La Funzione Compliance nelle banche

Relazione a cura di Marco Pigliacampo

2007

Indice:

1. Le funzioni di controllo in Italia

Nella giornata di formazione "*Il controllo interno e la funzione di Compliance*", organizzata lo scorso 23/2 da ISIDE – Istituto di Documentazione Economica, è stato possibile raccogliere informazioni sulle funzioni di controllo nel settore bancario italiano.

Un quadro sintetico sull'**evoluzione** di tali funzioni aiuta a comprendere la **varietà** delle **situazioni organizzative** in cui si trovano oggi le banche italiane.

La prima delle funzioni di controllo a diffondersi nelle banche è stata la funzione ispettiva, l'**Ispettorato**, che oggi è ancora attivo in banche di piccole e minori dimensioni. E' una funzione che nasce e si caratterizza come "longa manus" della Direzione Generale e ad essa fa capo. Ha un ruolo investigativo e, secondariamente, sanzionatorio. Non si fonda su alcuna particolare legge o normativa proveniente dalle Autorità di controllo e vigilanza.

La funzione del **Controllo Interno** nasce e viene stabilita per legge (art. 6 del TUF). Svolge un **compito settoriale**, cioè si concentra sui processi che riguardano i servizi di investimento, secondo quanto stabilito dalla legge e dalle normative emanate dalle Autorità, in particolare dalla Consob. Secondo norme, si caratterizza per l'**indipendenza** dalle funzioni produttive e per il compito di provvedere non solo al **controllo *ex post*** dei comportamenti operativi, ma anche al lavoro di **prevenzione *ex ante*** finalizzato a far rispettare le norme.

La funzione della **Revisione Interna** è stata istituita inizialmente per volontà dell'impresa. Contrariamente al Controllo Interno, svolge un **compito di carattere generale**, finalizzato a controllare potenzialmente tutte le attività svolte nell'azienda. Inizialmente, i compiti e gli obiettivi delle attività di revisione interna sono definiti dalla Direzione Generale. Negli anni successivi impatta sul suo funzionamento la normativa di Banca d'Italia.

Negli ultimi anni, con la diffusione del termine **Internal Audit**, c'è stata una progressiva "fusione" tra Revisione Interna e Controllo Interno. Questo ha comportato la creazione di una unica funzione, in grado di svolgere **sia un controllo di carattere generale** potenzialmente su tutte le attività aziendali **sia un lavoro focalizzato per i servizi di investimento**, basato sulla normativa Consob che caratterizzava il lavoro della funzione Controllo Interno.

In alcune realtà, il termine **Compliance** è stato aggiunto al nome Internal Audit ("*Funzione Internal Audit e Compliance*") proprio per indicare e mantenere quella particolare attività relativa ai servizi di investimento che *precede* la fase di controllo e il cui obiettivo è prevenire ex ante l'adempimento delle norme. Tale lavoro di prevenzione si è svolto soprattutto mediante la **stesura e la condivisione di procedure da rispettare** per adempiere alle norme.

Solo in un numero minore di realtà, tipicamente le banche internazionali presenti in Italia, la funzione Compliance era già esistente negli anni '90 e si caratterizzava per l'**indipendenza** sia dall'Internal Audit sia dalla funzione Legale.
Il suo compito era quello di **codificare la normativa** esistente, **tramutarla in regole e principi organizzativi interni** alla banca, **formare** il personale a seguire tali regole e **monitorarne** l'adempimento. Si tratta quindi di un lavoro basato su competenze manageriali e organizzative più che di auditing e controllo. Nel paragrafo successivo viene approfondito il modello statunitense di gestione della compliance.

Oggi le banche italiane si trovano a dover preparare un grande **salto di qualità** nel modello di gestione della compliance, sia quelle che hanno finora posizionato la funzione nell'ambito dell'Audit, sia quelle che già prevedono una funzione autonoma.
La necessità di tale salto in avanti è provocata da due fattori fondamentali: la **Legge 231** sulla Responsabilità Amministrativa e la proposta che proviene dal Comitato di **Basilea**.
Approfondiamo tutto ciò nel terzo paragrafo.

