C231

Divisione Legal
di Kreios S.r.l.

C231 PAPERS

L'incidenza dell'*Enterprise risk management* sulle tematiche riguardanti la responsabilità amministrativa dell'ente

Dott. Frivoli Mirko

www.c231.it

Dott. Frivoli Mirko

ABSTRACT

Il presente contributo affronta la sempre più rilevante tematica dell'interpolazione dei MOG 231 con il concetto di rischio aziendale.

*All'interno dell'elaborato viene prestata particolare attenzione all'apporto delle nuove funzioni aziendali dedicate alla gestione del rischio e, segnatamente, su come l'implementazione dell'*Enterprise Risk Management *all'interno di un'organizzazione risulti essere una strategia vincente rispetto alle problematiche connesse alla* compliance *aziendale.*

SOMMARIO: Considerazioni preliminari. La *compliance*. Le tipologie di rischio rilevanti. Il *Risk management.* *Enterprise Risk Management- Integrating with Strategy and Performance*. UNIISO 31000. Punti di interazioni tra le funzioni di ERM e l'implementazione del Modello organizzativo *ex* D.lgs. 231/01. Conclusioni.

Considerazioni preliminari

L'entrata in vigore del D.lgs. 231/01 – che impone una responsabilità diretta dell'ente a fronte della commissione di un illecito riconducibile ad uno o più reati presupposto – ha fatto sì che le società abbiano iniziato a porre un'attenzione maggiore al rispetto di norme tese a prevenire tale tipologia di rischi.

Da un punto di vista teorico, il rispetto della legge e di valori etici dovrebbe rappresentare un "*must*" di tutte le organizzazioni operanti sul mercato. Ciò nonostante, tale asserzione spesso si scontra con la realtà fattuale: in assenza di vincoli normativi, difatti, molte imprese sarebbero propense a perseguire finalità di profitto anche laddove tale agire si ponesse in antitesi col rispetto di principi etici.

In sostanza, fermo restando che la natura dell'ente non è quella di commettere reati, quest'ultimo, a causa di una sempre più complessa gestione del sistema organizzativo interno, può finire per ricorrere a delle *practies* in grado di configurare delle ipotesi di reato.

Per tale ragione, la capacità dell'ente di rendersi protagonista di fatti criminosi ha imposto al legislatore di immaginare un sistema che renda lo stesso punibile rispetto al verificarsi di tali accadimenti. In particolare, la necessità di introdurre la disciplina della responsabilità da reato delle società è venuta in rilievo, in modo esponenziale, al crescere del novero dei reati

riconducibili alle società, anche detti "*White Collar Crimes*". Tanto forte è stato l'incremento di tali reati quanto la volontà dell'intero sistema legislativo di arginarne la commissione.

La *Compliance*.

Prima di procedere oltre nella trattazione, si rende necessaria una breve disamina del concetto di *compliance*.

La nozione di *compliance* aziendale indica, in sostanza, l'osservanza, da parte di tutto il sistema organizzativo gestionale, delle regole riferibili, non solo alla tutela della legalità, ma anche ai profili concernenti il rispetto di codici etici interni, volontariamente adottati dalle organizzazioni attraverso l'individuazione di regole e comportamenti da seguire.

Con riferimento all'analisi dei sistemi di *compliance* (c.d. *Compliance Programs*[1]) sembra doversi prediligere una prospettiva integrata, tesa ad agevolare il flusso di informazioni comuni ai diversi sistemi adottati dall'azienda. In questi termini, attraverso un approccio non solo di tipo formale ma sostanziale, sarebbe possibile adottare, in modo adeguato, sistemi di prevenzione e gestione del rischio capaci di interpolarsi tra loro e, dunque, idonei a captare segnali di diversa natura in modo da aumentare in modo esponenziale la capacità dell'azienda di arginare il rischio.

Le tipologie di rischio rilevanti.

Rispetto alla variegata natura dei rischi rilevanti, può essere proposta, a fini meramente esemplificativi, una classificazione che tenga conto di molteplici fattori.

