OdV e Modello di Organizzazione Gestione e Controllo: vigilanza e cura dell'aggiornamento

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

L'estensore del Modello ex D. Lgs. 231/2001 ed in seguito l'Organo di Vigilanza che ne deve curare l'aggiornamento si trovano di fronte alla scelta dei principi a cui fare riferimento, quale metodologia usare e che strumenti utilizzare per far sì che il Modello produca gli effetti desiderati. Le linee guida ASSTRA accolgono i documenti CoSO, peraltro richiamati dalla circolare 83607/2012 della GdF Vol. III, essi, se integrati dai principi di revisione ISA riferiti ai rischi di illeciti, frodi ed errori, sono un sicuro riferimento in tal senso.

Metodologie e principi di riferimento

Tutte le aziende senza esclusione (Tavola 1) sono poste davanti all'incombenza di applicare il D.Lgs. n. 231/2001 e quindi al dilemma di come gli organi aziendali debbano organizzare pianificare ed eseguire il proprio intervento e «con quali strumenti» l'Organo di Vigilanza debba effettuare la funzione ad esso demandata (1).

L'estensore del Modello (2) e successivamente l'Organo di Vigilanza si trovano di fronte alla scelta dei principi a cui fare riferimento e conseguentemente a quale metodologia applicare per la costruzione del «Modello» ed infine quali strumenti impiegare perche questo produca gli effetti desiderati.

Il tema è tanto più complesso quanto ci si propone di applicarlo a società non quotate in generale ed alle PMI in particolare.

Vi sono documenti professionali ormai da anni di riferimento in dottrina quali i *Reports* emessi dalla *Treadway Commission* e detti *CoSO Reports I, II, III* (3).

Nella metodica seguita i tre documenti vanno integrati dai principi di revisione ISA (4) riferiti a rischi illeciti, frodi ed errori nonché dalla pratica professionale in materia di revisione contabile riferita alla costruzione del miglior controllo interno (specifici protocolli).

Questo metodo si basa, come già detto, sui documenti della Commissione CoSO (*Committee of Sponsoring Organizations of the Treadway Commission*) analizzati nel seguito (5).

Note:

(*) Revisore legale, Consulente Area D. Lgs. 231/2001, Presidente OdV di Trentino Trasporti Esercizio SpA, Karrell Srl.

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

(1) L'Art. 6.1.b del Decreto stabilisce che vi sia un Organismo deputato alla vigilanza sul funzionamento e osservanza del modello nonché la cura del suo aggiornamento.

(2) Si veda la «Il modello di organizzazione gestione e controllo ex D Lgs. n. 231/2001» WKI - IPSOA III Edizione 2011 e contributi in www.albertopesenato.net

(3) I concetti di risk management e risk Assessement enunciati nel documento CoSO II sono richiamati nelle linee guida ASSTRA da pag. 20 a pag 28 ed in appendice da pag. 169 a pag. 180; gli stessi sono pretesi dalla circolare 83607/2012 della GdF Vol. III pag.76 riga seconda.

(4) P.R. n. 240 - La responsabilità del revisore nel valutare la possibile esistenza di frodi ed errori, P.R. n. 250 - effetti connesi alla conformità a leggi e regolamenti, P.R. n. 315 - Comprendere l'impresa ed il suo contesto, valutare i rischi di errori significativi, P.R. n. 330 - Le procedure di revisione in funzione di rischi identificati, P.R. n. 440 - Valutazione degli errori identificati nel corso della revisione contabile, P.R. n. 550 - Le parti correlate, P.R. 560 - Gli eventi successivi, P.R. n. 570 - Continuità aziendale 1010 : Considerazione delle questioni ambientali nella revisione del bilancio.

(5) Il presente contributo è un'evoluzione di quanto affermato nel paragrafo 1.6 della III edizione Op, Cit. e del contributo pubblicato dagli stessi autori su *Amministrazione&finanza* n. 8/2011, «Modello di Organizzazione Gestione e Controllo: un approccio sistematico».

