© ISTOCK - LEO WOLFERT

Luci e ombre dell'enterprise risk management in Italia

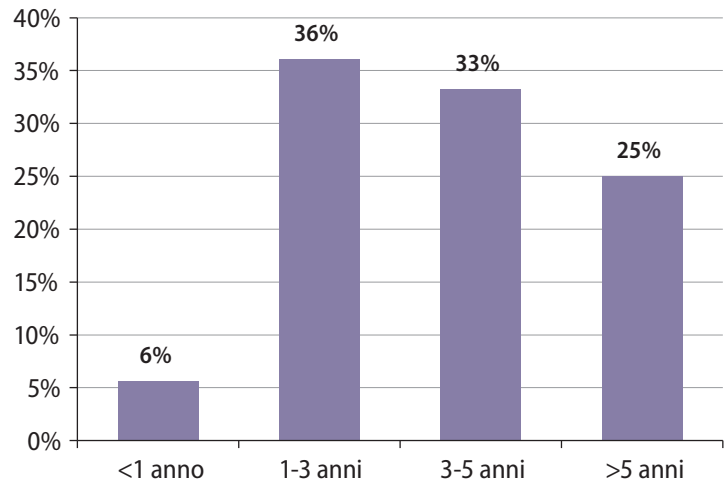
È oggetto di crescente attenzione all'interno delle aziende non solo per ragioni di compliance, ma anche per una migliore comprensione e gestione dei rischi in toto

di Massimo Livatino e Paola Tagliavini

Quanto è diffuso il risk management in Italia, e che livello di maturità ha raggiunto? Quali sono le ragioni che ne hanno incentivato l'adozione nelle imprese, e quali benefici ha effettivamente determinato? Ancora, quali ulteriori miglioramenti sono possibili nel prossimo futuro? Sono alcune delle domande al centro della terza indagine sullo stato dell'arte dell'ERM (*enterprise risk management*) in Italia (1), condotta nei primi mesi del 2016 dal Lab ERM della SDA Bocconi, in collaborazione con KPMG. La survey, inserita in un filone di ricerca intrapreso dal Lab ERM a partire dal 2010, ha coinvolto oltre 240 società quotate MTA e AIM operanti in ambito non finanziario, con un tasso di risposta del 20 per cento. I 49 quesiti della survey erano focalizzati principalmente sulle soluzioni organizzative adottate dalle imprese in tema di risk governance, evidenziando ruoli e responsabilità degli attori coinvolti nell'attività di risk management, nonché sugli approcci prescelti nelle diverse fasi dei processi di gestione del rischio: assessment, treatment, monitoring e reporting. Di seguito verranno presentate le principali evidenze emerse dalla survey, per pervenire quindi ad alcune conclusioni sulle prospettive future dell'ERM in Italia.

(1) L'ERM 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 e progettato per:
- individuare eventi potenziali che possono influire sull'attività aziendale;
- gestire il rischio entro i limiti del rischio accettabile;
- fornire una ragionevole sicurezza sul perseguimento degli obiettivi aziendali.

figura 1 | da quanti anni è stata istituita la funzione di ERM?



