ORDINE DEI DOTTORI COMMERCIALISTI E DEGLI ESPERTI CONTABILI
MILANO

FONDAZIONE COMMERCIALISTI ODCEC di MILANO

La convivenza dell'ODV231 nel sistema dei controlli interni

LA GESTIONE DEI RISCHI OPERATIIVI NELL'INFORMATIVA ALL'ODV 231

GIANLUCA BALSAMO

4 dicembre 2018

Definizione di rischio operativo

"the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. The definition includes legal risk but excludes strategic and reputational risk".

"il rischio di perdite … derivanti da disfunzioni a livello di procedure, personale e sistemi interni, oppure da eventi esogeni [omissis]".

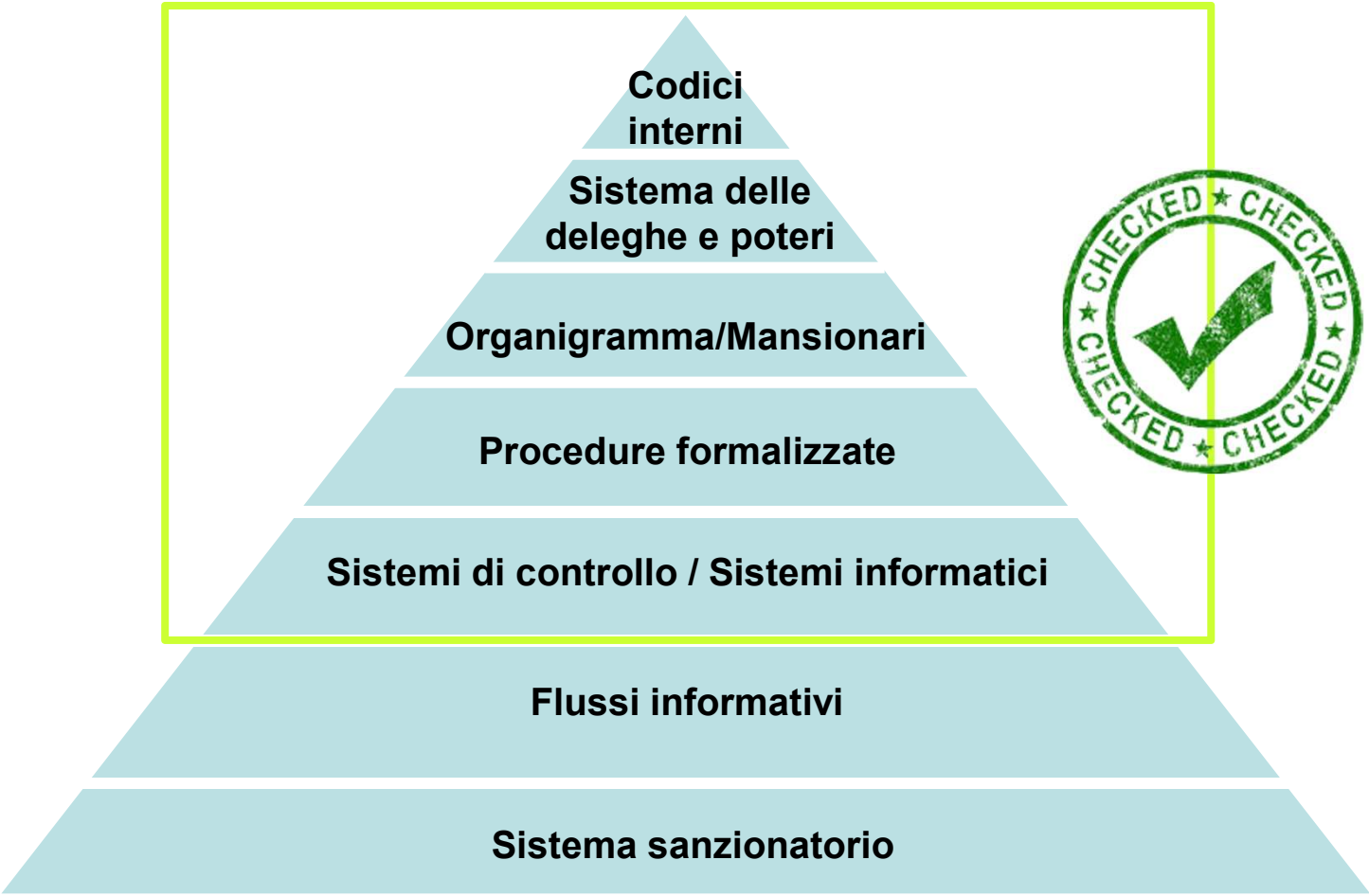
Fonte: «Prassi corrette (Sound practices) per la gestione e il controllo del rischio operativo» emanate dal Comitato di Basilea per la vigilanza bancaria (documento predisposto dal Risk Management Group del Comitato) – Febbraio 2003