Tale classificazione può essere effettuata in base:

alla natura interna o esterna all'azienda dell'evento che lo ha originato:

1. Rischi esterni

[1] Col termine di *Compliance Programs* si fa riferimento a quei modelli di organizzazione volti alla prevenzione di possibili frodi e/o illeciti, attraverso una cultura aziendale fondata su comportamenti etici e tramite delle procedure atte a mitigare i suddetti rischi.

2. Rischi interni

al legame con l'andamento economico generale:

1. Rischi sistematici (non diversificabili)
2. Rischi diversificabili (specifici)

agli effetti che producono sulle attività d'impresa:

1. Rischi speculativi
2. Rischi puri

In base alla suddivisione appena individuata, vengono in rilievo modi diversi di valutare e conseguentemente gestire il rischio. Al riguardo, si pensi all'eventuale violazione del trattamento dei dati personali di cui all'art. 35 del Regolamento (UE) 2016/679, alla disciplina sull'antiriciclaggio, dell'anticorruzione, alla materia dell'*antitrust* e al Codice della Crisi di impresa, che prevede che venga effettuata un'accurata analisi rispetto agli indicatori volti a prevenire tale crisi e di definire quindi un modello organizzativo che permetta la rilevazione di quest'ultimi.

Le sempre più complesse relazioni instaurate dalle diverse funzioni aziendali porta, soprattutto nelle grandi organizzazioni, ad avere la necessità di attuare un sistema adeguatamente flessibile, capace di adattarsi nel miglior modo possibile al mutamento delle numerose variabili in gioco.

Nell'analisi dei rischi connessi alla commissione dei reati presupposto riferibili alla responsabilità dell'ente, lo strumento attraverso il quale prevenirne la realizzazione è proprio la creazione di un Modello di Organizzazione, Gestione e Controllo, meglio conosciuto come MOG.

L'adozione di quest'ultimo non ha solo funzione preventiva. Esso, infatti, comporta notevoli vantaggi per le organizzazioni in merito:

- Al rispetto delle tematiche di *compliance*, riuscendo quindi a garantire una sinergia tra le varie procedure aziendali; ai *feedback* derivanti dalle esigenze del mercato, soprattutto in merito a clienti o fornitori che richiedono come criterio specifico

quello di avere dei rapporti commerciali in particolare con chi abbia implementato un modello organizzativo conforme ai requisiti del D.lgs. n. 231/01;

- Alla possibilità di partecipare alle gare pubbliche, in quanto l'adozione di un modello organizzativo conforme al D.lgs. n. 231/01 potrebbe costituire un requisito fondamentale per la partecipazione oppure favorire il raggiungimento di un miglior punteggio ai fini dell'aggiudicazione della gara;
- Al fine di evitare ogni forma di sospensione o interruzione dell'attività aziendale, che costituisce la ragione fondante di una società, la quale potrebbe essere lesa dalle sanzioni di tipo interdittivo o cautelare;
- Alla tutela del Consiglio di Amministrazione e del *management* dall'imputazione della responsabilità per i danni subiti dalla società, come conseguenza della mancata adozione del Modello Organizzativo conforme alle prescrizioni contenute nel D.lgs. 231/01.

Resta fermo che il legislatore quando introdusse tale disciplina non aveva gli elementi per tenere conto di tutti i processi innovativi che avrebbero portato oggi ad avere organizzazioni sempre più all'avanguardia, capaci di gestire, generare e ricevere una quantità di dati immensa; attività che ricade su tutte le funzioni aziendali (dalla gestione del magazzino, alla contabilità, alla qualità/conformità) e che consente, attraverso una visione olistica di taluni parametri, di aiutare il *top management* nelle decisioni aziendali. Pertanto, le linee guida dettate dal legislatore e di seguito da Confindustria non sono sufficienti operativamente ad assicurare una gestione della mappatura del rischio reato adeguatamente efficace. Ecco che allora si è cercato un modo per rendere quel MOG un "vestito su misura" per l'ente, che riesca ad essere efficacemente valido per la sua funzione principe, ovverosia quella di esimere da responsabilità l'ente.

