

# BANCA D'ITALIA

*Vigilanza Creditizia e Finanziaria*

## **NORMATIVA DI VIGILANZA IN MATERIA DI “CONFORMITA’ ALLE NORME (COMPLIANCE)”**

*Il presente documento fornisce un primo schema di Istruzioni di vigilanza inerenti al rischio di non conformità e alla relativa funzione. Eventuali osservazioni, commenti e proposte possono essere trasmessi, entro il 30 settembre 2006, all’indirizzo internet [cna.normativa@bancaditalia.it](mailto:cna.normativa@bancaditalia.it) oppure a Banca d’Italia, Servizio Concorrenza, Normativa e Affari Generali, Divisione Normativa, via Milano, 53, 00184 ROMA.*

**Documento per la consultazione**

**Agosto 2006**

## **1. Premessa**

Il rispetto della legalità e della correttezza negli affari è, da sempre, elemento indispensabile dell'attività bancaria, fondata sulla fiducia. Peraltro, l'evoluzione dei mercati finanziari, in termini di innovazione dei prodotti, di trasferimento di rischi e di proiezione internazionale, rende più complessi l'identificazione e il controllo dei comportamenti che possono costituire violazione delle norme, degli standard operativi, dei 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. Si richiede l'istituzione in ciascuna banca di un'apposita funzione di prevenzione e gestione del rischio di violazioni delle richiamate prescrizioni.

Le presenti istruzioni di vigilanza dettano principi di carattere generale, volti ad individuare le finalità e i principali compiti della funzione di conformità alle norme, riconoscendo nel contempo alle banche piena discrezionalità nella scelta delle soluzioni organizzative più idonee ed efficaci per realizzarli.

La funzione di conformità alle norme ha un'importanza determinante in termini di creazione di valore aziendale, conseguibile attraverso il rafforzamento e la preservazione del buon nome della banca e della fiducia del pubblico nella sua correttezza operativa e gestionale. Nel perseguimento di questi obiettivi, l'attenzione delle banche dovrà soprattutto rivolgersi agli utenti dei servizi offerti, non solo attraverso la puntuale e coerente applicazione della disciplina posta a tutela della clientela, ma anche assicurando un'informazione completa che promuova la consapevole assunzione delle scelte finanziarie.

## **2. Il rischio di non conformità alle norme**

Il rischio di non conformità alle norme è il rischio di incorrere in sanzioni giudiziarie o amministrative, perdite finanziarie rilevanti o danni di reputazione in conseguenza di violazioni di norme di legge, di regolamenti, ovvero di norme di autoregolamentazione o di codici di condotta.

In via generale, le norme più rilevanti ai fini del rischio di non conformità sono quelle che riguardano l'esercizio dell'attività di intermediazione, la gestione dei conflitti di interesse, la trasparenza nei confronti del cliente e, più in generale, la disciplina posta a tutela del consumatore.

Nell'ambito del rischio di non conformità assumono, altresì, rilievo le operazioni formalmente corrette, alle quali la banca collabora consapevolmente, poste in essere dalla controparte con l'obiettivo di aggirare l'applicazione di norme.

Per la gestione del rischio di non conformità è innanzitutto necessario che esso venga presidiato nel momento stesso in cui viene generato, attraverso la responsabilizzazione di tutti i dipendenti.

Un'efficace ed efficiente gestione del rischio di non conformità, più specificamente, richiede:

- una chiara e formalizzata individuazione e distinzione di ruoli e responsabilità ai fini della gestione del rischio, a tutti i livelli dell'organizzazione della banca;
- l'istituzione di un'apposita funzione incaricata della gestione del rischio;
- la nomina di un responsabile della conformità alle norme all'interno della banca;
- la redazione e formalizzazione di un documento interno concernente la funzione di conformità che indichi responsabilità, compiti, modalità operative, flussi informativi, programmazione e risultati dell'attività svolta.

### **3. Ruolo degli organi di vertice della banca**

Il consiglio di amministrazione e il collegio sindacale sono responsabili della supervisione complessiva del sistema di gestione del rischio di non conformità alle norme. Nel caso in cui le banche adottino un modello organizzativo diverso da quello tradizionale, detto compito spetta: nel modello dualistico, al consiglio di sorveglianza e al consiglio di gestione; nel modello monistico, al consiglio di amministrazione.

In particolare, il consiglio di amministrazione, sentito il collegio sindacale, con apposita delibera (non delegabile) approva le politiche di gestione del rischio in questione, ivi inclusa la costituzione di una funzione di conformità alle norme, permanente e indipendente. Per le banche che adottino il sistema di amministrazione e controllo dualistico, è opportuno che lo statuto della banca medesima preveda su dette materie una delibera del consiglio di sorveglianza, su proposta del consiglio di gestione. In caso di modello monistico, la delibera deve essere approvata, oltre che dal consiglio di amministrazione nel suo complesso, anche dalla maggioranza dei componenti il comitato per il controllo sulla gestione.

