BANCO POPOLARE
GRUPPO BANCARIO

Lo *use test*: soluzioni organizzative a supporto di misurazione e analisi del rischio operativo

Rischio operativo – Convegno annuale DIPO

Carlo Palego, *Chief Risk Officer*

Roma, 16 giugno 2014

Agenda

L'Operational Risk Management nell'area CRO

Vantaggi gestionali di un Framework AMA

- Un **approccio** efficace ed efficiente alla **gestione** e **misurazione del rischio operativo** presuppone **meccanismi di *feedback*** tra la funzione aziendale di *Operational Risk Management* (ORM) e l'area organizzativa CRO

- In prima istanza, l'area CRO necessita di disporre degli strumenti tipici di un Framework AMA al fine di:

  - ✓ **innalzare** la **capacità di analisi** delle informazioni gestionali inerenti il rischio operativo
  - ✓ **avere** una **visione completa**, **accurata** ed **integrata** dei rischi a cui la Banca è esposta e delle loro determinanti
  - ✓ **rafforzare** la **capacità di interlocuzione** con le altre funzioni aziendali (es. CFO)

Operational Risk Management

- ✓ **Rilevazione**, **gestione** e **monitoraggio** del rischio operativo (processo di *Loss Data Collection*, *Risk Self Assessment*, reportistica)
- ✓ **Capacità** di **intercettare** ed **interpretare** l'esposizione attuale e prospettica dl rischio operativo
- ✓ **Misurazione** con finalità gestionali e regolamentari dell'esposizione al rischio operativo

Area organizzativa CRO

- ✓ **Disponibilità** ed **utilizzo** di un **patrimonio informativo** strutturato riveniente dai processi di ORM
- ✓ **Consolidamento** dei **dati** di rischio con le informazioni desumibili dalle **altre funzioni di controllo di II° livello**, assicurando completezza e qualità delle informazioni
- ✓ **Rappresentazione integrata** a livello aziendale delle **istanze proprie** del **sistema dei controlli interni** relative all'**assunzione governata** e **consapevole dei rischi**

Il CRO nell'Operational Risk Management
Gestione "attiva" del rischio operativo

- In seconda istanza, la responsabilità della **gestione "attiva"** del rischio attribuita ad un'**area organizzativa CRO** incentrata su una **figura** di **coordinatore** dei controlli di II° livello permette di incrementare il ***leveraging* gestionale** del *Framework* AMA, anche attraverso la minimizzazione del rischio "*garbage in, garbage out*" che può affliggere sistemi di misurazione "scollegati" dagli aspetti di gestione del rischio

- In particolare, ciò si realizza principalmente mediante:
  - ✓ l'**arricchimento** delle **informazioni di rischio** rivenienti dai processi "*core*" di ORM, al fine di aumentarne l'interpretabilità
  - ✓ la **capacità** di **intercettare** con maggior completezza e tempestività i **fenomeni di rischio**, in quanto non occorre attendere il censimento delle informazioni nei processi di ORM

Area Organizzativa CRO *

L'area CRO è articolata su una **figura specialistica** di **coordinamento** (CRO) delle seguenti funzioni indipendenti e separate:

- ✓ **Risk Management** e **Compliance**, con responsabili titolari di autonomi compiti di *reporting* agli Organi Sociali e che partecipano di diritto ai Comitati manageriali (Comitato Rischi, Nuovi Prodotti, ecc.)
- ✓ **Convalida Interna**, quale funzione "rilevante" in ottica di validazione dei modelli interni di misurazione dei rischi
- ✓ altre funzioni (es. **Legale**), con un responsabile a riporto diretto del CRO

Ruolo del CRO

Tale modello permette al CRO di sviluppare una **visione "*all round*" dei rischi** e della genesi dei fenomeni di perdita operativa

** In conformità alla disposizioni regolamentari vigenti, tale modello deve perseguire il rafforzamento della linea di riporto diretta dei responsabili di Compliance/Risk Management agli Organi di vertice aziendale*

L'Operational Risk Management nel governo d'impresa
Condizioni di use-test

Un efficace ed efficiente **sistema di governo del rischio operativo** non può limitarsi alla semplice rilevazione del rischio nella misura in cui si sono verificate le perdite storiche, ma deve rispettare ulteriori **requisiti quantitativi** (vincoli alle tecniche di misurazione) e **qualitativi** (requisiti organizzativi):

