

Il risk assessment secondo il «Modello» ex D.Lgs. n. 231/2001

di Alberto Pesenato (*) e Elisa Pesenato (**)

I concetti di risk assesment e risk management sono richiamati dal documento CoSO II e dalla circolare 83607/2012 della GdF. Questo secondo contributo illustra le linee essenziali e le modalità applicative oltre a proporre una matrice applicativa utile alla mappatura dei rischi richiesta dal decreto.

Introduzione

Recentemente la Circolare della Guardia di Finanza n. 83607/2012 ha trattato diffusamente la composizione del Modello di organizzazione, gestione e controllo (1) dedicando alla stessa il Volume III, che così recita a pag. 76 «*Ai fini dell'elaborazione dei modelli, che devono essere costruiti secondo uno schema che riprenda i processi di risk assessment e risk management normalmente attuati nelle imprese, la relazione illustrativa evidenzia come la normativa preveda una maggiore tipizzazione dei modelli validi per i vertici, come risulta dal disposto dell'art. 6, comma 2, che tratteggia un modello ben strutturato, con un contenuto minimo obbligatorio e non derogabile*».

Individuare le attività nel cui ambito possono essere commessi reati (art. 6, co. 2, lett. a)

Tale requisito può essere soddisfatto attraverso l'introduzione di un processo sistematico di valutazione dei rischi potenziali (nella commissione dei reati) che prende il nome di risk assessment.

Il risk assessment rappresenta il cuore del processo di risk management e consiste nella misurazione e nella valutazione dei fattori di rischio identificati assegnando a ciascuno un valore di probabilità e un valore di impatto/danno nel valutare gli stessi. Si ritiene opportuno precisare che per rischio si intende la probabilità che un evento od una azione possa determinare effetti pregiudizievoli per l'Ente o la società. In questo contesto si

può parlare di rischio di commissione delle fattispecie di reato contemplate nel D.Lgs. n. 231/2001.

Il risk assessment o valutazione del rischio può essere definito come il processo di stima dei fattori di rischio associati a specifiche attività di una organizzazione. Esso comprende le attività di:

- 1) identificazione delle attività/processi;
- 2) individuazione delle minacce e dei fattori di rischio;
- 3) valutazione ed attribuzione del livello di rischio;
- 4) classificazione delle attività in base al rischio potenziale.

Identificazione delle attività/processi

La prima fase prevede un'analisi approfondita del contesto aziendale al fine di individuare i processi e le attività per i quali esiste il rischio di incorrere nelle fattispecie di reato previste dal D.Lgs. n. 231/2001.

I principali oggetti di riferimento dell'analisi in questione sono la struttura organizzativa dell'azienda, le procedure esistenti, le eventuali mappature dei processi interni e tutta la documentazione a supporto in grado di fornire informazioni utili ai fini della identifica-

Note:

(*) Consulente Area D.Lgs. 231/2001 (Presidente OdV Karrell Srl - Trentino trasporti esercizio SpA - FAR Maremma S.c.a r.l.)

(**) Auditor (SCI) Sistema di Controllo Interno - Consulente Area 231/2001

(1) Si veda Organo di Vigilanza e Modello di organizzazione gestione e controllo ex D.Lgs. n. 231/2001 WKI - IPSOA IV Edizione 2013 e contributi in www.albertopesenato.net.

zione delle attività a rischio (politiche aziendali, leggi e regolamenti, bilanci, procedure interne ecc.).

Nell'ambito di questa analisi è opportuno identificare i soggetti responsabili dei processi e delle attività potenzialmente a rischio ed effettuare delle interviste di dettaglio con l'obiettivo di delineare un quadro esaustivo della realtà aziendale.

A tal fine nella presente trattazione si propongono check lists e Questionari sul Controllo Interno (ICQ) per individuare le responsabilità e procedure.

Individuazione delle minacce e dei fattori di rischio

In questa seconda fase si procede all'elencazione di tutti i rischi potenziali, in questo caso quelli di incorrere nelle fattispecie di reato previste dal D.Lgs. n. 231/2001 ed alla loro attribuzione alle singole attività o ai singoli processi così come rilevati nella prima fase. Tale attività consente di evidenziare le possibili modalità di attuazione dei reati rispetto al contesto aziendale «mappato».

