

Client briefing

Settembre 2013

SOMMARIO

1. Introduzione	1
2. Controlli interni e presidio del rischio nelle nuove disposizioni di vigilanza	1
3. Autovalutazione e <i>gap analysis</i>	2
4. Tempistica degli adempimenti	3
5. La nuova disciplina in materia di esternalizzazioni	3
6. Adeguamento della contrattualistica.....	4
7. Obblighi di segnalazione e comunicazioni alla Banca d'Italia in materia di esternalizzazioni.....	5
8. Le implicazioni per l'operatività bancaria	5

Nuove disposizioni di vigilanza in materia di controlli interni ed esternalizzazioni: quali implicazioni per le banche?

1. Introduzione

Con provvedimento del 2 luglio 2013, la Banca d'Italia ha aggiornato le disposizioni di vigilanza prudenziale per le banche in materia di sistema dei controlli interni, sistema informativo e continuità operativa, introducendo altresì una specifica disciplina in materia di esternalizzazione delle funzioni aziendali.

Le nuove disposizioni sono entrate in vigore il 3 luglio 2013 e saranno efficaci a partire dal primo luglio 2014. Si prevede tuttavia che le banche provvedano ad effettuare, entro il 31 dicembre 2013, una autovalutazione della situazione aziendale rispetto alle previsioni della nuova normativa (c.d. *gap analysis*) e di individuare le misure da adottare per assicurarne il rispetto.

2. Controlli interni e presidio del rischio nelle nuove disposizioni di vigilanza

Le disposizioni in argomento introducono alcune novità di rilievo rispetto al vigente quadro normativo, imponendo alle banche di dotarsi un sistema dei controlli interni completo, adeguato, funzionale e affidabile.

In particolare, le nuove norme enfatizzano il ruolo dell'*organo con funzione di supervisione*

strategica nella definizione del modello di *business* e del *Risk Appetite Framework (RAF)*; a tale organo è richiesto anche di favorire la diffusione di una cultura dei controlli attraverso l'approvazione di un codice etico al quale sono tenuti a uniformarsi i componenti degli organi aziendali e i dipendenti.

All'**organo con funzione di gestione** è invece richiesto di dotarsi di un'approfondita comprensione di tutti i rischi aziendali e, nell'ambito di una gestione integrata, delle loro interrelazioni reciproche e con l'evoluzione del contesto esterno (incluso il rischio macroeconomico).

Le disposizioni richiedono ai vertici delle banche di prestare particolare attenzione nella definizione delle politiche e dei processi aziendali di maggiore rilievo, quali quelli riguardanti:

- la gestione dei rischi;
- la valutazione delle attività aziendali;
- l'approvazione di nuovi prodotti/servizi o dell'avvio di nuove attività nonché dell'inserimento in nuovi mercati;
- lo sviluppo e la convalida dei modelli interni di misurazione dei rischi non utilizzati a fini regolamentari.

Anche la disciplina delle funzioni aziendali di controllo (*internal audit*, *compliance* e *risk management*) è stata oggetto di una profonda rivisitazione; in particolare:

- la nomina e la revoca dei responsabili delle funzioni aziendali di controllo devono essere rimesse alla competenza esclusiva dell'organo con funzione di supervisione strategica, sentito l'organo con funzione di controllo;
- i responsabili della funzione di controllo dei rischi (c.d. *Chief Risk Officer*) e della funzione di conformità alle norme devono essere posti, almeno, alle dipendenze dell'organo con funzione di gestione, ferma restando la loro prerogativa di avere accesso diretto all'organo con funzione di supervisione strategica e all'organo con

funzione di controllo. Il responsabile della funzione di revisione interna deve, invece, risultare collocato a riporto gerarchico dell'organo con funzione di supervisione strategica;

- le tre funzioni aziendali di controllo devono essere indipendenti dalle aree di *business* e fra loro separate. Se coerente con il principio di proporzionalità, si consente alle banche di istituire un'unica funzione di conformità alle norme e di controllo dei rischi, ferma restando l'esigenza di mantenere in ogni caso separata la funzione di revisione interna per assicurare l'imparzialità dei controlli di *audit* sulle altre funzioni di controllo;
- i poteri della funzione di *risk management* risultano rafforzati. La funzione, oltre a collaborare alla definizione del RAF, è chiamata, tra l'altro, a fornire pareri preventivi sulla coerenza delle operazioni di maggiore rilievo con il RAF stesso. In caso di parere negativo, la decisione sull'operazione è rimessa all'organo con funzione di gestione;
- nell'ambito della disciplina sulla conformità alle norme – fermo restando che il presidio sul rischio di non conformità svolto dalla funzione di *compliance* si riferisce a tutte le disposizioni applicabili alle banche, ***incluse quelle di natura fiscale*** – il coinvolgimento della funzione è graduato in relazione sia al rilievo che le singole norme hanno per l'attività svolta e per le conseguenze della loro violazione sia all'esistenza all'interno della banca di altre forme di presidio specializzato a fronte del rischio di non conformità relativo a specifiche normative.