Principali fattispecie di rischio operativo

- ***frode interna*** - esempi: alterazione intenzionale di dati, sottrazione di beni e valori, operazioni in proprio basate su informazioni riservate;
- ***frode esterna*** - esempi: furto, contraffazione, falsificazione, emissione di assegni a vuoto, pirateria informatica;
- ***rapporto di impiego e sicurezza sul posto di lavoro*** - esempi: risarcimenti richiesti da dipendenti, violazione delle norme a tutela della salute e sicurezza del personale, attività sindacale, pratiche discriminatorie, responsabilità civile;
- ***pratiche connesse con la clientela, i prodotti e l'attività*** - esempi: violazione del rapporto fiduciario, abuso di informazioni confidenziali, transazioni indebite effettuate per conto della banca, riciclaggio di denaro di provenienza illecita, vendita di prodotti non autorizzati;
- ***danni a beni materiali*** - esempi: atti di terrorismo e vandalismo, terremoti, incendi, inondazioni;
- ***disfunzioni e avarie di natura tecnica*** - esempi: anomalie di infrastrutture e applicazioni informatiche, problemi di telecomunicazione, interruzioni nell'erogazione di utenze;
- ***conformità esecutiva e procedurale*** - esempi: errata immissione di dati, gestione inadeguata delle garanzie, documentazione legale incompleta, indebito accesso consentito a conti di clienti, inadempimenti di controparti non clienti, controversie legali con fornitori.

Fonte: «Prassi corrette per la gestione e il controllo del rischio operativo» emanate dal Comitato di Basilea per la vigilanza bancaria» - Febbraio 2003.

Elementi costituenti un Modello 231



..The definition includes **legal risk** but excludes..

Cosa comprende il rischio legale?

Il rischio di perdite derivanti da violazioni di leggi o regolamenti, da responsabilità contrattuale o extra-contrattuale ovvero da altre controversie (fonti varie).

Qual è il rapporto tra rischio legale e rischio operativo?

Rischio legale e rischio operativo

Rischio operativo e rischio reputazionale

Rischio reputazionale

Rischio legale

Rischio compliance

Rischio operativo

Attività prodromiche all'informativa…..

- mappatura dei reati applicabili
- assessment del livello di rischio di commissione del reato
- assessment del livello di efficacia del controllo presente
- assessment del livello di rischio residuo
- action plan per implementar le dovute azioni correttive

Teoria: coinvolgimento del Risk Management (1|3)

- utilizzando la metodologia RACI (Responsible, Accountable, Consulted, Informed), il Risk Management:

C mappatura dei reati applicabili

C assessment del livello di rischio di commissione del reato (impatto/frequenza => rischio inerente)

R assessment del livello di efficacia del controllo presente

A assessment del livello di rischio residuo

I action plan per eventualmente implementare le dovute azioni correttive

Teoria: coinvolgimento del Risk Management (2|3)

- Da www.portale231.com (estratto)

- L'OdV potrà facilmente trovarsi ad operare in contesti in cui siano presenti altri organi di controllo: il tema del coordinamento tra questi attori deve essere preso in considerazione e può tradursi in elementi migliorativi del più generale sistema di controllo interno dell'ente
- Più in generale, tra la molteplicità di organi di controllo di un ente, variabili in base al settore di operazioni e alla natura societaria dell'ente stesso, le controparti che un OdV si troverà più frequentemente a incontrare saranno ragionevolmente l'**Internal Audit**, la **Compliance**, il **Risk Management**.
- La strada da percorrere dovrebbe essere, a prescindere dall'identità tra i componenti dei singoli organi di controllo, quella del **reporting informativo**. Conoscere la quantità di informazioni già presenti nell'ente e la qualità dei dati prodotti dagli altri organi di controllo costituisce il terreno comune sul quale l'OdV può coordinare i flussi informativi senza incorrere in duplicazioni delle attività che possono rivelarsi costose, inefficienti e nel peggiore dei casi portare a conclusioni contraddittorie.
- Alcuni esempi chiarificatori: la tipologia, frequenza e contenuto dei verbali di audit interno può portare l'Organismo di Vigilanza a delegare all'Internal Audit l'attività di verifica sul campo, eventualmente addestrando il personale ai requisiti da controllare per la compliance aziendale al modello di organizzazione e gestione**. Il Risk Management rappresenta l'interlocutore ideale con cui analizzare i profili di rischio legati a eventuali modifiche al decreto (per esempio sotto il profilo dei reati presupposto),** mentre con la Compliance è possibile valutare gli impatti operativi collegati ai controlli da implementare a seguito dell'analisi di rischio.

