Dicembre 2013

L'aggiornamento della Circolare 263: profonde novità sul Sistema dei Controlli Interni delle Banche, nel sottile equilibrio tra costi e benefici

Dott. Luca Galli, partner Ernst & Young, FSO Advisory Services

La disamina delle cause e delle conseguenze connesse alla recente crisi finanziaria hanno confermato la centralità della *Governance* e dei Sistemi di Controllo Interno delle banche nel garantire la loro sana e prudente gestione e, per traslato, le stabilità del sistema finanziario e, in ultima analisi, dell'economia tutta.

Muovendo da tale consapevolezza, le autorità internazionali e all'unisono quelle domestiche hanno emanato una fitta serie di provvedimenti destinati a ridisegnare profondamente la cornice regolamentare entro la quale dovrà svilupparsi il mercato bancario europeo nel prossimo quinquennio.

In tale mutevole contesto e con medesimo spirito, si inseriscono le recenti previsioni introdotte da Banca d'Italia con il 15° aggiornamento della Circolare n. 263/2006 (luglio 2013), attraverso le quali la nostra Autorità di Vigilanza si propone di:

- Rafforzare la capacità delle banche nella gestione dei rischi aziendali;
- Rivedere organicamente l'attuale quadro normativo in materia di Sistema dei Controlli Interni, Sistemi Informativi e Continuità Operativa;
- Allineare la normativa nazionale alle previsioni comunitarie.

La Relazione di Autovalutazione

Tali e tante sono le novità introdotte dal menzionato aggiornamento che Banca d'Italia ha richiesto alle banche di predisporre una relazione recante un'autovalutazione della propria situazione aziendale rispetto alle previsioni della nuova normativa (*Gap Analysis*) e che dia altresì evidenza delle misure da adottare e della relativa scansione temporale per assicurarne il pieno rispetto *(Master Plan)*.

Il rilievo assunto da tale Relazione ha indotto EY ad organizzare il 25 novembre 2013 un workshop con la partecipazione dei primi 5 Gruppi bancari italiani e di numerosi altri primari istituti, durante il quale si è dialetticamente riflettuto attorno alla possibile

articolazione e ai contenuti della Relazione in parola e di cui si fornisce qui breve illustrazione:

- Un primo capitolo introduttivo nel quale descrivere almeno (i) il contesto normativo, (ii) il perimetro di riferimento, (iii) l'approccio seguito per l'esecuzione della *gap analysis*, (iv) il grado di coinvolgimento degli organi aziendali e gli eventuali momenti di approfondimento e condivisione intervenuti con essi, (v) possibili *caveat* riguardo situazioni di carattere straordinario (e.g. commissariamento, fusioni, …) o su temi rispetto ai quali si vuole attrarre l'attenzione di Bankit (e.g. enfasi sul "principio di proporzionalità").

- Un secondo capitolo contenente una sinossi della situazione *as-is* con particolare riferimento alla *governance* (ruoli, compiti e responsabilità degli organi aziendali), al sistema dei controlli interni (principi guida e sue principali componenti), al sistema informativo (con particolare enfasi su organizzazione, sicurezza, gestione dei dati e esternalizzazioni) e alla continuità operativa (strategie e governo del relativo processo, *business impact analysis* e piano di continuità).

- Un terzo capitolo riportante l'*Executive Summary* dell'autovalutazione unitamente ad una ragionata descrizione dei gap e delle misure da adottare.

- Un ultimo capitolo contenente, per ciascuna misura da adottare, il dettaglio - in forma tabellare - dei principali interventi realizzativi da intraprendere e la relativa scansione temporale *(Master Plan)*.

Quali sono le principali "misure da adottare" ?

- Aggiornamento delle responsabilità attribuite agli organi aziendali e conseguente revisione della normativa interna di riferimento.

- Definizione e implementazione del *Risk Appetite Framework (RAF)*.

- Revisione del posizionamento gerarchico delle funzioni di controllo di secondo livello.

- Predisposizione del documento di coordinamento tra funzioni e organi di controllo.

- Estensione del perimetro di competenza della funzione *Compliance, Risk Management e Internal Audit.*

- Definizione e implementazione del processo di gestione e approvazione delle Operazioni di Maggior Rilievo.

- Definizione e implementazione delle verifiche sul corretto monitoraggio andamentale del credito.

- Estensione del processo di convalida ai sistemi di misurazione dei rischi non utilizzati a fini regolamentari.

- Integrazione della mappatura dei processi, dei rischi associati e dei relativi presidi di controllo.

- Predisposizione delle politica aziendale in materia di esternalizzazione e adeguamento ai nuovi dettami normativi dei contratti di esternalizzazione.

- Revisione delle responsabilità legate al governo e alla complessiva organizzazione del sistema informativo.

- Definizione e implementazione di una processo di analisi e gestione dell'IT Risk e sua integrazione all'interno del *RAF*.

- Definizione della *policy* di sicurezza informatica e implementazione delle attività necessarie al suo rispetto.

- Definizione e implementazione di adeguate politiche aziendali in tema di *Data Governance*.

- Definizione e implementazione di un processo di stima dei rischi nei casi di esternalizzazione del sistema informativo o di sue componenti critiche.

- Revisione e aggiornamento della *Business Impact Analysis*, del piano di continuità operativa e delle procedure di gestione della crisi.

L'equilibrio costi e benefici

In conclusione, quanto si profila nei prossimi mesi per le banche di qualsiasi dimensione è la sfida (*rectius*: la "missione quasi impossibile") di trovare le risorse finanziarie e umane per porre in essere i menzionati interventi, in un contesto economico complesso. Sfida che potrà essere vinta, soltanto capitalizzando gli investimenti fatti in passato e prevedendo una "regia comune" che governi la realizzazione del Master Plan e che consenta di evitare l'introduzione di sovrastrutture organizzative e operative dettate dalla contingenza di dover rispondere alle pressanti ed eterogenee richieste del Regulator.