Associazione Nazionale fra le Banche Popolari

OSSERVAZIONI E COMMENTI SUL DOCUMENTO PER LA CONSULTAZIONE DELLA BANCA D'ITALIA

DISPOSIZIONI DI VIGILANZA PRUDENZIALE PER LE BANCHE SISTEMA DEI CONTROLLI INTERNI, SISTEMA INFORMATIVO E CONTINUITÀ OPERATIVA

Ottobre 2012

Introduzione

Il 4 settembre u.s. la Banca d'Italia ha diffuso per pubblica consultazione, con possibilità di fornire osservazioni, commenti e proposte, il documento "Disposizioni di vigilanza prudenziale per le banche - Sistema dei controlli interni, sistema informativo e continuità operativa", con cui l'Organo di Vigilanza intende riordinare il quadro normativo sulla materia.

Ciò si è reso necessario a seguito dell'emanazione di una lunga serie di disposizioni (di vigilanza, contabili, societarie, comprese tra l'altro quelle contenute nel Codice di Autodisciplina di Borsa italiana) che hanno interessato la strutturazione e l'organizzazione del Sistema dei Controlli Interni.

La nuova disciplina si propone di fare chiarezza nella ripartizione di ruoli e competenze tra i diversi presidi aziendali (organi sociali e strutture operative) deputati al governo, controllo e mitigazione dei rischi bancari, anche alla luce della prossima entrata in vigore (2013) della rinnovata normativa prudenziale sul capitale e sulla liquidità delle banche (Basilea 3).

L'Associazione Nazionale fra le Banche Popolari si è attivata al riguardo per coinvolgere le Associate con le seguenti finalità:

- approfondire e discutere congiuntamente il contenuto delle disposizioni riportate nel documento con l'obiettivo di tracciare indicazioni e linee guida dei possibili interventi operativi volti ad un'eventuale implementazione e/o riorganizzazione delle funzioni di controllo;
- formulare osservazioni e proposte sulla materia al fine di coordinare un testo comune da rendere all'Organo di Vigilanza in risposta alla richiesta di consultazione sul documento in parola.

Il presente elaborato, pertanto, pur esprimendo un lavoro di sintesi ascrivibile direttamente all'Associazione, è il frutto di un ampia consultazione cui ha contribuito la gran parte delle banche della Categoria. La trattazione si articola in valutazioni di ordine generale e valutazioni su temi specifici, concludendo con alcune osservazioni su aspetti di tipo operativo che interessano in particolare l'attività delle banche di piccole dimensioni.

Valutazioni di ordine generale

Il documento in consultazione definisce un quadro organico di principi e regole cui deve uniformarsi il Sistema dei Controlli Interni, che non mira, tuttavia, a ricomprendere ed esaurire le disposizioni sul tema. Non si tratta, infatti, di un "Testo Unico" volto a razionalizzare e, soprattutto, a semplificare l'intera materia, frutto dei tanti interventi regolamentari che si sono succeduti nel tempo; si tratta invece, in base a quanto enunciato nel documento stesso, di una "cornice normativa" entro cui si collocano gli

specifici ambiti disciplinari: la gestione dei singoli profili di rischio, le procedure per il calcolo dei requisiti patrimoniali, il processo ICAAP, la prevenzione del rischio di riciclaggio, ecc..

Di fatto però, in molte occasioni, le disposizioni poste dal documento integrano le normative vigenti e, se nella maggioranza dei casi tali indicazioni soddisfano la richiesta di chiarimenti riferite a precedenti indicazioni, accade anche che nuove prescrizioni si sovrappongano alle vecchie, generando nuove incertezze sulla corretta interpretazione delle norme e sulle soluzioni da adottare.

E' il caso, ad esempio, della ripartizione di ruoli tra gli organi aziendali nella nomina e revoca dei responsabili delle funzioni di controllo per cui non sussiste piena sintonia tra le disposizioni del documento in consultazione e le "Disposizioni sul Governo Societario" di marzo 2008. Anche il tema della sovrapposizione di competenze tra funzione compliance e revisione interna ravvisate nel Regolamento Congiunto tra Organo di Vigilanza e Consob sui servizi di investimento non trova le attese precisazioni nel documento in consultazione. Allo stesso modo, permangono aspetti controversi in materia di responsabilità amministrativa degli enti ex D.lgt. 231/01 per ciò che riguarda le modalità di integrazione e collocamento dell'Organismo di Vigilanza nel sistema complessivo dei controlli aziendali.

