CONSORZIO DI BONIFICA INTEGRALE COMPRENSORIO SARNO

MODELLO DI ORGANIZZAZIONE E GESTIONE AI SENSI DEL D.LGS. N. 231/2001
RISK ASSESSMENT – NOTA METODOLOGICA

1 INTRODUZIONE

La presente nota metodologica intende illustrare il metodo adottato nella valutazione del rischio (di seguito "*risk assessment*") mediante il supporto dell'applicazione *software* "*Valore 24-Modello Organizzativo 231*" (di seguito "*applicazione*").

Per *risk assessment* s'intende quell'attività di valutazione dei rischi ai quali è esposto un ente in relazione, da una parte, al grado di possibile emersione di reati rilevanti a norma del d.lgs. n. 231/2001 nelle varie "*aree di rischio*" (altrimenti dette "*attività sensibili*") esistenti presso il soggetto giuridico in esame, e, dall'altra, alla capacità dei presidi, posti in essere dall'ente, di mitigare tali rischi.

Il risultato di tale valutazione consentirà di individuare le aree di rischio che richiederanno nuovi ovvero ulteriori interventi di mitigazione del rischio (i cosiddetti "*piani di rimedio*") al fine di incrementare il relativo presidio fino a portarlo ad un livello ritenuto soddisfacente.

Come chiarito dalle Linee guida di Confindustria, *"quanto alle modalità operative della gestione dei rischi, soprattutto con riferimento ai soggetti o funzioni aziendali che possono esserne concretamente incaricati, le metodologie possibili sono sostanzialmente due:*

- *valutazione da parte di un organismo aziendale che svolga questa attività con la collaborazione del* management *di linea*
- *autovalutazione da parte del* management *operativo con il supporto di un tutore/facilitatore metodologico"*

2 LA METODOLOGIA ADOTTATA

L'applicazione, con il suo modulo di *risk assessment*, intende fornire uno strumento di supporto alla valutazione ovvero all'autovalutazione sopra citate.

Il metodo di *risk assessment* implementato nell'applicazione si ispira ai principi dell'"*Enterprise Risk Management*" (di seguito "*ERM*")[1], vale a dire ai metodi ed ai concetti generalmente utilizzati dalle imprese per gestire i rischi che possono emergere nel corso dell'attività imprenditoriale.

Tra i termini adottati nell'applicazione che fanno riferimento ai concetti tipici dell'ERM, ricordiamo:

- **IMPATTO ("I")** – si intende il danno di carattere economico, operativo e

[1] Ci si riferisce, in particolare, all'*Internal Control Integrated Framework* (CoSO Report) emesso dal *Committee of Sponsoring Organizations Commission* (CoSO) del 1992 ed aggiornato nel maggio 2013 in materia di sistema di controllo interno ed all'*Enterprise Risk Management Framework* (c.d. ERM), anch'esso emesso dal CoSO nel 2004 in materia di gestione dei rischi

reputazionale derivante dall'avveramento di un determinato evento avverso: nel presente contesto, l'emersione di un reato rilevante ai sensi del d.lgs. n. 231/2001 in una determinata area di rischio

- **PROBABILITÀ ("P")** – è il grado di quanto un evento avverso si possa o non si possa avverare in un determinato contesto e periodo temporale
- **RISCHIO INERENTE ("Ri")** – è il rischio potenziale valorizzato senza considerare le attività di mitigazione del rischio (il "*presidio*")
- **PRESIDIO ("M")** – è il livello di copertura del rischio realizzata mediante l'attivazione di protocolli (le regole ed i controlli interni, attinenti a processi, organizzazione, procedure, comportamenti) che tendono a mitigare il rischio inerente
- **RISCHIO RESIDUO ("Rr")** – è il rischio potenziale calcolato considerando anche l'effetto positivo delle attività di mitigazione del rischio

Nel *risk assessment*, ogni area di rischio potrà essere valutata dall'utente, in relazione ad ogni rilevante ai sensi del d.lgs. n. 231/2001, in termini di Impatto, Probabilità e Presidio sulla base di specifici fattori di valutazione. Il Rischio inerente ed il Rischio residuo sono invece calcolati automaticamente dall'applicazione grazie al proprio algoritmo nel seguito illustrato.

I valori dei vari fattori di valutazione sono determinati a cura dell'utente considerando il contesto specifico della società/ente in analisi, vale a dire sulla base della conoscenza, dell'esperienza, delle informazioni, e delle valutazioni quantitative e qualitative dei vari soggetti che contribuiscono alla specifica valutazione (ad esempio, *management*, soggetti valutatori, etc.).