Teoria: coinvolgimento del Risk Management (3|3)

- Secondo l'AODV (Associazione dei componenti degli Organismi di Vigilanza ex Dlgs 231/2001) il Risk Management:
  - potrebbe essere un possibile referente aziendale dell'ODV per le tematiche ex D.Lgs. 231/2001 con il ruolo di facilitatore nelle interazioni con l'OdV, specie con riferimento alla messa a disposizione di documenti e informazioni e nell'organizzazione delle interazioni con il management.
  - è una funzione con cui «scambiare informazioni sulle verifiche programmate in ottica di sinergia ed ottimizzazione con altre attività di verifica e monitoraggio svolte (ed al fine di evitare o comunque limitare duplicazioni di attività)» [omissis] «per la definizione delle tempistiche» [omissis] «per attivare, ove opportuno, eventuali flussi informativi specifici (richiedendo, ad esempio, l'inoltro dell'esito delle verifiche pianificate e svolte, ove non già previsto»

Pratica: coinvolgimento del Risk Management (1|3)

- In ambito industriale società operanti nell'ambito:
  - della GDO
  - di concessioni autostradali
  - della componentistica automotive e relativa al settore oil&gas
  - della produzione di macchinari (X)
  - della produzione di energia elettrica
  - della siderurgia (X)
  - della sanità e della biomedica
  - delle costruzioni edili (X) e della produzione di materiali per l'edilizia
  - della raccolta e trattamento dei rifiuti (X)
  - della farmaceutica (X)
  - della produzione e distribuzione di carburanti

hanno richiesto l'intervento di specialisti di corporate governance, nella fattispecie di risk & compliance supportati dal team legale dedicato

Pratica: coinvolgimento del Risk Management (2|3)

- Su un campione di 12 SGR immobiliari ove è stato svolto in passato il ruolo di Risk Manager nessuna SGR ha coinvolto la funzione nell'implementazione o nell'aggiornamento del Modello 231, né tantomeno nella richiesta delle relazioni periodiche prodotte dalla Funzione.
- In BNP è atteso a giorni un aggiornamento del Modello che prevede il coinvolgimento della funzione Risk Management nella produzione dei flussi informativi (al momento per «i rapporti predisposti dalle funzioni aziendali nell'ambito della loro attività di controllo dai quali possano emergere fatti che rappresentano profili rilevanti ai fini del rispetto del Modello»).
- Il coinvolgimento della Funzione è desiderabile in quanto alla funzione è demandato il monitoring dei rischi operativi (cfr. artt. 39 e 44 del Regolamento UE 231/2013).

Pratica: coinvolgimento del Risk Management (3|3)

- Secondo una ricerca ANRA (Associazione Nazionale dei Risk Manager e Responsabili Assicurazioni Aziendali) e FERMA (Federation Of European Risk Management Associations) in Italia solo il 54% dei risk manager è il primo responsabile nelle definizione di governance, framework e processi ERM (in UE la percentuale è al 76%)
- Inoltre, appena un 14% dei risk manager è responsabile dell'integrazione del risk management nelle strategie aziendali (il 74% in Europa). Tanto che gli stessi manager segnalano come molti dei rischi non siano pienamente sotto il loro controllo: va meglio con i rischi operativi (il 60% degli intervistati li ritiene di propria competenza) ma non con quelli strategici, legal e compliance (qui la percentuale scende al 24%) e con i rischi finanziari (20%)

Auspicabile coinvolgimento del Risk Management

- Potenziali flussi informativi sui rischi operativi inerenti:
  - Controlli di controparte ai fini antiriciclaggio e antiterrorismo
  - Controlli sulla corretta esecuzione degli obblighi Dlgs 81/2008
  - Controlli sui pagamenti (in particolare manuali)
  - Controlli sulle modifiche di basi dati sensibili
  - Controlli sulle modalità di svolgimento delle gare per l'affidamenti di appalti
  - Controlli sulle scritture contabili manuali
  - Controlli sulle procedure di selezione dei fornitori
  - Controlli sull'utilizzo e la performance dei sistemi informatici
  - Controlli sul processo di selezione delle risorse umane

Supporto del Risk Management: attività "core"

- mappatura dei reati applicabili
- assessment del livello di rischio di commissione del reato
- assessment del livello di efficacia del controllo presente
- assessment del livello di rischio residuo
- action plan per implementar le dovute azioni correttive

in quanto il Risk Management è la funzione metodologicamente più preparata in tale ambito

Grazie dell’attenzione