ENTERPRISE RISK MANAGEMENT E LINEE GUIDA DELLO STANDARD ISO 31000

A cura di Corrado Pomodoro e Tommaso Luccini, HSPI

Come nasce l'Enterprise Risk Management

Nell'ultima decade è cresciuto notevolmente l'interesse per le tematiche della gestione del rischio nell'ambito della *Corporate Governance* ed è diventata sempre più evidente la necessità di disporre di un valido modello di riferimento per identificare, valutare e gestire gli eventi e i loro potenziali impatti in modo efficace, al fine di gestire tutte le tipologie di rischio in modo integrato.

L'Enterprise Risk Management nasce a fronte di questa necessità, definito per la prima volta dal *Committee of Sponsoring Organizations* della *Treadway Commission* **(COSO)** istituita su iniziativa del settore privato americano che, sulla spinta dei drammatici eventi del settembre 2001 e del periodo di scandali finanziari e clamorosi fallimenti (Enron, Worldcom, Global Crossing, …) che avevano provocato ingenti perdite a partire dal 2001, sviluppò l'**Enterprise Risk Management – Integrated Framework**. Il noto Sarbanes-Oxley Act del 2002 negli Stati Uniti, fu un ulteriore effetto di quel periodo, emanato al fine di contenere il dilagare di deprecabili comportamenti finanziari.

Anche nel nostro Paese, dopo i tristemente noti crack di Cirio e Parmalat, con la Legge n.262 del 2005 si cercò di porre rimedio attraverso l'introduzione del dirigente "preposto"[1] alla redazione dei documenti contabili per le società quotate in borsa.

Sarbanes-Oxley Act e Legge n.262, evidentemente tendono ad alzare il livello di attenzione della corporate governance sul tema della regolazione e della supervisione delle istituzioni finanziarie e dei mercati finanziari.

Ma i lavori del COSO, sintetizzati nell'Enterprise Risk Management Framework del **COSO Report**, hanno ispirato l'evoluzione di tutti i modelli e **sistemi di controllo interno**[2] degli ultimi anni tra cui, il modello di riferimento definito dal *Comitato di Basilea*, il *Codice di Autodisciplina* per le società quotate in Borsa ("Codice Preda"), il *modello organizzativo* richiesto ai sensi del *D.Lgs. 231* (responsabilità amministrativa e penale delle società per reati compiuti nel loro interesse o vantaggio da amministratori, apicali o loro sottoposti), i controlli per il *contingency management* ed, ovviamente, per la *business continuity*, a protezione da **tutte le tipologie di rischio rilevanti per l'impresa**.

[1] Il "dirigente preposto" deve certificare l'attendibilità dei dati che derivano dalla contabilità e che quindi saranno utilizzati per redigere il bilancio d'esercizio e a tale scopo può utilizzare la funzione di internal audit per "mappare" le procedure contabili e quindi controllare la genesi dei dati contabili che andranno ad implementare prima la contabilità generale e in un secondo momento il bilancio d'esercizio.

[2] Il sistema di controllo interno (SCI) è un insieme di regole, procedure, misure organizzative e tecniche ritenute idonee rispetto agli obiettivi di gestione dei rischi d'impresa. Il SCI può essere, o meno, sviluppato sulla base di un approccio ERM e può includere tutte le tipologie di controlli che l'impresa decide di attuare. Per controllo, in generale, si intende qualsiasi misura tecnologica, procedurale, organizzativa, preventiva e/o reattiva indirizzata a mitigare impatti e/o probabilità di eventi che possano in qualche modo influenzare il raggiungimento degli obiettivi prefissati.

L'ERM ambisce a superare molti dei limiti di una gestione tradizionale dei rischi, a lungo trascurati nella loro importanza, **come quelli dovuti ad una visione settoriale e parcellizzata dei rischi**, che impediva – e impedisce tutt'oggi – di cogliere le correlazioni tra rischi di natura diversa[3] (es.: rischi finanziari e rischi operativi) o della stessa natura ma trattati da unità organizzative distinte (es.: linee produttive diverse), **quelli dovuti alla mancanza di collegamento tra i criteri di valutazione dei rischi** e il cambiamento nelle **strategie** aziendali, quelli dovuti alla mancanza di sensibilizzazione a tutti i livelli dell'organizzazione.