È da qui che nasce l'integrazione del concetto di *risk management* con quella che è la tematica della responsabilità amministrativa dell'ente.

Dott. Frivoli Mirko

Il *risk management*.

In via preliminare, si rende necessario spendere alcune parole in merito alla nozione di *risk management* e alla sua evoluzione (*Entreprise Risk Management*). Infine, si rende opportuno soffermare l'attenzione brevemente sulla definizione di rischio aziendale, al fine di cogliere al meglio la correlazione esistente tra i due sistemi.

Qualsiasi attività di impresa è connaturata alla nozione di rischio, poiché è, per sua vocazione, creativa ed aleatoria, nonché tesa ad interagire con l'ambiente che la circonda e con il mercato in cui opera.

Il concetto di rischio negli ultimi decenni si è evoluto all'evolversi di fenomeni intrinseci ed estrinseci all'attività aziendale, questo ha fatto sì che con tale mutamento aumentassero in modo esponenziale i rischi riferibili al concetto di responsabilità di impresa.

In particolare, il "sistema dei rischi di impresa", oggi, risulta caratterizzato da rischi che possiamo definire di natura generale e rischi di natura specifica.

Il rischio generale è quel tipo di rischio che l'azienda è costretta ad assorbire, riconducibile alla possibile verificazione di eventi, sia di natura esterna che interna all'organizzazione, frutto delle caratteristiche della propria attività gestoria e della propria struttura finanziaria.

I rischi specifici, a differenza dei predetti, sono quelli che si caratterizzano per essere connessi a determinati aspetti aziendali e, dunque, richiedono un trattamento specifico. La gestione di tali rischi all'interno dell'organizzazione è demandata ad una funzione creata *ad hoc.* Tale funzione prende il nome di *risk management*. Si tratta di un'innovazione all'interno della struttura manageriale, il cui obiettivo è quello di garantire una protezione rispetto agli eventi che potrebbero danneggiare la realtà aziendale.

Il *risk management* riguarda perciò tutti gli eventi rischiosi, indistintamente dalla possibilità che questi abbiano diversa natura o inquadramento. In molti casi, infatti, ci si trova in situazioni ove taluni influenzano in modo corposo altre variabili, è perciò facilmente decifrabile che tali non possono essere classificati come additivi, proprio per l'impossibilità di analizzarli disgiuntamente. Per tale ragione, essi impongono un approccio integrato che

consente di avere una visione globale in merito alla loro individuazione e di conseguenza alle modalità di trattamento.

La definizione di rischio, data anche dal noto cultore della materia Segal, è frutto della combinazione delle molteplici variabili che interagiscano con il sistema aziendale.

Le variabili in questione possono essere, in via teorica, suddivise in macro aree:

- Variabili produttive;
- Variabili economiche;
- Variabili istituzionali;
- Variabili finanziarie.

Definito il concetto di rischio e individuate le peculiarità della funzione del *risk management*, è necessario soffermare l'attenzione su come è cambiato il modo di concepire quest'ultima all'interno dell'organizzazione aziendale.

Oggi, emerge, in particolare, il concetto di gestione del rischio integrato, meglio conosciuto come *Enterprise Risk Management* (ERM): processo di pianificazione, organizzazione, conduzione e controllo delle attività di un'organizzazione al fine di ridurre al minimo gli effetti del rischio sul capitale e sugli utili di un'organizzazione.

La possibilità di ridurre concretamente i possibili effetti negativi sull'organizzazione impone di analizzare vari tipi di rischio: rischi finanziari, strategici e operativi, oltre ai rischi associati a perdite accidentali.

