Le nuove disposizioni di Vigilanza sul sistema dei controlli interni, sul sistema informativo e sulla continuità operativa

The road to compliance: the new regulation on Internal controls system in Italy

Le nuove disposizioni di Vigilanza in materia di sistema dei controlli interni, sistema informativo e continuità operativa non sono da considerarsi solo come reazione da parte del regulator alla crisi finanziaria. Esse sono rivolte a dare concretezza al principio di sana e prudente gestione declinandolo in una serie di azioni, impostazioni, presidi organizzativi, procedure che la banca deve adottare.

Rupert N. Limentani,
Normanna Tresoldi
Limentani & Partners

The recent Bank of Italy regulations will deeply change the framework of internal controls system for banking intermediaries in Italy.

1 Premessa

È fuori discussione che le nuove disposizioni di Vigilanza[1] siano state pubblicate in un momento senza precedenti per il sistema bancario: con il protrarsi della crisi, si sono moltiplicate le problematiche che le banche devono fronteggiare quotidianamente e con esse le pressioni contrastanti e contraddittorie alle quali sono sottoposte. Basti pensare alla difficoltà di riconciliare l'esigenza di aumentare la raccolta in un periodo in cui la clientela vede diminuire la possibilità di risparmio, mantenendo nel contempo lo sbilancio interessi a un livello accettabile; oppure alla crescente difficoltà di erogare il credito quando l'aumentata rischiosità dei clienti impone accantonamenti sempre più massicci, e ancora come mantenere posizioni di adeguata patrimonializzazione e di buona redditività con bassa rischiosità, oppure come coniugare liquidità e redditività. Mai come oggi i vertici delle banche si trovano a dover navigare un percorso accidentato fra una serie di possibili rischi in agguato, che minacciano la stabilità non solo dei singoli istituti ma di tutto il sistema.

Non sorprende neppure che la reazione immediata di tutti i regulator dei sistemi finanziari mondiali alla crisi sia stata di rendere molto più stringenti le azioni di supervisione e di verifica sull'intero sistema. Nell'Unione europea e in Italia in particolare molte norme sono state rafforzate, sono state imposte maggiori limitazioni sull'operatività e maggiori obblighi di natura patrimoniale e di liquidità, sono stati rafforzati i controlli e si è insistito molto sulla trasparenza. Inoltre, l'azione ispettiva è stata notevolmente potenziata negli ultimi anni sia con una maggiore frequenza delle ispezioni generali sia con una serie di ispezioni mirate su temi specifici quali crediti, antiriciclaggio, compliance. Si può quindi parlare di un'azione «a tutto tondo» che parte da una revisione fondamentale della normativa sino a comprendere il monitoraggio degli intermediari e le verifiche sui loro comportamenti.

Ma la domanda che viene spontanea è la seguente: le nuove normative sarebbero state necessarie se non si fosse verificata la crisi finanziaria degli ultimi anni? Posto in altri termini, le misure sul sistema dei controlli interni, sul sistema informativo e sulla continuità operativa sono da interpretarsi come risposta della Vigilanza alla

Keywords: controlli interni, vigilanza, crisi finanziaria

Jel codes: G21, G28, G01

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

crisi dei sistemi finanziari oppure è ipotizzabile che le misure sarebbero state varate comunque, indipendentemente dagli eventi degli ultimi anni?

Per rispondere alla domanda occorre non solo prendere in esame le misure contenute nella nuova normativa, ma anche ripercorrere lo sviluppo della stessa negli anni della crisi per comprendere se vi sia un nesso causale fra gli eventi e le innovazioni normative intervenute nel periodo.

Il presente articolo si pone quindi l'obiettivo di contestualizzare le nuove disposizioni di Vigilanza nel momento topico in cui sono state emanate e di svolgere alcune considerazioni sulle tematiche dell'evoluzione della normativa riguardante i controlli interni, i sistemi informativi e la continuità operativa.

La crisi finanziaria si è manifestata dopo un periodo in cui i sistemi bancari dell'intero mondo occidentale avevano subìto uno sviluppo senza precedenti. Questo sviluppo ha riguardato una serie di aspetti molto diversificati, quali:
- la sempre maggiore disintermediazione delle banche che si trovano a operare in settori sempre più distanti da quelli tradizionali dell'intermediazione di denaro; in particolare lo sviluppo delle attività di investment banking, soprattutto negli Stati Uniti e paesi anglosassoni, con conseguente crescita esponenziale di nuove tipologie di rischio;
- una crescente interdipendenza dei sistemi finanziari a livello globale con conseguenti rischi sistemici;
- una crescente dipendenza delle banche e di altri intermediari finanziari dal buon funzionamento dei sistemi informatici.

