Sintesi per gli utenti ([1])

Nuove disposizioni di vigilanza prudenziale per le banche (Circ. n. 263 del 27 dicembre 2006) – 15° aggiornamento "Sistema dei controlli interni, sistema informativo e continuità operativa"

A) Quali sono gli obiettivi?

L'intervento normativo è in linea di continuità con le previgenti disposizioni ed è volto a spingere le banche a rafforzare ulteriormente la propria capacità di gestire i rischi aziendali, richiedendo che queste si dotino di un sistema di controlli interni completo, adeguato, funzionale e affidabile.

La crisi finanziaria ha messo fortemente alla prova la capacità delle banche di gestire efficacemente le diverse tipologie di rischi e di reagire prontamente a situazioni di criticità; in tale contesto, è emerso con chiarezza che assetti di governo efficienti e funzioni di controllo autorevoli, attive e indipendenti, consentono di evitare o limitare le perdite conseguenti a situazioni di crisi intense e diffuse. Particolare importanza riveste il coinvolgimento attivo dei vertici aziendali nella gestione della banca e nella comprensione dei rischi insiti nell'operatività aziendale.

La disciplina fa leva su alcuni **principi di fondo,** coerenti con le migliori prassi internazionali e con le raccomandazioni dei principali *standard setter* (*Financial Stability Board*, Comitato di Basilea per la vigilanza bancaria, EBA); tra questi: il maggior coinvolgimento dei vertici aziendali; l'esigenza di assicurare una visione integrata e trasversale dei rischi; l'attenzione ai temi dell'efficienza e dell'efficacia dei controlli; la valorizzazione del principio di proporzionalità, che consente di graduare l'applicazione delle norme in funzione della dimensione e della complessità operativa delle banche.

L'intervento normativo, inoltre, **razionalizza e semplifica** il quadro regolamentare, riunendo in un'unica fonte normativa organica la disciplina di vigilanza relativa alle caratteristiche e ai requisiti di carattere generale del sistema dei controlli interni

B) Come si raccordano le nuove disposizioni con gli altri provvedimenti normativi che contengono regole di carattere organizzativo?

Le singole normative di vigilanza, in molti casi, prevedono presidi di tipo organizzativo e attribuiscono compiti e responsabilità ai vertici aziendali e alle funzioni di controllo per assicurare la realizzazione degli obiettivi regolamentari.

Tali presidi organizzativi e compiti non vengono meno con l'emanazione delle nuove disposizioni sul sistema dei controlli interni; anzi, essi si integrano in quest'ultima, definendo il complesso normativo in materia di organizzazione e controlli.

Secondo questa logica, la nuova disciplina sui controlli interni definisce i principi e le regole cui deve essere ispirato il sistema dei controlli interni. Essa costituisce, dunque, il perno (*hub*) del

([1]) Il presente documento ha finalità meramente illustrative e informative. Gli intermediari si attengono al testo delle disposizioni contenute nella Circolare n. 263 del 27 dicembre 2006, "*Nuove disposizioni di vigilanza prudenziale per le banche*", Titolo V, Capitoli, 7, 8 e 9.

sistema organizzativo e dei controlli, sul quale si innestano, come raggi ideali, le specifiche regole sui controlli dettate all'interno di specifici ambiti disciplinari (c.d. modello "*hub and spokes*") ([2]).

C) Quali sono le principali novità?

Le principali novità introdotte dalla nuova normativa riguardano: (i) la previsione di principi generali di organizzazione; (ii) i compiti degli organi aziendali; (iii) la definizione del *Risk Appetite Framework (RAF)*; (iv) il rafforzamento dei controlli di primo, secondo e terzo livello; (v) l'*outsourcing*; (vi) la disciplina del sistema informativo; (vii) la continuità operativa.

1) I principi generali di organizzazione

Il nuovo quadro regolamentare introduce alcuni principi generali di organizzazione che le banche devono rispettare nell'articolazione dei propri assetti organizzativi, che costituiscono, insieme alle regole di *governance*, i pre-requisiti di un sistema dei controlli interni ben funzionante.

In particolare, è richiesta la formalizzazione dei processi decisionali e l'affidamento di funzioni al personale, mediante la chiara individuazione dei compiti e delle responsabilità di ciascuna unità organizzativa, prevenendo eventuali situazioni di conflitti di interesse: a tal fine, va assicurata la separatezza tra funzioni operative e funzioni di controllo.

Le banche sono altresì chiamate a dotarsi di politiche di gestione delle risorse umane tali da assicurare che il personale sia provvisto delle competenze e delle professionalità necessarie per svolgere i compiti a esso attribuiti. Devono essere, in generale, prevenuti o minimizzati rischi legati a frodi o infedeltà dei dipendenti anche attraverso la diffusione, a tutti i livelli dell'organigramma, di una cultura della legalità.