La diffusione dell'ERM

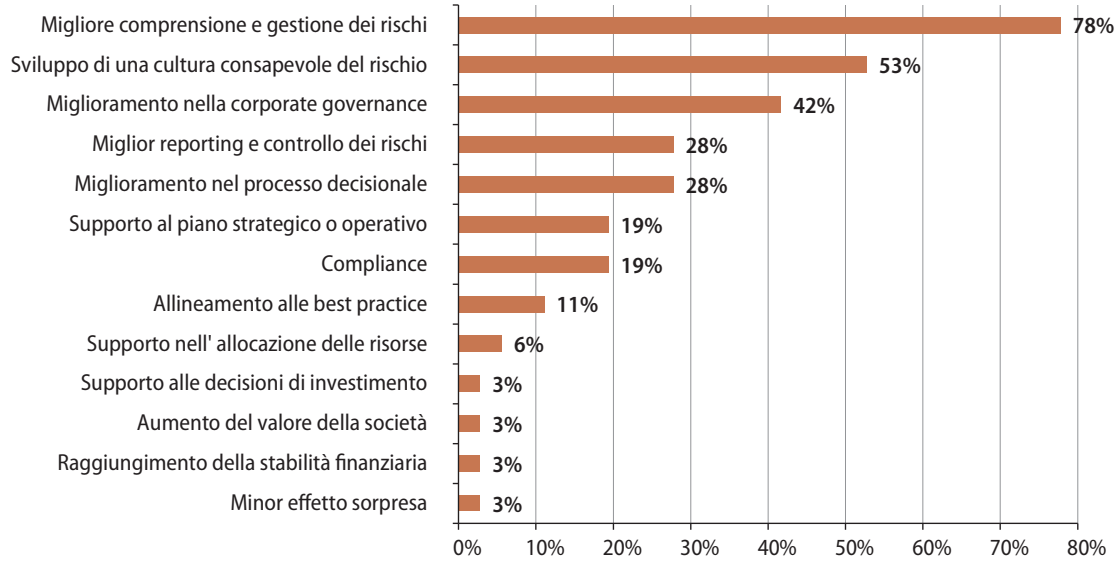
Stando alla survey, la funzione di ERM risulta sempre più diffusa nelle organizzazioni. Il 73 per cento dei rispondenti ha istituito una funzione di questo genere (+26 per cento rispetto ai dati della ricerca Lab ERM del 2012); tuttavia, non di rado tale responsabilità è posta in capo alla funzione di internal audit e solo in circa il 20 per cento dei casi il mandato di ERM è attribuito a una specifica funzione a cui è riconosciuto il titolo di Chief Risk Officer (percentuale ancora inferiore rispetto ai valori riscontrabili a livello internazionale) (2).

Un altro dato riguarda il timing dell'introduzione dell'ERM. La diffusione dell'ERM è relativamente recente (Figura 1): tra chi ha istituito la funzione di ERM, più del 40 per cento lo ha fatto negli ultimi tre anni, in particolare le aziende di dimensioni minori. Anche la maggior parte di chi non ha ancora istituito la funzione di ERM dichiara che lo farà nei prossimi tre anni. Nel segmento STAR la funzione di ERM è più giovane rispetto alle altre società del MTA ed è prevista un'ulteriore, significativa diffusione nell'immediato futuro.

Nella decisione di istituire la funzione di ERM, le costrizioni regolamentari sono determinanti, specie nelle aziende di minori dimensioni. Tuttavia le aziende si attendono vantaggi concreti dall'introduzione dell'ERM, che eccedono il solo perseguimento di obiettivi di conformità. La compliance normativa non è infatti indicata fra i principali benefici riscontrabili a seguito dell'introduzione dell'ERM; questi ultimi sono invece identificati nella più puntuale comprensione e gestione dei rischi, in una maggiore diffusione di cultura di rischio all'interno dell'organizzazione e in un complessivo miglioramento della corporate governance (Figura 2).

(2) KPMG, *CRO Survey. Chief Risk Officers' Role in Creating Value*, 2016; AON, *Global Risk Management Survey*, 2015.

figura 2 | benefici attesi dall'ERM



La risk governance

Se si considerano gli aspetti relativi alla risk governance, va innanzitutto osservato che i responsabili di ERM godono di un buon grado di autonomia: in continuità con evidenze raccolte nella survey Lab ERM del 2012, il 50 per cento degli stessi risponde gerarchicamente al Chief Executive Officer o al Chief Financial Officer, mentre la rimanente percentuale si distribuisce variamente fra presidenza, affari legali e audit. Il comitato controllo e rischi è invece un rilevante riferimento per il riporto funzionale; rispetto al 2012, si è riscontrata una sostanziale riduzione dei casi di riporto funzionale all'internal audit.