Per comprendere quanto sia cambiato velocemente il contesto esterno, basti mettere a confronto la situazione attuale con quella vigente alla fine degli anni Novanta: in quell'epoca la funzione Compliance non esisteva, se non nelle grandi investment bank statunitensi o tedesche; il Risk management non costituiva un settore a sé stante ma operava all'interno del controllo di gestione; l'Organismo di Vigilanza non esisteva, in quanto è stato istituito solo con il d.lgs. 231 del 2001.

Le risposte normative di questo periodo hanno riguardato i seguenti aspetti:

1 aspetti patrimoniali e di liquidità:
- la normativa Basilea 2 e successivamente Basilea 3, che impone alle banche di valutare più puntualmente un ampio ventaglio di tipologie di rischi, alla luce degli aspetti che si vanno delineando con l'evoluzione dell'Accordo;

2 aspetti di trasparenza e di correttezza sui mercati mobiliari:
- la direttiva MiFid – direttiva sui mercati degli strumenti finanziari – con i numerosi cambiamenti richiesti alle modalità operative tramite le quali le banche operano con la propria clientela;

3 aspetti organizzativi, che costituiscono uno degli aspetti normativi più percepiti dalle stesse banche:
- la normativa applicabile al settore bancario si estende non solo all'antiriciclaggio, alla trasparenza, alla responsabilità amministrativa ma considera la conformità dei processi di gestione e la qualità dei dati e delle informazioni di business come elementi fondamentali per l'applicazione dei modelli di valutazione del rischio di credito, del rischio operativo, del rischio legale, del rischio di conformità e del rischio reputazionale.

Infatti, una delle principali caratteristiche del settore finanziario è proprio il livello di regolamentazione, che risulta essere più elevato che in qualsiasi altro comparto del sistema economico, ed è finalizzato a preservare e tutelare la connotazione fiduciaria che lo contraddistingue.

Mentre è vero che i vincoli della regolamentazione devono essere controbilanciati con le tematiche competitive, strategiche e di mercato che gli operatori del settore affrontano quotidianamente, è altresì vero che le normative non sono intese esclusivamente come freno all'attività imprenditoriale delle banche, bensì a tutela della stabilità del sistema, elemento fondamentale per la sopravvivenza dell'intera categoria.

Non stupisce quindi che l'intervento normativo in esame si focalizzi sul terzo di questi aspetti: la parte organizzativa, che riguarda prevalentemente il settore dei controlli interni e quello dei servizi informatici.

La linea fondamentale dell'ultimo intervento che ha dato luce ai nuovi capitoli 7, 8 e 9 del titolo V della circolare

263 di Banca d'Italia[2] è quella dell'importanza fondamentale del controllo per garantire non solo la sana e prudente gestione ma anche per preservare il buon nome e la reputazione della banca e del sistema. È opportuno ricordare a questo punto i primi due paragrafi delle disposizioni di Vigilanza del 2007 che hanno istituito la funzione di Compliance[3]: «Il rispetto delle norme e la correttezza negli affari costituiscono elementi fondamentali nello svolgimento dell'attività bancaria, che per sua natura è fondata sulla fiducia. L'evoluzione dei mercati finanziari, in termini di innovazione dei prodotti, di trasferimento del rischio e di proiezione internazionale, rende più complessi l'identificazione e il controllo dei comportamenti che possono dar luogo a violazioni di norme, di standard operativi, di principi deontologici ed etici dell'attività di intermediazione. Nel mutato contesto è necessario, da un lato, promuovere una cultura aziendale improntata a principi di onestà, correttezza e rispetto non solo della lettera, ma anche dello spirito, delle norme; dall'altro, approntare specifici presidi organizzativi, volti ad assicurare il rigoroso rispetto delle prescrizioni normative e di autoregolamentazione».

Il paragrafo di apertura del nuovo capitolo 7 («Il Sistema dei Controlli Interni») del titolo V della citata circolare 263 riassume in parole semplici i motivi per i quali è stato emanato proprio ora un provvedimento di portata così ampia, che delinea come devono operare i controlli interni in banca: «Il sistema dei controlli interni è un elemento fondamentale del complessivo sistema di governo delle banche; esso assicura che l'attività aziendale sia in linea con le strategie e le politiche aziendali e sia improntata a canoni di sana e prudente gestione».