Gestione dei rischi tradizionale	Enterprise Risk Management [ERM]
Rischi come pericoli individuali (visione settoriale)	Rischi valutati nel contesto delle strategie di business
Identificazione e assessment dei rischi	Sviluppo del "portafoglio dei rischi"
Focus su rischi discreti (parcellizzazione dei rischi)	Focus su rischi ***critici*** per l'organizzazione
Mitigazione dei rischi (visione solo negativa)	Ottimizzazione dei rischi (rischi anche come opportunità)
Soglia di rischio	Strategia di rischio
Rischi senza responsabilità	Assegnazione di responsabilità ("risk ownership")
Quantificazione dei rischi non sistematica	Monitoraggio e misurazione dei rischi
"Il rischio non è di mia competenza"	"La gestione dei rischi è di competenza di tutti"

Tabella 1. Tratta da: "Enterprise Risk Management" David L. Olson, Desheng Dash Wu (2008, World Scientific Publishing Co. Pte. Ltd.)

Nonostante questa rinnovata sensibilità si assiste ancora al permanere di comportamenti settoriali e parcellizzati nella gestione del rischio, che portano le organizzazioni a non vedere alcuni rischi e alcune soluzioni, utilizzando in modo non efficiente le risorse.

Il COSO Report e i benefici dell'ERM

Secondo il COSO Report il sistema di controllo interno si caratterizza per i seguenti elementi:

- il controllo è un processo, svolto dal CdA, dai dirigenti e da tutto il personale aziendale, finalizzato a fornire una ragionevole certezza sul raggiungimento degli obiettivi aziendali che rientrano in particolare nelle seguenti categorie:
  - attendibilità delle informazioni di bilancio;
  - conformità alle leggi e regolamenti in vigore;
  - efficacia ed efficienza delle attività operative;
- l'attività di controllo va vista in senso dinamico e cioè va allineata agli obiettivi dell'impresa;
- **il concetto di controllo è strettamente collegato a quello di rischio**, definito come la possibilità che gli obiettivi non vengano conseguiti. In questo contesto, **il concetto di rischio si estende evidentemente ben oltre la tradizionale area finanziaria**; il controllo interno è attività che coinvolge tutti i soggetti

[3] Una classificazione delle tipologie di rischio deriva dagli accordi di Basilea2:
- -Rischio di Credito: "rischio riscontrato nell'ambito di un'operazione creditizia nel quale un debitore non assolva anche solo in parte ai suoi obblighi di rimborso di capitale e di pagamento degli interessi al suo creditore"
- Rischio di Mercato: "consiste nella possibilità che variazioni dei tassi di cambio, dei tassi di interesse o dei prezzi commodity possano influenzare negativamente sul valore delle attività, delle passività o dei flussi di cassa attesi"
- Rischio Operativo: "rischio di perdite a causa di inadeguati processi interni, errori umani, carenze nei sistemi operativi o a causa di eventi esterni". Alcuni esempi di fattori di rischio operativo:
  - Risorse Umane: esempio di UBS Warburg nel dicembre 2001 che subì una perdita di 50 milioni di dollari sul suo portafoglio azionario giapponese a causa di un errore di inserimento dati
  - Sistemi informatici: Denial of Service, perdita di dati, …

attivi nell'impresa: dal consiglio di amministrazione al personale in genere, dai livelli più alti a quelli inferiori.
- il controllo interno diviene **efficace se esiste la percezione di esso come parte integrante dell'attività** di impresa e non come adempimento sostanzialmente improduttivo;
- il controllo interno non è costituito solo dalle strutture di poteri e deleghe, dalle procedure, dai manuali o dagli organigrammi, ma anche dai **comportamenti e dalle attività delle persone**. Ciò ne costituisce anche il limite: la flessibilità e la discrezionalità connesse con l'intervento umano comportano che il controllo interno non possa assicurare in assoluto il conseguimento degli obiettivi prefissati.