La funzione di ERM è ancora di dimensioni non significative. La numerosità delle risorse dedicate è fortemente correlata alle dimensioni aziendali e alla natura del business. Nella maggior parte delle aziende interpellate – in linea con una tendenza riscontrabile anche in ambito internazionale (3) – la funzione consta di un numero di collaboratori frequentemente inferiore a cinque, con prevalenza di società che coinvolgono non più di due risorse alle dipendenze del responsabile (Figura 3); sono le aziende più grandi e articolate quelle che occupano il maggior numero di risorse nella funzione di ERM, con un 17 per cento di casi che supera i 10 FTEs.

Nell'ambito dei compiti attribuiti ai referenti di ERM, il maggior carico di attività è oggi riconducibile alla gestione del risk assessment, al monitoraggio dello stato di avanzamento delle azioni di *treatment* e alla predisposizione di reporting periodici sui principali rischi e sulle misure di contenimento degli stessi (Figura 4), a evidenza della crescente attenzione attribuita da più strutture al tema del rischio e della criticità della reportistica nei processi di risk management. Da sot-

figura 3 | risorse della funzione di ERM (escluso il responsabile)

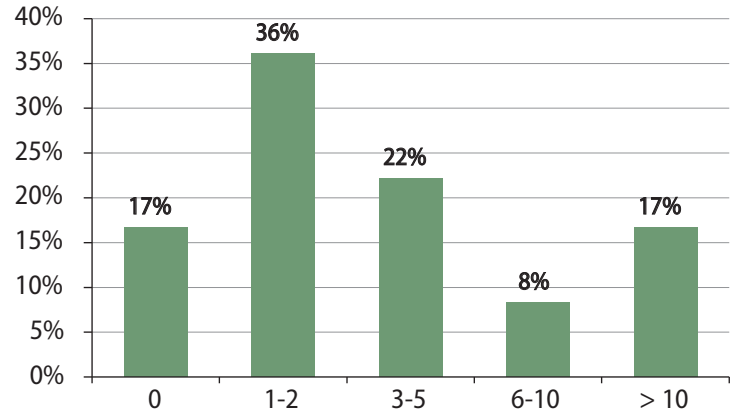
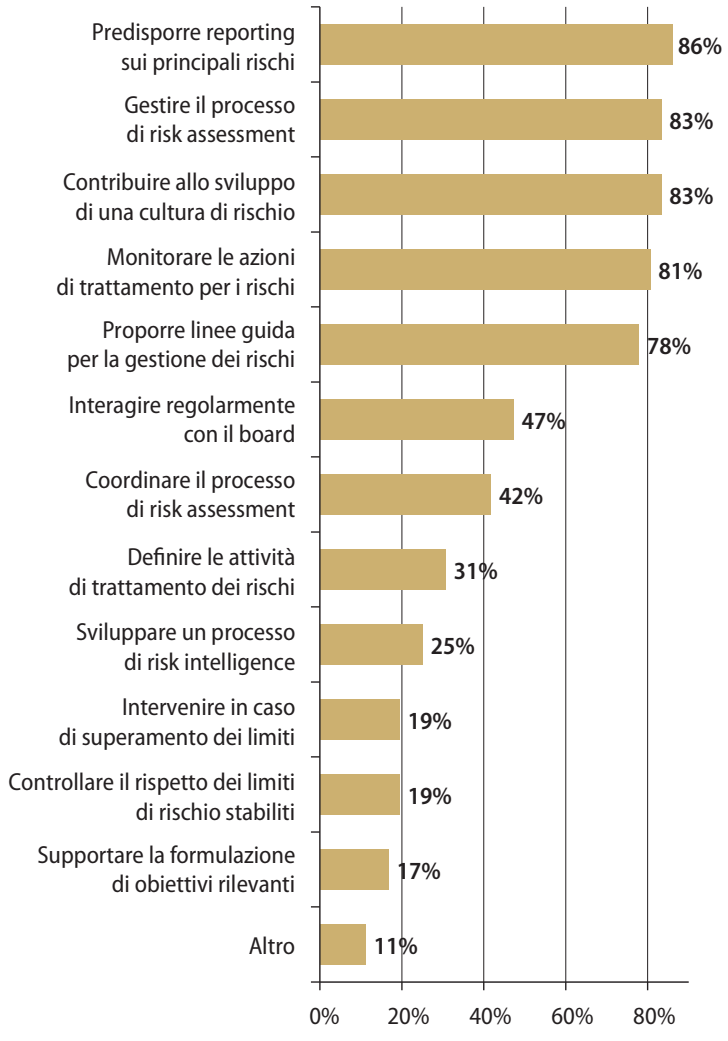