2. La compliance negli Stati Uniti

Nel "*Compliance Watch*" elaborato dalla **ABA – American Bankers Association** è possibile leggere informazioni statistiche sulla diffusione e il funzionamento della funzione Compliance presso le banche statunitensi.

Il rapporto ABA ha individuato innanzitutto **le normative** su cui sono concentrate le maggiori attenzioni (e i costi) delle banche americane in termini di programmi e interventi di compliance.

Le normative in cui le banche hanno investito di più in termini economici sono in ordine:

- Bank Secrecy Act (Anti-Money Laundering);
- Privacy Laws and Regulations;
- Truth in Lending;
- Real Estate Settlement Procedures Act;
- Home Mortgage Disclosure Act;
- Truth in Savings;
- Fair Lending Laws.

Quindi la maggior parte dei programmi di compliance si concentrano su quattro aree:

- la legislazione su **antiriciclaggio** et similia;
- le leggi sulla **privacy**;
- le normative sulla **trasparenza** delle condizioni e dei servizi;
- le norme di **condotta** sulla vendita di prestiti e mutui.

Tra i processi relativi ad ogni specifica normativa in cui è maggiormente impegnata la funzione Compliance ci sono in ordine:

- le attività di **analisi** e **pianificazione** del programma di adempimento;
- le attività di progettazione ed erogazione della **formazione**;
- le attività di **monitoraggio**;
- le attività di **reportistica** sui risultati raggiunti;
- le attività di controllo e **auditing**.

In una buona percentuali di casi, e anche in base alla normativa di interesse, l'attività di auditing sull'adempimento alla normativa viene svolta dalla funzione di Internal Audit.

Nella "**job description**" relativa al loro ruolo, i Compliance Officer delle banche americane hanno dichiarato di occuparsi di:

- sviluppo di **policy e procedure** per l'adempimento alle normative;
- **monitoraggio e analisi** dell'adempimento diffuso in azienda;
- osservazione delle leggi e delle novità regolamentari;
- progettazione ed erogazione di **formazione interna** sull'adempimento alle normative;
- relazione e coordinamento con l'Internal Audit;
- revisione dei programmi di compliance;

- **auditing** sull'adempimento alle normative;
- revisione della **documentazione interna** di compliance.

Inoltre si può segnalare che:

- durante la fase di **sviluppo di un nuovo prodotto o servizio** la funzione Compliance viene coinvolta "Sempre" (49%) o "Qualche volta" (43,7%). Solo nel 6,4% dei casi è coinvolta "Raramente" e nello 0,9% "Mai";
- la funzione Compliance si occupa di sottoporre ogni nuovo prodotto o servizio ad una specifica **valutazione del rischio di compliance**: "Sempre" nel 28,5% dei casi, "Qualche volta" nel 50,4%. "Raramente" e "Mai" rispettivamente nel 17% e 4%.

Il rapporto ABA mette in evidenza come siano identificabili nel settore **tre modalità di approccio** al tema della compliance: Reactive, Proactive, Managerial.

- L'approccio "*Reactive*" è ampiamente il più diffuso (60,3%) e consiste nel considerare i progetti di gestione della compliance "un male necessario che deve essere adeguatamente introdotto in azienda per permetterle di **tenersi fuori da guai** ben più gravi".

- Ancora non molto diffuso è l'approccio "*Proactive*" (19,8%), che consiste nel considerare la compliance come "una delle principali **chiavi di successo** dei servizi di gestione della clientela".

- Ancora meno diffuso (9,2%) è l'approccio "*Managerial*", secondo il quale "i costi della compliance servono a **minimizzare il rischio** di costi ulteriori ai profitti dell'azienda".

Uno degli elementi comuni alle variegate esperienze in atto è che la gestione della compliance richiede interventi e azioni che costano molto in termini economici. Si tratta infatti di programmare e avviare azioni su diversi piani, che richiedono investimenti economici non indifferenti.