Va altresì detto che lo sviluppo di sistemi che rendano adeguato l'approccio al rischio di tipo integrato consta di innumerevoli investimenti da parte dell'organizzazione, in quanto tutto il processo interno deve essere riadattato secondo i principi generali della materia di riferimento. Pertanto, per sviluppare ed adattare efficacemente un processo ai fini dell'individuazione, valutazione e gestione dei rischi in ottica integrata è importante che l'organizzazione si soffermi su taluni aspetti, tra i quali quelli di maggior rilievo sono i seguenti:

- Cultura del rischio: sviluppare una cultura aziendale che dia estrema importanza al concetto di rischio; decretare a monte, da parte del vertice aziendale, strategie di *policy* per favorire il coinvolgimento e la sensibilizzazione di tutto il personale, al fine di assicurare che tutte le procedure siano efficacemente prima assorbite e poi di conseguenza eseguite da parte di tutti i componenti inseriti nell'organigramma aziendale.
- L'organizzazione: per stabilire tutte le modalità connesse all'implementazione della cultura del rischio aziendale, sarà necessario che l'organizzazione adotti procedure specifiche che comprendono: la nomina di un *Chief Risk Officer* (CRO); costruire una funzione dedicata all'ERM; designare un gruppo di lavoro per supportare le attività del CRO; creare una funzione ERM indipendente; nominare dei *risk owner* (responsabili dell'identificazione e alla gestione di ogni rischio); circoscrivere (e di conseguenza comunicare) chiaramente i ruoli e le responsabilità nell'ambito del *risk management*; integrare il processo di ERM in tutte le funzioni e le unità aziendali; rendere complici tutti i dipendenti (a tutti i livelli) nel processo di ERM.
- Il processo: come detto più volte, fondamentale al fine di garantire l'implementazione nell'organizzazione di un processo integrato nella gestione dei rischi, è indubbiamente quello di attuare dei processi che standardizzino tutte le attività chiave in merito a questo. Pertanto, sarà necessario anzitutto identificare i rischi e classificarli nelle categorie di riferimento, creare un registro formalizzato e definire un processo formale per la loro valutazione; tale provvedimento non deve essere eseguito *una tantum*, in quanto l'obiettivo della gestione del rischio di tipo integrato è quello di rendere automatica la ripetizione periodica e automatizzata di tale processo, al fine di garantire che tutti i rischi possano essere identificabili in qualsiasi momento e da qualsiasi componente dell'organizzazione.

Dott. Frivoli Mirko

Sarà necessario inoltre implementare, da parte del *top management*, un adeguato *contingency plan*: programma operativo che delinea preventivamente le azioni di determinati soggetti od enti per il caso che si verifichi un evento dannoso o comunque pericoloso per una comunità.

Il piano prevede in genere delle linee guida, più o meno dettagliate, su cosa ciascuno dei soggetti od enti che devono dargli esecuzione debba fare al verificarsi dell'evento.

Enterprise Risk Management — Integrating with Strategy and Performance.

La diffusione di un approccio integrato ha avvicinato molti soggetti al mondo della gestione del rischio. Questo ha fatto emergere un'esigenza di maggiore chiarezza che consentisse di far fronte alla complessità che, per sua natura, connota questa materia.

Per questo motivo, si è fatto riferimento a due *standard* internazionali di rilievo, divulgati da *Commitee of Sponsoring Organizations of the Treadway Commission* (COSO) e dall'*International Organization of Standardization* (ISO). Tali istituzioni hanno fornito delle linee guida applicative per tutti coloro che si trovano a relazionarsi in via diretta o indiretta con il rischio aziendale.

Di seguito vengono esaminati i processi riferibili alle istituzioni sopra richiamate.

L'aggiornamento più recente rilasciato da COSO risale al 2017. Il documento è intitolato "*Enterprise Risk Management — Integrating with Strategy and Performance*". Esso definisce in maniera schematica i principi e le pratiche necessari per una corretta applicazione dell'ERM.