In queste poche righe si trovano tutti gli elementi che da tempo connotano gli interventi della Vigilanza e che chiaramente hanno ispirato anche la nuova normativa:
- il sistema dei controlli è «un elemento fondamentale del complessivo sistema di governo delle banche», pertanto deve interessare i vertici direttamente e nel continuo; costituisce uno degli elementi basilari della governance aziendale;
- il sistema dei controlli «assicura che l'attività aziendale sia in linea con le strategie e le politiche aziendali»; pertanto esso ha lo scopo di garantire che la banca riesca a tradurre in azioni, a tutti i livelli dell'azienda, ciò che viene deliberato dal vertice;
- il sistema dei controlli «assicura che l'attività aziendale [...] sia improntata a canoni di sana e prudente gestione», ribadendo quindi che le banche devono essere gestite in modo sano, nel pieno rispetto delle regole, e prudente, limitando il più possibile il livello di rischi assunti.

Il Testo unico bancario e il Testo unico della finanza attribuiscono alla Banca d'Italia il potere di regolamentare numerosi aspetti dell'attività degli intermediari bancari e finanziari, per assicurare stabilità, efficienza e competitività al sistema finanziario. All'interno del sistema di regole stabilite dalla Banca d'Italia, le banche devono adottare misure di tipo patrimoniale, organizzativo e gestionale per evitare eccessive esposizioni ai rischi e instaurare con il cliente una relazione basata su comportamenti corretti e trasparenti. È da molti anni che la Banca d'Italia sta progressivamente mettendo a punto l'impianto normativo sul complessivo sistema dei controlli, mettendo gli interventi in stretta correlazione con gli aspetti di governance societaria[4].

2 Risk management

Prendendo in esame i vari settori che compongono il complessivo sistema dei controlli interni è utile ripercorrere il loro sviluppo negli anni della crisi. Innanzitutto la funzione di Risk management: questa è stata «promossa» a funzione di controllo di secondo livello solo da pochi anni. In precedenza essa faceva parte tipicamente della funzione di controllo di gestione; in tale veste non disponeva della possibilità di riferire direttamente agli organi di vertice e i flussi informativi confluivano quasi esclusivamente nel Comitato Alm, se costituito.

La disciplina del Risk management ha avuto un'evoluzione molto rilevante con un'accelerazione forte proprio negli ultimi anni, nel periodo post-crisi. Da una visione prevalentemente «assicurativa» del rischio, che ha portato nel tempo a una ricerca di trasferimento del rischio verso l'esterno,

2 Circolare n. 263 del 27 dicembre 2006 e successivi aggiornamenti, «Nuove Disposizioni di Vigilanza Prudenziale per le Banche».
3 Disposizioni di Vigilanza del 10 luglio 2007, «La funzione di conformità (compliance)».

4 Al riguardo vedasi «Il sistema dei controlli interni nella governance bancaria», intervento del 6 giugno 2008 di Anna Maria Tarantola, all'epoca Direttore Centrale per la Vigilanza Creditizia e Finanziaria di Banca d'Italia, presso il Convegno Dexia Crediop *Il sistema dei controlli aziendali: alla ricerca di una governance*.

in primis verso il mondo delle assicurazioni, si è passati a una visione più «gestionale», che porta alla politica di trattare il rischio in modo più «attivo» valutando cosa sia opportuno trasferire, con strumenti derivati, e cosa invece è necessario trattenere e finanziare internamente, al fine di cogliere i vantaggi economici. Nell'evoluzione dell'approccio, si è assistito anche a un allargamento delle varie tipologie di rischio cui la banca è esposta. Tale evoluzione ha riguardato anche le competenze e le professionalità necessarie per assolvere al ruolo di Risk manager.

La crescente complessità dei rischi insiti nell'attività della banca, anche a causa della disintermediazione, rende più difficile il lavoro del Risk manager. Inoltre, la crescita in termini assoluti dei valori patrimoniali in gioco impone di avere la disponibilità di dati sui rischi in tempi sempre più brevi e con maggiore frequenza. Conseguentemente sono cresciuti i flussi informativi dal Risk management verso il CdA e non è insolito constatare che la tematica della posizione rischi sia presente come punto fisso all'ordine del giorno delle riunioni di Consiglio. Ai consiglieri stessi viene chiesta una maggiore dimestichezza in tutte le questioni che riguardano la gestione dei rischi. La nuova normativa impone loro di pianificare il rischio: infatti, uno dei punti cardine della normativa è di precisare il ruolo dell'organo con funzione di supervisione strategica nella definizione del Risk appetite framework.

