaggi e limiti. Quando tutte le parti interessate adotteranno un comune modello di gestione del rischio, questi vantaggi si manifesteranno concretamente.