Relativamente al rischio di comportamenti illeciti in materia di salute e sicurezza sul lavoro, tale sistema deve necessariamente tenere conto della legislazione prevenzionistica vigente e, in particolare, del D.Lgs. n. 81/2008 e successive modifiche ai sensi del quale i rischi lavorativi devono essere comunque integralmente eliminati in relazione alle conoscenze acquisite in base al progresso tecnico e, ove ciò non sia possibile, ridotti al minimo e, quindi, gestiti. Tale complesso normativo, infatti, delinea esso stesso un «sistema» di principi cogenti e adempimenti obbligatori la cui declinazione sul piano della gestione applicativa - laddove opportunamente integrata/adeguata in funzione del «modello organizzativo» previsto dal D.Lgs. n. 231/2001 - può risultare idonea a prevenire, agli effetti esonerativi dello stesso D.Lgs. n. 231/2001, la possibilità di una condotta integrante gli estremi del reato di omicidio o lesioni colpose gravi o gravissime commessi con violazione delle norme prevenzionistiche.

Valutazione ed attribuzione del livello di rischio

La fase successiva del processo di risk assessment prevede la assegnazione di un valore

specifico alle categorie di rischio identificate. In particolare si procede alla individuazione di un peso relativo tra le categorie di rischio ed alla valutazione dei singoli fattori di rischio per ciascuna delle attività e processi rilevati.

I criteri utilizzati per la valorizzazione del livello di rischio sono di norma soggettivi e conducono, in sintesi, alla utilizzazione di una scala di valori generalmente composta da tre o cinque elementi. (ad es.: Rischio Trascurabile, Rischio Basso, Rischio Medio, Effettivo, Rischio Alto).

Le componenti principali di questa valutazione sono: la probabilità di accadimento dell'evento la gravità e l'impatto/danno in termini conseguenze derivanti dal verificarsi dell'evento a rischio. Ad esempio è possibile individuare i danni in termini di immagine all'azienda o i danni in termini economico/finanziari in caso di accadimento dei fatti illeciti contemplati nel D.Lgs. n. 231/2001. A sua volta la probabilità di accadimento è determinata dall'oggettiva fattispecie dell'attività a rischio, anche in considerazione della frequenza di esecuzione, e dall'adeguatezza del Sistema di Controllo Interno (SCI) (procedure/protocolli) in essere.

Classificazione delle attività in base al rischio potenziale

Una volta assegnato il peso relativo ai singoli fattori di rischio e valutato l'impatto al verificarsi dell'evento potenziale, è possibile elencare quali attività o processi sono potenzialmente più a rischio. È possibile perciò stabilire una priorità di intervento sulle singole attività diretta a verificare lo stato dei controlli e le azioni intraprese dal management per la riduzione del rischio ad un livello tollerabile.

L'output ottenuto dal processo di risk assessment è pertanto una mappatura delle singole attività aziendali classificate in funzione del livello di rischio attribuito (matrice dei rischi Tavola 2), laddove per le attività a rischio potenziale più elevato è richiesta una priorità di attenzione e si rende necessario effettuare interventi specifici di verifica. L'attività di individuazione delle attività a rischio (risk assessment) deve essere caratterizzata da verifiche metodiche continue utilizzando il supporto di specialisti (organismo

dedicato), anche introducendo, ove possibile, tecniche di auto valutazione assistita.

Prevedere specifici protocolli diretti a prevenire i reati (art. 6 co. 2. lettera b)

Si tratta, ora, di definire le attività di verifica per controllare, ed eventualmente adeguare il Sistema di Controlli Interni (protocolli) per prevenire la commissione di reati, così come richiesto dall'art. 6.

