ORDINE DEI DOTTORI COMMERCIALISTI E DEGLI ESPERTI CONTABILI
BRESCIA

MODELLI EX D.LGS 231/2001 E SISTEMI DI CONTROLLO INTERNO: METODOLOGIE, BEST PRACTICE DI RIFERIMENTO E STRUMENTI DI SUPPORTO PER L'ATTIVITÀ DI VIGILANZA DEL COLLEGIO SINDACALE

A cura di Fabio Fada, Marco Bombardieri

Commissione Consultiva
Collegio sindacale:Controlli di legalità e Modello 231

Coordinatore: Cristarella Vincenzo - **Delegato del Consiglio:** Cossu Leonardo
Membri: Bombardieri Marco - Bonardi Walter - Caporale Nicola - Fada Fabio - Miglio Elena Francesca - Pelosi Francesca - Piatti Andrea - Ridoli Guido - Zola Mariacristina

1. Introduzione

Il presente documento vuole essere di ausilio ai professionisti che in qualità di componenti del collegio sindacale si trovino a valutare la bontà dei Modelli organizzativi adottati presso le Società per quanto riguarda la delicata fase del *risk assessment*: fase prodromica all' iniziale disegno del modello organizzativo e anche poi dei successivi aggiornamenti.

Non vuole essere un trattato esaustivo su come deve essere redatto un *risk assessment* ma vuole essere uno strumento pratico che permetta al professionista, ma anche alle aziende stesse, di effettuare una valutazione preliminare e sufficientemente ragionevole per addivenire alla conclusione che tale processo sia stato fatto correttamente e soprattutto se risulta formalizzato in una forma adeguata o necessiti di ulteriori approfondimenti e/o di una migliore e più efficace formalizzazione.

In coda al documento, dopo una disamina degli aspetti sostanziali ma anche formali del processo, si allega un "*Decision Tree*", collegato a quanto esposto nel documento, che ha lo scopo di aiutare il valutatore nel pervenire ad una conclusione circa l'adeguatezza dell'analisi dei rischi e relativo disegno dell'architettura dei presidi di controllo.

2. Il sistema di controllo interno

L'efficacia di un Modello Organizzativo e gestionale ai sensi del D.lgs 231/2001 ha innanzi tutto come presupposto un corretto collegamento, "innesto" o, meglio ancora, una vera e propria "integrazione", tra *compliance program*[1] *ex D.lgs 231/2001* e sistema di controllo interno dell'azienda.

Questa è probabilmente la fase dell'intero programma di adeguamento normativo in cui trova la propria espressione massima la doppia "natura" del percorso di analisi che deve essere attuato ai fini di una efficace implementazione di un Modello 231: "giuridico-penale", da un lato, e "aziendalistico", dall'altro.[2]

Se inizialmente nel disegno di siffatto Modello prevale la componente "giuridico-penale", necessaria per inquadrare i requisiti normativi, da un certo momento in poi occorre anche entrare nella realtà operativa dell'azienda. Sarà quindi necessario fare riferimento agli istituti, alle definizioni, alle metodologie, agli strumenti, propri delle materie aziendalistiche: primo fra tutti, la definizione stessa di sistema di controllo interno[3].

---

[1] Riferendoci alla più recente letteratura internazionale in materia, per *compliance program* qui intendiamo un sistema di programmi, procedure protocolli adottati dagli Enti nel rispetto di leggi, regolamenti, linee guida , disposizioni emanate da autorità ed organi governativi, locali e sovranazionali.

[2] Cfr. S. De Masi , *Compliance program* ex D.Lgs 231/2001 e sistemi di controllo interno: una chiave di lettura aziendalistico-giuridica delle metodologie, degli strumenti, delle *best practice* di riferimento e delle nuove Linea Guida di Confindustria. Master di II livello in Diritto penale dell'Impresa – Università Cattolica del Sacro Cuore, saldemasi@deloitte.it.

[3] Anche su tale ambito la letteratura è sterminata. Si preferisce quindi fare un richiamo che possa poi ricondurre a tutti gli altri. Cfr. C. Dittmeier, *Internal Auditing – Chiave per la corporate governance*, Egea, 2011.

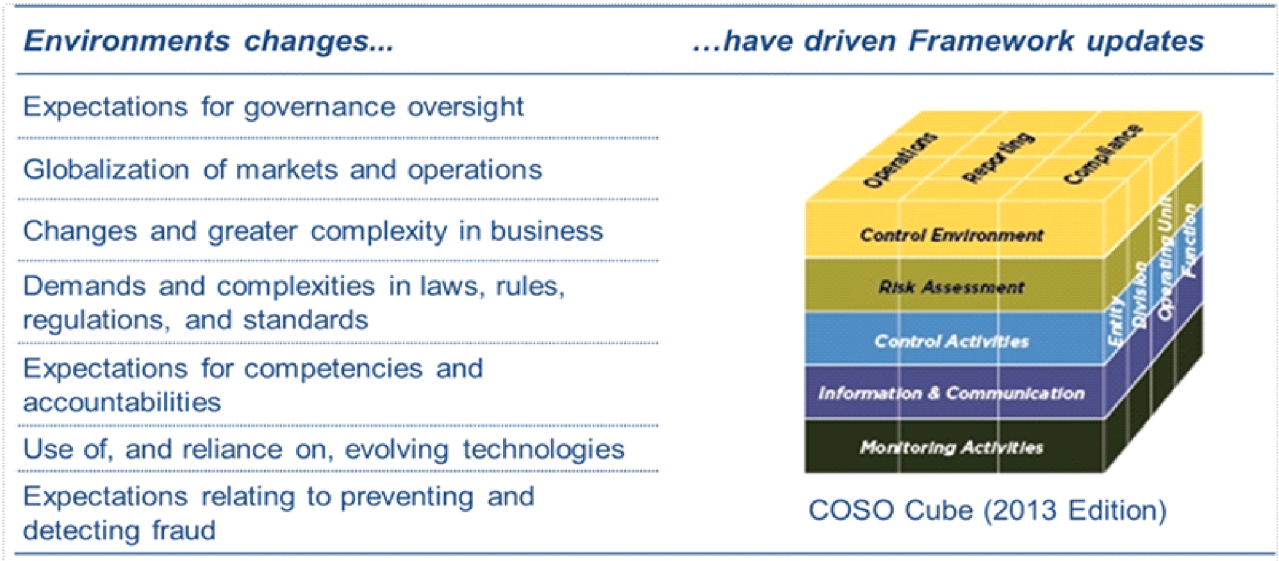
Per entrare nel merito dei sistemi di controllo interno si può facilmente ricorrere a metodologie e definizioni ormai consolidate nella dottrina aziendalistica.

In tal senso gli *standard* ed i *framework* di riferimento sono numerosi. Ai fini della presente trattazione si prenderà in considerazione quello che probabilmente può essere ritenuto il più rappresentativo e, sicuramente, quello che è stato aggiornato più recentemente: il *CoSO Framework*[4].

A maggio del 2013, il Committee of Sponsoring Organizations of the Treadway Commission ("CoSO") ha pubblicato l'aggiornamento dell'*Internal Control - Integrated Framework* che, dal 1992, è ampiamente riconosciuto come uno dei principali *standard* di riferimento internazionali per il disegno, l'implementazione e la gestione dei sistemi di controllo interno, nonché per la valutazione della loro adeguatezza ed efficacia.

Già nel 1992, il *CoSO Framework* nasceva per dare una risposta organica e strutturata alle numerose istanze di miglioramento e rafforzamento dei sistemi di controllo interno. Nel 2004, lo stesso CoSO pubblicava l'*Enterprise Risk Management - Integrated Framework*, come risposta alle crescenti esigenze di identificare, valutare e gestire i rischi di impresa in modo efficace.

Oggi, pur mantenendo valida l'impostazione originaria, il CoSO *Framework* (nella versione del 2013) intende fornire nuove e ulteriori risposte alle crescenti complessità del business e del contesto economico, alle nuove istanze che derivano dall'utilizzo della tecnologia e dai fenomeni di globalizzazione (si veda al riguardo la sintesi grafica sottostante, così come fornita dallo stesso *Committee of Sponsoring Organizations of the Treadway Commission*).



Negli anni, la definizione di sistema di controllo interno è comunque rimasta inalterata: "*il sistema di controllo interno è un processo, svolto dal consiglio di amministrazione, dai dirigenti e da altri soggetti della struttura aziendale, finalizzato a fornire una ragionevole sicurezza sul conseguimento*

[4] Cfr. Committee of Sponsoring Organizations of the Treadway Commission, *Internal Control – Integrated Framework*, 2013.

degli obiettivi delle attività operative, dell'informativa di bilancio e della conformità alle leggi e ai regolamenti in vigore"[5].