Si ravvisa, inoltre, un deciso ritorno a "norme di tipo prescrittivo" nella strutturazione e collocazione delle funzioni di controllo che supera di fatto il precedente approccio orientato verso una "normativa d'indirizzo" adottato dalla vigilanza per la regolamentazione prudenziale. Ciò, oltre a introdurre elementi di rigidità che rappresentano un ostacolo potenziale ad un corretto esercizio del principio di proporzionalità, non tiene conto delle soluzioni già leggittimamente adottate dagli intermediari, che in molti casi si vedranno costretti a riorganizzare uffici e strutture dovendone sostenere i relativi oneri.

Si vuole sottolineare, infine, l'impegno operativo e organizzativo richiesto dalle disposizioni in parola, in special modo, alle banche di piccola dimensione: è auspicabile che la giusta esigenza di garantire che tutti gli intermediari si dotino di presidi adeguati ed efficienti per il controllo e il contrasto dei rischi sia declinata con i livelli di rischio cui gli stessi intermediari sono effettivamente esposti, ovvero con i principi di proporzionalità ed economicità più volte richiamati dalla stessa normativa prudenziale, al fine di evitare incombenze economiche e organizzative eccessivamente gravose, e soprattutto ingiustificate, in particolare per le piccole banche.

Valutazioni su aspetti specifici

Il ruolo dell'organo di supervisione strategica *– Cap. 7, Sez. II, Par. 2*

Il documento in consultazione ribadisce che l'organo con funzione di supervisione strategica definisce il modello di business e assicura che l'intera struttura – compreso evidentemente il Sistema dei Controlli Interni - sia coerente con l'attività svolta e con il

modello di business adottato, evitando la creazione di strutture complesse non giustificate da finalità operative.

Ne deriva che "la discrezionalità" consentita alle aziende con minore complessità operativa di adottare soluzioni organizzative meno articolate e sistemi di controllo in qualche modo semplificati, che risultino comunque soddisfacenti nella "copertura" di tutti i rischi aziendali, debba anche essere interpretata, per converso, come un richiamo al contenimento di complessità e costi delle strutture, da commisurare in base alle caratteristiche e all'organizzazione di ogni istituto. Tra i principali parametri di valutazione alla base delle scelte di strutturazione del Sistema dei Controlli Interni è possibile elencare: dimensione e complessità operativa dell'intermediario; impiego complessivo di risorse e impegno logistico richiesto alla struttura aziendale; costi e tempi di implementazione; complesso di relazioni funzionali e soggettive che si vengono a determinare nella struttura organizzativa aziendale e segnatamente nel Sistema dei Controlli Interni. La quantità dei parametri di valutazione evidenzia la complessità delle scelte da realizzare e l'entità delle conseguenti responsabilità.

Il ruolo dell'organo con funzioni di gestione *– Cap. 7, Sez. II, Par. 3*

In tema di nomina e revoca dei responsabili delle funzioni di controllo, il documento in consultazione dispone che questi siano nominati (e revocati) dall'organo con funzione di gestione, previo accordo con l'organo con funzione di supervisione strategica, sentito l'organo con funzione di controllo. La disposizione non appare coerente con quanto previsto nell'ambito delle "Disposizioni sul Governo Societario" (Banca d'Italia – 04.03.2008) secondo cui "la nomina del responsabile delle Funzioni di revisione interna e di conformità rientra tra le attribuzioni non delegabili del C.d.A.".

Con riguardo all'organo con funzione di gestione, si segnala inoltre come a questo spetti, secondo il documento, di definire il processo connesso alla distribuzione di nuovi prodotti di investimento, mediante il quale dovranno essere definite le fasce di clientela a cui si intende praticare l'offerta, in base alla complessità dei prodotti stessi, alla loro rischiosità e ad eventuali vincoli normativi. Appare opportuno che tale previsione vada resa coerente con quanto previsto dalla vigente regolamentazione CONSOB in tema di obblighi di valutazione sull'adeguatezza da parte degli intermediari;