La voce di spesa più alta è il **costo del personale addetto** alla funzione Compliance o alle attività relative: stipendi e benefit. Tra le diverse attività che compongono la gestione della compliance, quelli che costano maggiormente sono in ordine:

- **l'auditing e il monitoring** sull'adempimento delle normative;
- **la formazione** delle persone sulle normative;
- **i convegni** e le conferenze interne sulla compliance;
- lo sviluppo e l'acquisto di **software di gestione** della compliance;
- la stesura e la stampa di **manuali e guide informative**;
- l'elaborazione e **la registrazione di dati** e informazioni;
- il coinvolgimento di **consulenti** esterni;
- altri processi interni di comunicazione e informazione.

Quanto alla assegnazione del **budget** alla funzione Compliance, la situazione delle banche è ancora molto variegata negli Stati Uniti, comunque le due opzioni più diffuse sono:

- il budget è assegnato alla Funzione Compliance come **"funzione unica" dell'azienda** (opzione diffusa generalmente presso le banche di dimensioni medio-grandi);
- il budget per la compliance è una parte del budget assegnato alla **funzione Audit** della banca (opzione diffusa nelle banche piccole).

In percentuale minore:

- il budget per la compliance è **distribuito in parti presso ogni unità organizzativa** di linea (opzione presente soprattutto in banche molto grandi);
- il budget per la compliance è una parte del budget assegnato alla **funzione Legale** della banca.

Riguardo più propriamente le **scelte organizzative** sono diffuse almeno cinque modalità diverse di organizzazione della Funzione Compliance o di gestione della compliance.
Le due più diffuse descrivono situazioni contrapposte:

- una larga percentuale di banche (soprattutto le piccole) ha il **Compliance Officer** ma non ha creato un apposito Dipartimento;
- una fascia ugualmente ampia (banche medie e grandi) ha sia sviluppato un **Dipartimento della Compliance** sia disseminato presso le unità organizzative di linea "**responsabili di linea della compliance**" che fanno a capo al Dipartimento e da esso sono coordinati.

Altre scelte sono, in ordine di diffusione:

- un Dipartimento della Compliance a livello centrale, senza collaboratori presso le unità di linea;
- un Compliance Officer centrale e vari Compliance Officers con il loro staff presso le principali unità organizzative;
- un Compliance Officer presso la holding di gruppo e vari Dipartimenti della Compliance presso le banche del gruppo.

Solo in misura minore sono presenti nel settore scelte organizzative "particolari" come:

- il coinvolgimento nei programmi di compliance delle persone che si occupano di Internal Audit;
- la delega del lavoro sulla compliance a società o consulenti esterni;
- la disponibilità di un Compliance Officer part-time.

Riguardo il titolo aziendale assegnato al Compliance Officer, è interessante sapere che:

- il 39% dei Responsabili Compliance è **Vice President**;
- il 13,6 % è Assistant Vice President;
- il 11,2% è Senior Vice President;
- il 11,7% è semplicemente il Compliance Officer.

Nella grande maggioranza dei casi, il Responsabile Compliance **riporta direttamente al CEO** o al top management.

Riguardo infine i Compliance Officer diffusi nelle banche americane, possiamo dire che:

- a livello di background professionale la maggior parte (44,9%) proviene dai **Servizi di Finanziamento** (Lending) e una buona parte (34,9%) dall'Internal Auditing. In percentuali minori hanno una esperienza professionale nei servizi di Certificazione (9,5%) e nel servizio Legale (2,1%).
- solo in parte minore (20,5%) hanno una formazione universitaria di compliance management, mentre in maggioranza (56,8%) hanno ricevuto **formazione interna all'azienda** sulla gestione della compliance.
- nel 15,4% dei casi hanno ricevuto il **CRCM – Certified Regulatory Compliance Manager** rilasciato dall'istituto di certificazione dell'ABA.

3. Il salto di qualità: D.Lgs. 231 e Basilea

3.1 D.Lgs. 231/2001

Il D.Lgs. 231/2001 introduce nel ns. ordinamento la nozione di responsabilità "amministrativa" dell'azienda per reati commessi dai propri dipendenti. E' una **responsabilità di natura penale**:

- deriva da un reato,
- è accertata con procedimento penale,
- comporta sanzioni particolarmente gravi tra cui l'**interdizione** temporanea o definitiva dell'azienda all'esercizio dell'attività.