Il sistema di controllo descritto nel COSO framework, nella sua rivisitazione del 2007, è costituito da 8 componenti interconnessi e integrati con i processi gestionali. Tutti i componenti devono coesistere affinché il sistema di controllo sia efficace:

- **Internal Environment** (consapevolezza dell'ambiente, cultura manageriale)
- **Objective Setting** (definizione obiettivi di controllo in linea con le strategie aziendali)
- **Event Identification** (processi di identificazione e registrazione degli eventi rilevanti)
- **Risk Assessment** (processi per individuare e valutare i rischi)
- **Risk Response** (processi per gestire i rischi individuati)
- **Control Activities** (insieme dei controlli selezionati per la gestione dei rischi)
- **Information & Communication** (processi per la comunicazione inerente ai rischi)
- **Monitoring** (processi di verifica di efficienza ed efficacia dei controlli)

L'Enterprise Risk Management promuove il paradigma di una gestione organica ed integrata di tutte le tipologie di rischio, mettendo in relazione i componenti di cui sopra, secondo tutte le **dimensioni aziendali** (unità di business, divisioni, gerarchie), con gli **obiettivi aziendali**: **strategici, di efficacia ed efficienza operativa, di attendibilità del reporting aziendale (es. informazioni di bilancio), nonché di conformità alle leggi e regolamenti in vigore.**

Uno dei benefici dell'ERM è evidentemente

Figura 1. COSO Framework

la maggiore capacità di individuare rischi ed opportunità e/o strategie di risposta che solo una vista d'insieme, non settoriale secondo una sola dimensione di rischio (es. finanziario), consente. Riportiamo di seguito due casi, citati nel saggio "Nuovi approcci di gestione dei rischi d'impresa: verso l'integrazione tra imprenditore e management" (Barbara Gaudenzi, 2006), esemplificativi ma non esaurienti di quanto detto. Il rischio finanziario, che incide sulla stabilità

finanziaria dell'azienda è legato sull'equilibrio tra flussi di cassa in ingresso ed uscita. L'accordo di Basilea2 (per il settore bancario) ha individuato tre tipologie di rischio finanziario: rischio di credito, rischio di mercato, rischio operativo. Si pensi ad esempio alla gestione del credito e del debito di fornitura, cioè alle dilazioni di pagamento concesse ai propri clienti (crediti di fornitura) e parallelamente concesse dai propri fornitori (debito di fornitura). La gestione della forbice tra tali crediti e tali debiti genera o assorbe liquidità a seconda della durata delle dilazioni, con evidenti effetti in ambito finanziario. La manifestazione di rischi nella gestione della liquidità può dipendere da cause diverse, imputabili ad esempio a specifiche scelte di gestione da parte dei sales manager o da parte dei buyer. Tutto ciò denota come per gestire adeguatamente il *rischio finanziario* si rende necessaria l'integrazione tra la finanza e le altre funzioni deputate all'assunzioni di scelte strategiche ed operative.

Un altro esempio può essere rappresentato dalla gestione del magazzino ed alla relativa politica delle scorte (*rischio operativo*). E' noto che il mantenimento di elevati livelli di scorte comporta un incremento dei costi di gestione del magazzino e un rischio di deperimento dei beni conservati. Inoltre, un elevato stoccaggio di prodotto finito comporta generalmente una minor flessibilità di risposta al mercato o una mancanza di trasparenza delle informazioni.

Per tutto quanto è stato introdotto fino ad adesso risulta chiaro come una gestione del rischio organica e sistemica si rifletta in una forte capacità da parte dell'organizzazione a reagire in modo rapido e flessibile ai potenziali eventi che possono rappresentare rischi od opportunità. Tutto ciò si traduce, da una parte in un vantaggio competitivo rispetto ai competitor, dall'altra nella maggiore fiducia da parte degli stakeholder. E' bene sottolineare soprattutto quest'ultimo punto considerando come l'obiettivo primo di qualsiasi organizzazione è proprio quello di creare valore per i propri investitori.
L'approccio dell'ERM, fortemente integrato nell'organizzazione, facilita il coinvolgimento di più livelli aziendali nella realizzazione del processo di gestione del rischio. Infatti, se l'alta direzione interviene nella definizione degli obiettivi strategici, il management si occupa della identificazione di eventuali contromisure da attuare a seguito del verificarsi di minacce od opportunità, mentre i risk owner (individuati negli owner dei processi operativi di business) contribuiscono alla creazione di mappe di rischio per ciascun processo core dell'organizzazione.