2) I compiti degli organi aziendali

La nuova normativa ha delineato in maniera puntuale i compiti e le responsabilità degli organi aziendali nella definizione del sistema dei controlli interni delle banche. In particolare, all'**organo con funzione di supervisione strategica** (il *board*) ([3]) spetta la definizione del modello di *business*, degli indirizzi strategici, dei livelli di rischio accettati e l'approvazione dei processi aziendali più rilevanti (quali, la gestione dei rischi, la valutazione delle attività aziendali e l'approvazione di nuovi prodotti/servizi). All'**organo con funzione di gestione** (ossia l'organo cui spetta la gestione corrente della banca) è richiesto di attuare gli indirizzi strategici, avendo piena comprensione di tutti i rischi aziendali e delle loro interrelazioni, tenuto anche conto dell'evoluzione del contesto esterno e del rischio macroeconomico. All'**organo con funzione di controllo** (collegio sindacale, consiglio di sorveglianza o comitato per il controllo) spetta, invece, il compito di vigilare sulla completezza, adeguatezza, funzionalità e affidabilità del sistema dei controlli interni e del RAF.

3) Il Risk Appetite Framework (RAF)

Tra le principali novità introdotte, vi è l'obbligo per le banche di definire il RAF, ossia quell'insieme di politiche, processi, controlli e sistemi che consente di stabilire, formalizzare, comunicare e monitorare gli obiettivi di rischio che una banca intende assumere. Esso è articolato in soglie e limiti di rischio, che consentono di individuare a priori i livelli e le tipologie di rischio che una banca intende assumere, e individua i ruoli e le responsabilità di tutte le strutture aziendali coinvolte nel processo di gestione dei rischi. È richiesto che il RAF sia coerente con il piano

([2]) Ad esempio, regole organizzative in materia di gestione di singoli profili di rischio, di sistemi interni di misurazione dei rischi per il calcolo dei requisiti patrimoniali, di processo ICAAP, di prevenzione del rischio di riciclaggio, ecc.

([3]) L'organo con funzione di supervisione strategica è l'organo aziendale che definisce gli indirizzi strategici della gestione della banca.

strategico e con le risultanze del processo interno di autovalutazione dell'adeguatezza patrimoniale (c.d. ICAAP). Le disposizioni indicano il contenuto minimale del RAF, la cui articolazione dipende dalle dimensioni e dalla complessità operativa di ciascuna banca. Per declinare in concreto gli obiettivi e i limiti di rischio, in base alla tipologia (rischio di mercato piuttosto che rischio di non conformità) e alla natura (quantificabile o meno) del rischio, sono utilizzati sia parametri quantitativi, quali ad esempio misure di capitale e di liquidità, sia parametri qualitativi.

4) Il rafforzamento dei controlli di primo, secondo e terzo livello

Molto rilievo è stato dato **all'articolazione e al corretto funzionamento dei controlli.** Sono stati potenziati i requisiti alla base dei controlli di primo livello, che prevedono il coinvolgimento delle stesse unità di *business*. È stata rivista la disciplina delle funzioni aziendali responsabili dei controlli di secondo livello (*risk management* e *compliance*) e di terzo livello (*internal audit*), con l'obiettivo di renderle più incisive e di assicurarne la vicinanza agli organi aziendali. È stata prestata massima attenzione al coordinamento dell'attività dei vari organi e funzioni di controllo, in modo da sfruttarne le sinergie ed evitare lacune nei controlli; le banche devono predisporre un documento che formalizzi le modalità di coordinamento.

Per assicurare **l'indipendenza e l'autorevolezza del *risk management,* della *compliance* e dell'*internal audit***, sono state previste rigorose procedure di nomina e di revoca dei responsabili, che coinvolgono gli organi aziendali; è richiesto che il personale addetto sia adeguato in termini quali - quantitativi; vengono richiesti presidi organizzativi per garantirne l'indipendenza dalle aree di *business*; sono delineate modalità di riporto, gerarchico e funzionale, verso gli organi aziendali.

Il ruolo del responsabile del ***risk management*** (***Chief Risk Officer*** - CRO) è stato significativamente ampliato. Al CRO sono, infatti, affidati compiti di ausilio all'organo con funzione di supervisione strategica nella definizione del RAF, di monitoraggio nel continuo dell'andamento della rischiosità aziendale e il potere di vagliare preventivamente le operazioni di maggior rilievo con possibilità di attivare procedure di *escalation* verso l'esecutivo aziendale (c.d. potere di veto). Al *risk management* è stato anche affidato un importante ruolo di verifica sul monitoraggio delle esposizioni creditizie, sui criteri di classificazione, sulla congruità degli accantonamenti e sul processo di recupero.