Almeno una volta l'anno il consiglio di amministrazione, sentito il collegio sindacale, valuta l'adeguatezza della funzione di conformità alle norme e a tal fine può avvalersi di un comitato costituito al suo interno; nel modello dualistico, detta valutazione è svolta dal consiglio di gestione e gli esiti della stessa sono comunicati al consiglio di sorveglianza, ovvero a un comitato costituito al suo interno.

Gli organi delegati, o nel modello dualistico il consiglio di gestione, e il direttore generale - secondo le specifiche competenze definite in via generale con riferimento al sistema dei controlli interni - devono assicurare una efficace gestione del rischio di conformità. A tal fine: definiscono adeguate politiche e procedure di conformità; stabiliscono canali di comunicazione efficaci per assicurare che il personale a tutti i livelli dell'organizzazione sia a conoscenza dei presidi di conformità relative ai propri compiti e responsabilità; verificano che le politiche e le procedure vengano osservate all'interno della banca; nel caso emergano violazioni accertano che siano apportati i rimedi necessari; delineano flussi di comunicazione volti ad assicurare agli organi di vertice della società piena consapevolezza sulle modalità di gestione del rischio di non conformità.

Inoltre, con la collaborazione della funzione di conformità, almeno una volta all'anno, gli organi delegati, o nel modello dualistico il consiglio di gestione, e il direttore generale - secondo le rispettive competenze - hanno il compito di:

- identificare e valutare i principali rischi di non conformità a cui la banca è esposta e programmare i relativi interventi di gestione. La programmazione degli interventi deve riguardare sia le eventuali carenze (di politica, procedurali, di implementazione o esecuzione) emerse nell'operatività aziendale, sia la necessità di affrontare eventuali nuovi rischi di non conformità identificati a seguito della valutazione annuale del rischio;
- riferire, di iniziativa o su richiesta, al consiglio di amministrazione (o a un comitato costituito al suo interno) e al collegio sindacale (o al consiglio di sorveglianza) sull'adeguatezza della gestione del rischio di non conformità attuata dalla banca;
- fornire tempestiva informazione al consiglio di amministrazione (o a un comitato costituito al suo interno) e al collegio sindacale (o al consiglio di sorveglianza o al comitato di controllo sulla gestione) su ogni violazione sostanziale della conformità alle norme (es. violazioni che possono comportare un alto rischio di sanzioni regolamentari o legali, perdita finanziaria rilevante o danno di reputazione).

#### **4. La funzione di conformità alle norme**

Il rischio di non conformità alle norme è un rischio diffuso a tutti livelli dell'organizzazione aziendale, soprattutto all'interno delle linee operative; l'attività di prevenzione deve svolgersi in primo luogo dove il rischio medesimo viene generato ed è pertanto necessaria un'adeguata responsabilizzazione di tutto il personale.

Una gestione dinamica e consapevole del rischio di non conformità richiede, inoltre, l'istituzione di un'apposita funzione, il cui compito specifico è quello di far sì che le procedure interne siano coerenti con la necessità di prevenire la violazione di norme di eteroregolamentazione (leggi e regolamenti) e autoregolamentazione (codici di condotta, codici etici) applicabili alla banca.

Detta funzione si inserisce nel quadro complessivo del sistema dei controlli interni, di cui le banche si dotano ai sensi del Titolo IV – Capitolo 11 – Sezione II delle Istruzioni di Vigilanza, al fine di controllare e gestire il rischio di non conformità.

I principali adempimenti che la funzione di conformità è chiamata a svolgere sono:

- l'identificazione nel continuo delle norme applicabili alla banca e la misurazione/valutazione del loro impatto su processi e procedure aziendali;
- la proposta di modifiche organizzative e procedurali finalizzata ad assicurare adeguato presidio dei rischi di non conformità identificati;
- la predisposizione di flussi informativi a tutte le strutture interessate (organi di vertice, revisione interna, gestione del rischio operativo);
- la verifica dell'efficacia degli adeguamenti organizzativi (strutture, processi, procedure anche operativi e commerciali) suggeriti per la prevenzione del rischio di conformità.

In relazione ai molteplici profili professionali richiesti per l'espletamento di tali adempimenti, le varie fasi in cui si articola l'attività della funzione di conformità possono essere affidate a strutture organizzative diverse già presenti nella banca (es. legale, organizzazione, gestione del rischio operativo), purché il processo di gestione del rischio e l'operatività della funzione siano ricondotti ad unità mediante la nomina di un responsabile che coordini e sovrintenda alle diverse attività, anche attraverso la predisposizione di un apposito programma di attività.