Il CoSO *Framework* articola tale definizione in un sistema integrato e pervasivo, che contempla tre categorie di obiettivi che consentono alle organizzazioni di focalizzarsi su diversi aspetti del controllo interno:

- *Operations Objectives*: afferente alla efficacia ed efficienza delle attività operative dell'impresa, che includono obiettivi di performance operativi e finanziari, nonché la salvaguardia del patrimonio e delle risorse aziendali;
- *Reporting Objectives*: afferente all'informativa finanziaria e gestionale interna ed esterna, alla sua attendibilità e integrità, tempestività, trasparenza o altri requisiti secondo quanto richiesto dai *regulators*, dagli *standard* di riferimento o dalle *policies* interne proprie dell'organizzazione;
- *Compliance Objectives*: afferente al rispetto di leggi e regolamenti ai quali l'azienda è chiamata a rispondere a vario titolo.

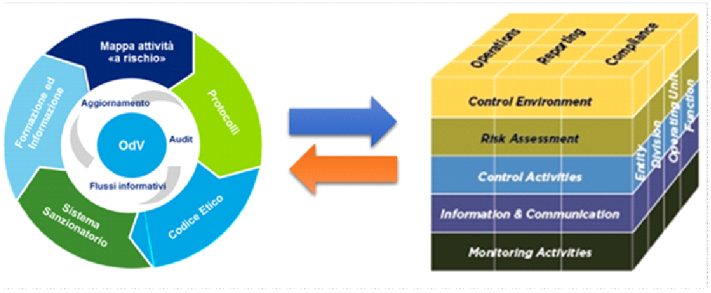
E' quindi possibile sviluppare in azienda un sistema di controllo interno ispirato a *framework* internazionali riconosciuti e collaudati da anni, integrati e pervasivi, in grado di abbracciare l'intera organizzazione - a livello centrale e periferico - attraverso le componenti *standard* del controllo: *Control Environment*; *Risk Assessment*, *Control Activities*, *Information and Communication* e *Monitoring*.
Occorre altresì tener presente che tale *framework* e il sotteso sistema di controllo, nasce all'interno dell'azienda per rispondere ad obiettivi e finalità diversi: di tipo operativo, di *financial reporting* e normativo.

Allorquando l'obiettivo sia disegnare, implementare, valutare l'adeguatezza e/o gestire un sistema di controllo interno, rispetto alle finalità specifiche di una normativa, sarà quindi necessario rileggerne tutte le componenti alla luce del dettato normativo di riferimento, in base alle caratteristiche che dovrà avere il *compliance program* cui si intende aderire.

Tale chiave di lettura è imprescindibile al fine di contenere il rischio che un sistema di controllo interno, magari idoneo dal punto di vista degli obiettivi di *performance* e operativi oppure di *financial reporting*, possa invece rivelarsi inadeguato rispetto a *standard* più rigidi imposti dal legislatore, per tutelare interessi esterni, in una accezione più ampia rispetto all'autodeterminazione che in alternativa si darebbe la *societas* in modo autonomo rispetto ai rischi di impresa più tipici. Questo è un aspetto critico, che a volte può sfuggire all'aziendalista che utilizzi questi strumenti in modo acritico.

Avendo così introdotto i tratti salenti del *Framework* di riferimento - utili a tratteggiare le caratteristiche del sistema di controllo interno secondo schemi e strumenti propri delle realtà aziendali - il passaggio successivo richiede necessariamente l'attento collegamento e l'integrazione dei due ambiti dei *compliance program* ex D.Lgs. 231/2001 e del sistema di controllo interno (così come schematizzato nel grafico qui di seguito riportato):

[5] Cfr. Edizione Italiana del CoSO Framework, *Il sistema di controllo interno – Un modello integrato di riferimento per la gestione dei rischi aziendali*, Il Sole 24 Ore, 2006



E’ con questa particolare chiave di lettura che appare pertanto necessario ripercorrere i passaggi salienti di almeno due momenti essenziali del sistema di controllo interno e del programma di *compliance* ai fini del D.Lgs 231/2001: l’identificazione dei rischi e il disegno dell’architettura dei presidi di controllo.

3. L’identificazione dei rischi

Una delle carenze più frequenti e anche a maggiore impatto sul grado di "tenuta" del modello al cospetto del Codice Penale si rinviene proprio nella inadeguatezza dell'analisi dei rischi (*Risk Assessment*), così come richiesta dal comma 2, lett. a), dell'art. 6 del Decreto.
In tal senso, le nuove Linee Guida di Confindustria per la costruzione dei modelli di organizzazione, gestione e controllo, aggiornate al marzo del 2014, introducono (rispetto alla versione precedente del 2008) un chiaro richiamo al CoSO Framework già descritto, evidenziando però le specificità applicative, "ferma restando l’esigenza che ogni impresa costruisca e mantenga in efficienza il proprio sistema di gestione dei rischi e di controllo interno anche in ottica di *compliance* integrata".

In particolare, viene in evidenza una specifica declinazione del concetto di rischio: "... per rischio si intende qualsiasi variabile o fattore che nell'ambito dell'azienda, da soli o in correlazione con altre variabili, possano incidere negativamente sul raggiungimento degli obiettivi indicati dal Decreto 231 ... pertanto, a seconda della tipologia di reato, gli ambiti di attività a rischio potranno essere più o meno estesi".

I passi operativi da compiere nello svolgimento del *Risk Assessment* ed i relativi output richiesti dalle *best practice* di riferimento, coerentemente con i requisiti del Decreto, possono essere a questo punto così sintetizzati:

i. inventariazione degli ambiti aziendali di attività a rischio (eventualmente distinguendo tra aree a rischio-reato in senso proprio e aree c.d. strumentali alla commissione di reati).
   Output: mappa delle aree a rischio e dei reati rilevanti;
ii. analisi dei rischi potenziali.
   Output: mappa documentata delle potenziali modalità attuative degli illeciti nelle aree a rischio;
iii. valutazione/costruzione/adeguamento del sistema di controlli preventivi.
   Output: descrizione documentata del sistema di controlli preventivi attivato e degli adeguamenti eventualmente necessari.

Premesso che qualsiasi sistema di gestione dei rischi deve necessariamente partire dalla individuazione degli obiettivi attesi - rispetto ai quali, per l'appunto, i rischi possono rappresentare delle evenienze avverse o addirittura favorevoli (c.d. "rischio-opportunità") - appare chiaro quanto importante sia definire correttamente la finalità specifica del "*Risk Assessment* 231" e quale tipo di errore possa facilmente derivare in fase di inventariazione e valutazione da un'applicazione acritica e impropria di una metodologia di stampo meramente aziendalistico, che non contempli il portato giuridico-normativo del programma di *compliance* di riferimento.

In tal senso, proprio al fine di mettere in evidenza i diversi modelli applicativi e gli aspetti sui quali riporre maggiore attenzione "nell'adattare" *il framework* di riferimento alle finalità del *compliance program*, si reputa opportuno fornire alcune esemplificazioni concrete.

Se l'obiettivo cui punta il sistema di controllo interno e il collegato framework di riferimento fosse, ad esempio, rivolto soltanto alla tutela dei rischi/opportunità di business proprie dell'impresa, quindi alla valorizzazione/salvaguardia delle risorse dell'azienda o delle performance operativo-gestionali, gli obiettivi rispetto ai quali andare a rintracciare i possibili rischi sarebbero quelli identificati nei piani strategici del Consiglio di Amministrazione. I criteri di identificazione e misurazione dei rischi sarebbero pertanto commisurati a parametri interni, propri ed esclusivi della sfera di interessi della società, quali ad esempio, il *risk appetite* e la *risk tolerance* dell'azionista e del *board*[6].

Non solo cambiano gli obiettivi, le modalità di misurazione e le soglie di accettabilità dei rischi ma, in funzione della diversa finalità del *Risk Assessment*, è necessario anche cambiare l'universo di riferimento alla base dell'*assessment* stesso (cioè l'oggetto della valutazione).

Se invece l'obiettivo si sposta, ad esempio, dai rischi di business ai rischi collegati alla corretta informativa finanziaria verso l'esterno, l'identificazione e la misurazione degli stessi deve prevedere approcci specifici, ad esempio, attraverso l'applicazione delle cosiddette soglie di "materialità", a loro volta collegate alla significatività del dato e dell'informativa di bilancio/contabile, quindi a concetti quali quelli dell'errore tollerabile ovvero di *material weaknesses*.

Come si intuisce, già in questa seconda esemplificazione, si sposta l'attenzione da obiettivi e interessi puramente e semplicemente interni all'impresa verso interessi riconducibili a soggetti esterni all'organizzazione, quali per l'appunto il pubblico dei risparmiatori o degli investitori operanti su mercati finanziari regolamentati e alla modalità con cui questi soggetti terzi prendono in considerazione l'informativa finanziaria per formulare loro valutazioni esterne sulla realtà aziendale in considerazione.

Continuando in questa disamina delle diverse finalità del *Risk Assessment*, appare adesso più chiaro che gli obiettivi sottesi alla identificazione dei rischi-reato saranno ancora diversi rispetto agli esempi fatti pocanzi e che questi nuovi rischi saranno necessariamente quelli che l'ordinamento

[6] L'Enterprise Risk Management (ERM) assicura che il management abbia attivato un adeguato processo di definizione degli obiettivi, di business e di governo, coerenti con la mission dell'azienda e in linea con i livelli risk appetite (propensione all'assunzione del rischio) e di rischio accettabile (soddisfazione dei rischi residui dopo le misure di mitigazione delle singole situazione di rischio)", Cfr. C. Dittmeier, Internal Auditing, cit.

stesso identifica come rischi collegati agli interessi tutelati dai singoli reati indicati nella parte speciale dello stesso D.Lgs. 231/2001.