Il ruolo dell'organo con funzioni di controllo *– Cap. 7, Sez. II, Par. 4*

Un'importante novità introdotta con le disposizioni in parola riguarda l'attribuzione delle funzioni dell'Organo di Vigilanza, ai sensi della legge 231/2001, all'organo con funzioni di controllo. Si ribadisce che solo in caso di particolari e motivate esigenze, le banche potranno affidare tali funzioni a un organismo appositamente istituito. Tale indicazione ribalta, di fatto, un orientamento che sembrava affermarsi in tema di responsabilità amministrativa degli enti, per cui si ipotizzava che l'O.d.V. dovesse essere istituito come organismo autonomo nella gran parte delle banche italiane: soltanto per piccole realtà bancarie si sarebbero valutate soluzioni alternative di tipo semplificato.

Il nuovo orientamento chiarisce in modo prescrittivo la soluzione da adottare. Pone tuttavia un problema di opportunità riferito in particolare alle competenze degli attuali componenti degli organi con funzione di controllo: il Collegio Sindacale, infatti, nasce essenzialmente come organo di controllo contabile e amministrativo. Le sue responsabilità sono state già ampiamente estese nel campo della gestione e valutazione dei rischi.

Le nuove competenze richieste in tema di responsabilità amministrativa degli enti, dei reati presupposto e del funzionamento del modello di vigilanza, necessitano di approfondimenti specifici nonché di una preparazione tecnico giuridica non usuale per gli attuali componenti di un organo di controllo.

La funzione di conformità alle norme *– Cap. 7, Sez III, Par. 3.2*

Una novità di rilievo introdotta con il documento in consultazione è l'attribuzione alla funzione compliance della verifica di conformità dell'attività aziendale alle normative di natura fiscale per evitare di incorrere in violazioni o elusioni di tali norme. In questo caso il rischio legale è strettamente legato ad un conseguente danno reputazionale, in considerazione del rilievo negativo avvertito dalla collettività per questo genere di inadempienze.

Anche in questo caso sembra opportuno focalizzare l'attenzione sugli intermediari di piccola e media dimensione: normalmente in queste banche la materia fiscale è gestita dall'area amministrativa che spesso si avvale di professionisti (studi) esterni, con il controllo successivo del collegio sindacale e delle società di revisione. Dato il consolidato *modus operandi*, appare problematico ipotizzare un'agevole e immediata collocazione della funzione compliance sulla materia, in primo luogo per la mancanza di accertate competenze tecniche in tema di fiscalità.

Su tale argomento, come ricordato nel documento in consultazione, è all'esame presso il Parlamento un disegno di legge delega che contempla per i soggetti di grandi dimensioni la previsione di sistemi aziendali strutturati di gestione e controllo del rischio fiscale, con una chiara attribuzione di responsabilità nel quadro del complessivo sistema dei controlli interni. In relazione a ciò, per evitare il rischio che con la delega in corso di attuazione gli intermediari si trovino a dover adottare disposizioni non pienamente coerenti, si auspica di attendere il completamento, previsto in tempi brevi, del relativo processo attuativo.

Il documento, infine, non chiarisce se la responsabilità della funzione compliance si estenda anche a quelle fattispecie per cui la normativa vigente impone la presenza di specifiche figure aziendali che riportano alle strutture di vertice, come ad esempio la normativa in materia di sicurezza sul lavoro. In tali casi si presume che alla funzione di conformità sia affidata esclusivamente la verifica che le suddette figure aziendali siano state correttamente istituite e le relative funzioni siano rese pienamente operative

La funzione di controllo dei rischi *– Cap. 7, Sez III, Par. 3.3*

Il documento ribadisce che, per rafforzarne l'indipendenza, il responsabile della funzione di risk management può essere collocato alle dirette dipendenze del comitato controllo e rischi, se esiste, o dell'organo con funzioni di supervisione strategica. Il collocamento è obbligato per le banche di classe 1 e 2 a fini SREP.

Al riguardo si ritiene che debbano essere definite in dettaglio le modalità di partecipazione della funzione ad eventuali comitati di gestione dei diversi rischi aziendali, così come va evitato che l'istituzione di tali comitati possa depotenziare le prerogative della funzione stessa, come peraltro viene evidenziato nel documento in consultazione.