L'attività dovrà essere condotta sui processi/attività individuati nella fase di risk assessment e consiste in:

- a) descrizione formalizzata e di dettaglio delle attività a rischio;
- b) individuazione e descrizione delle attività di controllo implementate;
- c) individuazione e descrizione dei controlli carenti ed inesistenti;
- d) verifiche (anche a campione) per esaminare la conformità dei comportamenti effettivi confrontandoli con quelli previsti nel modello.

a. Descrizione formalizzata e di dettaglio delle attività a rischio

La prima attività da svolgere per la valutazione dell'adeguatezza dei «protocolli» consiste nella rilevazione dettagliata dei processi potenzialmente a rischio. In particolare si tratta di effettuare una «ricognizione» (*survey*) ovvero una raccolta di tutte le informazioni utili sulle attività da esaminare. La ricognizione può essere effettuata utilizzando tecniche specifiche quali:

- interviste con i soggetti coinvolti nel processo;
- utilizzo di appropriati Questionari (ICQ) e check list (2);
- osservazioni sul posto;
- analisi delle procedure approvate e delle prassi aziendali;
- studio e comparazione delle relazioni tra informazioni di natura finanziaria e non finanziaria;
- predisposizione di diagrammi di flusso (*flow-charting*) per una descrizione schematica e dettagliata delle attività e dei controlli esistenti (quando ritenuto necessario).

Scopo di questa fase è quello di avere un quadro dettagliato di come si svolgono le at-

tività di processo, di quali sono i soggetti coinvolti e in quali fasi del processo questi ultimi intervengono.

b. Individuazione e descrizione delle attività di controllo implementate

Nell'effettuazione della attività di ricognizione deve essere data particolare enfasi ai processi di controllo implementati dal management. In sostanza occorre evidenziare quali strumenti di controllo delle attività e del processo sono stati introdotti per garantire il rispetto dell'obiettivo di conformità alle disposizioni del D.Lgs. n. 231/2001.

Per una migliore individuazione si possono utilizzare le seguenti classificazioni di controllo.

I controlli possono distinguersi in:

- preventivi, volti ad evitare il verificarsi di un evento negativo;
- rivelatori, diretti a rivelare l'anomalia nel momento in cui si manifestano;
- direttivi, servono ad indirizzare le attività di processo;
- correttivi, volti ad impedire che si verifichino effetti negativi quando l'evento negativo si è verificato.

Secondo gli obiettivi che si prefiggono possono essere distinti in:

- operativi;
- relativi alle informazioni di bilancio;
- conformità a leggi e regolamenti.

È possibile perciò effettuare una classificazione dei controlli riscontrati suddivisi per natura e per obiettivo. Ciò consente una più agevole valutazione dei controlli per categoria omogenea.

c. Individuazione e descrizione dei controlli carenti o inesistenti

Una volta rilevati i controlli nella fase di analisi del processo questi devono essere valutati per la loro efficacia ed adeguatezza. Tale valutazione consiste nel:

- verificare l'effettiva applicazione dei controlli esistenti: è possibile infatti che il

Nota:

(2) Op. cit.: OdV Governance: Check lists Cap. 7 e CD - OdV Unità Operative ICQ Internal Control Questionnaires Cap. 8 e CD.

controllo sia presente ma non venga utilizzato o venga eluso dai comportamenti (*walk through*);

- evidenziare i controlli carenti o mancanti: questo si ottiene confrontando i processi di controllo effettivamente riscontrati con una situazione «ipotetica» o «attesa». Le caratteristiche di un sistema di controllo «ipotetico» sono delineate utilizzando le *best practices* aziendali e modelli organizzativi e gestionali di riferimento.

Tale valutazione richiede una conoscenza approfondita di quelli che sono le componenti e le tecniche di controllo interno. Come detta la lettera a) comma 2. dell'art. 6. il modello deve essere, oltre che adottato, anche efficacemente attuato, se ne desume quindi che occorre prevedere una specifica attività di verifica dell'effettiva applicazione del modello, quindi dei comportamenti di quanti sono chiamati ad attuarlo nel contesto delle attività oggetto di verifica.

d. Verifiche (anche a campione) per esaminare la conformità dei comportamenti effettivi confrontandoli con quelli previsti nel modello

Al fine di supportare concretamente le osservazioni emerse dalla attività di individuazione e valutazione dei controlli esistenti si procede con una attività di verifica dei dati e della documentazione presente in azienda. Tale verifica può essere effettuata utilizzando diverse tecniche quali:

- interviste di dettaglio;
- check list e questionari di riferimento;
- tecniche di campionamento statistico (ove necessario);
- comparazione di documenti ufficiali;
- verifica diretta del patrimonio;
- osservazioni del comportamento dei soggetti coinvolti nel processo;
- verifica diretta della applicazione delle procedure.