Il Risk appetite framework – o Raf – rappresenta una novità importante in termini normativi. Anche se in numerosi istituti si era soliti definire *ex ante* il livello di rischio che il Consiglio potesse considerare accettabile, generalmente esprimendo il valore in termini di percentuale massima del patrimonio di vigilanza che la banca fosse stata disposta a perdere, imporre a tutte le banche di svolgere un'analisi del livello massimo di rischio accettabile rappresenta senz'altro un grosso passo avanti, in quanto obbliga il vertice non solo ad analizzare in modo particolareggiato i rischi attualmente in essere, ma anche a monitorarne l'andamento nel tempo e quindi a intensificare i flussi informativi fra Risk management e organi aziendali[5].

Nell'Allegato C viene esplicitato che vi deve essere «una stretta coerenza e un puntuale raccordo» fra il modello di business, il piano strategico, il Raf (e i parametri utilizzati per definirlo), il processo Icaap, i budget, l'organizzazione aziendale e il sistema dei controlli interni. La logica dello schema rimane quello di definire in anticipo i livelli di rischio considerati accettabili, monitorandone l'andamento nel tempo e fornendo al vertice aziendale e alle funzioni di controlli adeguati flussi informativi con la dovuta frequenza e tempestività.

3 Compliance

Nata negli anni Novanta dall'esigenza di evitare conflitti di interessi da parte di operatori in titoli che non dovevano operare anche per conto proprio, l'evoluzione della funzione di Compliance è stata costante. Essa deve garantire il presidio del rischio di conformità sull'intera attività della banca, indipendentemente dal fatto che si tratti o meno di normative puramente bancarie. Gli eventi della crisi finanziaria e gli effetti potenzialmente dirompenti del rischio reputazionale che si sono manifestati in alcuni paesi[6] hanno contribuito a focalizzare l'attenzione del legislatore sulla funzione di Compliance. Lo scopo ultimo della funzione rimane quello di evitare che un rischio di natura operativa si possa trasformare in rischio reputazionale e quindi possa instaurare una perdita di fiducia nella banca con conseguente crisi di liquidità[7].

La crescente rilevanza di questi rischi si accompagna a una serie di conseguenze. Al fine di ridurre i rischi, le banche sono chiamate a mettere in atto strategie volte ad ampliare i propri ricavi da commissioni per servizi, soprattutto quei servizi che non implicano rischi di natura finanziaria, oltre a difendere la propria quota di raccolta e impieghi (senza pregiudicarne la qualità) e nel contempo a preservare il margine di interesse, avendo cura che sul lato impieghi il margine copra il costo dei rischi effettivamente assunti. Inoltre, l'onere delle misure di prevenzione e presidio dei rischi è proporzionalmente più elevato nelle banche di piccola e media dimensione. Ciò crea uno scollamento in termini di minore redditività delle stesse, che rischia di accentuare la loro aggredibi-

5 R. Limentani, N.Tresoldi, *Compliance Handbook* 2, Bancaria Editrice, Roma, 2013.

6 Si ricorda, a tale proposito, il fallimento della banca britannica Northern Rock il 14 settembre 2007; la causa scatenante è stata la perdita di fiducia da parte dei clienti relativamente alla politica di funding della banca. La posizione di liquidità, già tesa, è stata resa insostenibile dalle richieste di molti clienti di ritirare i propri risparmi. Un altro esempio, sempre dal mondo anglosassone, riguarda il gruppo Royal Bank of Scotland, che nel giugno 2012 ha subìto un problema informatico che ha bloccato l'accesso dei clienti ai propri conti. Il problema è stato risolto solo dopo alcuni giorni e l'episodio ha contribuito a una diminuzione netta della raccolta diretta e indiretta della banca nei mesi successivi.

7 R. Limentani, N.Tresoldi, *Compliance Handbook* 2, Bancaria Editrice, Roma, 2013.

lità e di aumentare la probabilità che esse vengano assorbite da un grande gruppo nazionale o estero.

Altra area chiave nel complessivo sistema dei controlli è quella dell'antiriciclaggio[8], cresciuta anch'essa negli ultimi anni man mano che cresceva la consapevolezza a livello nazionale e internazionale che l'adempimento alla normativa antiriciclaggio non poteva essere considerata un freno all'attività bancaria, bensì un investimento e garanzia per la stabilità futura del contesto in cui operano tutte le banche. Va da sé che un investimento che possa aiutare la banca ad avere un portafoglio clienti «pulito», non inquinato né dal rischio di riciclaggio né da altre attività illecite, fornisce alla banca un vantaggio nel far aumentare in modo sano il proprio business: occorre sempre avere presente che la raccolta «pulita» è quella più stabile e i rapporti con clienti onesti sono quelli più duraturi in assoluto. La stabilità finanziaria della banca e la capacità di generare utili in modo duraturo dipendono in buona misura dalla capacità di discernere e di prevenire i fenomeni di allarme nel comportamento della clientela.