Non è quindi pensabile effettuare un *"Risk Assessment* 231" adottando in modo acritico gli strumenti e le metodologie nate per soddisfare finalità diverse. Già nella fase preliminare, di identificazione dei rischi applicabili, dovrà essere utilizzato un elenco specifico per i *corporate crimes*, del tipo qui di seguito schematizzato:

Tabella a)

ELENCO REATI PRESENTI NEL D.LGS.231/2001				
ARTICOLO	**GRUPPO REATI**	**SINGOLO REATO**	**LEGGE CHE LO INTRODUCE**	**Applicabilità**
Artt. 24 e 25	*Reati contro la PA*	Concussione Corruzione Malversazione a danno dello stato Indebita percezione di erogazioni a danno dello Stato Truffa a danno dello Stato o di un altro ente pubblico Truffa aggravata per il conseguimento di erogazioni pubbliche Frode informatica Induzione indebita a dare o promettere utilità	D. Lgs. 231/2001 Legge "Anticorruzione". n.190/2012 (modificato)	SI
Art. 24-bis	*Reati informatici*	Delitti informatici e trattamento illecito di dati	Legge 48/2008	SI
Art. 24-ter	*Criminalità organizzata*	Delitti di criminalità organizzata	Legge 94/2009 d.d.l. 1969-D, 19 settembre 2012 (modificato)	NO
Art. 25-bis	*Falso nummario* *Marchi e brevetti*	Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento	D.L. 350/2001, convertito con modificazioni dalla L n. 409/2001 (introdotto) Legge n. 99/2009 (modificato)	NO
Art. 25-bis.1	*Turbativa di mercato*	Turbata libertà dell'industria e del commercio	Legge n. 99/2009	SI
Art. 25-ter	*Reati societari*	False comunicazioni sociali Formazione fittizia del capitale Impedito controllo Indebita restituzione di conferimenti Illegale ripartizione di utili e di riserve Operazioni in pregiudizio dei creditori Illecita influenza sull'assemblea Aggiotaggio Omessa comunicazione di conflitto di interessi Ostacolo all'esercizio delle funzioni delle autorità di vigilanza Corruzione tra privati	D.Lgs.61/2002 Legge 262/2005 (modificato) D.Lgs. n. 39/2010 (modificato) Legge "Anticorruzione". n.190/2012 (modificato)	SI
Art. 25-quater	*Terrorismo*	Reati con finalità di terrorismo o eversione dell'ordine democratico	Legge n. 7/2003	NO
Art. 25-quater.1	*Lesioni personali*	Pratiche di mutilazione degli organi genitali femminili	Legge n. 7/2006	NO
Art. 25-quinquies	*Personalità individuale*	Delitti contro la personalità individuale	Legge n. 228/2003 d.d.l. 1969-D, 19 settembre 2012 (modificato)	SI
Art. 25-sexies	*Market Abuse*	Manipolazione di mercato Abuso di informazioni privilegiate	Legge n. 62/2005	NO
Art. 25-septies	*Sicurezza sul lavoro*	Omicidio colposo e lesioni colpose gravi o gravissime commessi in violazione delle norme antinfortunistiche e della tutela dell'igiene e della salute sul lavoro	Legge n. 123/2007	SI
Art. 25-octies	*Ricettazione e riciclaggio*	Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita	D.Lgs. n. 231/2007	SI
Art. 25-novies	*Diritto d'autore*	Delitti in materia di violazioni del diritto d'autore	Legge 99/2009	SI
Art. 25-decies	*Intralcio alla giustizia*	Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria	Legge 116/2009 D.Lgs. 121/2011 (modifica in 25-decies)	SI
Art. 25-undecies	*Ambiente*	Reati ambientali	D.Lgs. 121/2011	SI
Art. 25-duodecies	*Immigrazione clandestina*	Impiego di Cittadini di Paesi terzi il cui soggiorno è irregolare	D.Lgs. 121/2012	SI
Art. 10 Legge 146/2006	*Transnazionali*	Reati transnazionali di associazione a delinquere, traffico di migranti, etc.	Legge 146/2006	NO

L'analisi e la valutazione dei rischi-reato richiede quindi la disamina di ogni singolo reato in base alle caratteristiche dell'ente, al suo business e alla sua storia, ma anche una valutazione puntuale (verrebbe da dire "in punto di diritto") dell'elemento oggettivo e soggettivo propri di ogni reato presupposto, al fine di comprendere se, ed in quali circostanze e con quali modalità, un determinato illecito possa essere commesso nell'interesse o a vantaggio dell'ente.

L'ente è chiamato ad effettuare una ricognizione dei fattori di rischio e degli elementi di criticità del proprio agire in base ai requisiti normativi applicabili (che derivano dal catalogo dei reati-presupposto) e al contesto situazionale in cui opera, al fine di comprendere e limitare la pericolosità delle proprie condotte (non solo in via diretta, ma eventualmente anche nella forma del concorso nel reato altrui)[7].

Si intuisce agevolmente che tale analisi non può essere svolta "a tavolino": richiede necessariamente il coinvolgimento dei soggetti responsabili delle aree operative, attraverso un approfondito assessment dei rischi-reato specifici delle rispettive aree di competenza (eventualmente supportati da risorse interne e/o esterne esperte in materia legale, di *risk management, internal auditing* e sistemi di controllo interno).

Inoltre, poiché l'obiettivo finale è di poter dare evidenza di tale processo "maieutica" di analisi e autovalutazione dei rischi-reato anche all'esterno (i.e. pubblico ministero/giudice penale), sarà necessario documentare accuratamente tale analisi, attraverso appositi elaborati: le c.di "matrici delle potenziali modalità attuative degli illeciti nelle aree a rischio".

La tabella sottostante fornisce un esempio della struttura dei contenuti di tali documenti e una esemplificazione grafica della matrice:

A) *Processi sensibili aziendali in cui può verificarsi l'illecito*

B) *Attività aziendali potenzialmente esposte alla commissione del reato*

C) *Funzioni aziendali che per procura o delega o responsabilità gestorie potrebbero commettere il reato*

D) *Singola fattispecie di reato*

E) *Esempi di possibili modalità di realizzazione del reato*

F) *Protocollo associato*

[7] Cfr. in tal senso C. Piergallini, Paradigma dell'autocontrollo penale, cit.

Tabella b)

A)	B)	C)	D)																E)		F)
MATRICE DEL PROFILO DI RISCHIO POTENZIALE (D.LGS.231/2001)																					
Processo	Attività sensibile	Soggetti coinvolti	A. REATI CONTRO LA PUBBLICA AMMINISTRAZIONE Art. 24 D.Lgs. 231/2001	B. REATI INFORMATICI E TRATTAMENTO ILLECITO DI DATI Art. 24-bis D.Lgs. 231/2001	C. REATI DI CRIMINALITA' ORGANIZZATA Art. 24-ter D.Lgs. 231/2001	D. FALSO NUMMARIO Art. 25-bis D.Lgs.231/2001	E. REATI CONTRO L'INDUSTRIA E IL COMMERCIO Art. 25-bis.1 D.Lgs. 231/2001	F. REATI SOCIETARI Art. 25-ter D.Lgs. 231/2001	G. TERRORISMO Art. 25-quater. D.Lgs. 231/2001	H. REATI DI MUTILAZIONE DEGLI ORGANI GENITALI FEMMINILI Art 25-quater.1 D.Lgs. 231/2001	I. REATI CONTRO LA PERSONALITÀ INDIVIDUALE Art. 25-quinquies D.Lgs. 231/2001	J. REATI ED ILLECITI AMMINISTRATIVI DI ABUSO DI MERCATO Art. 25-sexies D.Lgs. 231/2001	K. SALUTE E SICUREZZA Art. 25-septies D.Lgs. 231/2001	L. RICETTAZIONE E RICICLAGGIO Art. 25-octies D.Lgs. 231/2001	M. REATI IN MATERIA DI VIOLAZIONE DEL DIRITTO D'AUTORE Art. 25-novies D.Lgs. 231/2001	N. INTRALCIO ALLA GIUSTIZIA Art. 25-decies D.Lgs. 231/2001	O. REATI AMBIENTALI Art. 25-undecies D.Lgs. 231/2001	P. REATI TRANSNAZIONALI art. 10 L. 146/2006	Q. IMPIEGO DI CITTADINI DI PAESI TERZI IL CUI SOGGIORNO E' IRREGOLARE Art. 25-duodecies D.Lgs. 231/2007	Modalità di commissione del reato	Note	Protocollo associato
Gestione di rapporti commerciali con Clientela del settore pubblico e privato	Trattative Commerciali: Individuazione e selezione dei clienti, contatto con clienti pubblici / privati, produzione offerte, trattativa mediante dipendenti della società e gestione dei rapporti con i clienti)	**Direzione commerciale** **Ufficio Commerciale, Responsabile Vendite preposto ai Grandi Clienti** **Ufficio Commerciale, Addetti alle Vendite** **Direzione Commerciale, Forza Vendita**	✓		✓			✓						✓							**Associazione a delinquere** In via teorica l'attività presenta un potenziale profilo di rischio di commissione del reato di associazione a delinquere tramite la promozione, costituzione od organizzazione di associazioni criminali con i soggetti terzi allo scopo di commettere delitti che portino ad un vantaggio indebito per la Società. **Ricettazione** In via teorica l'attività presenta un potenziale profilo di rischio funzionale alla commissione del reato di ricettazione, ad esempio attraverso la vendita a clienti non etici i cui pagamenti saranno effettuati con denaro proveniente da attività illecite. **Riciclaggio e impiego di utilità di provenienza illecita** Inoltre, anche se in via del tutto teorica come per il caso precedente, l'attività presenta un profilo di rischio di commissione del reato di riciclaggio e/o impiego di utilità di provenienza illecita attraverso, ad esempio, la movimentazione di denaro di provenienza illecita. **Corruzione** L'attività in esame potrebbe presentare profili di rischio inerenti la commissione di reati corruttivi: dazione o promessa di utilità al funzionario pubblico a fronte di indurre il funzionario della Pubblica Amministrazione a sottoscrivere un contratto di fornitura con la Società oppure non escludere la Società dalla fornitura in assenza dei requisiti tecnici-economici. **Induzione indebita a dare o promettere utilità** Inoltre tale attività potrebbe presentare profili di rischio inerenti il reato di "induzione indebita a dare o promettere utilità a pubblico ufficiale o incaricato di pubblico servizio" nel caso in cui, in occasione di partecipazione a trattative verso clienti pubblici, la società sia indotta a dare o promettere denaro o altra utilità. **Corruzione tra Privati** Il reato potrebbe concretizzarsi in occasione di incontri per la presentazione di prodotti / servizi, mediante l'offerta di denaro o altra utilità (ad esempio omaggi di valore rilevante) ad un dipendente della società Cliente, al fine di indurre lo stesso a concludere l'acquisto a favore della Società offerente per valori in linea o superiori a quelli di mercato ma per prodotti di qualità inferiore allo standard di mercato / inferiori a quelli degli altri competitor.		- Codice Etico - Protocollo "Gestione dei rapporti commerciali "
			✓					✓													