figura 4 | attività del responsabile centrale di ERM



(3) AON, *op. cit.*

tolineare altresì il coinvolgimento dei referenti di ERM nello sviluppo di una cultura di rischio all'interno delle organizzazioni. Tali attività sono coerenti con un percorso di sviluppo dell'ERM che, nella maggior parte delle aziende, è ancora nelle fasi iniziali di introduzione. Le attività più proprie di un ERM in fase di maturità, come per esempio il controllo di limiti di rischio stabiliti, registrano ancora percentuali decisamente basse.

L'81 per cento dei rispondenti, in crescita rispetto alle precedenti indagini, dichiara di adottare modelli integrati di gestione dei rischi ispirati a standard internazionali. In particolare, il CoSO ERM Framework si conferma il principale riferimento (4), con un utilizzo crescente rispetto alle precedenti ricerche, mentre risulta ancora limitata la diffusione dell'ISO 31000.

Le unità specialistiche di rischio sono ancora scarsamente diffuse. Quando istituite, le unità specialistiche mirano principalmente a fronteggiare i rischi finanziari, i rischi legati all'ambiente, alla salute e alla sicurezza, i rischi assicurativi e quelli legati alle ICT. Nella maggior parte dei casi non è previsto riporto delle unità specialistiche, né gerarchico né funzionale, verso il responsabile di ERM.

Il ruolo del board

Nelle attività di risk management, i board hanno un ruolo sempre maggiore. L'80 per cento dei board è formalmente coinvolto nell'approvazione delle linee di indirizzo del sistema di controllo interno e di gestione dei rischi, contro il 40 per cento del 2012, e il 66 per cento dei board ha approvato una policy di gestione dei rischi, contro il 37 per cento del 2012. Secondo quanto dichiarato dai rispondenti, tali percentuali sono destinate a crescere ulteriormente nei prossimi tre anni.

La valutazione dei rischi nella pianificazione strategica appare ancora migliorabile, specie se comparata con il contesto internazionale (5): benché oltre il 70 per cento degli intervistati dichiari di formulare il piano strategico considerando i potenziali rischi a cui è esposto, meno della metà di costoro ha in effetti attivato un processo strutturato in tal senso, prevalendo per contro il mero coinvolgimento informale dei risk manager.

La gran parte dei board definisce limiti di *risk appetite*, specie per i rischi finanziari e i rischi strategici (6). Ben il 21 per cento dichiara di definire limiti per tutti i rischi, mentre solo il 28 per cento dei board non definisce limiti per alcun rischio.

Il ruolo dei comitati

I comitati controllo e rischi in seno al board hanno un'ampia diffusione: in ottemperanza alle indicazioni del Codice di Autodisciplina, la gran parte delle aziende del campione (86 per cento) ha istituito il comitato controllo e rischi; nel 55 per cento dei casi è stato istituito anche il comitato per le operazioni con parti correlate. Per contro, sono ancora poco diffusi i comitati rischi manageriali, presenti con funzioni consultive verso il CEO o il board solo in un terzo delle società interpellate; essi si occupano prevalentemente di rischi finanziari.