Tale politica è ancora più importante alla luce della necessità di tutelare l'immagine della banca; infatti sarebbe molto elevato il danno che ne deriverebbe, con conseguente rischio reputazionale, nel caso in cui venisse reso pubblico che una banca non si è adoperata con sufficiente impegno nella lotta al riciclaggio. La salute del sistema bancario dipende dalla capacità delle singole banche di mantenere intatta la fiducia incondizionata della propria clientela. La lotta al riciclaggio è un attività che va a beneficio di tutti: banche, clienti e collettività.

4 Internal audit

Fra le funzioni di controllo quella di Internal audit è certamente quella maggiormente conosciuta sia all'interno sia all'esterno delle banche, in quanto trattasi della funzione che è attiva da più anni.

Il provvedimento del 2 luglio 2013 esplicita chiaramente le funzioni dell'Internal audit, o revisione interna, nelle banche[9]: «La funzione di revisione interna è volta, da un lato, a controllare, in un'ottica di controlli di terzo livello, anche con verifiche in loco, il regolare andamento dell'operatività e l'evoluzione dei rischi, e, dall'altro, a valutare la completezza, l'adeguatezza, la funzionalità e l'affidabilità della struttura organizzativa e delle altre componenti del sistema dei controlli interni, portando all'attenzione degli organi aziendali i possibili miglioramenti, con particolare riferimento al Raf, al processo di gestione dei rischi nonché agli strumenti di misurazione e controllo degli stessi. Sulla base dei risultati dei propri controlli formula raccomandazioni agli organi aziendali».

La funzione di Internal audit ha sempre avuto il compito di operare su tutte le attività della banca, senza limitazioni di nessun genere, con lo scopo di verificare e assicurare *in primis* il rispetto delle norme interne ed esterne. Il nuovo provvedimento rafforza il ruolo di monitoraggio dei processi e di rilevazione di carenze organizzative con la formulazione di pareri per allineare l'operatività della banca con le best practice diffuse nel settore.

A tal fine risultano fondamentali i rapporti e lo scambio di flussi informativi fra audit e le altre funzioni di controllo di secondo livello, in particolare la Compliance e il Risk management. Viceversa, nella propria attività core la funzione di Internal audit non conosce limiti o confini. Essa riporta direttamente al Consiglio e può agire nei confronti di qualsiasi altra funzione della banca, ivi comprese le funzioni date in outsourcing a provider esterni. Infatti, il nuovo provvedimento sottolinea l'importanza dell'interazione fra Internal audit e outsourcers; rivestono fondamentale importanza gli accertamenti dell'audit sull'affidabilità complessiva dei sistemi informativi (Ict audit).

5 Altre funzioni di controllo

Il provvedimento indica che compiti di controllo vengano attribuiti, oltre alle funzioni aziendali di controllo di secondo e di terzo livello, anche a specifiche funzioni o a comitati interni all'organo amministrativo, la cui attività va in-

8 Vedi «La funzione antiriciclaggio in banca: adempimento o investimento?», di R. Limentani, N. Tresoldi, in *Bancaria*, n. 5/2013.

9 Circolare n. 163 del 26 dicembre 2006, 15° aggiornamento, titolo V, capitolo 7, sezione III, paragrafo 3.4.

quadrata in modo coerente nel sistema dei controlli interni. Al riguardo il provvedimento cita in modo specifico la funzione dell'Organismo di Vigilanza eventualmente istituita[10] ex d.lgs. 231/2001 e il dirigente preposto alla redazione dei documenti contabili societari, nel caso di banche con azioni quotate.

Il coordinamento della pluralità di funzioni di controllo riveste importanza fondamentale, non solo per evitare sovrapposizioni nelle mansioni ma soprattutto per evitare che possano sussistere lacune o aree non coperte da nessuna delle funzioni di controllo. Il coordinamento di tali funzioni viene attribuito all'organo con funzione di supervisione strategica, che deve approvare un apposito documento con il quale vengono specificati compiti e responsabilità delle varie funzioni: «Per assicurare una corretta interazione tra tutte le funzioni e organi con compiti di controllo, evitando sovrapposizioni o lacune, l'organo con funzione di supervisione strategica approva un documento, diffuso a tutte le strutture interessate, nel quale sono definiti i compiti e le responsabilità dei vari organi e funzioni di controllo, i flussi informativi tra le diverse funzioni/organi e tra queste/i e gli organi aziendali e, nel caso in cui gli ambiti di controllo presentino aree di potenziale sovrapposizione o permettano di sviluppare sinergie, le modalità di coordinamento e di collaborazione».