Tale strumento svolge anche l'importante funzione di "accompagnare" il percorso dei soggetti che dall'esterno (appunto il giudice o anche un componente esterno dell'organismo di vigilanza), partendo dall'elemento giuridico-penale del reato-presupposto debbano ricostruirne, *step by step*, la dinamica di autorappresentazione dello stesso nella complessa realtà dell'azienda: dalla identificazione delle attività aziendali esposte (di cui al punto B), alla individuazione delle funzioni interessate nella complessa struttura organizzativa (punto C), fino ad "entrare" nell'operatività dei processi aziendali sensibili (punto A).

In altri termini, lo strumento menzionato può rappresentare uno dei principali elementi di raccordo tra i requisiti normativi espressi dal legislatore (fronte giuridico-penale) e la vita operativa della complessa organizzazione d'impresa (fronte aziendalistico).

Non solo. Ai fini di un *assessment* completo e ben strutturato, sarà opportuno dare evidenza anche delle ragioni per cui alcuni reati sono stati eventualmente ritenuti non applicabili. Anche in questo caso vale il doppio livello di analisi: aziendalistico e giuridico-penale attraverso una accurata valutazione degli elementi oggettivi e soggettivi del reato, calati sulla specifica realtà in esame.

In conclusione e prima di entrare nel merito dei sistemi di controllo preventivi all'interno dei processi aziendali, occorre inquadrare correttamente i termini della valutazione finale dei rischi-reato: incardinata sui concetti di rischio inerente, rischio residuo e rischio accettabile[8].

In sede di valutazione dei rischi-reato, così come nella metodologia standard del *Risk Assessment,* è possibile distinguere tra rischio inerente (cioè in assenza di controlli) e rischio residuo (cioè il rischio al netto dell'azione mitigante dei controlli).
Nel caso specifico del *compliance program*, però, occorre fare molta attenzione nella valutazione finale del rischio in termini di "rischio residuo accettabile".
Per quanto il rischio, in astratto, non possa essere mai eliminato integralmente per sua stessa natura (altrimenti non sarebbe tale), l'obiettivo prevenzionistico dell'ente ai sensi del Decreto deve essere finalizzato a contenerlo integralmente - ad impedire cioè la realizzazione della condotta dolosa/colposa o l'accadimento dell'illecito - nei termini indicati dalla stessa normativa (questo del resto è il tipo di responsabilità che l'ordinamento ha introdotto a carico dell'ente).

Più specificamente, per i reati dolosi, la soglia di accettabilità del rischio-reato è rappresentata da un sistema di prevenzione tale da non poter essere aggirato se non fraudolentemente (ai sensi dell'art. 6, comma 1, lett. c), del Decreto). Il modello organizzativo, di gestione e controllo, deve arginare il rischio-reato in una misura per cui l'agente non solo dovrà volere la commissione del reato, ma potrà attuare il proprio proposito criminoso soltanto aggirando fraudolentemente le indicazioni dell'ente[9].

[8] Si rinvia alla nota 5 e al lavoro di C. Dittmeier, Internal Auditing, cit

[9] Cfr. C. Piergallini, Paradigma dell'autocontrollo penale, Cit.

Peraltro, come ha recentemente indicato la giurisprudenza[10], la frode cui allude il Decreto non richiede veri e propri artifici e raggiri (che renderebbero quasi impossibile realizzare l'efficacia esimente del modello), tuttavia non è neppure riconducibile ad una mera violazione per mancato rispetto delle prescrizioni del modello, per comportamenti meramente omissivi: una violazione del modello mediante un aggiramento delle misure di sicurezza e presidio ivi previste, idoneo a forzarne l'efficacia, è comunque necessaria.

Nel caso invece dei reati colposi, dove per definizione si è in assenza di una volontà criminosa e fraudolenta da parte dell'agente, la soglia di accettabilità del rischio è rappresentata da una condotta in violazione del modello organizzativo di prevenzione, nonostante la puntuale osservanza degli obblighi di vigilanza previsti dal Decreto stesso (ad. 6, comma 1, lett. c)).

Come si intuisce si tratta di un passaggio estremamente delicato e a volte distante dai classici paradigmi di valutazione dei rischi di impresa, basati su ragionamenti di economicità (i.e. costo-opportunità) e su logiche sensibilmente differenti. Se il rischio-reato inerente è, per una data realtà in un dato momento un rischio reale e concreto, è assolutamente necessario che i presidi siano al massimo livello di prevenzione ed efficacia inibitoria, anche qualora una valutazione di mera convenienza e opportunità economica dovesse portare a scelte differenti.

D'altro canto, il concetto di "violazione fraudolenta", di evidente derivazione giuridica, deve essere "calato" nelle dinamiche dell'organizzazione aziendale, delle gerarchie e degli schemi di condotta/comportamento che ne regolano l'operato e quindi, in qualche modo, ricondotto al concetto di "esercizio" ovvero di "abuso" di una posizione/funzione, in relazione al "ruolo" ricoperto e alle "mansioni" esercitate dalla persona fisica all'interno della persona giuridica.

Si fornisce di seguito un esempio di formalizzazione della valutazione dei rischi - reato relativamente al processo della gestione degli approvvigionamenti di beni e servizi sulla base di criteri di significatività/complessità e probabilità di accadimento.

Intendendosi per *EX ANTE* la stima del rischio intrinseco, con riferimento alle risorse, ai prodotti e ai processi aziendali considerati come se non fosse in atto alcuna misura di trattamento del rischio, formalizzata o meno; mentre per *EX POST* la stima del rischio residuo, con riferimento alle risorse, ai prodotti e ai processi aziendali comprensivi di tutte le misure di trattamento del rischio in atto al momento della valutazione, formalizzate o meno.

