Circolare n. 263 del 27 dicembre 2006 (Fascicolo «Nuove disposizioni di vigilanza prudenziale per le banche») - 15° aggiornamento del 2 luglio 2013 ([1])

Con il presente aggiornamento sono inseriti nel Titolo V della Circolare n. 263 del 27 dicembre 2006 "Nuove disposizioni di vigilanza prudenziale per le banche" il Capitolo 7 "Il sistema dei controlli interni", il Capitolo 8 "Il sistema informativo" e il Capitolo 9 "La continuità operativa".

Il Capitolo 7 definisce un quadro organico di principi e regole cui deve essere ispirato il sistema dei controlli interni, senza tuttavia esaurire le disposizioni organizzative applicabili alle banche. Le disposizioni ivi contenute, infatti, rappresentano la cornice di riferimento nella quale si inquadrano le regole sui controlli dettate all'interno di specifici ambiti disciplinari (ad es., 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) (c.d. modello "*hub and spokes*").

Le disposizioni introducono alcune novità di rilievo rispetto al vigente quadro normativo, al fine di dotare le banche di 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*; 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 avere 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 porre particolare attenzione alla 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.

La disciplina delle funzioni aziendali di controllo (*internal audit*, *compliance* e *risk management*) è stata profondamente rivisitata; in particolare:

— la nomina e la revoca dei responsabili delle funzioni aziendali di controllo sono di 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 sono 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 è, invece, sempre collocato a riporto gerarchico dell'organo con funzione di supervisione strategica;

— le tre funzioni aziendali di controllo sono indipendenti dalle aree di *business* e fra loro separate. Se coerente con il principio di proporzionalità, è consentito alle banche di

(1) Il testo dell'aggiornamento è disponibile sul sito informatico della Banca d'Italia all'indirizzo http://www.bancaditalia.it/vigilanza/banche/normativa/disposizioni/vigprud.

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* sono stati 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.

Per assicurare il coordinamento e l'interazione tra le varie funzioni e organi con compiti di controllo (previsti dalla normativa societaria, contabile o di vigilanza), l'organo con funzione di supervisione strategica approva uno specifico documento in cui sono precisati compiti, responsabilità e modalità di coordinamento/collaborazione tra le varie funzioni di controllo coinvolte.

È stata, poi, introdotta una disciplina organica in materia di esternalizzazione. Le banche sono 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. Due specifici procedimenti amministrativi sono stati definiti per il divieto dell'esternalizzazione di funzioni operative importanti o di controllo, rispettivamente, al di fuori o all'interno del gruppo bancario (cfr. Sezioni IV e V); tali procedimenti integrano il Provvedimento del 25 giugno 2008, in materia di individuazione dei termini e delle unità organizzative responsabili dei procedimenti amministrativi di competenza della Banca d'Italia.

Il Capitolo 8 contiene la disciplina del sistema informativo che è stata integralmente rivista, anche per recepire le principali evoluzioni emerse nel panorama internazionale. Sono stati, tra l'altro, disciplinati: la *governance* e l'organizzazione del sistema informativo; la gestione del rischio informatico; i requisiti per assicurare la sicurezza informatica e il sistema di gestione dei dati. Le disposizioni, inoltre, prevedono che nella definizione dei presidi di sicurezza per l'accesso a sistemi e servizi critici tramite il canale internet trovino applicazione le Raccomandazioni della BCE in materia di sicurezza dei pagamenti in internet.

Il Capitolo 9 disciplina la materia della continuità operativa, riorganizzando le disposizioni 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. Inoltre, è stato definito un processo di rapida escalation da incidente a emergenza in modo da assicurare che la dichiarazione dello stato di crisi avvenga nel minor tempo possibile dalla rilevazione dell'incidente. Il tempo complessivo di ripristino non dovrà superare le quattro ore, inclusi i tempi per le fasi di analisi, decisionali, intervento tecnico e verifica.

Le presenti disposizioni sono state sottoposte a consultazione pubblica e ad analisi di impatto della regolamentazione. Nel sito internet della Banca d'Italia sono pubblicati il resoconto della consultazione, la relazione sull'analisi di impatto e le osservazioni pervenute nella fase di consultazione.