Le novità che vengono introdotte tramite questo aggiornamento sono le seguenti:

- Fornisce una visione più approfondita del valore della gestione del rischio aziendale durante l'impostazione e la realizzazione della strategia.
- Migliora l'allineamento tra prestazioni e gestione del rischio aziendale al fine di definire in maniera più efficiente gli obiettivi aziendali e, allo stesso tempo, comprendere l'impatto del rischio sulla *performance*;

- Soddisfa le aspettative della *Governance*;
- Espande il *reporting* per rispondere alle aspettative di una maggiore trasparenza degli *stakeholder*;
- Si adatta alle tecnologie in evoluzione e alla proliferazione dei dati;
- Stabilisce definizioni, componenti e principi fondamentali per tutti i livelli di gestione coinvolti nella progettazione, implementazione e conduzione di pratiche di gestione del rischio aziendale.

UNISO 31000.

Con riferimento alle norme ISO, pare evidente la scelta di una maggiore standardizzazione delle disposizioni emanate: in particolare, tutte le nuove norme ISO sono state strutturate tenendo in considerazione la nuova impostazione *risked based thinking* e, dunque, in base alla valutazione e alla pianificazione dei rischi e delle relative opportunità.

Con riferimento alla normativa specifica emanata da tale organizzazione, ovvero la UNI ISO 31000, l'aggiornamento più recente risale al 2018. Tale revisione è indubbiamente dovuta al fatto che le tipologie di rischio nel tempo sono mutate notevolmente e, pertanto, servivano delle linee guida di facile attuazione al fine di supportare le organizzazioni nella pianificazione, valutazione e gestione del rischio in modo da rendere più efficiente il processo nella sua interezza.

Le novità introdotte dall'ultima revisione ruotano intorno a tre punti chiave:

- *Leadership*: si è scelto di porre in rilievo il concetto di *leadership*, sensibilizzando il *Top Management* nella gestione del rischio, tenuto conto del fatto che quest'ultima deve essere di natura integrata rispetto a tutto il sistema gerarchico e indistintamente dal tipo di attività. Pertanto, attraverso tale sensibilizzazione si è voluto consolidare il principio secondo il quale chi è nei posti di vertice debba fungere da esempio per tutti i componenti dell'organizzazione.

- Interazione continua con l'ambiente esterno: al fine di garantire un miglioramento continuo nel tempo, tale processo prevede che l'organizzazione, con riferimento alla gestione del rischio, sia volta ad analizzare l'ambiente circostante al fine di adeguarsi al mutamento del contesto esterno.
- "Gestione interattiva" del rischio: rispetto al punto precedente, l'adeguamento al continuo mutamento dell'ambiente esterno impone di favorire l'analisi e l'elaborazione dei dati che sono stati acquisiti, al fine di definire azioni e controlli di processo volti a garantire la gestione dei rischi derivanti.

Punti di interazione tra la funzione di ERM e l'implementazione del Modello organizzativo *ex* D.lgs. 231/01.

In considerazione di quanto esaminato nei paragrafi precedenti, si rende necessario soffermare l'attenzione sul modo in cui, dal punto di vista operativo, la funzione di ERM si possa coniugare con l'implementazione di un Modello di Organizzazione, Gestione e Controllo *ex* D.lgs. 231/01.

Si pensi ad un'organizzazione che valuta i rischi in modo distinto. Essa, nello specifico, si limita ad individuare la tipologia di rischio e ad adottare strumenti adeguati alla sua gestione. A primo impatto, quello appena descritto può sembrare un procedimento efficace; tuttavia, un'analisi più attenta suggerisce un esito diverso, poiché, operando in questo modo, si potrebbe rischiare di perdere "per strada" qualcosa in merito alla corretta identificazione delle tipologie di rischio rilevanti. Difatti, in organizzazioni più complesse, valutare un rischio singolarmente può essere efficace al fine di gestire e arginare quest'ultimo, ma non consente di capire quanto quell'evento rischioso possa, in via di principio, influenzare l'accadimento di altri eventi seguendo un effetto a cascata, una sorta di azione-reazione in grado di innescare una molteplicità di possibili rischi non identificabili a

priori attraverso l'approccio sopra indicato. Peraltro, in questo modo l'organizzazione è in grado di venire a conoscenza di questi eventi solo dopo il verificarsi del primo evento rischioso, in quanto costretta ad operare *ex-post* (si badi bene, non per mancanza di attuazione di politiche di *risk management*, bensì per non aver sposato, in modo adeguato, una gestione del rischio di tipo integrato, capace di offrire una visione olistica di tutta l'organizzazione e di conseguenza di tutti i possibili rischi specifici che la interessano).