CoSO Report (I) Il sistema di controllo interno - Un modello integrato per la gestione dei rischi aziendali - Progetto Corporate Governance per l'Italia (2008)

Il documento *CoSO* (I) tratta del miglior sistema per costruire un adeguato ed efficiente sistema di
controllo interno per la gestione dei rischi aziendali.
Il Documento esemplifica le cinque componenti del controllo interno (6):
1) ambiente di controllo;
2) valutazione dei rischi;
3) attività di controllo;
4) informazione e comunicazione;
5) monitoraggio.

CoSO Report (II). La gestione del rischio aziendale (ERM Entreprise Risk Management)

È opportuno premettere che il documento analizza il generale rischio strategico di gestione aziendale e propone la gestione dello stesso (risk management).
La valutazione del rischio (risk assessment) e la gestione dello stesso (risk management) (7) sono aspetti che riguardano il complesso dell'attività dell'azienda all'interno della quale possono essere commessi i reati ed illeciti previsti dal dereto e non si riferisce solamente e specificatamente ad essi.
Esso fa riferimento ai rischi strategici della gestione aziendale, gli obiettivi aziendali possono essere cosi' individuati (8):
• strategici: sono espressi in termini generali e devono essere allineati alla mission aziendale e la devono supportare. Riflettono la scelta del management di come l'azienda si adopera per creare valore per i suoi stakeholders;
• operativi: riguardano l'efficacia e l'efficienza delle operazioni aziendali. È necessario che riflettano l'ambiente micro - macro economico nel quale l'azienda opera. Il manage-

Note:
(6) Op.cit. Tali principi sono esplosi in adeguate check list nel testo da pag. 233 a pag. 277 (Cap. 5) e nel CD: ai punti 11.1 e 11.2 del Dossier Governance. E in Unità Operative da pag. 428 a pag. 661 Cap. 6) e nel Cd: file Unità Operative.
(7) Argomenti di indubbio interesse che saranno oggetto di prossimi contributi.
(8) «La gestione del rischio aziendale» *ERM Enterprise Risk Management (CoSO II)* Il Sole 24Ore - Pagg. 3, 4, 22, 23.

Tavola 1 - Ambito di applicazione del D.Lgs. n. 231/2001

Corte di Cassazione - Sentenza 18941/2011:
«...peraltro è indubbio che la disciplina dettata dal decreto 231/2001 sia senz'altro applicabile alle società a. responsabilità limitata c.c. ''unipersonali'' così come è notorio che molte imprese individuali ricorrono ad una organizzazione interna complessa che prescinde dal sistematico intervento del titolare dell'impresa per la soluzione di determinate problematiche che può spesso involgere la responsabilità di soggetti diversi dall'imprenditore ma che operano nell'interesse della persona individuale.
Ed allora una lettura costituzionalmente orientata della norma in esame dovrebbe conferire al disposto di cui al comma 2 dell'articolo 1 del decreto in parola una portata più ampia, tanto più che non cogliendosi nel testo alcun cenno riguardante le imprese individuali, la loro mancata indicazione non equivale a un'esclusione, ma, semmai a un'implicita inclusione enll'area dei destinatari della norma.
Si ricorda qui che nel 2004 la stessa Corte di Cassazione aveva sostenuto che la responsabilità amministrativa poteva essere applicata solo agli enti dotati di personalità giuridica che siano strutturati in forma societaria o pluripersonale.»
Legge regionale 27 maggio 2011 n. 15.
In vigore dallo scorso 9 giugno, la legge impone agli enti dipendenti e strumentali della Regione Abruzzo, con o senza personalità giuridica, ai consorzi, alle agenzie e alle aziende regionali, nonché alle società controllate e partecipate dalla Regione ad esclusione degli enti pubblici non economici, di conformarsi al DLgs. 231/2001. Detto obbligo è motivato dal riconoscimento dell'importanza dei principi di legalità, trasparenza, eticità, lealtà e correttezza nell'affidamento, esercizio ed espletamento dei servizi di pubblica utilità e della normativa in materia di sicurezza del lavoro. Nel testo normativo si legge che, ''al fine di realizzare i presupposti per l'esenzione della responsabilità amministrativa per gli illeciti amministrativi dipendenti da reato'', i soggetti elencati dovranno adottare entro sei mesi i modelli di cui agli artt. 6 e 7 del DLgs. 231/2001 che prevedono, in relazione alla natura dei servizi e delle attività svolte e alla dimensione dell'organizzazione, misure idonee a garantire il rispetto della legalità, dell'eticità e della trasparenza, nonché a individuare e ad eliminare preventivamente e tempestivamente eventuali situazioni a rischio.