- ***Risk mapping*** – Identificare tempestivamente le aree di operatività in cui si generano potenziali rischi operativi
- ***Risk measurement*** – Implementare tecniche di misurazione del rischio operativo su *input* quantitativi (es. perdite storiche e prospettiche) e qualitativi (rivenienti dalle attività periodiche di valutazione dei fattori causali / del contesto operativo)
- ***Risk reporting*** – Sviluppare flussi informativi strutturati e con adeguato livello di dettaglio ed interpretabilità in ottica *business*, finalizzati a garantire una rendicontazione periodica del rischio operativo ai centri di responsabilità e agli Organi di vertice aziendale (Alta Direzione, Organo con funzione di gestione, ecc.)
- ***Risk mitigation*** – Razionalizzare l'insieme delle evidenze derivanti dai processi di misurazione e gestione del rischio operativo, nell'ottica di individuare criticità operative rilevanti e progetti / interventi di mitigazione del rischio destinati agli Organi di vertice aziendale

Il rispetto di tali requisiti è necessario ai fini dell'ottenimento della validazione di Banca d'Italia all'utilizzo in chiave regolamentare dei Framework AMA

Peculiare natura del rischio operativo: trasversalità e capillarità
Elementi qualificanti l'implementazione di Framework avanzati di ORM

- Il rischio operativo si identifica come un **rischio intrinseco** e **trasversale** all'operatività aziendale, diffuso in ogni processo operativo della Banca e da presidiare con adeguati sistemi, controlli e risorse

- Inoltre, a differenza dei rischi finanziari e di credito, il semplice **dato storico non rappresenta** necessariamente una "**buona**" *proxy* **del rischio operativo** e **non esistono metriche di misurazione** *standard* di emanazione regolamentare e/o consolidate nella prassi

- Tali caratteristiche giustificano, in sede di implementazione di Framework avanzati di ORM, l'attivazione di un **adeguato modello organizzativo** in cui la struttura di Risk Management coordina un **ampio** e **capillare** *network* **di ORM decentrati** presso le Unità Organizzative rilevanti della Banca

- Tale struttura decentrata di ORM assume infatti un **ruolo attivo** e **cruciale** in tema di:

✓ ***Data quality*** – Attività necessarie a garantire la corretta e tempestiva rilevazione e segnalazione delle perdite operative

✓ **Analisi soggettiva del rischio** – Insieme delle attività di valutazione del rischio in ottica prospettica da parte di *Business Expert* pre-individuati, che contribuiscono all'interpretazione delle dinamiche di rischio operativo e alimentano le tecniche di misurazione di tale tipologia di rischio (in coerenza con le istruzioni di Vigilanza Prudenziale)

Tecniche di misurazione: la rilevazione del rischio operativo
L'importanza della rilevazione qualitativa del rischio

L'**analisi soggettiva del rischio**, realizzata con il coinvolgimento "attivo" degli ORM decentrati, si configura indirettamente come una **componente di misurazione del rischio operativo**, in quanto consente di:

- ✓ intercettare, pur tenendo conto della rischiosità passata, **aspetti di rischio molto rilevanti** in ottica "*forward-looking*", indotti da cambiamenti nel contesto operativo interno / esterno non già manifestatisi in termini di perdite
- ✓ indirizzare una **misurazione del rischio** non soltanto per *Risk Class* / *Event Type* (come per la rilevazione LDA) ma **per *Event Type* / Unità Organizzativa (Processi)**, la quale risulta efficace in sede di *risk reporting* (*report* direzionale / operativo) e *mitigation* (nella misura in cui l'intervento mitigativo è più precisamente delimitato)

Alla luce di quanto detto, una struttura "forte" – in termini di *commitment* e formazione professionale – degli ORM decentrati garantisce un'**elevata qualità** dell'**analisi soggettiva** e della **misurazione del rischio**, in sede di svolgimento:

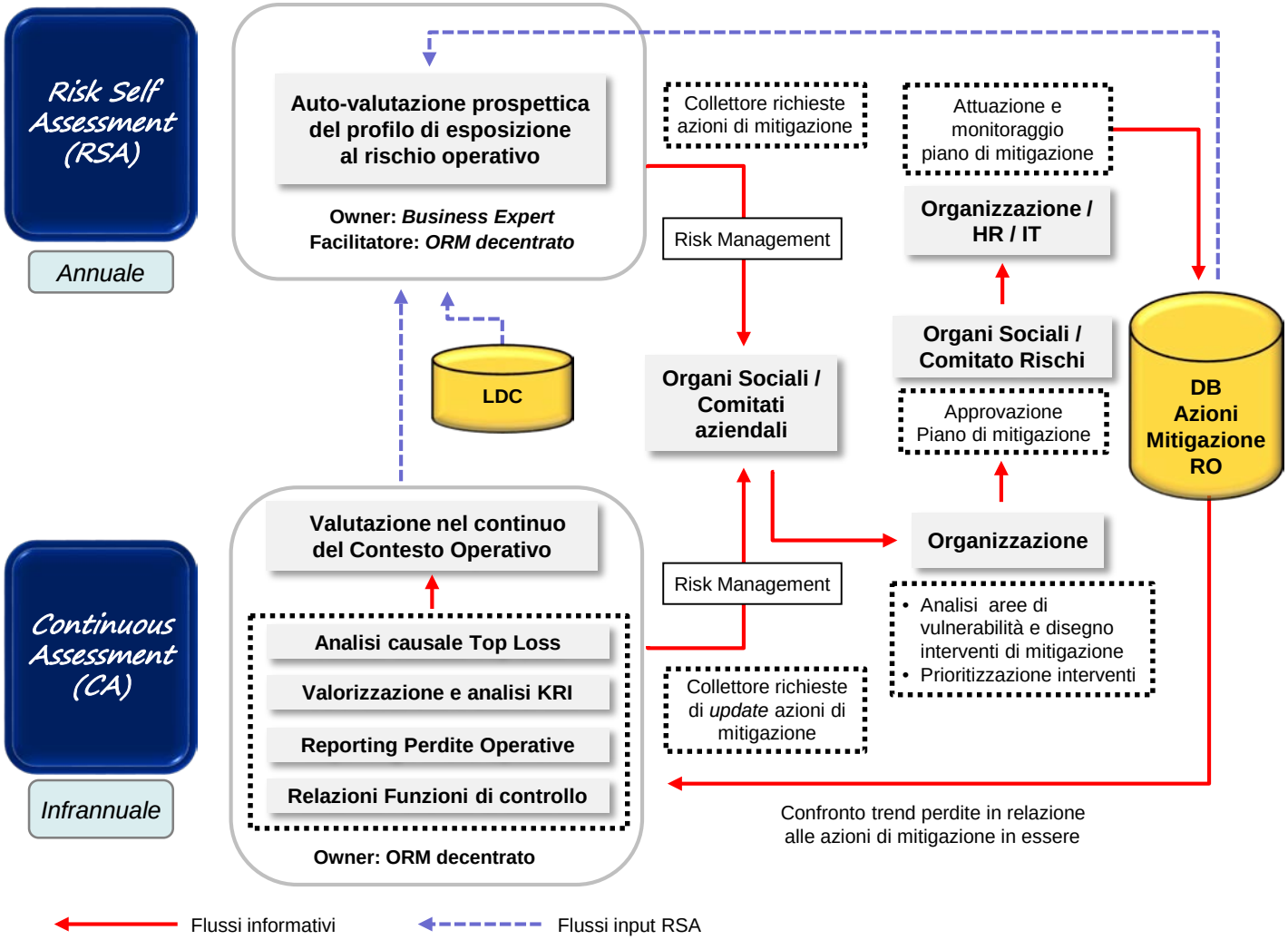
- ✓ del ***Risk Self Assessment*** annuale, dove è necessario sviluppare una dialettica costruttiva al fine di "facilitare" la formulazione di stime soggettive di perdita da parte dei *Business Expert*
- ✓ delle **attività di valutazione del contesto operativo** (c.d. *Continuous Assessment*), assicurando l'identificazione e il monitoraggio di eventuali cambiamenti / dinamiche che generano rischi operativi per l'ambito di competenza

Approcci gestionali innovativi: il Continuous Assessment

Interazione tra le componenti del Framework di Operational Risk Assessment (1/2)

Processo

Owner, attività e flussi informativi tra RSA e VCO



Key points

L'attivazione del processo di **Continuous Assessment** costituisce una risposta di natura organizzativa e gestionale all'implementazione di Framework avanzati ed evoluti di ORM, in grado di:

- **intercettare** nel continuo l'**evoluzione** del **profilo di rischio**, evitando di limitare le attività di *assessment* al solo esercizio annuale di RSA
- favorire il **monitoraggio degli interventi di mitigazione del rischio**

Le attività di valutazione del contesto operativo supportano pertanto l'esecuzione del **RSA**, contribuendo:

- ad **attivare** una reale e costruttiva **dialettica** con i *Business Expert*, a partire dagli esiti delle analisi periodiche svolte
- al **miglioramento** del livello di "azionabilità del *reporting*"
- alla **quantificazione del requisito di capitale** a fronte del rischio (tramite una più consapevole valutazione in sede RSA)
- a **rafforzare l'intero sistema di ORM**, rendendo più efficienti i processi / controlli ed indirizzando gli opportuni interventi di mitigazione del rischio