I benefici in questo senso sono vari: il primo è che si assiste alla correlazione degli obiettivi strategici, stabiliti dall'alta direzione, con le iniziative intraprese nell'ambito delle attività operative per la riduzione del rischio; il secondo è che si è avviato un percorso di integrazione e comunicazione delle politiche di gestione del rischio all'interno di tutta l'organizzazione in modo da sensibilizzare e responsabilizzare le persone verso un approccio di ERM.

Riportiamo di seguito un esempio di policy di risk management, copiato e tradotto dal sito web del colosso **BHP Group** (http://www.bhpbilliton.com/home/aboutus/ourcompany/Documents/Risk%20Management%20Policy.pdf), che riflette pienamente gli intenti di ERM:

- La capacità di comprendere e gestire i rischi aumenta la fiducia di stakeholder, impiegati, clienti e fornitori.
- Una gestione del rischio efficace può rappresentare un vantaggio competitivo.
- I rischi a cui è esposta l'organizzazione devono essere gestiti in maniera organica ed integrata.
- La gestione del rischio deve essere integrata nelle attività, nei processi e nelle funzioni di business critiche per l'azienda. Il processo decisionale deve prendere in considerazione elementi quali la comprensione e la tolleranza al rischio.
- I controlli per la gestione dei rischi devono essere progettati ed attuati al fine di assicurare il raggiungimento degli obiettivi aziendali. L'efficacia dei controlli deve essere sistematicamente revisionata e, dove necessario, migliorata.
- Le prestazioni della gestione del rischio devono essere monitorate, revisionate e comunicate. La supervisione dell'efficacia

dei processi di gestione dei rischi, darà maggiore fiducia al management e agli stakeholder.

Firmato Chip Goodyear

NdR: attraverso la diffusione in tutta l'organizzazione della cultura del rischio è stato ridotto drasticamente la dimensione del dipartimento: *3 persone, guidate da Grant Purdy, in 4 anni di lavoro hanno impostato e portato a regime l'ERM della BHP, 200.000 impiegati, 80.000 risk owner e 12.000 risk assessment.*

ISO31000 - Linee guida per l'attuazione di un ERM

Esistono diverse best practice, framework e standard di Enterprise Risk Management. COSO ne è un esempio, la ISO 31000, più recente, ne è un altro.

La ISO 31000 si propone, in effetti, come una **linea guida** piuttosto che come uno standard finalizzato ad una certificazione. **La ISO recepisce molti dei principi dell'ERM contenuti nel COSO** e si basa sulla consolidata esperienza dello standard neozelandese AS/NZS 4360:2004, di cui rappresenta l'evoluzione.

Riteniamo utile richiamare gli elementi chiave dei tre capitoli su cui si incardina la ISO: ***i principi, il framework, i processi.***

ISO31000 - I principi

a. Il *Risk Management crea e protegge valore.* Contribuisce ad un misurabile raggiungimento degli obiettivi e al miglioramento delle prestazioni.
b. *Il Risk Management è parte integrante di tutti i processi aziendali.* Non è un processo stand-alone, è parte delle responsabilità del management e parte integrante di tutti i processi aziendali dalla pianificazione strategica ai processi di gestione di progetti e cambiamenti.
c. *Il Risk Management è parte integrante dei processi decisionali.* Aiuta a prendere decisioni più consapevoli, a dare priorità alle azioni e a distinguere tra diverse alternative.
d. *Il Risk Management indirizza l'incertezza.* Poiché tiene di conto dell'incertezza, della sua natura e di come può essere affrontata.
e. *Il Risk Management è sistematico, strutturato e puntuale.* Un approccio sistematico, strutturato e puntuale contribuisce all'efficienza, alla consistenza, alla confrontabilità e alla ripetibilità dei risultati.
f. *Il Risk Management è basato sulle migliori informazioni disponibili.* Gli input alla gestione dei rischi sono basati su diverse fonti quali dati storici, esperienze, riscontri degli stakeholder, osservazioni, previsioni, pareri esperti. Chi prende decisioni deve considerare tutti i limiti dei dati utilizzati e le possibili divergenze tra esperti.
g. *Il Risk Management è customizzato.* E' allineato al contesto interno ed esterno e al profilo di rischio della realtà.
h. *Il Risk Management prende in considerazione fattori umani e culturali.* Riconosce le capacità, le percezioni e le intenzioni di persone interne ed esterne all'organizzazione che possono agevolare o intralciare il raggiungimento degli obiettivi.
i. *Il Risk Management è trasparente e inclusivo.* Un appropriato e puntuale coinvolgimento degli stakeholder e di chi prende decisioni a tutti i livelli dell'organizzazione, assicura che il processo di gestione dei rischi sia rilevante ed aggiornato. Il coinvolgimento permette inoltre che gli stakeholder siano opportunamente rappresentati e che i loro punti di vista siano presi in considerazione nella determinazione dei criteri di valutazione dei rischi.
j. *Il Risk Management è dinamico, iterativo e reattivo ai cambiamenti.* Percepisce e risponde ai cambiamenti. Quando si manifestano eventi interni o esterni, cambiamenti del contesto e delle conoscenze, si attua una revisione dei rischi, emergono nuovi rischi, alcuni si modificano altri scompaiono.
k. *Il Risk Management facilita il miglioramento continuo dell'organizzazione.* Le organizzazioni dovrebbero sviluppare ed attuare strategie per misurare e migliorare il loro livello di maturità nella gestione dei rischi così come per tutti gli altri aspetti dell'organizzazione.