3. Autovalutazione e *gap analysis*

Come accennato, le banche devono provvedere ad effettuare entro il **31 dicembre 2013** una

autovalutazione della situazione aziendale rispetto alle previsioni della nuova normativa (*gap analysis*). In tale ambito devono essere inoltre individuate le misure da adottare per assicurarne il rispetto.

Entro la medesima data, le banche sono inoltre tenute a comunicare alla Banca d'Italia i contratti di esternalizzazione in essere alla data di entrata in vigore del provvedimento, indicando la relativa durata.

4. Tempistica degli adempimenti

In linea generale, le banche sono tenute a conformarsi entro il **1 luglio 2014** al dettato delle nuove disposizioni. Tuttavia, in considerazione della complessità ed articolazione della materia l'Autorità di Vigilanza ha previsto un regime più graduale in relazione a taluni specifici ambiti di intervento.

Conseguentemente, la tempistica è la seguente:

Area di intervento	Termine per la conformità
Sistemi dei controlli interni (ad eccezione delle aree evidenziate di seguito)	1 luglio 2014
Disposizioni in materia di continuità operativa	1 luglio 2014
Disposizioni in materia di sistema informativo	1 febbraio 2015
disposizioni sulle funzioni aziendali di controllo di secondo livello	1 luglio 2015
Adeguamento dei contratti di esternalizzazione delle funzioni aziendali	Entro la prima scadenza contrattuale e comunque entro il 1 luglio 2016
Adeguamento dei contratti di esternalizzazione del sistema informativo	Entro la prima scadenza contrattuale e comunque entro il

	1 luglio 2016
--	---------------

5. La nuova disciplina in materia di esternalizzazioni

Tra gli elementi di novità della normativa in commento, si segnala l'introduzione di una disciplina organica in materia di esternalizzazione (*outsourcing*).

Al riguardo, l'Autorità di Vigilanza prescrive che le banche siano tenute a presidiare attentamente i rischi derivanti dall'esternalizzazione, mantenendo la capacità di controllo e la responsabilità delle attività esternalizzate nonché le competenze essenziali per re-internalizzare le stesse in caso di necessità. Disposizioni specifiche riguardano le condizioni per esternalizzare funzioni aziendali importanti o di controllo.

Requisiti meno stringenti sono invece previsti nel caso di esternalizzazione all'interno di un gruppo bancario.

Le banche che ricorrono all'esternalizzazione di funzioni aziendali devono presidiare adeguatamente i rischi derivanti dalle scelte effettuate e sono tenute a mantenere la capacità di controllo e la responsabilità sulle attività esternalizzate nonché le competenze tecniche e gestionali essenziali per re-internalizzare, in caso di necessità, il loro svolgimento.

La decisione di ricorrere all'*outsourcing* per lo svolgimento di determinate funzioni aziendali (anche non rilevanti) deve inoltre risultare coerente con la politica aziendale di tempo in tempo adottata in materia di esternalizzazione.

In coerenza con il principio di proporzionalità, tale politica deve stabilire:

- il processo decisionale per esternalizzare funzioni aziendali (livelli decisionali; funzioni coinvolte; valutazione dei rischi, inclusi quelli connessi con potenziali conflitti di interesse del fornitore di servizi, e l'impatto sulle funzioni aziendali; valutazione dell'impatto in termini di continuità operativa; criteri per la scelta e la *due diligence* del fornitore);

- il contenuto minimo dei contratti di *outsourcing* e i livelli di servizio attesi delle attività esternalizzate;
- le modalità di controllo, nel continuo e con il coinvolgimento della funzione di revisione interna, delle funzioni esternalizzate;
- i flussi informativi interni volti ad assicurare agli organi aziendali e alle funzioni aziendali di controllo la piena conoscenza e governabilità dei fattori di rischio relativi alle funzioni esternalizzate;
- i piani di continuità operativa (clausole contrattuali, piani operativi, ecc.) in caso di non corretto svolgimento delle funzioni esternalizzate da parte del fornitore di servizi.