[10] Cfr. Cassazione Penale, Sezione V, n. 4677, 30 gennaio 2014: Sentenza Impregilo

Tabella c)

GESTIONE DEGLI APPROVIGIONAMENTI DI BENI E SERVIZI

ATTIVITÀ / RISK OWNERS		EX-ANTE	DIR. PRODUZIONE	RESP. ACQUISTI	RSPP	QUALITÀ				EX-POST
			APPLICAZIONE DEI PROTOCOLLI, DELLE PROCEDURE E DEL CODICE							
Selezione e valutazione dei fornitori diretti e indiretti	R.R. =	medio		●		●				basso
	PR. =	bassa								molto bassa
Gestione dei terzisti	R.R.=	basso	●	●						basso
	PR. =	bassa								molto bassa
Emissione ed invio degli ordini d'acquisto al fornitore	R.R.=	basso		●						basso
	PR. =	bassa								molto bassa
Gestione delle manutenzioni preventiva, predittiva e programmata	R.R.=	molto basso	●	●	●					molto basso
	PR. =	molto bassa								molto bassa

RISCHIO-REATO:	R.R.	●	soggetti coinvolti nell'attività
PROBABILITÀ DI ACCADIMENTO:	PR.	●	soggetto responsabile dell'attività

4. I presidi di controllo e l'architettura dei controlli interni

Un ulteriore elemento di criticità e, sovente, di debolezza dei modelli di organizzazione, gestione e controllo ex D.Lgs. 231/2001, deriva dalla difficoltà di calibrare correttamente l'articolazione dei controlli e dei presidi nei protocolli di prevenzione di cui all'art. 6. comma 2, lett. b) del Decreto: da un lato si corre, infatti, il rischio di elaborare e predisporre una sovra-struttura regolatoria interna che si sovrappone al corpus procedurale eventualmente preesistente, appesantendo oltremodo l'operatività aziendale; dall'altro lato, in senso opposto, si corre il rischio di realizzare un modello troppo "leggero" ed incompleto, che si ferma all'enunciazione di principi astratti e troppo distanti dalla realtà operativa dell'ente o che reputa erroneamente sufficienti dei controlli interni che in realtà nascono per finalità diverse, ad esempio secondo logiche di costo-opportunità.
In entrambi i casi, l'effetto finale si traduce in una difficile, se non impossibile, implementazione ed efficace attuazione del modello.

Per inquadrare correttamente il tema, prima ancora di entrare nel merito del contenuto delle "cautele" dei controlli interni e della loro "resistenza" al vaglio del giudice penale, è utile premettere alcune riflessioni di carattere sistemico. In particolare, ci si riferisce alla pacifica constatazione empirica che anche imprese di medie dimensioni relativamente complesse hanno al loro interno sistemi e sotto-sistemi di gestione a loro volta normati (per esigenze interne o per normative specifiche di settore).

Spesso tali sistemi preesistono al *compliance program* ai fini del D.Lgs. 231/2001 e hanno un loro disegno, una loro documentazione, regole e procedure interne, attività di monitoraggio e talvolta anche forme di certificazione rispetto a standard di riferimento.

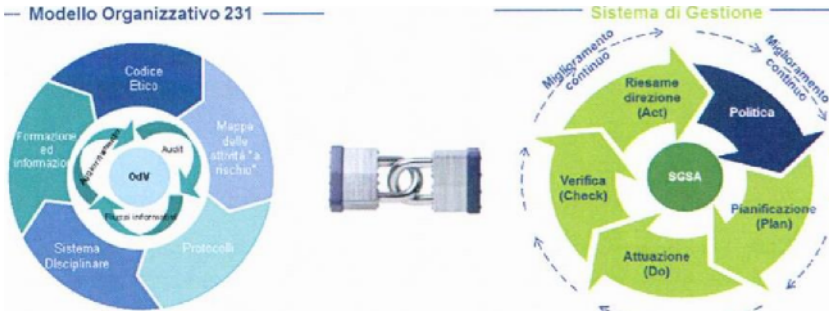
Viene in considerazione, in primissima battuta (così come del resto anche richiamato dallo stesso legislatore e dalle Linee Guida di Confindustria), il sistema di gestione per la salute e sicurezza sul lavoro (i.e. SGSSL).

Tale sistema ha dei propri standard e *framework* di riferimento definiti da apposite organizzazioni e che spesso sono riconosciuti e hanno validità a livello internazionale, sulla stessa lunghezza d'onda di quanto visto in precedenza per il CoSO *Framework*, con riferimento al più ampio e articolato sistema di controllo interno dell'azienda.

Nel caso specifico, è stato lo stesso legislatore che ha seguito un approccio sinergico in tema di sistemi di minimizzazione e gestione dei rischi per la salute e la sicurezza dei lavoratori, intrecciando la disciplina prevenzionistica del D.Lgs. 81/2008 con quella della responsabilità degli enti del D.Lgs. 231/2001.

L'art. 30, comma 5. del D.Lgs. 81/2008 stabilisce infatti che i modelli adottati sulla base di sistemi di gestione in materia di salute e sicurezza identificati in maniera puntuale (i.e. Linee guida UNI-INAIL del 2001 o British Standard OHSAS 18001:2007) si presumono conformi ai requisiti di idoneità ai fini dell'efficacia esimente dalla responsabilità da reato dell'ente (per lo meno in termini di astratta idoneità, salvo verificare nel concreto la efficace attuazione degli stessi).

Nell'ambito di un inquadramento sistemico, in questa sede interessa enfatizzare il rapporto sinergico che si crea tra i due modelli, come esemplificato graficamente qui di seguito:



L'integrazione tra il modello di organizzazione, gestione e controllo ex D.Lgs. 231/2001 ed i sistemi di gestione sottostanti è in realtà pervasiva e si deve estendere a tutti i sistemi aziendali, proprio al fine di garantire il superamento dei limiti da cui si è partiti in questa riflessione.

Soltanto attraverso un corretto "innesto" del Modello 231 nei sistemi di gestione aziendale sarà possibile garantire una effettiva efficacia del modello nell'operatività concreta dei processi aziendali e, al contempo, consentire una rilettura e adeguamento degli stessi al fine di meglio rispondere ai requisiti imposti dal Decreto, in termini di rischi da prevenire e standard prevenzionistici minimi.

In tal senso, numerosi sono i sistemi di gestione "auto-normati" o "etero-normati" che si trovano di frequente preesistenti in azienda:

- Rispetto ai reati ambientali: sistemi di gestione ambientale (ad es. UNI EN ISO 14001. Emas, ecc.);
- Rispetto ai reati in materia di produzione e commercio: sistema qualità (ad es. UNI EN ISO 9001);
- Rispetto ai reati societari e del TUF: con riferimento alle società quotate i programmi di *compliance* ex Legge 262/2005. Sarbanes Oxley Act, *Financial lnstruments and Exchange Act — J-Sox*, ecc.;
- Rispetto ai reati di riciclaggio: i sistemi antiriciclaggio (i.e. AML *programs*) adottati dai destinatari del D.Lgs. 231/2007;
- Rispetto ai reati informatici: i programmi di *compliance* per l'IT *Governance* e l'IT *General Computer Controls* (i.e. Cebit, ISO 27001, ecc.):
- Rispetto ai reati contro la Pubblica Amministrazione e la corruzione: i programmi *anti-bribery* e and *corruption* adottati da organizzazioni ad elevato rischio con esposizione in contesti transnazionali (i.e. Anti-Bribery *Compliance* Model, cit.);
- Tutta la normativa e relativi programmi di *compliance* dei soggetti sottoposti a vigilanza (i.e. Banca d'Italia, IVASS, CONSOB, ecc.).

Come si intuisce, l'elenco potrebbe continuare con molti altri esempi via via più tecnici e specialistici, che tuttavia non rilevano ai fini della presente trattazione.

Resta il medesimo schema di riferimento: la relazione è di uno (il Modello 231) a molti (i singoli *compliance program* specialistici). Il Modello 231 deve essere in grado di innestarsi su questi

programmi, chiedere che essi siano integrati con eventuali controlli e presidi ulteriori, laddove necessario per il rispetto dei diversi requisiti imposti dal rischio-reato, verificarne il corretto disegno e l'effettivo funzionamento nell'applicazione concreta, nell'ambito dell'operatività aziendale.

Inoltre, laddove tali sistemi siano "etero-normati", da una norma di legge o da un regolamento, essi si configureranno come presidi di *hard law*, rendendo in tal modo più agevole per l'ente la propria difesa in base alla idoneità del *compliance program* ai fini della responsabilità amministrativa da reato. In altri termini, il fatto stesso che il legislatore (come ad esempio nel caso della salute e sicurezza dei lavoratori) abbia indicato in positivo i requisiti minimi prevenzionistici richiesti, rende più facile per l'ente identificare il tipo di presidi da attivare, sapendo che quelle misure saranno necessarie ma anche sufficienti per l'esimente.

Qualora invece il riferimento non sia una normativa esterna che detta in modo puntuale i presidi richiesti, sarà opportuno ricorrere ai cosiddetti presidi di soft law, cioè alle *best practice* di riferimento, adattate e integrate sulla base delle specificità dell'ente, del suo business e della sua organizzazione.

In ultima istanza, ci sarà poi sempre la prassi operativa specifica, disegnata ad-hoc sulla base del profilo di rischio-reato proprio dell'ente, che dovrà tenere in considerazione le logiche di valutazione del rischio-reato descritte nel paragrafo precedente e sviluppare dei presidi specifici per rispondere a tali istanze.
Sulla base di tali premesse, i paragrafi seguenti intendono sinteticamente illustrare quali possono essere le componenti di un sistema di controllo preventivo, che dovranno essere attuate a livello aziendale per l'efficacia del modello, seguendo la traccia fornita dalla Linee Guida di Confindustria.

In particolare, si fa riferimento alle seguente componenti:

- Codice etico o di comportamento con riferimento ai reati considerati ("Codice Etico");
- Sistema organizzativo sufficientemente aggiornato, formalizzato e chiaro;
- Poteri autorizzativi e di firma;
- Procedure e presidi di controllo;

4.1. Codice Etico (cenni)

Il sistema di controllo preventivo trova la propria più alta legittimazione e fondamento all'interno dei principi etici e dei valori aziendali cui l'impresa si ispira, espressi all'interno del proprio Codice Etico (c.d. “tone at the top”)[11]. Si tratta in realtà di una componente talmente importante del *compliance program* che, anche nelle linee guida di riferimento, richiede una trattazione specifica.