Questa attività si rende necessaria affinché le anomalie riscontrate siano supportate da informazioni sufficienti, qualificate, rilevanti ed utili, ovvero che queste siano adeguatamente provate e giustificate.

La metodologia adottabile «as is analysis» o analisi dell'esistente

In definitiva la metodologia si configura come un'analisi dell'esistente (*as is analysis*) vale a dire una stima delle misure già attuate dall'organizzazione per controllare i fattori di rischio già rilevata (fasi 1 - 2 - 3 - 4) e sulle azioni da compiere per impedire che il reato possa essere compiuto tramite l'applicazione di ulteriori specifici protocolli (fasi 5 - 6). Un riepilogo è proposto in Tavola 1 (3).

L'output di questa fase sarà valutazione del Modello adottato con indicazione di carenze riscontrate e suggerimenti per l'adeguamento del Modello stesso.

Gli strumenti operativi

L'obiettivo degli strumenti qui illustrati (4) è quello di individuare ed analizzare quelle attività, i così detti processi «sensibili» aziendali, all'interno delle quali possono concretizzarsi le fattispecie di reato esplicitamente previste dal D.Lgs. n. 231/2001.

Si provvede a mappare le aree aziendali a rischio in conseguenza delle potenziali modalità attuative degli illeciti e reati. Tali operazioni sono completate attraverso una valutazione del sistema delle procedure e dei controlli preventivi esistente ad oggi (i cosiddetti protocolli previsti dallo stesso D.Lgs 231/2001 e dalle *Linee Guida per la costruzione dei modelli di organizzazione, gestione e controllo ex D.Lgs. n. 231/2001* di Confindustria e ASSTRA aggiornate) e con la successiva indicazione in merito al suo adeguamento, quando ciò sia stato ritenuto necessario. La mappatura, esaustiva dei rischi derivanti dalle occasioni di coinvolgimento delle strutture organizzative aziendali, consente di individuare le aree e i processi che necessitano di maggiore attenzione e per i quali si rende opportuna la definizione e l'applicazione di specifiche procedure e controlli.

Note:

(3) Op. Cit. *Organo di Vigilanza e Modello di organizzazione gestione e controllo ex D.Lgs. n. 231/2001* V Edizione 2013 WKI IPSOA.

(4) Op. cit. Gli strumenti operativi qui riportati, validi per ogni tipologia di reato, vanno ad aggiungersi la a quelli proposti nei Capp. 7 e 8 (Rischio di Infrazione) per i reati cosiddetti di bilancio che hanno manifestazione finanziaria).

Illeciti e Reati in bilancio e fuori bilancio

La commissione di illeciti e reati può essere allocata in due particolari categorie:

a) reati ed illeciti che sono rilevabili nelle scritture contabili come fatti di gestione artefatti ed occultati tramite espedienti ed accorgimenti basati su falsa documentazione, accordi fittizi ed altro;

b) illeciti e reati che nulla hanno a che vedere con i fatti di gestione registrati nelle scritture contabili e nei prospetti di bilancio (*financials reporting*) ma che possono essere commessi ugualmente recando documento all'Ente od azienda.

Ecco che la metodologia applicata nel primo caso si sviluppa con l'*auditing* e la verifica delle procedure in essere, con la ricerca dei punti di debolezza nelle stesse determinando

il rischio di infrazione (5) con la successiva interruzione e chiusura delle falle. Ben diversa è la metodologia che l'OdV deve adottare nel secondo caso dove la normale conoscenza delle procedure aziendali deve essere non solo assistita ma addirittura confermata da opportune e qualificate professionalità esterne all'uopo ingaggiate (sicurezza sul lavoro, IT, ambiente, diritti d'autore ed altro).

In Tavola 2 si presenta una matrice che ben

Nota:

(5) Chi scrive ritiene che l'OdV essendo organico all'ente o azienda, in quanto incardinato in essa da una legge specifica, può attivamente stimolare gli altri organi di controllo esterni all'azienda (Collegio Sindacale, Revisore Legale) al fine di attuare un «sistema integrato di controlli». (Si veda in proposito dello stesso autore: «OdV, Revisore Legale, Collegio Sindacale: attori di un sistema integrato di controlli» in *Amministrazione & Finanza* n. 12/2012).