Il ruolo della funzione di internal audit

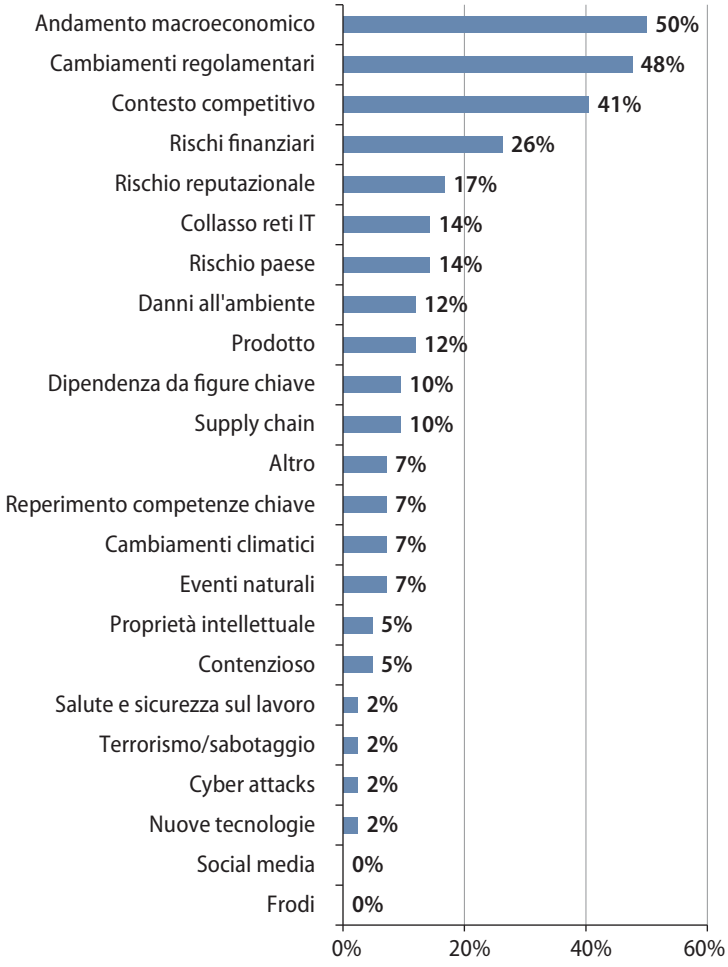
Nel sistema dei controlli la funzione di internal audit rappresenta la terza linea di difesa, con la responsabilità di fornire *assurance* sulla qualità del disegno e sull'effettivo funzionamento del modello di gestione dei rischi. Dalla survey si rileva tuttavia che in numerosi casi la funzione di internal audit non svolge solo un ruolo di garanzia, ma è anche attiva nella gestione del processo di risk management. Tale circostanza deriva dal fatto che un terzo delle aziende – con incidenza elevata nelle imprese di minori dimensioni – ancora attribuisce il mandato di ERM alla funzione di audit. Ciò comporta che l'internal audit affianchi ai propri tradizionali compiti di *assurance* anche le responsabilità operative del processo di gestione dei rischi, in particolare gestisca direttamente il processo di risk assessment e promuova l'implementazione delle azioni correttive. In tal caso la seconda e la terza linea di difesa vengono a coincidere.

(4) Il CoSO ERM framework è il framework di riferimento in tema di ERM più diffuso in ambito internazionale. Il CoSO (Committee of Sponsoring Organizations of the Treadway Commission) è un'organizzazione privata indipendente, creata nel 1985 dalle cinque principali organizzazioni della professione contabile e degli internal auditor americane, allo scopo di rendere operative le raccomandazioni della Treadway Commission in tema di controlli interni e assetti societari.

(5) Chartered Global Management Accountant, *Global State of Enterprise Risk Oversight. Analysis of the Challenges and Opportunities for Improvement*, 2015.

(6) Il *risk appetite* riflette la propensione al rischio dell'azienda, e consiste nel grado di rischio che l'organizzazione è disposta ad assumere per raggiungere i propri obiettivi strategici. Si differenzia dalla *risk tolerance*, che è il livello di perdite potenziali che l'organizzazione sarebbe in grado di assorbire qualora si manifestassero nel perseguimento dei propri obiettivi.

figura 5 | top risk aziendali



Il processo di ERM

Stando alla survey, il processo di risk assessment registra negli anni una diffusione sempre maggiore nelle aziende italiane ed è sempre più strutturato: il 63 per cento del campione, in marcata crescita rispetto al 2012, effettua l'attività di risk assessment in modo sistematico almeno una volta all'anno, e un ulteriore 14 per cento effettua tale attività in modo più saltuario. In oltre il 50 per cento dei casi gli esiti del risk assessment di ERM sono impiegati anche da altre funzioni aziendali, tipicamente internal audit e amministrazione, finanza e controllo, per finalità correlate alle proprie specifiche attività.