Il documento non è certo sostitutivo dei regolamenti già esistenti delle varie funzioni stesse né tantomeno è sostitutivo del progetto di governo societario. Potrebbe essere considerato un documento che espliciti l'architettura del sistema dei controlli che metta in rilievo i punti di incontro fra le diverse funzioni e i flussi informativi che esse si scambiano.

6 Outsourcing

Oltre a fornire indicazioni sulle funzioni di controllo, il provvedimento dedica un'intera sezione al tema dell'outsourcing (sezione IV del capitolo 7), che si collega al successivo capitolo 8 («Il Sistema Informativo»). Oltre a ribadire i principi generali e i requisiti particolari per l'outsourcing, la sezione tratta in modo specifico l'esternalizzazione delle funzioni aziendali di controllo, le comunicazioni che le banche sono tenute a inviare alla Banca d'Italia qualora intendano esternalizzare in tutto o in parte funzioni operative importanti o di controllo; viene considerata in modo separato l'esternalizzazione del trattamento del contante, per la quale sussistono requisiti specifici.

In materia di esternalizzazione viene sottolineato non solo che le banche sono tenute a presidiare attentamente i rischi derivanti dall'esternalizzazione, mantenendo la capacità di controllo e la responsabilità delle attività esternalizzate, ma che esse devono mantenere le competenze essenziali per re-internalizzare le stesse in caso di necessità. Il provvedimento contiene disposizioni specifiche che riguardano:
- le condizioni per esternalizzare funzioni aziendali importanti o di controllo;
- l'esternalizzazione all'interno di un gruppo bancario;
- il divieto dell'esternalizzazione di funzioni operative importanti o di controllo, al di fuori del gruppo.

Il capitolo 8 e il capitolo 9 trattano, rispettivamente, il sistema informativo e la continuità operativa, entrambe tematiche strettamente correlate alla sezione 4 del precedente capitolo 7, Outsourcing. Oltre a disciplinare in modo più organico le regole di governo del sistema informatico, il provvedimento esplicita la procedura della gestione delle crisi operative con la formalizzazione del ruolo del Codise (Continuità di servizio della piazza finanziaria italiana), 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.

7 Principali innovazioni del provvedimento

Il capitolo 7 tratta il sistema dei controlli interni. In particolare, si enfatizza il ruolo dell'organo con funzione di supervisione strategica nella definizione del modello di business e del Risk Appetite Framework; a tale organo è richiesta anche l'approvazione di un codice etico.

All'organo con funzione di gestione è invece richiesto di

10 Il provvedimento precisa che «L'organo con funzione di controllo svolge, di norma, le funzioni dell'organismo di vigilanza – eventualmente istituito ai sensi del d.lgs. n. 231/2001, in materia di responsabilità amministrativa degli enti – che vigila sul funzionamento e l'osservanza dei modelli di organizzazione e di gestione di cui si dota la banca per prevenire i reati rilevanti ai fini del medesimo decreto legislativo».

avere un'approfondita comprensione di tutti i rischi aziendali e di porre attenzione alla definizione di politiche per:
- la gestione dei rischi;
- la valutazione delle attività aziendali;
- l'approvazione di nuovi prodotti/servizi;
- lo sviluppo dei modelli interni di misurazione dei rischi non utilizzati ai 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 (cosiddetti 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;
- la funzione di Risk management è chiamata a contribuire alla definizione del Raf, nonché a fornire pareri preventivi sulla coerenza delle operazioni di maggiore rilievo con il Raf stesso.
- 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, mentre 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.

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.

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;
- esternalizzazione all'interno di un gruppo bancario;
- divieto dell'esternalizzazione di funzioni operative importanti o di controllo, rispettivamente, al di fuori o all'interno del gruppo.

Il capitolo 8 contiene la disciplina del sistema informativo.

Sono stati disciplinati:
- la governance e l'organizzazione del sistema informativo;
- la gestione del rischio informatico;
- i requisiti per assicurare la sicurezza informatica
- il sistema di gestione dei dati.

Il capitolo 9 disciplina la materia della continuità operativa. Tra le novità di maggiore rilievo:
- la formalizzazione del ruolo del Codise;
- la definizione di 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.

Entro il 31 dicembre 2013 i destinatari della 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 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.