Tavola 1 - Riepilogo as is analysis

	Fase	Descrizione	Strumenti
1	Check up aziendale	Conoscenza generale ed approfondita dell'azienda ed acquisizione relativa documentazione	Dossier Permanente - Dossier Imposte - <i>Dossier Governance</i> - Check lists: 10 - CoSO Report I :11.1 11.2 - 14.1 14.2 14.3 14.4 - 16 17 18. Dossier Unità Operative - 1 (<i>Rischio Intrinseco</i>)
2	Valutazione SCI	Analisi del Sistema del di Controllo Interno (SCI) esistente	Unità Operative - ICQ da 3 a 25 (<i>Rischio di Controllo</i>)
3	Identificazione attività e processi	Analisi delle procedure nel dettaglio	Walk Through Determinazione <i>Livello (Rischio) di Identificazione</i>
4	Individuazione fattori di rischio	Individuazione dei punti di forza e dei punti di debolezza da monitorare	Determinazione del <i>Rischio di Infrazione</i> Verifiche di conformità alle procedure rilevate (da mettere in comune con Matrice dei Rischi)
5	Mappatura aree sensibili e processi a rischio	Determinazione dei reati possibili e probabili	<i>Matrice dei Rischi</i> Da utilizzare per Reati contabili e non Tav. 2
6	Valutazione rischio reato	Analisi del rischio di commissione di uno dei reati presupposto	Classificazione finale del rischio Tav. 3

Tavola 2 - Matrice per la classificazione del Rischio

G Gravità Impatto	P Probabilità			
	1	2	3	4
1	1	2	3	4
2	2	4	6	8
3	3	6	9	12
4	4	8	12	16

I valori individuati da 1 a 2 indicano un rischio trascurabile, 3 e 4 rischio basso, 6, 8, 9, 12 e 16 rischio alto.

si adatta sia nell'ipotesi a) sopra descritta, confortando le analisi delle procedure che l'OdV ha il compito di eseguire nelle proprie verifiche, sia nell'ipotesi b) dove l'OdV può, con il supporto delle professionalità interne all'azienda, affrontare le aree che necessitano di particolare e specifica competenza per poi decidere come affrontare la procedura magari ricorrendo ad esperti esterni. (6)

La metodologia adottabile: la matrice dei rischi

Il *risk assessment* può essere applicato ai più svariati settori, (7) come ad esempio sicurezza, assicurazioni, banche, investimenti, medicina, I.T, matematica, alimentare (in associazione al Metodo HACCP), nello sviluppo di sistemi di gestione ambientale (analisi ambientale) e controllo interno aziendale.

È quindi applicato anche in economia e nella gestione dei fatti e processi aziendali e quindi si estende anche nella ricerca della possibilità di commissione di illeciti e reati all'interno di società o enti.

In generale si può ricorrere a questa metodologia quando si intende valutare la pericolosità di un evento indesiderabile ai fini di definire la priorità o l'urgenza delle misure necessarie per tenerlo sotto controllo e conseguentemente può essere applicabile al rischio di commissioni dei reati indicati dal D.Lgs. n. 231/2001.

La metodologia suddetta va distinta nelle seguenti fasi:

- descrizione del reato od illecito con la raccolta di informazioni e di dati sull'organizzazione dell'Ente (8), le procedure in essere, sui settori e/o sugli ambienti interessati (ovviamente con riferimento dell'obiettivo finale della commissione del reato) ecc.

La descrizione si concentrerà su aspetti differenti, ai fini dell'individuazione dei rischi. In genere è importante arrivare ad una schematizzazione delle procedure per facilitare la successiva fase di individuazione reato dei pericoli di commissione dello stesso:

- individuazione dei potenziali pericoli: mediante l'analisi delle informazioni raccolte nella fase precedente si individuano tutti i pericoli riconducibili all'oggetto di studio;
- stima dei potenziali rischi (nel nostro caso rischio reato): a pericolo individuato si stima la probabilità di accadimento e la gravità o

l'impatto degli effetti che può determinare tenendo conto delle eventuali misure preventive o protettive già in essere;

- determinazione della classe di rischio: alto, medio, basso, trascurabile (Tavola 3).

A seconda dell'entità del rischio reato così determinato si dovranno poi definire, attuare e controllare i programmi di eliminazione o di riduzione e gestione del rischio stesso.