Tra le imprese risulta sempre più diffusa la predisposizione dei risk model aziendali, ovvero delle tassonomie di rischio tipiche d'azienda: il 65 per cento del campione ha sviluppato una propria tassonomia.

Nell'ambito delle attività di assessment è cruciale la definizione delle metriche in base a cui selezionare e rendicontare i rischi più critici, che riceveranno poi diversa attenzione tra i soggetti aziendali variamente coinvolti nella gestione degli stessi, in funzione del grado di criticità e dei differenti ambiti di responsabilità. Nella survey è stato chiesto di esprimere il numero dei rischi identificati come «top» e da rendicontare al board. Nell'ultima attività di assessment il 53 per cento del campione ha identificato un numero superiore a 10 top risk e ben il 14 per cento ne ha individuati più di 20. Questi valori, che possono apparire elevati ai fini di una rendicontazione selettiva al board, appaiono in realtà coerenti con fasi iniziali di sviluppo dell'ERM, in cui di frequente i vertici richiedono nei primi anni una rendicontazione piuttosto estesa delle principali criticità rispetto a cui assumere decisioni.

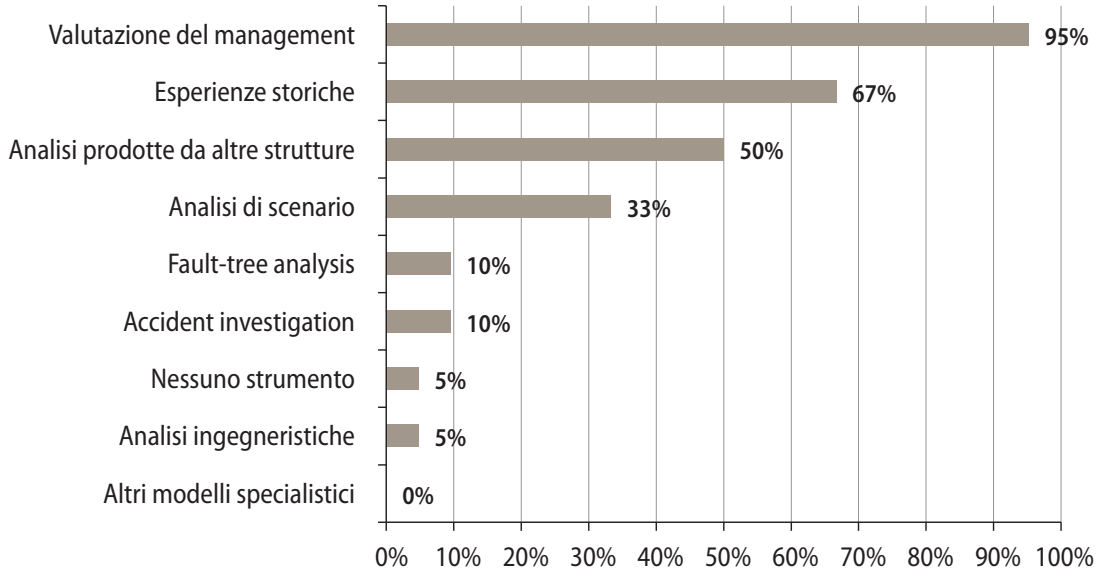
Le attività di assessment evidenziano che i rischi che più preoccupano le imprese sono di origine esterna (Figura 5): andamento macroeconomico, cambiamenti regolamentari, contesto competitivo. Cala, rispetto al passato, la considerazione dei rischi legati alla supply chain, mentre sorprendentemente non sono considerati i rischi connessi ai social media e il rischio di frodi. Un approfondimento meritano senz'altro i rischi legati al sistema ICT (collasso delle infrastrutture e, in particolare, *cyber attacks*), che sono scarsamente considerati dalle imprese italiane nonostante figurino ai primi posti – insieme al rischio reputazionale – tra le maggiori minacce identificate nelle più recenti survey a livello internazionale (7).