8 Conclusioni

Tornando alla domanda posta in apertura, ci si chiedeva se le nuove normative sarebbero state necessarie se non si fos-

se verificata la crisi finanziaria degli ultimi anni, se le misure sul sistema dei controlli interni, sul sistema informativo e sulla continuità operativa siano da interpretarsi come «risposta» della Vigilanza alla crisi dei sistemi finanziari, oppure se sarebbero state varate comunque, indipendentemente dagli eventi degli ultimi anni.

La risposta non può che essere una combinazione fra le due alternative: le misure sono senz'altro da considerare una risposta alla crisi finanziaria, poiché la crisi si è propagata in modo particolarmente severa grazie anche all'insufficienza, in molti casi, di adeguate procedure per riconoscere i rischi incombenti e per adottare tempestivamente adeguate misure per evitarli.

D'altra parte ciò non significa che le misure non sarebbero state necessarie se in questi anni la crisi non si fosse manifestata. Come precisato dal paragrafo di apertura del capitolo 7: «il sistema dei controlli interni è un elemento fondamentale del complessivo sistema di governo delle banche; esso assicura che l'attività aziendale sia in linea con le strategie e le politiche aziendali e sia improntata a canoni di sana e prudente gestione».

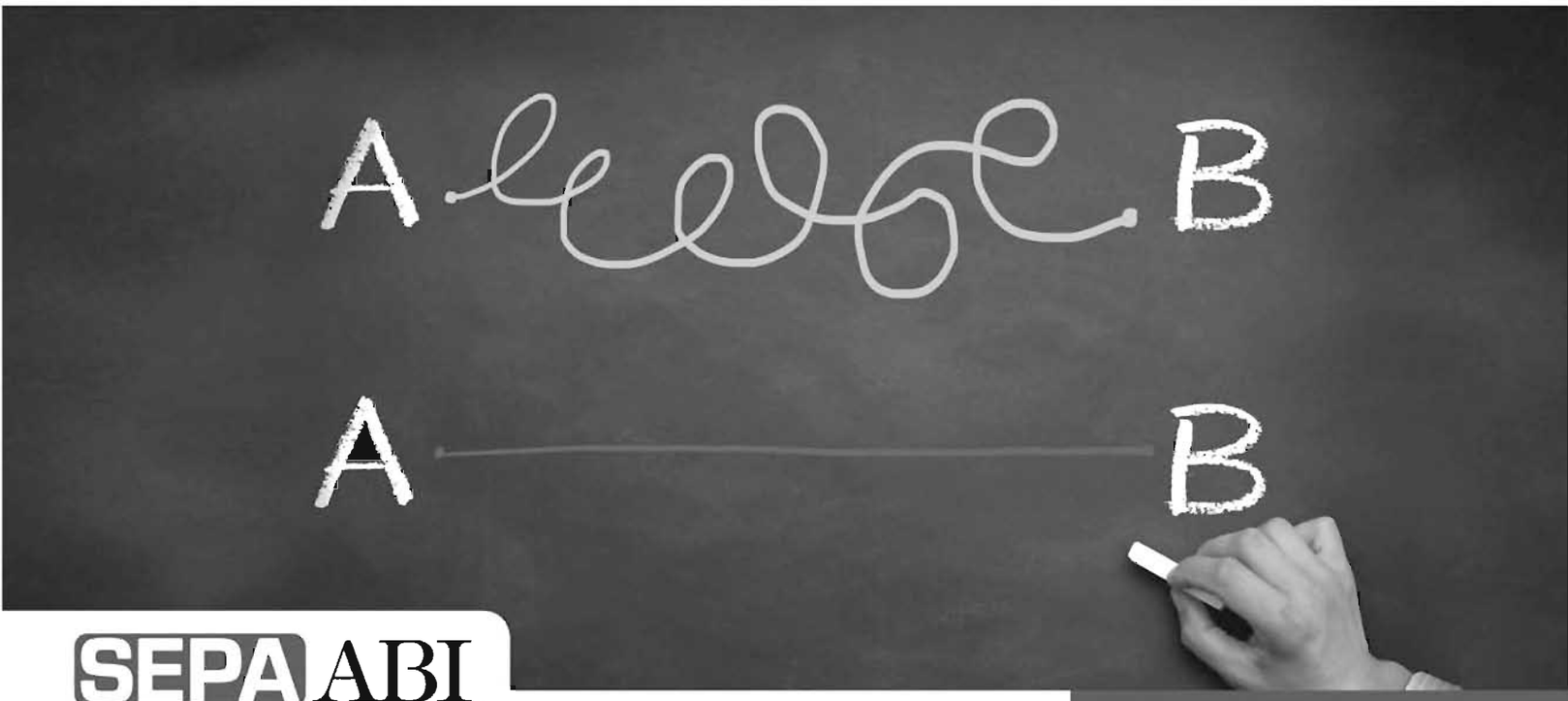
Con il provvedimento si concretizzano i canoni della sana e prudente gestione, onde evitare che questa rimanga un'espressione priva di significato operativo. Il provvedimento declina il principio di sana e prudente gestione in una serie di azioni, impostazioni, presidi organizzativi, procedure operative e flussi informativi che la banca deve adottare. Esso richiama tutti i livelli, a partire dagli Organi con funzione di supervisione strategica e di controllo, alle proprie responsabilità richiamando il principio che la stabilità del sistema finanziario costituisce un presupposto indispensabile per lo sviluppo economico dell'intero sistema produttivo.