Per le ragioni appena descritte, pare evidente che adottare un sistema integrato rispetto alla gestione del rischio possa risultare molto complesso e possa comportare notevoli costi per l'organizzazione, tra i quali quelli inerenti alla riorganizzazione del sistema di controllo, all'adeguamento di strumenti volti a rendere tale processo immediato e efficiente, nonché, infine, alla formazione del personale.

Vero questo, non si può negare come l'implementazione di un sistema integrato generi, nel complesso, benefici ben maggiori rispetto ai costi.

Dal punto di vista operativo, per disegnare un sistema efficace di gestione del rischio, la prima fase che si rende necessaria è quella della predisposizione del *risk assessment*, vero e proprio "cuore pulsante" dell'ERM.

Nel caso di specie, alla luce del contesto di riferimento, l'individuazione del rischio non potrà che riguardare il rischio di commissione delle fattispecie di reato contemplate dal D.lgs. n. 231/01.

La prima fase prevede un'analisi del contesto aziendale, al fine di individuare i processi e le attività per i quali esiste il rischio di incorrere nei reati presupposto della responsabilità dell'ente.

Gli obiettivi di questa fase sono i seguenti:

1. Individuazione delle principali aree a rischio reato;
2. Identificazione dei soggetti interessati;
3. Individuazione delle possibili modalità di commissione dei reati.

Dal punto di vista operativo, per raggiungere gli obiettivi sopra descritti, si procede compiendo le seguenti attività:

1. raccogliendo ed analizzando le informazioni rilevanti;
2. compiendo interviste finalizzate all'acquisizione di informazioni in merito a situazioni in cui si sono verificati comportamenti non conformi alle procedure aziendali e/o condotte in grado di integrare uno dei reati di cui al D.lgs. n. 231/01 (c.d. Analisi Storica);
3. somministrando questionari preliminari finalizzati ad ottenere informazioni sui soggetti che intrattengono rapporti con terzi rilevanti ai fini del Decreto 231, sulla natura e sulla frequenza di tali apporti e sull'individuazione, con l'ausilio di professionisti, di possibili modalità di commissione dei reati.

Con riferimento all'attività di raccolta dei dati e di analisi delle informazioni rilevanti, si provvede a raccogliere e ad esaminare la documentazione preliminare (organigrammi, *mission statement*, procedure, ecc.) necessaria alla:

1. comprensione della struttura organizzativa e dei processi aziendali;
2. definizione del perimetro dell'analisi.

Una volta compiuti tali passaggi, vengono identificate le aree di rischio reato, ovvero quelle aree nell'ambito delle quali, alla luce elle informazioni raccolte e condivise con i responsabili delle funzioni, si identifica la possibilità che venga commesso una delle fattispecie previste nel novero dei reati presupposto.

Tali aree vengono interpolate con l'identificazione di ulteriori aree, definite strumentali, relative alla gestione di strumenti di tipo finanziario (e/o mezzi sostitutivi) che possono supportare la commissione di illeciti penali nelle aree a rischio reato (contabilità, tesoreria, amministrazione del personale, gestione dei sistemi informativi).

Viene infine individuato il c.d. "universo di analisi"' e delle possibili modalità di commissione dei reati, che rappresenta la mappatura formale delle aree aziendali potenzialmente

impattate dal D.lgs. n. 231/01. È l'*output* dell'attività di identificazione delle "aree a rischio reato", delle "aree strumentali" e dei soggetti interessati.

In questa fase l'ODV, l'ufficio legale/società di consulenza o il legale esterno che struttura il MOG, identifica le potenziali modalità di attuazione dei reati per ciascuna area a rischio, ossia le modalità concrete con cui i reati previsti dal decreto potrebbero trovare attuazione nello svolgimento delle attività "sensibili", individuate all'interno di ciascuna area a rischio reato.