Riguardo alle modalità impiegate per identificare e valutare i rischi, le imprese adottano combinazioni di più tecniche, in linea con le best practice internazionali: le più utilizzate sono le interviste individuali, seguite dai questionari e dalle desk review; è invece modesta la rilevanza associata ai workshop e ai focus group con il coinvolgimento di team interdisciplinari.

Per la valutazione dei rischi coesistono tecniche qualitative e quali-quantitative: il 47 per cento del campione adotta approcci quali-quantitativi – in linea con la preferenza riscontrabile a livello inter-

(7) KPMG, *Global CEO Outlook*, 2016; Allianz, *Allianz Risk Barometer. Top Business Risk*, 2016.

figura 6 | supporti nella valutazione dei rischi



nazionale (8) – e circa il 35 per cento, in specie le aziende di minori dimensioni, valuta i rischi ricorrendo ad approcci meramente qualitativi.

La valutazione soggettiva del management è la fonte informativa principale per l'analisi del rischio (95 per cento), seguita dall'esame delle esperienze storiche e dagli esiti di analisi svolte da funzioni specialistiche (IT, safety, security); pochi sono i rispondenti che dichiarano di utilizzare tecniche analitiche, come ad esempio l'*accident investigation* e la *fault-tree analysis* (10 per cento) (Figura 6). Anche tali aspetti sono da giudicare coerenti con fasi iniziali di sviluppo dell'ERM.

Nel 67 per cento dei casi è strutturato un processo di risk reporting periodico sui principali rischi. Tale valore è da valutarsi molto positivamente, perché tempi e modalità con cui è svolta la rendicontazione influenzano notevolmente le percezioni dei rischi e, quindi, la definizione di opportune strategie di gestione. Sono poche le aziende che rendicontano sui rischi solo al verificarsi di particolari eventi.

I principali destinatari dell'informativa di rischio, che in oltre la metà dei casi avviene con periodicità trimestrale o semestrale, sono gli amministratori incaricati (tipicamente il CEO), seguiti dal comitato controllo e rischi (CCR) e dal CFO. Il board viene in genere informato su base annuale. Le informazioni più frequentemente riportate sono i risultati del risk assessment, ma il CEO e il CCR ricevono anche le analisi di approfondimento su rischi specifici, sulle azioni di trattamento previste e sullo stato di attuazione dei piani, mentre il CdA è destinatario dei risultati del processo di monitoraggio.

Il 63 per cento delle aziende, in sensibile crescita rispetto al 40 per cento del 2012, opera il monitoraggio dei principali rischi, prevalentemente tramite la revisione periodica dei piani di trattamento e lo svolgimento di audit. Solo il 26 per cento delle aziende analizza l'evoluzione di *key risk indicators* e ancora più ridotto è il monitoraggio di *risk limits*.

Con frequenza crescente le attività di assessment, reporting e monitoring sono supportate da strumenti informatici; tuttavia, questi ultimi continuano ad assumere prevalentemente la forma di strumenti semplici e software generici (53 per cento), e in misura ben inferiore di tool dedicati (20 per cento).

ERM di qualità: condizioni e ostacoli

Le attività di ERM sono quindi in crescente diffusione in Italia; ma quali sono i fattori che possono garantirne un'efficace implementazione, e quali invece gli ostacoli da affrontare? Tra i primi, il commitment del top management è giudicato come l'elemento principale; altri aspetti rilevanti sono la focalizzazione su un numero limitato di rischi, la promozione dell'integrazione dei processi di gestione dei rischi e la formazione di amministratori e dirigenti. La creazione di comitati interfunzionali non è ritenuta un elemento di rilevante impulso.

Il 55 per cento del campione investe in progetti finalizzati a creare consapevolezza, migliorare la conoscenza e sensibilizzare l'organizzazione sulle tematiche di ERM. Tra le modalità più utilizzate per svilup-

(8) North Carolina State University, *Report on Current State of Enterprise Risk Oversight. Update on Trends and Opportunities*, 2015.

pare una cultura di rischio all'interno dell'organizzazione le più frequenti sono la formazione, di base e personalizzata, e la formulazione di specifiche policy e linee guida aziendali. Ancora poche (14 per cento) le aziende che ricorrono ad attività di *board induction* sul tema della gestione dei rischi. Risultano inutilizzati sistemi di misurazione delle performance e incentivi remunerativi collegati all'ERM.

