NUOVE SINERGIE "TAILOR MADE" PER UN'EFFICACE GESTIONE DEL RISCHIO IN AZIENDA

Come gestire il rischio in azienda? Un rompicapo che spesso non tiene conto di quale rischio gestire. L'analisi preventiva è dunque fondamentale, al fine di individuare i punti di contatto fra due discipline: Risk Management e Governance, Risk e Compliance.

A cura di Riccardo Pandolfi, Manager di HSPI e Corrado Pomodoro, Senior Manager di HSPI

Introduzione

Il rischio è un elemento complesso che accompagna l'impresa lungo tutta la sua esistenza. Ha un impatto su diversi aspetti relativi alla realizzazione delle strategie aziendali e al conseguimento degli obiettivi di business. Per citarne alcuni: processi, immagine aziendale, strutture organizzative, conoscenze e competenze, gestione delle informazioni, sicurezza informativa, continuità operativa.
L'accresciuta importanza che le aziende attribuiscono alla gestione del rischio dovrebbe essere anche accompagnata dalla consapevolezza di "quale rischio" gestire, fondamentale per attuare un'adeguata gestione delle diverse tipologie da fronteggiare quotidianamente e per assicurare che questo avvenga in una visione olistica e cioè considerando tutte le diverse componenti ed esigenze.
Per raggiungere questi obiettivi è necessario un cambio di mentalità. La gestione del rischio deve entrare a far parte della "normale operatività" dell'azienda. Deve quindi essere estesa sia alle funzioni aziendali gestionali per le tipologie di rischio a loro riferibili, che a livello complessivo a specifiche funzioni di risk management, ad oggi presenti prevalentemente in società del settore finanziario e in settori a forte rischio per la comunità (ad esempio in ambito sanità, energia, ecc.).
La gestione del rischio deve quindi essere considerata fra i processi aziendali con tutto ciò che ne consegue: chiare responsabilità, conoscenze e competenze, metodologie, regole e procedure, strumenti per assicurare una completa ed adeguata presa in carico e gestione dei diversi rischi nel loro ciclo di vita.

Risk Management e GRC - Governance, Risk & Compliance

Spesso si usano termini e locuzioni come risk management, risk assessment, risk analysis o, il più recente, GRC - Governance, Risk & Compliance, senza una chiara distinzione.
I più diffusi standard e best practice, come ISO 31000, ISO/IEC 27005 o il COSO framework, sono concordi nel definire "**Risk management**" come il complesso dei processi di **definizione del contesto** di riferimento, di **assessment**, di **trattamento** e **accettazione**, di **monitoraggio** e **comunicazione** dei rischi.
Il processo di Risk assessment a sua volta è di norma scomposto in risk identification, attività volta ad individuare i fattori di rischio ai quali l'azienda è sottoposta nello svolgimento delle proprie attività (minacce, vulnerabilità, controlli esistenti), risk analysis per l'analisi complessiva di tali rischi (calcolo delle probabilità e degli impatti), risk evaluation per valutare le necessità ed opzioni di trattamento e l'accettabilità dei rischi residui. Ha quindi come obiettivo "…. *to provide evidence-based information and analysis to make informed decisions on how to treat particular risks and how to select between options*", come descritto nello standard IEC/ISO 31010.

Spesso si distingue anche tra IRM (Information Risk Management) ed ERM (Enterprise Risk Management), al fine di meglio specificare il perimetro di riferimento. Il primo – **IRM** - ha come perimetro di riferimento la gestione del rischio associato alla sicurezza delle informazioni (riservatezza, disponibilità, integrità, ecc.) e ha come framework di riferimento ad esempio COBIT 5 o ISO/IEC 27005); il secondo - **ERM** - è rivolto a tutte le tipologie di rischio aziendale, con framework

di riferimento il C.O.S.O. - Committee of Sponsoring Organizations of the Treadway Commission ed ISO 31000 (*si veda anche questo articolo* ***http://www.hspi.it/enterprise_risk_management_e_linee_guida_dello_sta.html***).

Con **Governance**, **Risk** e **Compliance**, si fa riferimento ad un approccio che mira ad integrare i processi di Governance aziendale, di gestione dei rischi e di gestione della conformità (a normative di legge, regolamenti, policy e procedure interne).
Esso ha quindi un'accezione più ampia del Risk management e mira ad assicurare una maggiore efficienza nei processi di governance e management supportando le attività di controllo - Sistema dei Controlli Interni - con una base di dati ed informazioni consolidata. L'acronimo "**GRC**", a quanto sembra usato per la prima volta da Gartner, è quindi spesso associato ad una categoria di **strumenti software** che hanno l'obiettivo di supportare attraverso una piattaforma unica ed una base dati consolidata, i processi di governance, risk management e compliance aziendale. Può essere specifico (ad esempio in ambito finanziario o IT) o esteso a tutti gli ambiti aziendali (ERM).
Gli strumenti GRC includono, tra le altre, funzionalità di:

- gestione documentale (per documentare e distribuire opportunamente policy e procedure interne, normative di riferimento, processi aziendali – in relazione con il sistema qualità aziendale);
- modellazione e classificazione degli asset;
- risk assessment;
- compliance assessment;
- registro dei rischi (eventi ed incidenti significativi);
- monitoraggio dei piani di remediation;
- reporting e cruscotti direzionali.

Tali strumenti si sono particolarmente sviluppati soprattutto nel corso degli ultimi anni, per rispondere a specifiche situazioni che hanno portato ad una richiesta crescente da parte delle aziende *(ad esempio per la Legge Sarbanes – Oxley in USA e Legge 262/05 in Italia, D. Lgs 231/01, incremento dell'attenzione alla gestione dei rischi aziendali, ecc.)* ed alla necessità di riuscire a creare dei **modelli di gestione integrata dei rischi e della compliance**.