È importante sottolineare pertanto che, in caso di procedimento nei confronti della società per la commissione di reati *ex* D.lgs. n. 231/01, la corretta esecuzione dell'attività di *risk assessment* (e quindi la susseguente idonea previsione ed attuazione del MOG) servirà a dimostrare che la società ha identificato, in modo corretto, i rischi di commissione di reati potenzialmente verificabili, le modalità con cui tali reati possono essere commessi e i presidi di controllo volti a prevenirli. È importante quindi che la metodologia ed i criteri con cui è stato costruito il sistema di controllo nell'ambito del MOG sia ripercorribile.

A tal fine, uno strumento molto utile è indubbiamente la predisposizione di questionari *check list* che consentono di valutare l'adeguatezza del Sistema di Controllo Interno. Tali *check lis*t vengono elaborate utilizzando le conoscenze delle aree oggetto di analisi e sono adattate, successivamente, sulla base delle informazioni acquisite durante le interviste dirette ad identificare i controlli chiave.

Oltre a tali questionari, per raccogliere in maniera puntuale tutte le informazioni necessarie, saranno predisposte delle interviste, le quali consentiranno di convalidare l'attinenza e completezza dei questionari nonché acquisire una serie di informazioni aggiuntive che non si otterrebbero attraverso il solo invio dei questionari.

Alla luce delle informazioni acquisite dall'analisi preliminare, dei documenti organizzativi e normativi e nel corso delle interviste, si effettua una valutazione comparativa tra il sistema di controllo esistente ("*as is*") ed i controlli "attesi" a mitigazione dei fattori di rischio (*to be*).

Dott. Frivoli Mirko

In questo modo, è possibile valutare l'idoneità dei meccanismi di controllo interno rispetto alla prevenzione del rischio reato e, di conseguenza, individuare eventuali *gap* che necessitano di controlli correttivi. Al termine delle fasi precedentemente descritte, si elaborerà un *output* contenente i suggerimenti per il miglioramento del Sistema di Controllo Interno (SCI).

Una volta identificati i controlli presenti all'interno dell'azienda, si procederà alla relativa valutazione al fine di determinarne l'efficacia ed efficienza degli stessi nella riduzione del rischio inerente. La valutazione dei controlli porterà alla determinazione dei rischi residuali, che potranno essere uguali o inferiori rispetto ai rischi inerenti, a seconda che i controlli individuati siano più o meno efficaci.

Il livello di rischio può essere calcolato analiticamente attraverso la combinazione di due variabili:

1. Impatto: inerente alle conseguenze derivanti dal verificarsi dell'evento;
2. Probabilità: ovvero la possibilità con il quale un evento si verifichi.

Il rischio può essere valutato secondo due livelli:

1. Rischio inerente: è il rischio valutato a prescindere dall'efficacia e dall'operatività degli strumenti di gestione del rischio adottati;
2. Rischio residuale: è il rischio valutato tenendo conto dell'adozione ed implementazione di strumenti di gestione dei rischi.

Il rischio inerente è dato dalla probabilità che si verifichi un determinato evento rischioso moltiplicato per l'impatto che potrà conseguire a quel determinato accadimento.

$R = p * i$

Chiaramente questa è una situazione che non tiene conto di quelle che possono essere le coperture esistenti, ovvero l'adozione di determinate misure cautelari al fine di evitare che a monte si verifichino fattori di rischio. Pertanto, una volta attuate tali misure si determina il valore del rischio residuo, in grado di attenuare o addirittura annullare il rischio inerente.

$R' = p * i - \varepsilon$

Dott. Frivoli Mirko

Nell'ambito delle aree a rischio reato e strumentali saranno poi individuate, in base alla priorità riscontrata:

1. le aree ad alto rischio che saranno inserite nel piano delle attività dell'Organismo di Vigilanza e soggette ad *audit*;
2. le aree a rischio medio/basso che potrebbero essere oggetto di *audit* da parte dell'Organismo di Vigilanza.