Le disposizioni di vigilanza contemplano altresì dei limiti. In particolare, **la banca**, attraverso il ricorso all'esternalizzazione, **non può**:

- delegare le proprie responsabilità, né la responsabilità degli organi aziendali. In linea con questo principio, a titolo esemplificativo, non è ammessa l'esternalizzazione di attività che rientrano tra i compiti degli organi aziendali o che riguardano aspetti nevralgici del processo di erogazione del credito (ad es., il processo di valutazione del merito di credito e di monitoraggio delle relazioni creditizie); l'esternalizzazione delle funzioni aziendali di controllo è consentita entro particolari limiti e nel rispetto di determinate condizioni;
- alterare il rapporto e gli obblighi nei confronti dei suoi clienti;
- mettere a repentaglio la propria capacità di rispettare gli obblighi previsti dalla disciplina di vigilanza né mettersi in condizione di violare le riserve di attività previste dalla legge;
- pregiudicare la qualità del sistema dei controlli interni;
- ostacolare l'attività ed i compiti di vigilanza.

6. Adeguamento della contrattualistica

Ferma restando l'esigenza di assicurare, per ogni tipologia di esternalizzazione, il corretto

svolgimento della stessa da parte del fornitore, il buon funzionamento del sistema dei controlli interni e il monitoraggio continuo dell'attività svolta dal fornitore di servizi, nel caso in cui intendano esternalizzare funzioni operative importanti le banche devono assicurare che la contrattualistica soddisfi le seguenti condizioni:

- nel contratto (da perfezionarsi per iscritto) tra la banca e il fornitore di servizi sono formalizzati e chiaramente definiti:
 - a) i rispettivi diritti e obblighi; i livelli di servizio attesi, espressi in termini oggettivi e misurabili, nonché le informazioni necessarie per la verifica del loro rispetto; gli eventuali conflitti di interesse e le opportune cautele per prevenirli o, se non possibile, attenuarli; le condizioni al verificarsi delle quali possono essere apportate modifiche all'accordo; la durata dell'accordo e le modalità di rinnovo nonché gli impegni reciproci connessi con l'interruzione del rapporto;
 - b) i livelli di servizio assicurati in caso di emergenza e le soluzioni di continuità compatibili con le esigenze aziendali e coerenti con le prescrizioni dell'Autorità di vigilanza. Sono altresì stabilite le modalità di partecipazione, diretta o per il tramite di comitati utente, alle verifiche dei piani di continuità operativa dei fornitori.

Devono inoltre essere previste **clausole risolutive espresse** che consentano alla banca di porre termine all'accordo di esternalizzazione in presenza di eventi che possano compromettere la capacità del fornitore di garantire il servizio oppure quando si verifichi il mancato rispetto del livello di servizio concordato;

- il fornitore di servizi:
 - a) deve disporre della competenza, della capacità e delle autorizzazioni richieste dalla legge per esercitare, in maniera professionale e affidabile, le funzioni esternalizzate;
 - b) deve informare la banca di qualsiasi evento che idoneo ad incidere sulla sua capacità

di svolgere le funzioni esternalizzate in maniera efficace e in conformità con la normativa vigente; in particolare, comunicando tempestivamente il verificarsi di incidenti di sicurezza, anche al fine di consentire la pronta attivazione delle relative procedure di gestione o di emergenza;

c) deve garantire la sicurezza delle informazioni relative all'attività della banca, sotto l'aspetto della disponibilità, integrità e riservatezza; ***in quest'ambito, è tenuto ad assicurare il rispetto delle norme sulla protezione dei dati personali.***

- la banca deve:
 - a) conservare la competenza richiesta per controllare efficacemente le funzioni esternalizzate e per gestire i rischi connessi con l'esternalizzazione, inclusi quelli derivanti da potenziali conflitti di interessi del fornitore di servizi; in tale ambito, la banca è tenuta ad individuare, all'interno della propria organizzazione, un responsabile del controllo delle singole funzioni esternalizzate dotato di adeguati requisiti di professionalità (“referente per le attività esternalizzate”);
 - b) acquisire i piani di continuità operativa del fornitore di servizi o dispone di informazioni adeguate, al fine di valutare la qualità delle misure previste e di integrarle con le soluzioni di continuità realizzate all'interno;
- la banca, i suoi soggetti incaricati della revisione legale dei conti e le Autorità di vigilanza devono avere effettivo accesso ai dati relativi alle attività esternalizzate e ai locali in cui opera il fornitore di servizi. ***Il diritto di accesso per l'Autorità di vigilanza deve risultare espressamente nel contratto, senza oneri aggiuntivi per l'intermediario,***
- la sub-esternalizzazione (ovverosia la possibilità del fornitore di esternalizzare a sua volta una parte delle attività oggetto del contratto di esternalizzazione) non deve mettere a repentaglio il rispetto dei principi e delle