Le disposizioni chiariscono che la funzione di ***compliance*** assicura, secondo un approccio *risk based*, il presidio del rischio di non conformità con riferimento a tutte le norme applicabili alle banche; il suo coinvolgimento è stato graduato in relazione al rilievo che le singole norme hanno per l'attività svolta, alle conseguenze della loro violazione e all'esistenza all'interno della banca di altre forme di presidio specializzato. È stato inoltre introdotto un riferimento esplicito al presidio del rischio di non conformità alla normativa fiscale; in particolare, alla *compliance* si richiede almeno: (i) la definizione di procedure volte a prevenire violazioni o elusioni di tale normativa e ad attenuare i rischi connessi a situazioni che potrebbero integrare fattispecie di abuso del diritto, in modo da minimizzare le conseguenze sia sanzionatorie, sia reputazionali derivanti dalla non corretta applicazione della normativa fiscale; (ii) la verifica dell'adeguatezza di tali procedure e della loro idoneità a realizzare effettivamente l'obiettivo di prevenire il rischio di non conformità.

5) L'outsourcing

Il ricorso all'esternalizzazione è funzionale ad accrescere la flessibilità organizzativa delle banche che possono così dedicare maggiori risorse al *core business* oltre che perseguire obiettivi di riduzione dei costi. Le nuove disposizioni introducono un'organica disciplina in materia di esternalizzazione di funzioni aziendali. In particolare, il ricorso all'***outsourcing*** è ammesso, in coerenza con l'apposita politica che deve essere definita in materia, purché le banche presidino attentamente i rischi derivanti dalle scelte effettuate e mantengano la capacità di controllo e la responsabilità delle attività esternalizzate. I requisiti richiesti per procedere all'*outsourcing* di

funzioni aziendali sono graduati in modo diverso a seconda che l'esternalizzazione riguardi funzioni operative importanti o di controllo.

Nel caso di esternalizzazione all'interno del gruppo bancario, invece, è stata definita una disciplina specifica, improntata a maggiore flessibilità e con requisiti meno stringenti in modo da facilitare l'integrazione dei controlli a livello di gruppo anche in considerazione del fatto che il gruppo bancario può essere considerato un unico soggetto economico e che l'esternalizzazione avviene presso società soggette al potere di direzione e coordinamento della capogruppo.

6) La disciplina del sistema informativo

Un **sistema informativo** sicuro ed efficiente consente di sfruttare le opportunità offerte dalla tecnologia per accrescere la qualità e l'efficienza dei processi aziendali, per migliorare i flussi informativi all'interno della banca nonché per ampliare e migliorare i prodotti e i servizi per la clientela. Data la sua centralità per la buona gestione della banca, è stata introdotta una disciplina organica del sistema informativo. In particolare, sono stati analiticamente disciplinati la *governance* e l'organizzazione del sistema informativo, le modalità di gestione del rischio informatico, i requisiti per assicurare la sicurezza informatica, il sistema di gestione dei dati; le disposizioni recepiscono inoltre le raccomandazioni della BCE per la sicurezza delle transazioni bancarie tramite internet.

7) La continuità operativa

Sono state riorganizzate le disposizioni in materia di **continuità operativa**, attualmente contenute in diverse fonti. Tra le novità di maggiore rilievo, vi è la formalizzazione del ruolo del CODISE, struttura per il coordinamento della gestione delle crisi operative della piazza finanziaria italiana presieduta dalla Banca d'Italia.

C) Il principio di proporzionalità è applicabile alle presenti disposizioni?

Il principio di proporzionalità riveste un ruolo molto importante nella nuova disciplina. Partendo dal presupposto che "*one size does not fit all*", il testo regolamentare contiene numerose previsioni che consentono di applicare requisiti meno stringenti a quelle banche che si caratterizzano per dimensione e complessità operativa contenute. A titolo di esempio, tali banche possono avere un'unica struttura incaricata dei controlli di secondo livello e possono esternalizzare le funzioni aziendali di controllo anche a soggetti non rientranti nel gruppo bancario di appartenenza.

D) Quali sono i principali benefici?

Ci si attende che le novità introdotte dalla normativa in materia di sistema dei controlli interni, sistema informativo e continuità operativa contribuiscano a rafforzare gli assetti organizzativi delle banche in modo da renderle più consapevoli delle tipologie e dei livelli di rischio assunti e meglio preparate nella gestione degli stessi rischi. Ciò avrà effetti benefici diretti per la sana e prudente gestione delle singole banche e, di conseguenza, per il sistema bancario nel suo complesso.

E) Quali sono le date di entrata in vigore e di efficacia?

Le nuove disposizioni sono entrate in vigore il 3 luglio 2013 e saranno efficaci, salvo talune eccezioni, a partire dal 1° luglio 2014; la disciplina del sistema informativo sarà efficace dal 1° febbraio 2015. L'adeguamento alle novità introdotte con questo intervento normativo presuppone,

infatti, interventi significativi sulla struttura organizzativa, che richiedono tempo per essere realizzati. Alle banche è stato comunque richiesto di effettuare, entro il 31 gennaio 2014, una autovalutazione della propria situazione aziendale rispetto alle previsioni della nuova normativa (*gap analysis*) e di individuare le misure da adottare per assicurarne il rispetto.