ISO31000 - Il framework

Rappresenta l'approccio da adottare per eseguire una corretta gestione e monitoraggio del rischio.

Si compone delle seguenti fasi (N.B.: risulta evidente la correlazione con il ciclo di Deming PDCA):

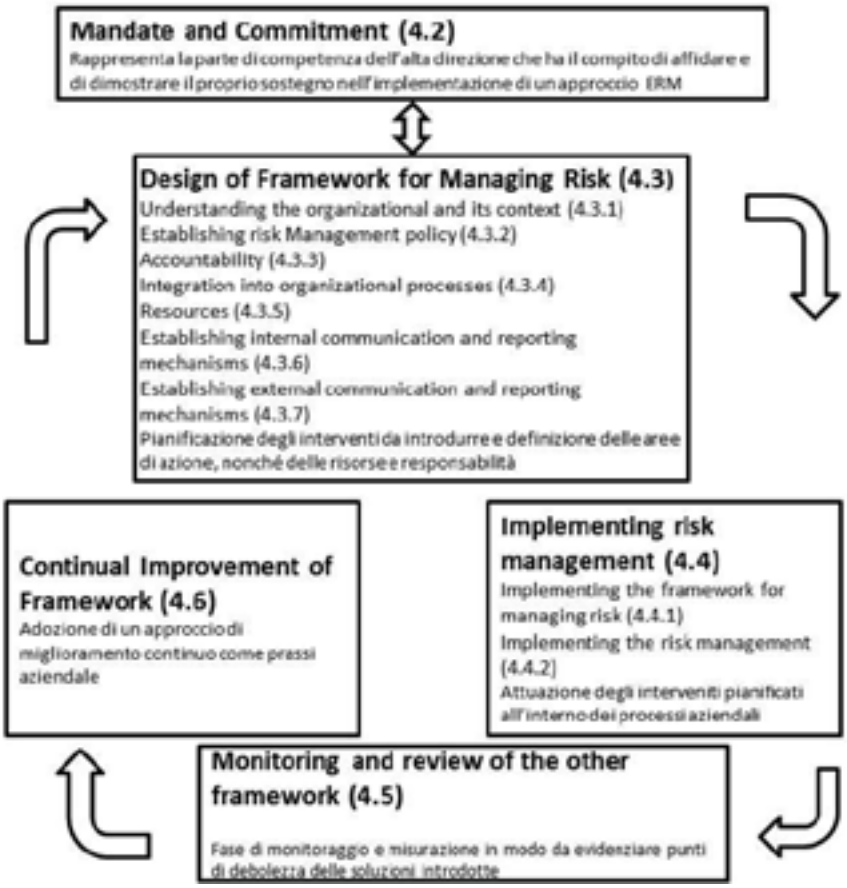

Figura 2. ISO31000 Framework

ISO31000 - I processi

Il processo è scomposto nelle attività rappresentate nella figura sottostante (Risk Management Processes ISO 31000:2009).