ment deve assicurarsi che gli obiettivi siano reali, riflettano le esigenze del mercato e siano espressi nei giusti termini al fine di consentire un'attendibile valutazione della performance;
• di reporting: riguardano le informazioni, che devono essere accurate, complete e coerenti con i fini perseguiti;
• di conformità: le aziende devono condurre le loro attività (e spesso assumere provvedimenti particolari) in conformità alle leggi e ai regolamenti in vigore.
Lo studio (ERM) ha identificato otto componenti del sistema di controllo tra loro interconnessi.
Questi componenti sono:
• ambiente interno: il management formula la filosofia di base e determina il livello di accettabilità del rischio. Determina, in termini generali, i modi in cui il rischio è considerato e affrontato dalle persone che operano in azienda;
• definizione degli obiettivi: gli obiettivi devono essere fissati prima di procedere all'identificazione degli eventi che possono pregiudicare il loro conseguimento;
• identificazione degli eventi: devono essere identificati gli eventi che possono avere un impatto sull'attività aziendale. Comporta l'identificazione di fatti potenziali di origine interna e esterna che possono pregiudicare il conseguimento degli obiettivi.
È necessario distinguere gli eventi che rappresentano rischi da quelli che rappresentano opportunità;
• valutazione del rischio: i rischi identificati (rischi di gestione) sono analizzati al fine di determinare come devono essere gestiti. I rischi sono collegati agli obiettivi e possono pregiudicarne il raggiungimento. I rischi sono valutati sia in termini di rischio inerente (9) (qui inteso come rischio in assenza di qualsiasi intervento) sia di rischio residuo (rischio dopo aver attivato interventi per ridurlo), determinando la probabilità che il rischio si verifichi e il relativo impatto;
• risposta al rischio: il management identifica e valuta le risposte possibili al rischio, che potrebbero essere: evitare, accettare, ridurre e compartecipare il rischio. Seleziona una serie di azioni per allineare i rischi emersi con la tolleranza al rischio e al rischio accettabile;
• attività di controllo: devono essere definite e realizzate politiche e procedure per assicurare che le risposte al rischio siano efficacemente eseguite;
• informazioni e comunicazione: le informazioni pertinenti devono essere identificate, raccolte e diffuse nella forma e nei tempi che consentano alle persone di adempiere alle proprie responsabilità. Si devono attivare comunicazioni efficaci in modo che queste fluiscano per l'intera struttura organizzativa: verso il basso, verso l'alto e trasversalmente;
• monitoraggio: l'intero processo deve essere monitorato e modificato se necessario.
Il monitoraggio si concretizza in interventi continui, integrati nella normale attività operativa aziendale, in valutazioni oppure in una combinazione dei due metodi.
In definitiva si determinano gli obiettivi, identificano gli eventi ed affrontano l'eventuale rischio aziendale che è essenzialmente un «rischio di gestione» che dipende dalla strategia adottata dal CdA.
In effetti gli eventi che si devono analizzare a dai quali discendono i possibili rischi derivano da fattori esterni ed interni (10).

Fattori esterni (esogeni)
• l'economia: oscillazione prezzi, disponibilità capitale, liquidità, concorrenza, disoccupazione;
• l'ambiente: inondazioni, incendi, terremoti, inquinamento, rifiuti, energia, sviluppo sostenibile;
• la politica: cambiamenti del contesto politico,legislazione, politiche pubbliche, regolamentazione;
• il sociale: terrorismo, demografici, dei costumi ed abitudini, privacy;
• la tecnologia: Cambiamenti tecnologici, commercio elettronico, tecnologia emergente.