[11] Anche in questo caso un lavoro su tutti. Cfr. G.M. Garegnani, E.P. Merlotti, A. Russo, Scoring Firms' Codes of Ethics: An Explorative Study of Quality Drivers, in Journal of Business Ethics, Springer, 2013.

Non a caso, nella prassi applicativa è formalizzato all'interno di un apposito documento, distinto dal Modello 231, anche se entrambi sono parte di un corpus organico diretto alla diffusione di una cultura dell'etica, della correttezza e della legalità.

Il Modello 231 detta prescrizioni specifiche, finalizzate a prevenire le diverse tipologie di reato, secondo le disposizioni del Decreto. Il Codice Etico è la carta di valori e principi, che deve ispirare la condotta della *societas* nel perseguimento degli obiettivi sociali.

Appare quindi opportuno sottolineare gli elementi di sinergia tra i due documenti. Come detto, il Codice Etico, nel fissare le scelte di politica aziendale in tema di rispetto della legalità, fa da base su cui impiantare il sistema di controllo preventivo e fornisce una ulteriore legittimazione dello stesso. In tal senso, ne traccia i principi ispiratori, quali ad esempio, l'imprescindibile rispetto di leggi e regolamenti vigenti in tutti i paesi in cui l'ente opera e i principi di base relativamente ai rapporti con soggetti pubblici.

A differenza del Modello 231, che è destinato a disciplinare le componenti organizzative, di gestione e controllo proprie dell'ente (pertanto necessariamente "endosocietario"), il Codice Etico è un documento tipicamente utilizzabile sia all'interno (come codice di condotta in senso stretto) sia all'esterno, nei confronti di clienti, fornitori e controparti in genere. Pertanto diventa una strumento di fondamentale importanza anche per regolare gli standard etici e di comportamento che ci si attende dai terzi.

4.2. Il sistema organizzativo

Il Modello 231 deve fornire una chiara rappresentazione del sistema di *governance* e organizzativo dell'ente, una "carta di identità" che fotografa la configurazione giuridico-societaria ed operativa in modo chiaro e dando atto di eventuali modificazioni intercorse nel tempo.

Se l'ente fa parte di un "gruppo di imprese" (ed a maggior ragione se il gruppo ha una *governance* che totalmente o in parte afferisce a soggetti esteri), è necessario riportare le forme di collegamento societario e le modalità con cui eventualmente si esercita, in seno al gruppo, la direzione e coordinamento, nella definizione delle strategie di business e delle modalità di interazione nell'esercizio dei poteri di gestione e controllo.

La chiara declinazione dell'assetto societario e organizzativo è di fondamentale importanza al fine di poter esprimere un giudizio in ordine all'idoneità del modello rispetto alla sfera dei rischi-reato potenzialmente applicabili. Una evidente sfasatura tra le dimensioni strutturali ed operative dell'ente e la forma societaria organizzativa dello stesso costituisce già di per sé un primo segnale di una potenziale inadeguatezza giuridico-strutturale della *governance* societaria[12].

La struttura organizzativa aziendale (divisioni, funzioni di linea, funzioni di supporto, ecc.) deve essere chiaramente definita, soprattutto con riferimento all'attribuzione di responsabilità, alla

[12] Cfr. C. Piergallini, Paradigma dell'autocontrollo penale, cit.

corretta identificazione delle linee di dipendenza gerarchica o funzionale, alla puntuale descrizione dei compiti e assegnazione delle mansioni. Inoltre, devono essere correttamente identificati gli organismi e i comitati interni, le funzioni degli stessi, la loro promanazione, il mandato e l'ambito di competenze di ognuno di essi.

Il sistema organizzativo deve peraltro prevedere una adeguata articolazione delle funzioni di controllo ai diversi livelli, in relazione alla complessità organizzativa e alla tipologia di business, nonché riflettere adeguatamente - nella struttura formale dell'organigramma aziendale e nella dinamica dei riporti funzionali e gerarchici - coerenti linee di gestione degli stessi, al fine di salvaguardarne gli elementi di indipendenza che li connaturano.

In particolare, le organizzazioni complesse oppure operanti in settori altamente regolati, dovranno prevedere tre livelli di controllo da *best practice*[13] come indicati a seguire:

- Controlli di 1° livello, cosiddetti controlli di linea, insiti nei processi operativi (pertanto a diretto contatto con le fonti di rischio) svolti generalmente da risorse interne della struttura, sia in "autocontrollo" da parte dell'operatore sia da parte del preposto/dirigente responsabile dell'area;

- Controlli di 2° livello, svolti da strutture tecniche competenti in materia e indipendenti da quelle di primo livello (ad esempio *compliance officer*, *risk manager*, ecc.);

- Controlli di 3° livello, caratterizzati dal massimo grado di indipendenza possibile all'interno della struttura gerarchico-organizzativa. Si tratta delle attività proprie dell'*Internal Auditing*, la cui esaustiva definizione è fornita dai relativi standard professionali: 'attività indipendente ed obiettiva di *assurance* e consulenza, finalizzata ai miglioramento dell'efficacia e dell'efficienza dell'organizzazione. Assiste l'organizzazione nel perseguimento dei propri obiettivi tramite un approccio professionale sistematico, che genera valore aggiunto in quanto finalizzato a valutare e migliorare i processi di gestione dei rischi, di controllo e di *governance*"[14].

E' inoltre opportuno sottolineare, con le stesse Linee Guida, l'importanza di garantire una adeguata contrapposizione di funzioni (in ossequio al principio di segregazione delle funzioni), nonché la necessaria competenza, esperienza e professionalità di tutti i soggetti chiamati a rivestire ruoli e mansioni di rilievo rispetto ai temi trattati.

[13] Cfr. Confindustra, Linee guida per la costruzione dei modelli di organizzazione, gestione e controllo ai sensi del D.Lgs. 231/2001, 2014.

[14] Cfr. Associazione Italiana Internai Auditors, International Professional Practice Framework (IPPF), 2013

4.3. Il sistema delle procure e delle deleghe: poteri autorizzativi e di firma

Rispetto al tracciato delle Linee Guida di Confindustria, che si è deciso di seguire, appare opportuno a questo punto anteporre il tema dei poteri autorizzativi e di firma rispetto al tema delle procedure, in quanto strettamente collegato al punto precedente con riferimento alla modalità di declinazione puntuale della *governance* aziendale e di attuazione del modello organizzativo nella sua concreta operatività.

Il sistema delle deleghe e delle procure consente la ripartizione dei poteri e dei correlativi doveri all'interno dell'ente, individuando i soggetti chiamati ad assumere responsabilità di organizzazione, di direzione, di gestione e di spesa all'interno delle diverse funzioni / dipartimenti in cui l'ente si articola.

In prima battuta, spetta al Consiglio di Amministrazione assegnare le deleghe e i poteri di firma coerentemente con le responsabilità organizzative e gestionali dei designati, prevedendo una puntuale indicazione delle soglie di autonomia e di approvazione delle spese.

Il sistema di procure e deleghe può inoltre contemplare dei meccanismi di sub-delega di alcune funzioni da parte dei delegati, in considerazione delle effettive complessità aziendali e della necessità che le responsabilità siano effettivamente il più possibile vicino all'origine dei rischi e delle attività per le quali si renda necessario disporre adeguati presidi.

Nell'ambito che qui interessa approfondire, secondo la chiave di lettura propria di un *compliance program*, e cioè con riferimento non solo a rischi generici ma a più specifici rischi-reato, il disegno del sistema delle deleghe richiede cautele ulteriori, al fine di evitare possibili -cortocircuiti" sul piano sia delle responsabilità personali sia di quelle dell'ente.

Infatti, laddove le funzioni delegate e i ruoli organizzativi implichino l'assolvimento di posizioni di garanzia penalmente rilevanti - così come previste dallo stesso ordinamento in relazione ai diversi reati-presupposto - l'istituto in oggetto esce dalla sfera privatistica e deve fare i conti con il disposto normativo (nel caso specifico, ad esempio, dell'art. 16 del D.Lgs. 81/2008, in materia di salute e sicurezza dei lavoratori) e con gli orientamenti della giurisprudenza penale su tali aspetti[15].

Questo implica che, laddove esista una posizione di garanzia a fronte di un determinato rischio-reato, non tutte le funzioni e responsabilità del garante sono delegabili; in ogni caso, la delega di ciò che è trasferibile risulta valida solo se effettuata secondo le modalità, formali e sostanziali, previste dall'ordinamento.