In particolare, le attività di Risk Assessment descritte dalla clausola 5.4 della ISO31000, sono oggetto di approfondimento nello standard internazionale ISO/IEC 31010.

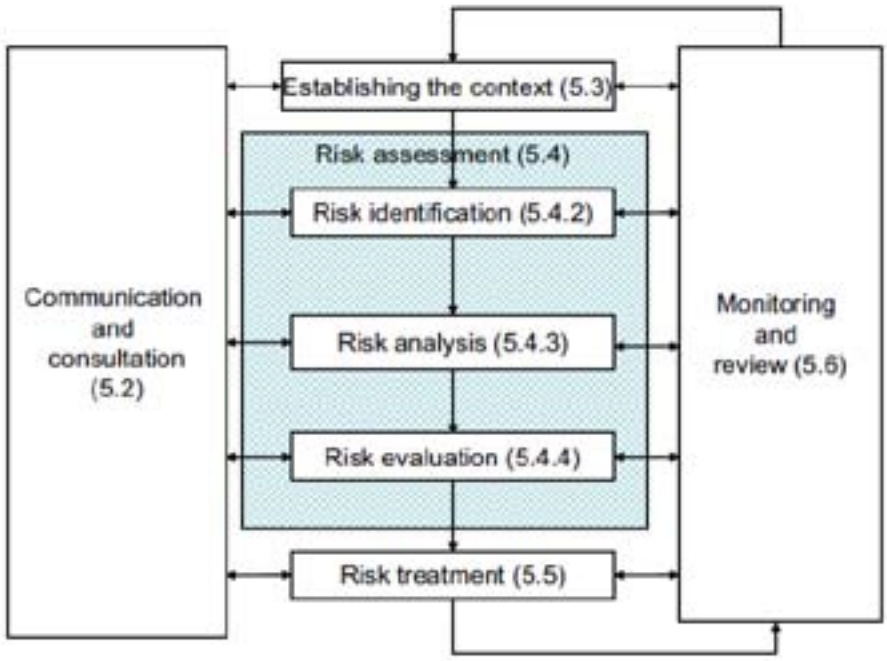

Figura 3. ISO31000 Processi

I ruoli nell'Enterprise Risk Management

La ISO31000 non entra nel merito del modello organizzativo ma sostiene con decisione la necessità della integrazione delle attività che supportano il processo all'interno di tutti i processi operativi aziendali, responsabilizzando i diversi ruoli già esistenti rispetto al framework di gestione dei rischio.

Questo approccio elimina o, almeno riduce in modo consistente (*come dimostra il sopracitato caso del BHP Group*), la necessità di una struttura organizzativa preposta alla gestione dei rischi, demandando alla funzione di audit il compito di monitorare il funzionamento del sistema individuando le aree di sofferenza e/o di eccellenza e alle altre funzioni di management il compito di progettare e attuare i controlli con sistematicità e integrazione.

Tuttavia permane l'esigenza di promuovere, assistere, facilitare, coordinare, consolidare i risultati, le prassi, i meccanismi, le strategie, gli strumenti che sostengono e alimentano il processo integrato a tutti i livelli aziendali, attraverso una funzione autorevole di ***Chief Risk Officer***. Inoltre è fondamentale che il sistema di controllo interno sia fatto evolvere in linea con i cambiamenti esterni ed interni.

Questi concetti ci sembrano particolarmente ben rappresentati nel semicerchio che riportiamo di seguito realizzato dall'associazione IIA (The Institute of Internal Auditors) nel "*IIA position paper: The Role of Internal Auditing in Enterprise-wide Risk Management*" (gennaio 2009).