condizioni per l'esternalizzazione previste nella presente disciplina; a tal fine, il contratto con il fornitore di servizi prevede che eventuali rapporti di sub-esternalizzazione siano preventivamente concordati con la banca e siano definiti in modo da consentire il pieno rispetto di tutte le condizioni sopra elencate relative al contratto primario, inclusa la possibilità per l'Autorità di vigilanza di avere accesso ai dati relativi alle attività esternalizzate e ai locali in cui opera il sub-fornitore di servizi.

7. Obblighi di segnalazione e comunicazioni alla Banca d'Italia in materia di esternalizzazioni

Le banche che intendono esternalizzare, in tutto o in parte, lo svolgimento di funzioni operative importanti o di controllo ne danno comunicazione preventiva alla Banca d'Italia. La comunicazione, corredata di tutte le indicazioni utili a verificare il rispetto dei criteri indicati nella presente Sezione, è effettuata almeno 60 giorni prima di conferire l'incarico e specifica le esigenze aziendali che hanno determinato la scelta. Entro 60 giorni dal ricevimento della comunicazione la Banca d'Italia può avviare un procedimento amministrativo d'ufficio di divieto dell'esternalizzazione che si conclude entro 60 giorni.

Entro il **30 aprile** di ogni anno le banche trasmettono alla Banca d'Italia una relazione, redatta dalla funzione di revisione interna - o, se esternalizzata, dal referente aziendale - con le considerazioni dell'organo con funzione di controllo e approvata dall'organo con funzione di supervisione strategica, relativa ai controlli svolti sulle funzioni operative importanti o di controllo esternalizzate, alle carenze eventualmente riscontrate e alle conseguenti azioni correttive adottate.

8. Le implicazioni per l'operatività bancaria

Destinatari del provvedimento sono sia le banche italiane che le succursali di banche estere.

Sotto il profilo oggettivo, le disposizioni in commento sono destinate ad influenzare operativamente diverse funzioni e processi aziendali, comportando un significativo impegno da parte degli intermediari al fine di verificare prima, ed adeguare tempestivamente *governance* e contrattualistica alle prescrizioni recentemente introdotte.

* * *

In considerazione della complessità e novità delle nuove disposizioni di vigilanza prudenziale, CBA Studio Legale e Tributario ha costituito uno specifico gruppo di lavoro ed è a disposizione per fornire gli opportuni chiarimenti e approfondimenti e prestare la necessaria consulenza ed assistenza in materia di *governance* e contrattualistica.

L'occasione è gradita per porgere i più cordiali saluti.

Avv. Marco Cerritelli, LLM

Avv. Gerolamo Pellicanò

Contatti

Per ulteriori informazioni, Vi invitiamo a contattare:

Avv. Marco Cerritelli, LLM
Partner
Tel +39 06 89262900
marco.cerritelli@cbalex.com

Avv. Gerolamo Pellicanò
Of Counsel
Tel +39 02 778061
gerolamo.pellicano@cbalex.com

CBA Studio Legale e Tributario

20122 MILANO

Galleria San Carlo, 6
Tel. +39 02 778061
Fax +39 02 76021816

00196 ROMA

Via Flaminia, 135
Tel. +39 06 89262900
Fax +39 06 89262921

35137 PADOVA

Galleria dei Borromeo, 3
Tel. +39 049 0979500
Fax +39 049 0979521

30174 VENEZIA

Santa Croce, 251 - Palazzo Condulmer
Tel. +39 041 2440266
Fax +39 041 2448469

80539 MÜNCHEN

Ludwigstraße 10
Tel. +49 (0) 89 99016090
Fax +49 (0) 89 990160999

Disclaimer

Le informazioni contenute nel presente documento hanno carattere generale e non sono da considerarsi un esame esaustivo né intendono esprimere un parere o fornire una consulenza di natura legale-tributaria e non prescindono dalla necessità di ottenere pareri specifici con riguardo alle singole fattispecie descritte. Di conseguenza, il presente documento non costituisce un (né può essere altrimenti interpretato quale) parere legale, né può in alcun modo considerarsi come sostitutivo di una consulenza legale specifica.