In tal senso, può valere la pena un richiamo al primo comma, dell'art. 16 del D.Lgs. 81/08 già citato: "La delega di funzioni da parte del datore di lavoro, ove non espressamente esclusa, è ammessa con i seguenti limiti e condizioni:

[15] Per una trattazione esaustiva del tema si rinvia alla recente quanto esaustiva giurisprudenza della Corte di Cassazione a sezioni riunite. Cfr. Cassazione Penale, Sezioni Unite, 18 settembre 2014, n. 38343: sentenza Thyssenkrupp.

a) che essa risulti da atto scritto recante data certa;

b) che il delegato possegga tutti i requisiti di professionalità ed esperienza richiesti dalla specifica natura delle funzioni delegate;

c) che essa attribuisca al delegato tutti i poteri di organizzazione, gestione e controllo richiesti dalla specifica natura delle funzioni delegate;

d) che essa attribuisca al delegato l'autonomia di spesa necessaria allo svolgimento delle funzioni delegate;

e) che la delega sia accettata dal delegato per iscritto".

In aggiunta, nel quadra più ampio delle *best practice* di riferimento e della giurisprudenza, è opportuno che:

f) si prevedano soluzioni dirette a consentire una verifica sul corretto esercizio dei poteri delegati;

g) si possa disporre l'applicazione di sanzioni in caso di violazioni dei poteri delegati;

h) vi sia rispetto e coerenza con il principio di segregazione;

i) ci sia coerenza con i regolamenti aziendali e con le altri disposizioni interne applicabili oltre che conformità alle disposizioni di legge applicabili.

Occorre altresì che l'intero sistema sia coerente ed integrato, tempestivamente aggiornato alla luce delle modifiche normative e variazioni organizzative, nonché adeguatamente documentabile al fine di una sua eventuale ricostruzione a posteriori.

4.4. Procedure e presidi di controllo

I protocolli di prevenzione dei rischi-reato devono riprodurre la procedimentalizzazione del sistema decisionale e dei processi operativi interni specifici dell'ente, al fine di poter adeguatamente tracciare come i rischi-reato si delineano e si collocano all'interno della complessa organizzazione aziendale, tra le differenti aree funzionali, processi, sistemi informativi e soggetti coinvolti a vario titolo e con differenti responsabilità (organizzative, dirigenziali, gestorie, esecutive, di controllo e di spesa).

I protocolli hanno come obiettivo primario quello della "cautela", cioè l'apprestamento di misure idonee a disciplinare lo svolgimento delle attività operative per prevenire e ridurre il rischio-reato, ed in tal senso il loro nucleo vitale è rappresentato dai presidi di controllo specifici previsti nella procedimentalizzazione dei processi e delle attività sensibili.
Ancora una volta, nell'intento costruttivo di evidenziare tutti quei passaggi maggiormente critici che derivano dall'applicazione in ambito giuridico-penale degli strumenti e delle tecniche aziendalistiche, appare opportuno sottolineare, anche in questo ambito, quali rischi possano derivare da un'applicazione acritica delle tecniche e delle metodologie normalmente utilizzate in azienda.

Appare infatti evidente come e quanto possa risultare "inidonea", per le finalità del Decreto, una procedura operativa volta meramente e semplicemente a disciplinare, ad esempio, il flusso operativo e informativo delle attività di un determinato processo, senza però prevedere adeguati momenti di controllo; oppure, come possa risultare "debole", quella procedura che preveda momenti di controllo esclusivamente orientati agli obiettivi interni dell'ente (i.e. performance, profitto, salvaguardia delle risorse, ecc.) e non anche agli obiettivi più ampi e articolati propri dei rischi-reato, rispetto alla tutela di interessi di terzi (secondo la chiave di lettura che è stata fornita nei precedenti paragrafi).

Tale insidia appare ancora più concreta quando si consideri, in ottica aziendalistica, la valutazione del "costo", effettivo o figurato (di burocratizzazione dell'attività), che ogni controllo in più comporta, in una chiave di lettura di pura e semplice razionalità economica.

Come è naturale che accada, l'organizzazione tende, anche in questo caso, ad applicare criteri di valutazione economici, di costo-opportunità, prima di introdurre un nuovo controllo o un nuovo presidio nelle proprie prassi operative. Ne deriva che, se la valutazione di opportunità si ferma al solo interesse interno privatistico dell'azienda, probabilmente il "costo" del controllo/presidio aggiuntivo, necessario invece a tutelare l'interesse esterno, potrebbe non apparire giustificato e sostenibile. L'effetto sarà quello di un "modello inidoneo" a prevenire il rischio-reato, dal punto di vista del giudice.

Si provi però anche a pensare al caso opposto, cioè alle implicazioni che possano derivare dall'istanza esterna di introdurre controlli e presidi che, a tutti i costi, debbano sempre e comunque quantomeno intercettare il rischio-reato, auspicabilmente impedendo l'illecito. Probabilmente. il costo/onerosità del presidio potrebbe quantomeno "ingessare" l'operato efficiente dell'organizzazione, fino a rendere economicamente non più conveniente lo svolgimento di determinate attività a rischio-reato.

Si pensi, ad esempio, all'esigenza di introdurre un controllo puntuale da parte dell'Organismo di Vigilanza, su tutte le comunicazioni al mercato che promanino dal Presidente o dall'Amministratore Delegato, al fine di verificare che non siano difformi da quanto definito nel processo di predisposizione del comunicato stampa, secondo una corretta segregazione dei compiti, portata però fino all'estrema condizione, addirittura fuori dal perimetro aziendale, da parte dell'organo di controllo indipendente. Seguendo questo orientamento, si potrebbe arrivare al paradosso di dover convocare una riunione dell'Organismo di Vigilanza, ogni volta che si presenti l'esigenza di emettere un comunicato stampa, al fine di creare quella barriera che impedisca il reato di aggiotaggio da parte dei vertici aziendali[16].
E' evidente quindi la necessità di raggiungere un compromesso tra le diverse istanze, interne ed esterne. Da un lato, sarà necessario adattare il paradigma privatistico attraverso Interventi di autoregolazione e presidi di controllo finalisticamente orientati alle aspettative delle parti esterne; dall'altro lato, i soggetti esterni dovranno riconoscere la bontà (e i limiti connaturati) degli sforzi prevenzionistici del privato, compatibilmente con quanto sostenibile e coerente con le finalità stesse

[16] Una siffatta prospettiva ci è sembrato di poter scorgere tra le diverse motivazioni della sentenza Impregilo. Cfr. Cassazione Penale, Sezione V, n. 4677, 30 gennaio 2014: Sentenza Impregilo.

dell'impresa, che non potrà comunque trasformarsi in un organo di polizia giudiziaria rispetto ai propri dipendenti.

Chiarito il perimetro all'interno del quale si collocano i protocolli ex art. 6. comma 2, lett. b), ed il ruolo centrale che hanno ai fini prevenzionistici dei rischi-reato propri dell'ente, si può procedere all'identificazione dei principi di riferimento per il disegno e la valutazione di adeguatezza dei presidi di controllo.

Non potendo in questa sede neanche tentare una elencazione dei singoli presidi di controllo specifici, per ogni processo e per ogni rischio-reato[17], si fornirà a seguire una descrizione dei principi di riferimento come indentificati nella migliore prassi applicativa, al fine di fornire alcuni spunti e chiavi di lettura per una coerente previsione di presidi operativi e di controllo specifici che siano "idonei" alla prevenzione di illeciti ed al contempo adeguatamente e concretamente applicabili dall'ente nella propria operatività:

a) Esistenza di principi comportamentali da rispettare nell'esecuzione delle specifiche attività;

b) Verificabilità, tracciabilità, coerenza e congruenza di ogni operazione:

c) Applicazione del principio di separazione delle funzioni (nessuno può gestire in autonomia un intero processo);

d) Esistenza di adeguati e chiari livelli autorizzativi nell'ambito dei processi decisionali connaturati ad aree sensibili;

e) Documentabilità dei controlli.

<u>Principi comportamentali generali</u>.

Si richiede l'esistenza di regole comportamentali di carattere generale a presidio delle attività svolte nell'ambito dei singoli processi sensibili e/o strumentali alla commissione di reati.

L'ente, in particolare, deve adottare principi etici in relazione ai comportamenti che possono generare la commissione degli illeciti previsti dal Decreto quale sistema di controllo di tipo preventivo.

Tali principi possono essere definiti in termini generali nel Codice Etico e/o essere oggetto di autonoma e più dettagliata previsione in specifiche direttive interne (es. protocolli comportamentali).

[17] Con riferimento ai presidi orientati a combattere i reati di corruzione, si rinvia al poderoso lavoro di S. Giavazzi, con il supporto di F. Cottone e M. De Rosa, The ABC Program: *an anti-bribery compliance program recommended to corporations operating in a multinational environment*, in S. Manacorda ed al., cit.

Documentabilità dei processi operativi e procedure

Si richiede l'esistenza di adeguate e diffuse procedure che documentino le modalità operative e di controllo dei processi, nel rispetto dei principi di tracciabilità degli atti e oggettivazione del processo decisionale.