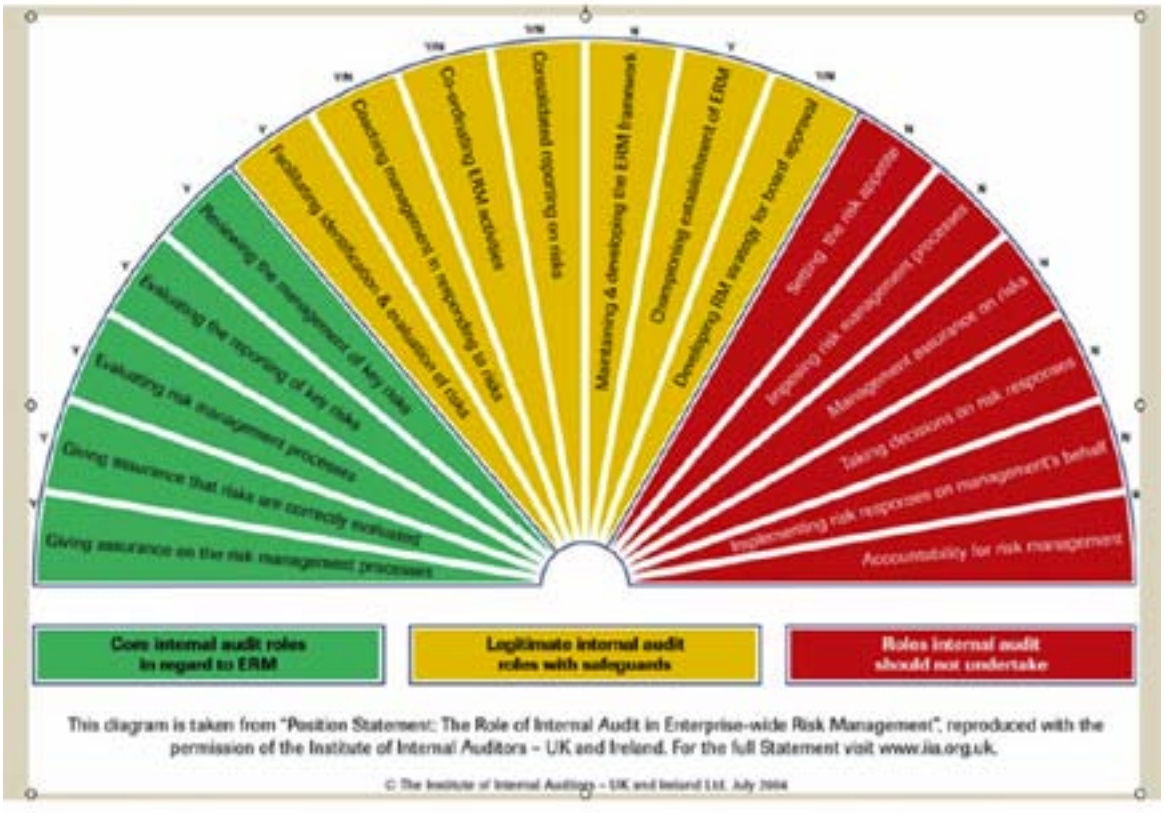

Figura 4. Diagramma delle responsabilità (IIA)

In questa figura, gli spicchi a sinistra del semicerchio elencano le responsabilità che più tipicamente sono della funzione di Audit, gli spicchi a destra del semicerchio elencano le responsabilità distribuite a tutti i livelli di management dell'organizzazione ed, infine, le responsabilità riportate negli spicchi centrali possono essere prerogativa della sopra citata funzione di **Chief Risk Officer**.

Ulteriore fattore di successo per l'ERM, insieme all'allineamento con gli obiettivi strategici, è l'allineamento delle funzioni di assurance che insieme al CRO, laddove istituito, devono garantire un'efficace ed organico sistema di monitoraggio per l'identificazione delle aree di sofferenza e di miglioramento: **Audit** (interno od esterno), **Consiglio di Amministrazione, Organismo di Vigilanza, Dirigente preposto, Collegio sindacale, Information Security, Safety.**

L'integrazione non si esaurisce qui: essendo l'ERM un sistema profondamente radicato in tutti i livelli organizzativi, assume particolare importanza il coinvolgimento ed il sostegno delle funzioni Risorse Umane ed Organizzazione e il loro contributo attivo nella revisione ed integrazione degli assetti organizzativi, delle mansioni, delle politiche aziendali per la gestione dei rischi. Ne va dell'efficacia dell'ERM stesso.

HSPI SpA - Consulenti di Direzione
Viale Aldo Moro 16 - 40127 Bologna (Italy)
P.IVA 02355801206

Tel. +39 051 2960545 | Fax. +39 051 6568695
BOLOGNA | MILANO | ROMA
www.hspi.it | e-mail: info@hspi.it