Fattori interni (endogeni)
• le infrastrutture: investimenti per realizza-

Note:
(9) Si fa notare come nella pratica professionale per la determinazione del rischio di infrazione il rischio intrinseco abbia come significato che i fatti aziendali ovvero le operazioni registrate possano contenere operazioni cosiddette «sensibili».
(10) «La gestione del rischio aziendale» ERM Enterprise Risk Management (CoSO II) Il Sole 24Ore - Pagg. 48 - 49 - 53.

re un programma di manutenzione, un call center;
• il personale: scioperi, risorse umane, salute e sicurezza;
• i processi: tutto ciò che può causare perdite delle quote di mercato, inefficienze ecc.;
• la tecnologia: integrità dei dati, scelte di sistema, sviluppo, diffusione;
Si analizzano i fattori e conseguentemente si identificano gli eventi che possono pregiudicare il conseguimento degli obiettivi aziendali.
Questo approccio si basa sul «rischio di gestione» che dipende dalla strategia aziendale.

CoSO Report (III). Il controllo interno per l'attendibilità del Financial Reporting (2009)

Il documento CoSO (III) si concentra sulle *Smaller Company* (11) anche qui indicando la metodologia migliore per produrre dei *financial reporting* attendibili (si intende come *financial reporting* quanto viene presentato dall'azienda come bilancio e relativa informativa economico finanziaria).
Orbene, si può affermare che se un buon controllo interno produce una corretta informativa economico finanziaria ed esso può confortare il management su una regolare esecuzione delle procedure e che il sistema messo in atto sia efficace nel controllo dell'operato delle Unità Operative.
Ne risulta che i fatti di gestione sono correttamente riportati nelle scritture contabili ma anche che derivano da procedure statuite verificate da più persone competenti e per questo motivo non soggette a ledere l'azienda producendo un illecito o reato.
Ecco che l'intervento che qui si propone consiste nella verifica innanzitutto della moralità del management e nella sua capacità di trasmettere la stessa a tutti i collaboratori nonché nella rigorosa applicazione dei collaboratori nel seguire le procedure (quei specifici protocolli indicati dall'art. 6) statuite.
Ne consegue che è l'attenzione che porrà l'Organo di Vigilanza nel creare, affinare ed aggiornare i necessari metodi di contrasto da inserire negli usuali processi operativi che determinerà il costante carattere esimente del modello nelle parti operative degli organi di *governance* e nelle Unità Operative (12).
Sono le voci del bilancio conseguenti alla registrazioni contabili, prodotte dai fatti di gestione, rilevate nel corso dell'anno (esercizio) che possono contenere fatti di gestione «sensibili» o illeciti.
È nel bilancio che devono principalmente essere ricercate, nel corso delle verifiche proprie dell'Organo di Vigilanza, le eventuali commissioni dell'illecito o reato previsto dal Decreto 231/2001.
La ricerca dovrà partire, *in primis*, dalle transazioni finanziarie (13) ed eventualmente da altri comportamenti o carenze di regole che possono portare alla commissione di illeciti o reati in altri settori che non riguardano direttamente transazioni finanziarie (i.e. sicurezza sul lavoro, abbandono di rifiuti, diritti d'autore, false dichiarazioni ecc.).
Come già detto il sistema che qui si propone fa riferimento ai documenti CoSO I, II e III integrati dalla metodologia e *best practice* in materia di revisione contabile per determinazione del cosiddetto *rischio di revisione* che può ben facilmente essere interpretato come rischio di infrazione.
Nell'eseguire i controlli l'OdV dovrà porre particolare attenzione ad eventi o transazioni significative.
Un fatto di gestione significativo può essere espressione di una operazione irregolare, illecita o essere manifestazione di un reato ed è per questo motivo che queste transazioni devono essere verificate sia come legittimità sia nel merito.
Per quanto riguarda i reati che non hanno espressione sul bilancio, (si pensi alla sicurezza sul lavoro, i reati informatici ecc) l'OdV dovrà predisporre altri strumenti (14) e consultare altre professionalità per individuare la possibilità di commissione degli stessi.

Note:
(11) Si fa notare che il significato è strettamente riferito ad entità «più piccole» che non si identificano con PMI.
(12) Op. cit. Vedere Par. 1.2.3.
(13) Si escludono tutti quei reati che non comportano transazione finanziaria come quelli riferiti alla sicurezza sul lavoro, parte dei diritti d'autore, parte dei reati informatici, reati contro la personalità individuale e così via per i quali si devono adottate apposite e più specifiche metodologie di ricerca.
(14) L'argomento,di indubbio interesse, sarà oggetto di prossimi contributi.