La funzione di conformità deve essere coinvolta nella valutazione *ex ante* della conformità alla regolamentazione di riferimento di tutti i progetti innovativi che la banca intenda intraprendere nonché nella prevenzione e nella gestione dei conflitti di interesse, sia tra le diverse attività svolte dalla banca sia con riferimento ai dipendenti e agli esponenti aziendali.

Altra area di particolare rilievo in cui la funzione di conformità deve costituire un importante punto di riferimento per le decisioni degli organi di vertice è rappresentata dalla verifica della coerenza del sistema premiante (in particolare retribuzione e incentivazione del personale) con gli obiettivi di rispetto delle norme, dello statuto nonché di eventuali codici etici o altri *standard* di condotta applicabili alla banca.

Rientrano nell'ambito della funzione di conformità anche la consulenza e assistenza nei confronti degli organi di vertice della banca in tutte le materie in cui assume rilievo il rischio di non conformità nonché la collaborazione nell'attività di formazione del personale al fine di prevenire il rischio di non conformità attraverso la conoscenza delle disposizioni applicabili alle attività svolte e di favorire la diffusione di una cultura aziendale improntata ai principi di onestà, correttezza e rispetto dello spirito e della lettera delle norme.

Ferma restando la discrezionalità delle banche nell'organizzare la funzione di conformità, in coerenza con le proprie peculiarità dimensionali e operative nonché con l'assetto organizzativo e strategico della gestione dei rischi, è comunque necessario che la medesima funzione:

- sia indipendente. A tal fine è necessario che: vengano formalizzati lo *status* e il mandato della funzione attraverso l'indicazione di compiti, responsabilità, addetti, prerogative, flussi informativi diretti agli organi di vertice; venga nominato un responsabile indipendente; sia assicurata la presenza di adeguati presidi per prevenire i conflitti di interesse attraverso, in particolare, la previsione di flussi informativi separati e dedicati;
- sia dotata di risorse qualitativamente e quantitativamente adeguate ai compiti da svolgere. Sotto il profilo delle risorse umane, va rilevato che le attività di conformità possono essere svolte da personale inserito in una struttura organizzativa dedicata e gerarchicamente dipendente dal responsabile della funzione ovvero da dipendenti integrati nelle diverse aree operative. Indipendentemente dalla soluzione organizzativa prescelta, il personale che svolge funzioni di conformità deve essere adeguato per: numero; competenze tecnico – professionali; aggiornamento, anche attraverso l'inserimento in programmi di formazione nel continuo. Inoltre, attraverso l'attribuzione di risorse economiche eventualmente attivabili anche in autonomia, dovrà essere consentito alla funzione il ricorso a consulenze esterne, in relazione alla particolare complessità di specifiche innovazioni normative e/o operative;
- abbia accesso a tutte le attività della banca svolte sia presso gli uffici centrali sia presso le strutture periferiche nonché a qualsiasi informazione rilevante per lo svolgimento dei propri compiti, anche attraverso il colloquio diretto con il personale.

Le banche di dimensioni contenute o caratterizzate da una limitata complessità operativa potranno affidare lo svolgimento della funzione di conformità alle strutture esistenti incaricate della gestione dei rischi o a soggetti terzi (es. altre banche, società di revisione ovvero organismi associativi di categoria), purché dotati di caratteristiche idonee in termini di professionalità e indipendenza. Resta in ogni caso ferma la necessità di nominare un responsabile della funzione all'interno dell'azienda, dotato delle caratteristiche e prerogative indicate nel paragrafo seguente, al quale spetta il compito di referente interno per il soggetto incaricato della funzione nonché la complessiva supervisione dell'attività di gestione del rischio, posto che la responsabilità per la corretta gestione del rischio di non conformità resta in capo alla banca.

L'esternalizzazione della funzione di conformità deve essere formalizzata in un accordo, che almeno definisce:

- gli obiettivi della funzione;
- la frequenza minima dei flussi informativi nei confronti del responsabile interno all'azienda e degli organi di vertice aziendali, fermo restando l'obbligo di corrispondere tempestivamente a qualsiasi richiesta di informazioni e consulenza da parte di questi ultimi;
- gli obblighi di riservatezza delle informazioni acquisite nell'esercizio della funzione;
- la possibilità di rivedere le condizioni del servizio al verificarsi di modifiche nell'operatività e nell'organizzazione della banca.

## **5. Il responsabile della funzione di conformità alle norme**

Al fine di assicurare l'efficacia della funzione di conformità è necessario che il responsabile possieda requisiti adeguati di indipendenza, autorevolezza e professionalità.