Approcci gestionali innovativi: il Continuous Assessment

Metodologia e processo di valutazione del contesto operativo (2/2)

Facendo leva sul presidio decentrato di ORM, il processo di **Continuous Assessment** consente di **indagare** le **variazioni qualitative** intervenute nei fattori di contesto operativo, permettendo tra l'altro di **arricchire** il *set* di **attività** di **analisi gestionale** e ***reporting*** del rischio operativo

Ambito	Descrizione
Esecuzione del processo – Rilevazione input "qualificanti"	▪ **Reporting gestionale / operativo** – Rilevazione ed analisi dell'esposizione a consuntivo ai rischi operativi ▪ **Key Risk Indicators** (KRI) – Valorizzazione e analisi degli indicatori di rischio (ambiti *Business* e IT) ▪ Informazioni desumibili dalle **relazioni** redatte da **altre funzioni aziendali** (Audit, Compliance, ecc.) ▪ Rilevazione di **cambiamenti nel contesto** organizzativo **interno** (es. nuovi prodotti) ed **esterno** (es. normativa esterna) in grado di influenzare la frequenza/l'impatto di perdita conseguente alla manifestazione di rischi operativi
Esecuzione del processo – Monitoraggio e Valutazione del contesto operativo	▪ **Schede di analisi – Formalizzazione** delle **chiavi di lettura** rilevate, con indicazione di aree di vulnerabilità, fenomeni di rischiosità emergenti, cause generatrici di rischio, suggerimenti in materia di mitigazione ▪ **Questionario qualitativo – Rilevazione** e **valutazione** degli **eventi di rischio** (tassonomia di Gruppo) con **variazione significativa** nell'**esposizione potenziale** rispetto alle precedenti sessioni di RSA, in termini di: ➢ **Grado di esposizione in termini assoluti** al rischio operativo (cd. *Rischio inerente*) ➢ **Livello dei presidi** – adeguatezza del sistema dei controlli interni a presidio del rischio in esame ➢ **Grado di esposizione netta** al rischio operativo (cd. *Rischio residuo*)
Output "gestionali"	▪ **Monitoraggio** dell'**efficacia** e dei **livelli di prioritizzazione delle azioni di mitigazione** attivate / in fase di implementazione, anche a seguito della rilevazione di criticità operative "emergenti" ▪ **Integrazione** dei **contenuti del Report Direzionale**, con riepilogo delle evidenze desumibili dal presidio decentrato di ORM, da sottoporre all'attenzione di Organi / Comitati aziendali, contribuendo alla diffusione della cultura del rischio ▪ "**Rilascio**" di elementi qualitativi atti a **ridurre** i **margini di soggettività** e **facilitare** l'**esecuzione** del processo di RSA (es. aggiornamento del *risk-mapping*)

Intraprendere un percorso di validazione AMA

Fattori critici e sfide progettuali

L'attivazione e il completamento di un percorso di validazione AMA sono "ancorati" ad una pluralità di **fattori critici** che risentono di un contesto progettuale influenzato da **fattori esogeni**, **evoluzione** della **realtà aziendale** interessata e **"spinte" regolamentari** esercitate dal *Regulator*

Sfide progettuali

- ***Pianificazione progettuale non comprimibile oltre 24 mesi***
- ***Concomitanza con altre progettualità che "assorbono" più risorse ed interessi***
- ***Evoluzioni regolamentari (es. 15° agg. Circ. 263, passaggio alla Vigilanza Unica)***
- ***Evoluzione contesto aziendale (es. riorganizzazione rete distributiva)***

Fattori critici

1. Attivazione di un progetto con forte componente di ***change management*** e di **radicamento della cultura del rischio**
2. Forte ***commitment*** del ***Top Management*** e **partecipazione "multidisciplinare"** costante di tutte le funzioni rilevanti di Capogruppo e Controllate (es. Organizzazione, strutture IT, Funzioni di Controllo)
3. Presenza di **risorse con *skill* specialistici** (quantitativi e qualitativi) presso l'ORM Centrale e le Funzioni di Controllo (Audit, Convalida)
4. ***Leverage* "continuativo"** e **integrato** di ***advisory*** sulle *best practice* di mercato e delle soluzioni di frontiera
5. Sviluppo di un ampio e capillare ***network* di ORM decentrati** (es. rete dei Referenti ORM)
6. ***On-boarding*** delle **funzioni di controllo** sin dall'avvio del progetto
7. ***Leverage*** su **investimenti IT "propedeutici"** ad una gestione più efficiente dei processi di ORM, minimizzando gli *effort* richiesti alle strutture aziendali e assicurando l'elevata qualità dei dati di perdita
8. **Ingaggio immediato del *Regulator***