Il coinvolgimento del risk manager nei lavori del board o, se costituiti, dei comitati interni ad esso, non deve comunque pregiudicare la distinzione di ruoli e responsabilità: da un lato, la definizione di politiche e indirizzi nonché la verifica di adeguatezza su tutta la struttura dei presidi aziendali, dall'altro, la valutazione, il controllo e la gestione dei rischi della banca. Si ritiene pertanto che la partecipazione del responsabile della funzione di risk management ai lavori dei comitati di vertice debba essere necessariamente di natura tecnica e consultiva.

Si sottolinea, infine, che le soluzioni organizzative che prevedono la figura del Chief Risk Officer (CRO), inteso come figura di coordinamento della funzione di controllo rischi, funzione di conformità ed eventuali altre funzioni, richiedono ampie discrezionalità di azione, poiché il collocamento della figura sarà condizionato dalle specifiche connotazioni dell'intermediario in termini di governance, di complessità operativa nonché di configurazione della già esistente struttura di controllo.

Esternalizzazione di funzioni *– Cap. 7, Sez IV*

In tema di esternalizzazione delle funzioni di controllo si richiede di impostare in modo differenziato le previsioni contenute nella relativa sezione a seconda di esternalizzazioni infragruppo o esternalizzazione verso terzi. La raccomandazione appare debole e si auspica una più marcata differenziazione di trattamento tra accentramento (presso la capogruppo) ed esternalizzazione. Si tratta infatti di fattispecie del tutto eterogenee che devono essere opportunamente valorizzate anche con riferimento al principio di economicità e alla ricerca di soluzioni volte al contenimento delle strutture e degli impatti organizzativi.

Il sistema dei controlli nei gruppi *– Cap. 7, Sez V*

Con riferimento ai controlli interni di gruppo, si ritiene poco efficiente e scarsamente efficace l'obbligo di riporto sistematico a livello gerarchico da parte dei referenti delle unità periferiche. Ciò in particolare per i gruppi bancari che detengono un limitato numero di enti partecipati, i quali assumono rischi di un qualche rilievo nel solo territorio nazionale. La complicazione operativa che deriva da tale prescrizione non appare sempre giustificata dai potenziali livelli di rischio.

Sempre con riferimento ai controlli interni di gruppo, si osserva che l'istituzione di una unità di revisione interna deputata ad effettuare in via esclusiva controlli su base individuale sulle controllate sarebbe fonte di un'eccessiva articolazione della struttura dei controlli. Tale approccio, peraltro, contravviene al criterio prevalente di specializzazione delle risorse di auditing in funzione dei processi o degli ambiti della gestione aziendale. Tale impostazione sembra garantire una maggiore efficacia di risultati rispetto a quella fondata sul controllo delle singole entità partecipate.

Governo e organizzazione dell'ICT *– Cap. 8, Sez I e II*

L'organo con funzioni di supervisione strategica delibera l'architettura dei sistemi informativi e delle linee di indirizzo in materia di approvvigionamento delle risorse (personale, sistemi, software, fornitori, ecc.). Approva inoltre il quadro di riferimento organizzativo e metodologico per l'analisi del rischio informatico ed il livello di tolleranza del rischio informatico.

In considerazione della rilevanza ai fini di un più generale rischio operativo, l'attenzione posta nel documento di consultazione sul processo di governo e di organizzazione dell'ICT appare quanto mai opportuna. Permane in ogni caso una problematicità sui criteri di valutazioni da adottare per definire il livello di tolleranza del rischio informatico.

La stessa identificazione, valutazione, mitigazione e monitoraggio di tale rischio richiedono professionalità specifiche che non risiedono generalmente nella funzione risk management, anche nel caso sussista una funzione dedicata specificatamente al rischio operativo. Potrebbe essere opportuno richiamare esplicitamente ad una stretta collaborazione tra il gestore del rischio informatico e la funzione di risk management o di operational risk management: in molti casi, ad esempio, le prefigurazioni di scenari di rischio e le relative valutazioni di impatto sono già sviluppate dalla funzione di operational risk management, anche con riguardo ai sistemi informativi.

La gestione del rischio informatico *– Cap. 8, Sez. III*

Nelle realtà più complesse è prevista la nomina del Direttore dei sistemi informativi (o equivalente), che assume la generale responsabilità della funzione e riferisce direttamente all'organo con funzione di gestione, a garanzia dell'unitarietà della gestione sul rischio informatico. Il Direttore dei sistemi informativi non può avere responsabilità operative dirette nel sistema stesso, a garanzia della sua indipendenza.