Da ultimo, è fondamentale stabilire il ruolo del SCI (sistema di controllo interno) in merito al D.lgs. n. 231/01 e, in particolare, la capacità del medesimo, in tale contesto, di fornire una ragionevole sicurezza in merito alla capacità delle misure messe in atto dall'ente di dissuadere, prevenire ed individuare l'attuazione dei reati previsti dal decreto.

È chiaro che tutti i sistemi di controllo interno, per quanto possano essere stati sviluppati con la massima attenzione, non sono in grado di garantire in maniera assoluta la conformità delle attività alle leggi e ai regolamenti, in quanto, la probabilità di realizzazione degli obiettivi risente dei limiti insiti in tutti i sistemi di controllo interno.

Possono incidere su questi limiti:

1. Gli errori fatti in merito ad un controllo di un soggetto che in quel momento non ha agito con l'attenzione dovuta.
2. La possibilità che un *manager* trovi un *escamotage* per derogare al controllo interno al fine di trarre vantaggi personali.
3. Un *deficit* di controllo frutto di un atto di collusione tra due o più individui.

In ogni caso, preme sottolineare come l'efficace predisposizione ed attuazione del sistema di controlli interni assicuri notevoli vantaggi all'organizzazione, legati alla prevenzione del rischio reato. In questo modo, difatti, l'azienda può evitare:

1. Danni di immagine e reputazionali;
2. Controlli sul valore dei titoli in caso di società quotate;
3. Altri problemi derivanti dalla commissione di illeciti di rilievo penale.

Dott. Frivoli Mirko

Con riferimento all'analisi dell'ambiente di controllo, essa è diretta a verificare se ricorrano le condizioni per garantire l'esistenza di un sistema affidabile di controllo.

Nella valutazione dell'ambiente di controllo devono essere considerati i seguenti fattori:

1. struttura organizzativa, le responsabilità e le attitudini del *management* sono tali da garantire un controllo effettivo ed efficace sulle attività della società;
2. se gli amministratori ed il *management* (in particolare quelli con diretta responsabilità finanziaria) sono competenti e hanno l'esperienza per attuare le decisioni del Consiglio e gestire i mutamenti dell'attività aziendale.

In altri termini, si può dire che l'organizzazione ed il controllo interno rappresentano, per le società, dei veri e propri obblighi rispetto alla prevenzione di fattori in grado di pregiudicare il raggiungimento degli obiettivi prefissati ma, allo stesso tempo, rappresentano l'opportunità di conseguire ulteriori vantaggi, quali:

1. Efficacia ed efficienza delle operazioni;
2. Ritorno di immagine/Reputazione;
3. Riconsiderare la propria organizzazione ed i propri comportamenti *standard*/abitudini;
4. Risparmio di Costi;
5. Responsabilizzazione delle persone;
6. Prevenzione dei problemi;
7. Credibilità dei soggetti (anche per i rapporti con eventuali finanziatori).

Conclusioni.

In conclusione, l'adozione di un sistema riferibile alla gestione dei rischi integrata è senza dubbio uno strumento che, se sviluppato in maniera adeguata, è in grado di offrire ottimi risultati in punto di individuazione di tutti i rischi che possono manifestarsi all'interno dell'organizzazione. Inoltre, esso consente di intercettare anche quei rischi che potremmo

definire “invisibili”, ovvero che non potrebbero essere individuati senza l’adozione di un approccio integrato.

Gli stessi benefici si riscontrano con riferimento ai rischi connessi alla commissione di uno o più reati presupposto *ex* D.lgs. n. 231/01. Difatti, anche in questo caso, l’adozione di un approccio integrato nella gestione del rischio consente di rilevare e, di riflesso, arginare tutte le tipologie di rischi potenziali, anche quelle che non sarebbero individuabili a priori attraverso una gestione del rischio “tradizionale”. Così facendo, è possibile dunque preservare l’organizzazione da possibili esternalità negative ancorate ad un’individuazione tardiva (e, dunque, *ex post*) del fattore di rischio.