I requisiti minimi richiesti per le procedure interne si sintetizzano come segue:

- chiara definizione di ruoli e responsabilità, nel rispetto del principio di separazione tra il soggetto che inizia il processo decisionale, il soggetto che lo gestisce e lo conclude, e il soggetto che lo controlla;
- oggettivazione dei processi decisionali, mediante criteri e logiche di obiettività e misurabilità (laddove possibile);
- tracciabilità delle operazioni e delle transazioni attraverso adeguati supporti documentali ed opportuni livelli autorizzativi individuando i soggetti a vario titolo coinvolti (distinzione tra autorizzazione, effettuazione, registrazione e verifica dell'operazione);
- previsione di specifici meccanismi di controllo e monitoraggio su più livelli, compatibilmente con le dimensioni e la complessità dell'organizzazione;
- modalità di gestione e documentazione delle eccezioni e delle anomalie.

Livelli autorizzativi e tracciabilità dei processi decisionali

Si richiede resistenza e la chiara rappresentazione all'interno delle procedure e dei protocolli aziendali dei livelli autorizzativi da parte dei diversi soggetti coinvolti, a garanzia di un adeguato presidio sul processo decisionale.

Il sistema di autorizzazioni, deleghe e poteri di firma, deve rispettare altresì gli elementi indicati in precedenza, nel paragrafo specifico su tale punto.

Segregazione dei compiti

Si richiede, per quanto possibile rispetto alla dimensione ed articolazione della struttura organizzativa dell'ente, l'attuazione del principio di separazione dei compiti nella gestione dei processi e sotto-processi sensibili e a rischio.

Il sistema organizzativo della società, più in generale, deve rispettare i requisiti di:

- chiara e formale comunicazione delle linee di dipendenza gerarchica e funzionale;
- assegnazione delle attività operative in coerenza con una separazione dei ruoli, ovvero articolazione delle strutture organizzative in modo da evitare sovrapposizioni funzionali e concentrazioni su un solo soggetto di attività tra loro "incompatibili" / con elevato grado di rischio.

Attività di controllo e monitoraggio

Si richiede l'esistenza di specifiche attività di controllo e monitoraggio, distinguendo tra:

- controlli di linea, finalizzati ad assicurare il corretto svolgimento delle attività operative, da parte dei soggetti aziendali coinvolti;
- attività di monitoraggio, finalizzata alla rilevazione, da parte di strutture indipendenti da quelle operative, di eventuali anomalie e/o violazioni delle procedure aziendali.

Nell'ambito dell'attuazione pratica di un sistema di controllo efficace, particolare attenzione dovrà essere posta nel disciplinare e presidiare la gestione finanziaria ed i flussi finanziari, quale processo strumentale trasversale alla commissione di diversi illeciti.

Più in generale, i protocolli e i presidi fin qui descritti devono, in ogni caso, coprire non soltanto quei processi sensibili in quanto di diretta pertinenza con le aree a rischio-reato identificate, ma anche quei processi strumentali che, apparentemente estranei all'area di rischio, possono in realtà rivelarsi essenziali per la realizzazione della condotta illecita (si pensi ad esempio al processo di selezione e assunzione del personale, quale processo strumentale per reati corruttivi, oppure il ricorso a consulenze esterne, in sé astrattamente lecite, ma potenzialmente finalizzate all'ottenimento di indebiti vantaggi per l'ente).

Alla luce della pur breve disamina effettuata con riferimento al complesso tema delle procedure e dei presidi di controllo, appare chiaro come sia pressoché impossibile (se non in realtà organizzative estremamente semplici) prevedere una sovrastruttura procedurale specifica e autonoma ai fini dell'adeguamento normativo al D.Lgs. 231/2001.

L'ampiezza del catalogo dei reati, la trasversalità e la pervasività degli stessi rispetto ai diversi ambiti e processi aziendali, richiede necessariamente quell'operazione di "innesto" di cui si è scritto in precedenza. Secondo le logiche dell'integrazione del sistema di controllo interno anche rispetto al tema della *compliance* integrata.

4.5 *Risk Assessment* e GAP Analysis ex D.Lgs 231/2001

Una volta identificate le attività potenzialmente rilevanti in merito alle nuove fattispecie di reato introdotte all'interno del D.Lgs. 231/2001 e individuato i potenziali profili di rischio delle aree sensibili è fondamentale fare un inventario di tutti i presidi e degli ulteriori processi ed i meccanismi di controllo in essere evidenziando poi gli eventuali disallineamenti/punti di miglioramento rispetto alle *best practice*.

Una volta che si sono evidenziati i processi rilevanti e potenzialmente soggetti alla commissione dei reati previsti dal D.Lgs. 231 piuttosto che a rappresentare attività strumentali al compimento degli stessi per ciascuno di essi è importante predisporre una sintesi del processo di *Analisi del Sistema di Controllo interno* e conseguente *Piano di intervento* per il rafforzamento dello stesso.

Si fornisce di seguito una scheda di sintesi quale possibile esempio di formalizzazione :

Tabella d)

Attività…… potenzialmente esposta alla commissione di reati
Profilo di rischio

Presidi esistenti	Proposte di intervento
1. Deleghe e Procure	
2. Codice Etico	
3. Procedure/Controlli	
4. Segregazione delle funzioni	
5. Tracciabilità	

5. Conclusioni

I sistemi di controllo interno nascono in un contesto prettamente privatistico, si sono sviluppati negli anni e anche nelle migliori tradizioni e pratiche internazionali secondo logiche aziendalistiche di natura economico- privata, volte a tutelare interessi privati. La risposta alle nuove istanze, nel paradigma della partnership prevenzionistica pubblico-privato, non può dunque che ricercarsi e ritrovarsi nel necessario adattamento degli obiettivi, delle caratteristiche e degli strumenti del sistema di controllo interno, al fine di tener conto di tali diverse e sempre più pregnanti aspettative esterne, di natura normativa, volte a tutelare interessi collettivi via via più ampi, secondo un nuovo modello di *corporate liability* e *corporate responsibility*.

Come indicato in premessa, obiettivo di questa riflessione è stato anche evidenziare l'importanza della doppia natura giuridico-aziendalistica dei *compliance program* ed i risvolti pratici che ciò comporta ai fini della idoneità ed efficacia dei modelli di organizzazione, gestione e controllo ai sensi del D.Lgs. 231/2001, nonché per il rafforzamento dei sistemi di controllo interno in generale, come supporto dei settore privato nel contrasto alla corruzione ed ai crimini economici.

Lo si è fatto con riferimento ai due principali pilastri dei *compliance program 231*: la valutazione dei rischi- reato e i protocolli di prevenzione: mettendone in evidenza i limiti e indicando gli accorgimenti che si rendono necessari per una piena ed efficace attuazione delle metodologie, delle tecniche e degli strumenti a disposizione dell'aziendalista.

In sintesi, si può ora provare a stilare un elenco dei principali *steps* necessari per raggiungere l'obiettivo di un *compliance program* coerente con i requisiti del D.Lgs. 231/2001:

1. Il *Risk Assessment* deve essere finalizzato rispetto agli obiettivi della normativa e del programma di *compliance*. Non può essere condotto solo in relazione ai rischi di business, ma deve considerare gli specifici rischi-reato in ambito.

2. I criteri di analisi dei rischi-reato devono riflettere le istanze normative. E' necessario entrare nella valutazione dell'elemento oggettivo e soggettivo dei singoli reati presupposto, ricostruirne e documentarne le dinamiche all'interno dell'organizzazione, attraverso matrici esaustive in grado di collegare l'elemento normativo all'elemento aziendale.

3. Il sistema di controllo interno è necessariamente unico e integrato. Il Modello 231 deve essere in grado di integrarsi nei sistemi aziendali e questi, a loro volta, devono adattarsi alle istanze della normativa. L'alternativa è una crisi di rigetto da parte della struttura e l'inefficacia del Modello.

4. Il Codice Etico deve esprime la chiara volontà dell'ente di muoversi in una dimensione di legalità, coerentemente con la visione del vertice aziendale.

5. L'organizzazione dell'ente deve essere coerente con le sue dimensioni e con le caratteristiche del business, non solo in un'ottica di adeguata gestione e valorizzazione delle risorse, ma anche nell'ottica di un adeguato livello di controllo interno.

6. L'attribuzione di ruoli e responsabilità attraverso la delega di funzioni e l'assegnazione di poteri di spesa deve essere coerente non solo con le esigenze di efficienza gestionale ed operativa, ma anche con i requisiti normativi, con le posizioni di garanzia che in taluni casi l'ordinamento specificatamente prevede per determinati ruoli e funzioni.

7. I protocolli di comportamento non devono essere soltanto finalizzati alla corretta proceduralizzazione delle attività interne, ma devono prevedere anche adeguati principi e momenti di controllo, non solo in una chiave di lettura interna (per le finalità proprie dell'ente) ma, anche e soprattutto, per soddisfare le aspettative prevenzionistiche dell'ordinamento normativo nel quale si opera.

Concludiamo allegando un *Decision Tree* che vuole sintetizzare il percorso logico per pervenire ad una conclusione in merito all'adeguatezza di un Modello di organizzazione, gestione e controllo con riferimento a due aspetti essenziali della *compliance* ai fini del D.lgs 231/2001: l'identificazione dei rischi ed il disegno dell'architettura dei presidi di controllo.

Decision Tree - Risk Assessment 231 (Identificazione dei rischi e disegno dell'architettura dei presidi di controllo)