Terminologia

La terminologia di riferimento è la seguente:

- Rischio: è il risultato dell'interpretazione della «Matrice» (9) qui propostasi intende la pericolosità di un evento ed è determinato dal prodotto tra P (probabilità dell'evento) e G (gravità/impatto), secondo la seguente formula:

$$R = P \times G$$

Qui viene distinta in 4 livelli (Tavola 2).

- Probabilità (P): si intende la probabilità che l'evento (Reato o Illecito) indesiderato si possa verificare tenendo conto delle misure precauzionali già in essere al momento della valutazione. In genere viene distinta in 4 classi (Tavola 3);

- Gravità/Impatto (G): detta anche Magnitu-

Tavola 3 - Classificazione del Rischio

1 - 2	Rischio Trascurabile
3 - 4	Rischio Basso
6 - 8	Rischio Medio
9 - 12 - 16	Rischio Alto

Note:

(6) Ecco quindi l'opportuna autonomia finanziaria assegnata dal legislatore all'OdV.

(7) «Risk management has emerged more or less independently in a number of areas including: safety, insurance, banking, investment, medicine, artificial intelligence, mathematics, public policy analysis, and internal control.» Leitch M. *Intelligent internal control and Risk Management..*

(8) Possono essere di aiuto le appendici del P.R. 240 Le responsabilità del revisore relativamente alle frodi nella revisione contabile del bilancio 315: «L'individuazione e la valutazione dei rischi di errori significativi mediante la comprensione dell'impresa e del contesto in cui opera» e la determinazione del rischio Intrinseco.

(9) Anche Università degli studi di Padova CESQA (Centro Studi Qualità Ambiente).

do (M), è intesa come la gravità delle conseguenze dell'evento indesiderato. In genere viene distinta in 4 classi;

– Pericolo, sorgente di rischio: si intende l'entità o l'evento in grado di provocare il danno o i danni.

Valutazione del Rischio di Infrazione

Si deve prendere in considerazione da un lato, la Gravità/Impatto che tali reati presupposto possono provocare (Gravità - Impatto G), dall'altro la probabilità che tali comportamenti accadano e la copertura del modello organizzativo attualmente applicato e finalizzato a mitigare il rischio che tali fattispecie si realizzino (Probabilità P).

Al fattore «Gravità - Impatto G» è stato assegnato un valore crescente da 1 a 4, in base alla maggiore o minore «sensibilità» del processo/attività in esame, alla frequenza di esecuzione e alle considerazioni emerse rispetto alle responsabilità coinvolte. All'interno di tale fattore, sono contenute anche valutazioni generali in merito alla tipologia (sanzioni pecuniarie e sanzioni interdittive) e alla gravità delle sanzioni nelle quali l'ente può incorrere. Tutto ciò premettendo che l'Ente mira a presidiare l'accadimento di qualsiasi fatto illecito contemplato nel D.Lgs n. 231/2001 per prevenire ogni tipologia di ricaduta in termini di immagine o di danno economico finanziario.

Il fattore «Probabilità - P» sempre con valore assegnato da 1 a 4 è stato invece valorizzato in base alla presenza degli elementi individuati quali: documenti di principio/indirizzo, procedure/registrazioni, controlli,...), diretti a mitigare i rischi connessi alla concretizzazione dei reati.

La conseguenza è che la scala individuata è inversa rispetto al fattore gravità/impatto cioè il giudizio di minore probabilità (presidio/procedura) efficace è pari a 1 mentre quello di presidio/procedura meno efficace (alta probabilità) è uguale a 4.

La classificazione del rischio

È quindi il risultato della moltiplicazione tra i fattori «Probabilità - P» e «Gravità - Impatto G». Si può andare quindi da un potenziale Rischio Minimo 1 (dove entrambi i fattori sono valorizzati con 1) ad un Massimo Ri-

schio avvalorato con 16 (dove entrambi i fattori sono stati stimati con valore pari a 4).

La classificazione finale del rischio è quindi il risultato della moltiplicazione tra i fattori: G - Gravità - Impatto (10) P - Probabilità. (mitigata dall'indice di copertura)

G - Gravità - Impatto

Rappresenta la conseguenza materiale dell'evento

P - Probabilità.

Rappresenta la probabilità che il fatto si verifichi.