Compliance Handbook. Nuova edizione 2014

La nuova edizione del volume, di R. Limentani e N. Tresoldi, appena pubblicato da Bancaria Editrice, *Compliance Handbook*, oltre a contenere tutti i principi dettati dalle recenti disposizioni normative sul sistema dei controlli, con particolare riferimento alla funzione di Compliance, delinea in modo puntuale i nuovi ambiti di attività della funzione, ivi compresa la materia fiscale, esemplificando in uno schema le tipologie di controllo da applicare. Propone una ridefinizione del modello, assegnando il presidio di materie non core a funzioni specialistiche già presenti nella banca e indica come ricondurre a unità tali presidi. Delinea inoltre i contenuti del documento sull'architettura dei controlli; precisa in modo tabellare, facilmente consultabile, l'informativa all'Organo di Vigilanza; illustra, a titolo esemplificativo, le verifiche effettuate dalle funzioni aziendali di controllo, ognuna per le parti di competenza, su uno dei processi più rilevanti della banca: il processo del credito. Il testo propone anche un modello di gap analysis, adatto per effettuare in ogni occasione che si renda necessaria una valutazione sulla funzione di Compliance e sulle altre funzioni di controllo, al fine di avere una visione complessiva dello stato delle stesse, onde adottare eventuali misure per l'adeguamento alle disposizioni normative e per il potenziamento del sistema dei controlli, qualora ciò si rendesse necessario.
La nuova edizione del *Compliance Handbook* ha previsto, inoltre, un nuovo capitolo dedicato ai controlli di Compliance sui servizi di investimento, che costituiscono una parte rilevante delle attività della funzione. Il manuale di Compliance per i dipendenti, contenuto in appendice, è stato rivisitato per poter essere integrato nel Codice Etico, richiamato nel recente Provvedimento Banca d'Italia del 2 luglio 2013.
Il testo contiene schemi e tabelle che lo rendono facilmente consultabile, adatto a un utilizzo quotidiano per l'espletamento dei compiti della funzione di Compliance, ma soprattutto indispensabile per tutto il personale della banca, non solo per la diffusione della cultura di conformità, ma anche per la comprensione delle tematiche relative al Sistema dei Controlli, conoscenza imprescindibile dal buon funzionamento della banca.

SEPA ABI

La via più facile per SEPA



SEPA ABI BLUEBOOK

Tutti i documenti SEPA ABI pubblicati nel 2014, raggruppati in fascicoli e già forati per una comoda archiviazione in pratici raccoglitori a fogli mobili

Tutti gli aggiornamenti normativi e i documenti prodotti da Commissione Europea, Banca Centrale Europea, European Payments Council e altre fonti specializzate

Traduzione italiana esclusiva di tutti i documenti

ABBONAMENTO **2014**

Associati ABI	€ 256
Non associati	€ 320

SEPA ABI **2007-2011**

Associati ABI	~~€ 1.280~~	€ 640
Non associati	~~€ 1.600~~	€ 800

SEPA ABI ONLINE

L'intera raccolta dei documenti SEPA ABI sempre disponibili e consultabili online

Accesso 24 ore su 24 con password personale

Un potente e veloce motore di ricerca

Aggiornamento in tempo reale con i nuovi documenti disponibili online immediatamente dopo l'emanazione

Servizio di e-mail alert

ABBONAMENTO **2014***

Associati ABI	€ 256
Non associati	€ 320

*Prezzi per singola postazione con password personale d'accesso.
IVA 22% esclusa.
Sconti quantità per postazioni multiple.

BANCARIA EDITRICE
LA CASA EDITRICE DELL'ABI

Per info: tel. **06.6767.395-568** • fax. 06.6767.250
e-mail: **sepa@bancariaeditrice.it**
www.bancariaeditrice.it