3 I FATTORI DI VALUTAZIONE

Con riferimento ad ogni singolo ambito di valutazione, rappresentato dall'abbinamento tra un'area di rischio ed un reato rilevante ai sensi del d.lgs. n. 231/2001, i fattori di valutazione da quantificare qualitativamente nell'analisi sono:

- per la determinazione dell'**IMPATTO**:
  - **L'IMPATTO ECONOMICO** - il danno di carattere economico che subirebbe l'ente nel caso di emersione del reato rilevante ai sensi del d.lgs. n. 231/2001: tra i vari elementi da considerare per questo fattore troviamo le sanzioni amministrative previste dal d.lgs. n. 231/2001 ed i danni economici diretti ed indiretti che potrebbero derivare dall'evento avverso
  - **L'IMPATTO OPERATIVO** - il danno di carattere operativo che subirebbe l'ente nel caso di emersione del reato rilevante ai sensi del d.lgs. n. 231/2001: tra i vari elementi da considerare per questo fattore troviamo le sanzioni di carattere interdittivo e le possibili misure preventive e cautelari adottate dall'autorità giudiziaria
  - **L'IMPATTO REPUTAZIONALE** - il danno di carattere reputazionale, quale ad esempio la perdita d'immagine, la pubblicità negativa e la perdita di fiducia da parte degli utenti o di *partner* commerciali a seguito dell'emersione del reato rilevante ai sensi del d.lgs. n. 231/2001

Per tali fattori la scala di valutazione è la seguente:

[1] trascurabile

[2] basso

[3] medio

[4] alto

[5] molto alto

- per la determinazione della **PROBABILITÀ**:
  - **INCENTIVI AL *MANAGEMENT*** – si richiede di indicare un livello d'incidenza nell'area di rischio degli incentivi al *management* (ad esempio, premi di risultato, partecipazione agli utili, piani di *stock options*, etc.) sul presupposto che quanto maggiore sarà l'interesse manageriale a raggiungere il proprio obiettivo tanto maggiore potrà essere la pressione a "*forzare la mano*" verso comportamenti illeciti: ad un maggiore grado di incentivo manageriale corrisponde quindi una maggiore probabilità di avveramento dell'evento avverso
  - **RAPPORTI CON PUBBLICA AMMINISTRAZIONE O TERZE PARTI** – è qui richiesto di indicare la rilevanza delle attività verso la pubblica amministrazione, l'Unione Europea o terze parti rispetto all'attività nel suo complesso: in questo caso il presupposto consiste nel ritenere maggiore la probabilità di avveramento di un evento avverso (in particolare i reati contro la pubblica amministrazione, la corruzione tra privati, i reati transnazionali, la frode a danno dell'Unione Europea, etc.) laddove sia maggiore la rilevanza dell'attività verso tali soggetti
  - **FREQUENZA** – s'intende il grado di operatività di una determinata attività dell'area di rischio: l'ipotesi di base è che in un'attività poco frequente (ad esempio, la quadratura del magazzino effettuata una volta l'anno) sia meno probabile l'avveramento di un evento avverso e che, al contrario, ad una maggiore frequenza corrisponda una maggiore probabilità
  - **RILEVANZA** – è il grado d'importanza dell'area di rischio in esame, in termini di dimensione o contributo proprio ai risultati economici, rispetto all'attività dell'ente nel suo complesso (ad esempio, in termini di risorse umane impiegate dall'area rispetto all'organico complessivo dell'ente oppure alla contribuzione al fatturato dell'area rispetto al fatturato complessivo della persona giuridica): ad una maggiore rilevanza corrisponde una maggiore probabilità
  - ***OUTSOURCING*** – è il grado di utilizzo da parte dell'ente di fornitori terzi (di seguito "*outsourcer*") per svolgere le proprie attività. Si suppone che quanto maggiore sia l'utilizzo di approvvigionamento esterno tanto maggiore possa essere la probabilità di accadimento di un

evento avverso: tale relazione deriva dalla difficoltà di applicazione di un sistema di controllo interno lungo la catena di approvvigionamento (in particolare nel caso di appalti e subappalti)

- **IMPREVEDIBILITÀ** – indica il grado d'indeterminazione ed imprevedibilità dei processi. Maggiore è tale grado, maggiore è la probabilità di accadimento dell'evento avverso: ad esempio un processo fortemente standardizzato e regolato – quindi prevedibile nel suo svolgimento – ha minori probabilità di incorrere in illeciti, viceversa nell'ambito di un processo non predeterminato potrebbero emergere comportamenti illeciti

Per tali fattori la scala di valutazione è la seguente:
[1] remota
[2] improbabile
[3] moderata
[4] probabile
[5] molto probabile