La nomina e la revoca del responsabile della conformità sono di competenza, esclusiva e non delegabile, del consiglio di amministrazione (consiglio di gestione) sentito il collegio sindacale (consiglio di sorveglianza). Le banche provvedono a comunicare tempestivamente all'Autorità di Vigilanza la nomina e l'eventuale revoca del responsabile della conformità.

Il responsabile della funzione di conformità deve rivestire un ruolo all'interno della banca tale da conferire autorevolezza alla funzione medesima: può essere nominato responsabile della funzione anche un componente dell'organo amministrativo purché non sia destinatario di deleghe. Se il responsabile della funzione è un'esponente del management della banca non deve avere responsabilità dirette di aree operative né deve essere gerarchicamente dipendente da soggetti responsabili di dette aree.

Il personale incaricato di compiti di conformità, anche se inserito in aree operative, riferisce direttamente al responsabile della funzione per le questioni attinenti a detti compiti. Tali flussi informativi separati possono non essere necessari nelle ipotesi in cui il personale appartenga a strutture indipendenti della banca (es. legale, gestione del rischio).

## **6. Rapporti con altre funzioni aziendali**

Rilevanti interrelazioni sussistono tra la funzione di conformità e diverse altre funzioni aziendali (revisione interna, gestione del rischio operativo, funzione legale, organizzazione, organismo di vigilanza individuato ai sensi della legge 231/2001, ecc.). La collaborazione con le richiamate funzioni consente a quella di conformità di sviluppare le proprie metodologie di gestione del rischio in modo coerente con le strategie e l'operatività aziendale, assicurando nel contempo processi conformi alle normative esterne e ausilio consultivo.

Il principio di indipendenza della funzione di conformità non preclude in alcun modo la possibilità e l'opportunità di una stretta collaborazione con altre aree aziendali. L'indipendenza della funzione, in un contesto caratterizzato da forti interrelazioni, viene assicurata attraverso la formalizzazione del mandato che ne sancisce l'autonomia rispetto sia alle strutture operative sia a quelle di controllo interno, attraverso la definizione espressa di ruoli e competenze.

L'adeguatezza ed efficacia della funzione di conformità devono essere sottoposte a revisione periodica da parte della revisione interna. Per l'efficacia e l'imparzialità della revisione è necessario che la funzione di conformità non sia affidata alla funzione di revisione interna. In ogni caso, attesa la contiguità tra le due attività, dovranno essere chiaramente individuati e comunicati all'interno della banca i compiti e le responsabilità delle due funzioni, in particolare per quanto specificamente attiene alla suddivisione delle competenze in materia di misurazione dei rischi, alla consulenza in materia di adeguatezza delle procedure di controllo nonché alle attività di verifica delle procedure medesime.

Specificata attenzione dovrà essere posta nell'articolazione dei flussi informativi tra le due funzioni; in particolare il responsabile della revisione interna dovrà informare il responsabile della conformità per le eventuali inefficienze nella gestione del rischio di conformità emerse nel corso delle attività di verifica di competenza della funzione di revisione interna.

*Riguardo alla separatezza delle due funzioni si è rilevato che alcune banche si sono già dotate di strutture incaricate della conformità, collocando organizzativamente i relativi compiti nella funzione di revisione interna. In proposito, si fa presente che l'adeguamento alle nuove istruzioni di vigilanza potrà avvenire in modo graduale, fermo restando che entro 12 mesi dalla pubblicazione delle istruzioni stesse le due funzioni dovranno essere rese organizzativamente e operativamente separate e indipendenti.*

## **7. La funzione di conformità nelle strutture di gruppo**

Le Istruzioni di vigilanza in materia di conformità trovano applicazione alle banche e ai gruppi bancari secondo un criterio di proporzionalità.

Per le banche organizzate in strutture di gruppo alcune attività di conformità potranno essere accentrate, al fine di conseguire economie di scala e creare unità specializzate all'interno del gruppo medesimo; resta, comunque, fermo che in ciascuna banca del gruppo dovrà essere nominato un responsabile della conformità, che costituirà il referente della corrispondente struttura di gruppo.

Particolare attenzione richiederà l'articolazione della funzione nei gruppi con operatività internazionale, tenuti al rispetto delle regole vigenti in tutti i paesi in cui prestano le proprie attività. In questi casi le banche dovranno individuare le soluzioni organizzative più

idonee (es. *compliance officer* locali) per assicurare la corretta gestione del rischio derivante dalla necessità di rispettare tutte le disposizioni applicabili in relazione ai diversi ambiti di operatività.

E' altresì opportuno che società controllate da banche italiane operanti all'estero adottino i medesimi presidi di conformità della capogruppo italiana, anche nei casi in cui la normativa dei paesi in cui la controllata è stata costituita non preveda analoghi livelli di attenzione.