La responsabilità dell'azienda su reati commessi dai propri dipendenti viene esclusa se l'azienda prova di avere:

- adottato ed implementato **modelli di organizzazione e gestione idonei** a prevenire i reati;
- affidato ad un proprio **organismo interno** il compito di vigilare sul funzionamento, l'osservanza e l'aggiornamento costante dei modelli suddetti.

Questo "organismo di controllo" coincide oggi sempre più spesso con la nuova **Funzione Compliance**.

In alcune realtà si è deciso di affidare la 231 all'Internal Audit, ma non è una scelta corretta: si tratta di gestire un'attività più ampia dell'Audit e sempre più rilevante per l'azienda, che quindi va controllata a valle: l'Internal Audit non può controllarsi da solo.

Secondo legge, l'organismo di controllo preposto deve:
- essere dotato di **poteri autonomi** di iniziativa e controllo;
- stabilire autonomamente le proprie regole organizzative;
- godere di **obblighi di informazione** nei suoi confronti da parte delle altre funzioni;
- godere di poteri di richiesta e acquisizione di informazioni;
- disporre di un **budget idoneo**;
- non subire alcun vincolo di subordinazione gerarchica;
- essere un **ente interno** all'azienda, pur potendo avvalersi di soggetti esterni.

Su questo punto, l'ABI ha espresso l'opinione che le banche di credito cooperativo possano esternalizzare la funzione a livello accentrato alle Federazioni locali.

Secondo il modello organizzativo, condiviso a livello di categoria, le fasi fondamentali sono:
- **identificazione dei rischi** di commissione dei reati;
- **monitoraggio dei rischi reali** in azienda;
- analisi delle **criticità** e verifica del **livello di controllo esistente** con il **livello di controllo teorico** necessario per la prevenzione dei reati;
- identificazione di un **piano di prevenzione**, controllo e sanzione;
- realizzazione e gestione del **piano di intervento** in azienda, al fine di adeguare l'organizzazione in modo coerente alla prevenzione dei rischi.

L'introduzione della 231 ha sollecitato nelle aziende un aumento immediato della priorità di adottare un modello efficace di gestione del rischio di non conformità alle norme.

3.2 La proposta di Basilea

Nell'ottobre dello scorso anno il **Comitato di Basilea** ha fornito la seguente definizione della Funzione Compliance: "**An independent function** that **identifies, assesses, advise on, monitors and reports** on the bank's **compliance risk**, that is, **the risk of legal or regulatory sanctions, financial loss, or loss to reputation** a bank may suffer as a result of its failure to **comply with all applicable laws, regulations, codes of conduct** and **standards of good practice**".

La proposta di Basilea impatta fortemente sulle scelte organizzative delle banche riguardo la funzione Compliance per almeno due fatti fondamentali:
- essa conferisce alla funzione Compliance un **ambito ampio e diversificato**, attribuendole la missione onerosa di individuare e valutare i rischi che l'azienda corre

per il mancato rispetto di leggi, regolamenti, procedure, persino codici interni e best practices;

- essa conduce la gestione della compliance in un approccio che è quello proprio della "**gestione del rischio**", la cui finalità – esattamente come nella gestione del Rischio Operativo - è la salvaguardia dell'integrità economica della banca attraverso la **mitigazione** del "**rischio di non adempimento**", considerato a tutti gli effetti come un rischio del business bancario.

In questa visione, la natura delle attività gestite dalla funzione Compliance evolve dal presidio di procedure in grado di garantire l'adempimento delle normative di impatto generale verso un **modello di gestione di rischio** che utilizza **differenti strumenti** di informazione, formazione e sensibilizzazione al fine di creare e trasferire a tutti i livelli aziendali **un sistema di corporate governance** in linea con i **principi etici e deontologici** dichiarati dall'azienda.

Un approccio di questo tipo prelude ad un **cambiamento strategico** nella gestione del rischio, in quanto l'obiettivo finale è quello di dotarsi di **una funzione di riferimento generale**, per l'appunto la funzione Compliance, a fronte di una pluralità di funzioni coinvolte nella gestione dello stesso (Internal Audit, Risk Management., Organizzazione, Aree di Business e la stessa funzione Compliance).