- per la determinazione del **PRESIDIO**, con riferimento all'area di rischio e al reato rilevante ai sensi del d.lgs. n. 231/2001:
  - **PROCEDURE** - è la valutazione riferita all'esistenza ed all'applicazione di procedure (ad esempio, linee guida, istruzioni operative, manuali di processo, procedure operative, etc.)
  - **SEGREGAZIONE DEI COMPITI** (di seguito "*segregation of duties*") - è la valutazione riferita alla separazione dei ruoli e dei poteri esecutivi nell'ambito di una specifica attività, tra chi definisce la strategia, vale a dire chi "*decide cosa fare*" ("*origination*"), chi esegue quanto stabilito di fare ("*execution*"), e chi controlla l'operato ("*control*")
  - **DELEGHE** - è la valutazione sull'esistenza di un sistema di deleghe e procure nella gestione dell'ente o di particolari progetti: in tale valutazione deve essere considerata l'attualità e la coerenza tra i poteri conferiti e le risorse umane
  - **TRACCIABILITÀ** - è la valutazione sulla capacità dell'ente di ricostruire nel tempo l'attivazione, lo svolgimento e la conclusione di un determinato processo, anche a posteriori, ad esempio mediante la memorizzazione dei relativi documenti ed il tracciamento delle modifiche intervenute sui dati dell'ente e sugli utenti che le hanno operate
  - **MONITORAGGIO** - è la valutazione sulla capacità dell'ente di monitorare una determinata attività, vale a dire di misurare e controllare gli effetti e l'avanzamento di tale attività

  Per tali fattori la scala di valutazione è la seguente:

  [1] inesistente
  [2] parziale
  [3] esistente

4 IL CALCOLO DI IMPATTO, PROBABILITÀ, RISCHIO INERENTE E RISCHIO RESIDUO

Nella determinazione del risultato complessivo dell'Impatto, il Modello prende in considerazione il valore massimo attribuito ai relativi fattori di valutazione, vale a dire il massimo danno potenziale.

Nella determinazione del risultato complessivo della Probabilità e del Presidio, sono invece presi in considerazione i valori medi (media aritmetica) dei relativi singoli fattori di valutazione.

A seguito della valutazione dell'Impatto ("I") e della Probabilità ("P"), il Rischio inerente ("Ri") è determinato come segue:

$Ri = I \times P$

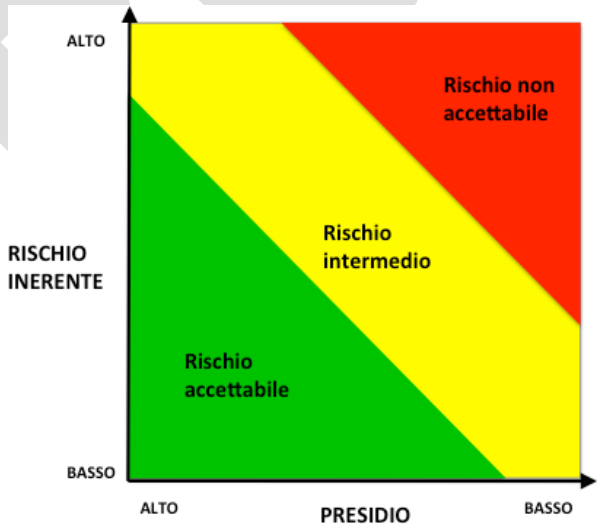
Poiché il Presidio è valorizzato su una scala da 1 a 3, anche il valore di Rischio inerente viene ricondotto ad una scala comparabile da 1 a 3, mediante la seguente formula:

$Ri^2 = -(I \times P) \times 2/24 + 3{,}0833333$

Il risultato del **RISCHIO RESIDUO** è quindi calcolato mediante la seguente formula: $Rr = 10 - (P \times Ri)$

5 VALUTAZIONE DI ACCETTABILITÀ DEL RISCHIO RESIDUO

La valutazione di accettabilità o meno del Rischio residuo è determinato dalla matrice Rischio inerente e Presidio, laddove, considerando gli estremi, risulta ottimale un Rischio inerente basso unitamente ad un Presidio alto e, viceversa, particolarmente critico un Rischio inerente alto in presenza di un Presidio basso.

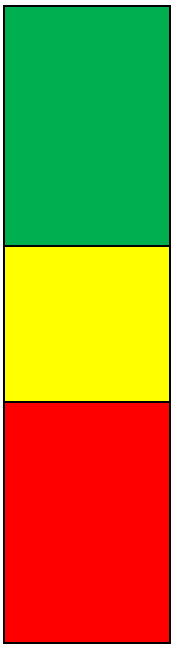


[2] Rischio inerente ricondotto da una scala "da 1 a 5" ad una scala "da 1 a 3"

Le zone contrassegnate con il colore verde, giallo e rosso sono determinate secondo le seguenti soglie di Rischio residuo:

- VERDE (accettabile), per valori di rischio residuo minori o uguali a 6,44
- GIALLO (intermedio), per valori di rischio residuo maggiori 6,44 e minori di 8
- ROSSO (non accettabile), per valori di rischio residuo uguali o maggiori di 8

La valutazione finale del Rischio residuo consente quindi di individuare le seguenti casistiche:



AREE DI RISCHIO VERDI - presentano un livello di Rischio residuo accettabile: per queste aree non sono richiesti interventi

AREE DI RISCHIO GIALLE - necessitano di un monitoraggio e di azioni di miglioramento del livello di presidio o azioni che consentano una diminuzione delle probabilità di avveramento del rischio

AREE DI RISCHIO ROSSE - richiedono interventi immediati volti ad aumentare il relativo livello di presidio