Le principali barriere all'introduzione dell'enterprise risk management sono proprio di natura culturale: in particolare dalla survey emergono la non chiara percezione dei benefici che ne derivano e la sottostima del valore aggiunto correlato alla sua adozione; diversamente dal passato, la carenza di risorse da destinare allo scopo non è più percepita come ostacolo particolarmente rilevante. Significative sono le differenze con lo scenario internazionale, ove considerazioni di costo/opportunità identificano la più rilevante barriera nella scarsità di risorse in presenza di altre priorità.

E quindi...

Dall'analisi dei dati raccolti, appare evidente come le società italiane dedichino crescente attenzione al tema dell'ERM, considerato processo necessario per assumere e gestire adeguatamente i rischi, per raggiungere obiettivi strategici definiti in presenza di contesti di riferimento dinamici. Dall'ERM, pur solitamente introdotto per esigenze di compliance, le aziende si attendono vantaggi concreti quanto alla comprensione e gestione dei rischi da fronteggiare.

Anche se il divario con il contesto internazionale si è ridotto, restano da compiere ulteriori passi, specie riguardo al formale coinvolgimento del referente di ERM nel processo di pianificazione strategica, all'integrazione della gestione dei rischi nei processi di business, all'aumento dei dati a supporto dei processi di risk analysis, alla separazione della responsabilità dell'ERM dalla funzione di internal audit.

Grande attenzione dovrà altresì essere posta alla più puntuale e tempestiva identificazione di nuovi fattori di vulnerabilità per poter valutare le capacità di reazione delle organizzazioni e per poterli mitigare tempestivamente (per esempio, rischi legati alla maggiore complessità sistemica, rischi connessi alla natura dell'economia digitale e all'informatizzazione dei processi, rischi reputazionali), al maggiore ricorso a tool informatici dedicati, all'utilizzo di sistemi di misurazione delle performance e incentivi collegati all'ERM. ■

Esplora e&mplus su www.economiaemanagement.it

In sintesi

La terza indagine sullo **stato dell'arte dell'enterprise risk management** in Italia, condotta dal Lab ERM della SDA Bocconi, evidenzia come la funzione di ERM sia sempre più diffusa nelle organizzazioni, anche se è spesso associata a quella di internal audit.
Le aziende italiane considerano l'ERM un processo necessario per assumere e gestire adeguatamente i rischi e per raggiungere obiettivi strategici.
I rischi che più preoccupano le imprese italiane sono di origine esterna: in particolare andamento macroeconomico, cambiamenti regolamentari, contesto competitivo.
Le principali barriere che ancora ostacolano l'introduzione dell'ERM in Italia sono di natura culturale, come **una scarsa comprensione dei vantaggi che esso può offrire**. In particolare, rispetto al quadro di riferimento internazionale, le aziende italiane sembrano sottovalutare la portata dei rischi legati al sistema ICT (*cyber attacks*).

Massimo Livatino
è docente e ricercatore presso l'Università Bocconi e la SDA Bocconi. È responsabile scientifico dell'Osservatorio di Revisione e Direttore del Lab ERM della SDA Bocconi. È dottore commercialista e revisore legale, e amministratore indipendente, presidente o componente di diversi collegi sindacali e organismi di vigilanza, anche in società quotate.
massimo.livatino@unibocconi.it

Paola Tagliavini
è docente presso l'Università Bocconi e la SDA Bocconi, ed è stata Visiting Researcher presso la Wharton School. È condirettore del Lab ERM di SDA Bocconi. È Managing Partner presso DGPA Risk, revisore legale e amministratore indipendente di diverse società quotate. Ha diretto team specialistici in tema di rischio presso Marsh, Oliver Wyman, AON.
paola.tagliavini@unibocconi.it