Il presente aggiornamento entra in vigore il giorno di pubblicazione sul sito internet della Banca d'Italia.

Le banche si conformano alle disposizioni contenute nel Capitolo 7 (*Il sistema dei controlli interni*) entro il 1° luglio 2014 (data di efficacia), fatto salvo quanto segue:

— con riferimento alle funzioni aziendali di controllo di secondo livello (*risk management* e *compliance*), le banche si conformano entro il 1° luglio 2015 (data di efficacia) a quanto previsto dalla Sezione III, par. 1, lett. b), secondo alinea, secondo periodo ("linee di riporto dei responsabili di tali funzioni");

— con riferimento all'esternalizzazione di funzioni aziendali (Sezioni IV e V), le banche adeguano i contratti di esternalizzazione in essere alla data di entrata in vigore delle presenti disposizioni alla prima scadenza contrattuale e comunque entro tre anni dall'entrata in vigore (1° luglio 2016).

Le banche si conformano alle disposizioni contenute nel Capitolo 8 (*Il sistema informativo*), incluse le raccomandazioni della BCE in materia di sicurezza dei pagamenti in internet, entro il 1° febbraio 2015 (data di efficacia). Le banche adeguano i contratti di esternalizzazione del sistema informativo (Sezione VI) in essere alla data di entrata in vigore delle presenti disposizioni alla prima scadenza contrattuale e comunque entro tre anni dall'entrata in vigore (1° luglio 2016).

Le banche si conformano alle disposizioni contenute nel Capitolo 9 (*La continuità operativa*) entro il 1° luglio 2014 (data di efficacia).

Entro il 31 dicembre 2013 i destinatari della presente disciplina inviano alla Banca d'Italia una relazione recante un'autovalutazione della propria situazione aziendale rispetto alle previsioni della nuova normativa (*gap analysis*). La relazione indica altresì le misure da adottare e la relativa scansione temporale per assicurare il pieno rispetto delle presenti disposizioni. Entro la stessa data, le banche comunicano alla Banca d'Italia i contratti di esternalizzazione in essere alla data di entrata in vigore delle presenti disposizioni e la relativa durata.

Dalla data di efficacia delle norme contenute nei Capitoli 7 (Il sistema dei controlli interni), 8 (Il sistema informativo) e 9 (La continuità operativa) sono abrogate le seguenti disposizioni:

— *Sistema dei controlli interni, compiti del collegio sindacale*, contenute nelle "Istruzioni di vigilanza per le banche", Circolare n. 229 del 21 aprile 1999, Titolo IV, Capitolo 11, ad eccezione della Sezione V (Emissione e gestione di assegni bancari e postali);

— *Continuità operativa in casi di emergenza* (Comunicazione del luglio 2004, cfr. Bollettino di vigilanza n. 7 – luglio 2004);

— *La gestione e il controllo dei rischi. Ruolo degli organi aziendali*, contenute nelle "Nuove disposizioni di vigilanza prudenziale per le banche", Circolare n. 263 del 27 dicembre 2006, Titolo I, Capitolo I, Parte Quarta;

— *Disposizioni di vigilanza – Requisiti particolari per la continuità operativa dei processi a rilevanza sistemica* (Comunicazione del marzo 2007, cfr. Bollettino di vigilanza n. 3 – marzo 2007);

— *Disposizioni di vigilanza – Esternalizzazione del trattamento del contante* (Comunicazione del 7 maggio 2007), limitatamente agli aspetti concernenti le banche e le capogruppo di gruppi bancari;

— *Disposizioni di vigilanza - la funzione di conformità* (compliance) (Comunicazione del luglio 2007, cfr. Bollettino di vigilanza n. 7 – luglio 2007);

— *Comunicazione del 30 dicembre 2008 – Valutazione del merito di credito* (cfr. Bollettino di vigilanza n. 12 – dicembre 2008), limitatamente agli aspetti concernenti le banche e le capogruppo di gruppi bancari.