Caratteristica comune agli strumenti GRC e agli strumenti di supporto al Risk management, è la loro utilità nell'automazione di molte delle attività inerenti alle fasi di assessment (dei rischi e/o della compliance), fornendo basi precostituite e personalizzabili di rischi, eventi, normative, controlli e contromisure, al fine di analizzare e valutare la probabilità di accadimento dei rischi e gli scostamenti tra il sistema dei controlli esistente ed obiettivo.

Le principali tecniche di Risk Assessment Management e GRC - Governance, Risk & Compliance

Sono presenti diverse tecniche di risk assessment, da quelle più specifiche per determinati settori o obiettivi, a quelle più generiche (per scopi legati all'ERM o all'IRM).
Occorre precisare che non è possibile indicare quale sia la migliore, quella valida sempre, in quanto la scelta del metodo e della tecnica dipenderà dal contesto di riferimento e dalla accuratezza e dettaglio da ottenere rispetto ai principali step del processo di risk assessment (risk identification, risk analysis e risk evaluation) e con riferimento ai fattori influenzanti tale processo (tra gli altri, la complessità del metodo utilizzato, la natura ed il livello delle informazioni disponibili, le risorse da impiegare nelle attività, la loro esperienza professionale, le tempistiche definite, i costi, ecc.). Tuttavia, in generale, come indicazione di massima è possibile segnalare che, a prescindere dalle diverse tecniche e metodi utilizzati, le principali informazioni che dovrebbero essere gestite riguarderanno i seguenti aspetti:

- definizione dei requisiti e degli obiettivi del processo;
- descrizione dei vincoli;
- analisi delle minacce e del loro impatto;
- individuazione della probabilità di accadimento;
- identificazione dei controlli e delle contromisure
- descrizione della conformità ai requisiti ed agli obiettivi;
- individuazione del rischio residuo.

A titolo di riferimento, segnaliamo che lo standard ISO/IEC 31010 riporta 31 strumenti e tecniche, con indicazione, nella tabella A.1, della loro applicabilità all'interno del processo di risk assessment.

Cosa contraddistingue uno strumento di Risk assessment da uno strumento GRC

In base a quanto sopra descritto, quali valutazioni ulteriori dovrebbero essere fatte per indirizzare la scelta di uno strumento a supporto della gestione dei rischi?
Meglio scegliere uno strumento di risk assessment o un più evoluto e completo GRC?

Evidentemente la decisione dipenderà dagli obiettivi a breve termine, da quelli di medio e lungo e dalla disponibilità di budget.
Nell'ambito più generale della gestione dei processi aziendali, uno strumento GRC comprende ed estende le capacità e funzioni di uno strumento di risk assessment, con costi evidentemente crescenti.
Molti degli strumenti di risk assessment stanno evolvendo in strumenti GRC, riconoscendo l'impellenza della compliance e la necessità di fornire "evidenza" della buona governance dei controlli interni (due diligence).
Ulteriore elemento da tenere in considerazione per la scelta è la principale prerogativa dello strumento in termini di tipologie di rischio. Sebbene la maggior parte degli strumenti GRC consenta una gestione di diverse tipologie di rischio (in coerenza con un processo ERM), è anche vero che ciascun di questi ha una genesi spesso ben identificata che può essere quella di gestione dei rischi finanziari, di rischi legati alla sicurezza delle informazioni o di rischi di compliance normativa.
In funzione della natura del business aziendale, della maggiore o minore pervasività e dipendenza dai Sistemi informativi, della complessità normativa, sarà quindi possibile confrontare e selezionare con consapevolezza la migliore soluzione.

Conclusioni

Per sintetizzare quanto sopra brevemente descritto, qualora una società voglia attivare un progetto di analisi del rischio, per poter indirizzare al meglio le proprie attività ed eventualmente scegliere uno strumento che la supporti, dovrà tenere in considerazione:

- il settore di riferimento e le dimensioni aziendali;
- la natura dei processi e il grado di dipendenza dai sistemi informativi;
- la maturità dei processi e della cultura aziendale in merito alla gestione dei rischi;
- il quadro normativo di riferimento;
- la complessità del sistema dei controlli interni;
- gli obiettivi di breve e medio termine.

Solo la piena consapevolezza delle proprie necessità e degli obiettivi complessivi del progetto potrà orientare correttamente e coerentemente le scelte verso un tipo di processo ed eventualmente uno strumento che possa adeguatamente supportarlo, assicurandone anche una gestione coerente e completa nel tempo.

Fonti:

1. *Magic Quadrant for Enterprise Governance, Risk and Compliance Platforms di Gartner Inc.*
2. *ISO/IEC 27005:2011 - Information technology -- Security techniques -- Information security risk management*
3. *ISO 31000 - Risk management — Principles and guidelines*
4. *ISO/IEC 31010 - Risk management – Risk assessment techniques*
5. *http://blogs.gartner.com/paul-proctor/2013/05/13/why-i-hate-the-term-grc/*
6. *IT Governance e Information Risk Management: un connubio perfetto http://www.hspi.it/itgov_risk_connubio.html*
7. *Enterprise Risk Management e linee guida dello standard ISO 31000 http://www.hspi.it/enterprise_risk_management_e_linee_guida_dello_sta.html*
8. *https://www.bancaditalia.it/vigilanza/normativa/norm_bi/circ-reg/vigprud*

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

Tel. +39 051 509861 | Fax. +39 051 509737
BOLOGNA | MILANO | ROMA
www.hspi.it | e-mail: info@hspi.it