Le probabilità che il management deve assegnare al fatto che l'evento si verifichi

Livello

Si può andare quindi da un potenziale Rischio Trascurabile 1 (dove entrambi i fattori sono valorizzati con 1) ad un Rischio Alto valutato con 16 (dove entrambi i fattori sono stati stimati con valore pari a 4).

La classificazione in fasce di gravità riportata in Tavola 3 (Rischio Trascurabile, Basso, Medio, Alto) consente di individuare congruamente le priorità di attuazione delle azioni stesse e quindi le aree e i processi nei quali è necessario intervenire per mitigare/eliminare il rischio.

Possono essere consigliate delle azioni di miglioramento anche nel caso di rischi valutati come trascurabili, nella direzione di un miglioramento complessivo dell'intero sistema.

Come si utilizzano Matrice e schema

La Matrice è utile sia per la categoria dei reati che possono essere rilevati nelle scritture contabili (già con rischio infrazione assegnato in base alla procedura descritta) sia per gli altri reati dando una metodologia di approccio che il componente l'OdV può utilizzare sia con l'ausilio degli altri organi di controllo (i.e. Collegio sindacale, Revisore legale ecc.) sia con professionalità interne adatte ai vari settori operativi (I.T., ufficio legale, SSPP, Ambiente ecc) sia con esperti esterni all'uopo incaricati dalla società o dall'OdV stesso in base all'autonomia finanziaria che il legislatore ha voluto concedergli). La matrice dalla quale si decide la rilevanza

Nota:

(10) Magnitude Of The Potential Loss.

di possibilità che vi siano procedure fuorvianti va utilizzata dopo che l'OdV ha individuato il Rischio di Infrazione (per i reati di bilancio) e dopo aver consultato le professionalità sopra indicate e verificato le procedure per i reati di altro tipo. Ecco che l'OdV dopo aver deciso in base alla

Matrice la probabilità di commissione del reato potrà elencare, utilizzando la Tavola 3 il livello di Rischio di commissione del reato specifico. prima di procedere ad un successivo intervento sulle procedure (Specifici Protocolli) al fine di migliorare le procedure in essere.

LIBRI

Manuale del revisore legale

di Alberto Pesenato

V Edizione, Ipsoa, 2012, pagg. 1900, € 99,00

Con Cd-Rom

Il Manuale fornisce, a chi svolge l'attività di sindaco e revisore legale, ogni strumento necessario per poter eseguire in modo completo la revisione legale nell'ambito delle aziende industriali e commerciali non quotate nonché nelle PMI applicando il metodo del **Risk Approach**. Ogni strumento qui presentato fa esplicito riferimento agli I.S.A. (International Standards on Auditing) richiamandoli in tutte le carte di lavoro proposte.

La quinta edizione del Manuale del revisore legale è integrata con nuove check lists sul **Controllo della Qualità**, una più omogenea esposizione dei capitoli dedicati alla determinazione del Rischio di Revisione, Rischio Intrinseco e di altri strumenti operativi oltre che rivisitata nel testo.

Il volume risulta essere la più completa, esaustiva ed aggiornata trattazione sul tema specifico e, sotto l'aspetto metodologico ed applicativo, rimane a tutt'oggi un'assoluta novità, il più completo riferimento nel panorama editoriale professionale in materia di revisione contabile in Italia.

Il punto di forza del volume è il **Cd-Rom allegato** che contiene tutti gli strumenti operativi per svolgere la revisione legale con riferimento agli I.S.A.; ogni strumento evidenzia il capitolo di riferimento per una immediata e facile consultazione.

Tutti i questionari, programmi di revisione, formulari e check lists sono tratti dai Principi di Revisione I.S.A., dalla «Pratica Professionale» italiana ed internazionale (Auditing Guidelines) e dai principi statuiti dalla Treadway Commission nei CoSO Report I e III che sono considerati quale *best practice* per la costruzione di un efficace sistema di controllo interno e nel Financial Reporting.

Per ulteriori informazioni o per l'acquisto:

Redazione: tel. 02.82476085

- **Servizio Informazioni Commerciali Ipsoa**
Tel. 02.82476794 - fax 02.82476403
- **Agenzie Ipsoa di zona**
(www.ipsoa.it/agenzie)
- **www.ipsoa.it**