Ne consegue un problema di individuazione della figura: il Direttore dei sistemi non deve avere responsabilità operative ma, per la natura delle materie di cui dovrà occuparsi, deve necessariamente possedere competenze tecniche specifiche.

In merito alla definizione e collocazione del processo di analisi del rischio informatico e della funzione a ciò preposta, emerge una necessità di maggiore chiarezza, in particolare rispetto alla figura dell'"utente responsabile". Il documento prevede che il processo di analisi del rischio informatico debba essere svolto dall'utente responsabile

con la partecipazione del personale tecnico, secondo una metodologia definita dall'organo di gestione. Si sottolinea pertanto la centralità di tale figura nella gestione del rischio in parola, per cui se ne auspica una più chiara qualificazione in termini di competenze, responsabilità, possibili soluzioni di inquadramento e collocamento.

Valutazioni in risposta a richieste specifiche formulate nel documento

BOX 1 - Determinazione della tolleranza al rischio - Appetito per il rischio

Si condivide l'utilizzo di variabili di natura sia quantitativa che qualitativa per la determinazione della tolleranza al rischio, che già oggi viene declinata dalla gran parte degli intermediari, a livello individuale e consolidato. Il processo di determinazione della tolleranza al rischio potrebbe basarsi, ad esempio, sulla verifica di adeguatezza dei seguenti parametri:

- Solidità patrimoniale, espressa sia in termini di misure regolamentari (Core Tier I Ratio) sia interne (rapporto tra risorse finanziarie disponibili e capitale interno complessivo).
- Equilibrio della struttura finanziaria, espresso sia in termini di corretto equilibrio tra le fonti e gli impieghi (NSFR) sia in termini di adeguate riserve in forma liquida per fronteggiare situazioni di crisi (LCR).
- Creazione di valore (ad es. metodo EVA).
- Valutazione del posizionamento di mercato, basato sulla determinazione del rating come target tendenziale.
- Assetto organizzativo e dei controlli, basato sulla minimizzazione dei possibili impatti derivanti dai rischi, perseguibile con l'adozione di policies, rigorosi presidi organizzativi, metodologie di misurazione dei rischi e strumenti di mitigazione.

Coerentemente con gli obiettivi complessivi di propensione al rischio, viene declinato il capitale allocato a fronte dei rischi misurabili. Sulla base del capitale allocato sono definiti a cascata i limiti operativi.

BOX 2 - Identificazione delle operazioni di maggior rilievo oggetto del parere preventivo della funzione di controllo dei rischi

In coerenza con l'approccio seguito per la definizione della tolleranza al rischio, si ritiene opportuno lasciare all'autonomia delle singole banche la determinazione delle modalità di individuazione delle operazioni rilevanti. La definizione di soglie normative prescrittive per l'identificazione delle operazioni di maggior rilievo, potrebbe esporre alle seguenti controindicazioni:

- le soglie sarebbero difficilmente determinabili in modo uniforme per tutti i modelli operativi, quantomeno a causa delle peculiarità di composizione dei portafogli di clientela di ciascuna realtà destinataria (es. portafoglio prevalentemente retail vs

corporate; portafoglio di composizione nazionale vs portafoglio con importante componente estera, etc.);

- l'utilizzo del concetto di rilevanza in termini deterministici rischierebbe di far confinare nell'area di irrilevanza alcune categorie di operazioni caratterizzate da rischiosità non facilmente misurabile (es. operazioni che espongono a rischio reputazionale).

BOX 3 - Declinazione del principio di proporzionalità

Non si ritiene opportuno declinare ulteriori elementi caratterizzanti il principio di proporzionalità rispetto a quelli già espressi dalla normativa vigente. Si ritiene, peraltro, che il richiamo costante ai principi di economicità e proporzionalità debba trovare il conseguente riscontro nella formulazione di richieste regolamentari e di resocontazione semplificate quando riferite a intermediari di dimensione contenuta o contrassegnati da limitata complessità operativa e bassa propensione al rischio, individuati, ad esempio, sulla base delle macrocategorie indicate a fini SREP.

BOX 4 - Interazioni tra rischio informatico e rischi operativi

Si considera a tutti gli effetti il rischio informatico come un sottoinsieme molto importante dei rischi operativi. Per motivi di coerenza complessiva non si considera opportuno un trattamento ad hoc se non all'interno della gestione dei rischi operativi. Resta confermata la necessità di garantire una adeguata comprensione a tutti i livelli della struttura aziendale di questa tipologia di rischio come esplicitamente raccomandato nel documento in consultazione.

BOX 5 - Controllo dei sistemi in Cloud Computing

Pur comprendendo le importanti implicazioni derivanti dalla soluzione in oggetto si ritiene opportuno attendere un adeguato periodo di operatività che consenta di apprezzare fino in fondo le implicazioni sulla sicurezza di tale soluzione che esternalizza, di fatto, la collocazione di dati sensibili.

Osservazioni su aspetti di tipo operativo

La regolamentazione introduce profili di notevole complessità e la sua applicazione si presenta senz'altro gravosa per le banche di piccola dimensione (ad esempio le banche di classe 3 a fini SREP), laddove le disposizioni - sia quando riferite all'esercizio di nuove attività sia quando riferite alla predisposizione di policies, regolamenti interni, resoconti all'Organo di Vigilanza, ecc. – introducono prescrizioni inedite e pertanto da attuare integralmente.

L'impegno operativo richiesto ai piccoli istituti, e segnatamente alle "*limitate*" risorse assegnate stabilmente alle funzioni di controllo - che provvedono di fatto alla prepara-

zione di tutta la documentazione in materia, anche di quella formalmente emanata dai vertici aziendali - appare in qualche caso eccessivo e non sempre giustificato.

Si elencano di seguito i principali impegni operativi posti dalle nuove prescrizioni con le relative valutazioni di opportunità.

- Revisione interna – ICT Audit (pag. 17) e connesse valutazioni di merito da riportare nel piano e nel resoconto annuale di Audit: l'attività richiede competenze tecniche normalmente non possedute dalle funzioni che operano in piccole realtà. Si tenga conto, peraltro, delle problematiche di tipo tecnico e logistico legate all'accesso presso gli eventuali outsourcer informatici.
- Revisione interna – Riferimento alle verifiche sulle attività aziendali (pag. 20): significa di fatto controllare tutto l'attivo di bilancio. Si pone una criticità in ordine alle competenze e all'impegno richiesti alla funzione e si ravvede una duplicazione di attività con quanto è già chiamata a fare la revisione esterna con la certificazione delle determinazioni contabili e di bilancio.
- Policy di esternalizzazione (pag. 23): si tratta di un documento inedito che si presenta impegnativo in quanto molto dettagliato per ciò che attiene ai livelli di servizio e alla previsione delle possibili mancanze da parte dell'outsourcer.
- Revisione interna - Relazione sui controlli di outsourcing da inviare annualmente all'Organo di Vigilanza (pag. 25): anche in questo caso il documento è inedito.
- Procedure di allerta interna (pag. 31): si tratta di processi e procedure interne da realizzare integralmente.
- Politica di gestione dei rischi operativi (pag. 40): rappresenta una nuova policy su temi già in gran parte oggetto di trattazione nella risk policy aziendale.
- Politica di gestione della leva finanziaria (pag. 40): è un'ulteriore policy che si pone in parziale sovrapposizione, oltre che con la risk policy aziendale, con quella riferita alla gestione del rischio di liquidità.
- Governo ICT (pag. 47 e seguenti): tutto il capitolo sembra focalizzato sull'attività di banche di grandi dimensioni risultando piuttosto distante dalle modalità operative di una piccola banca. In materia di ICT, il C.d.A. dovrà emanare 4 policies e 2 procedure di gestione di nuova adozione; deliberare un piano annuale e approvare 3 rapporti annuali di valutazione.

Si ritiene, pertanto, che la raccomandazione al contenimento di strutture e risorse in ossequio ai principi di economicità e proporzionalità, che lo stesso documento in consultazione pone come riferimenti costanti nel processo di implementazione del Sistema dei Controlli Interni, dovrebbe essere accompagnata da richieste regolamentari e di resocontazione semplificate e proporzionalmente ridotte quando riferita a intermediari di dimensione contenuta o contrassegnati da limitata complessità operativa e bassa propensione al rischio.