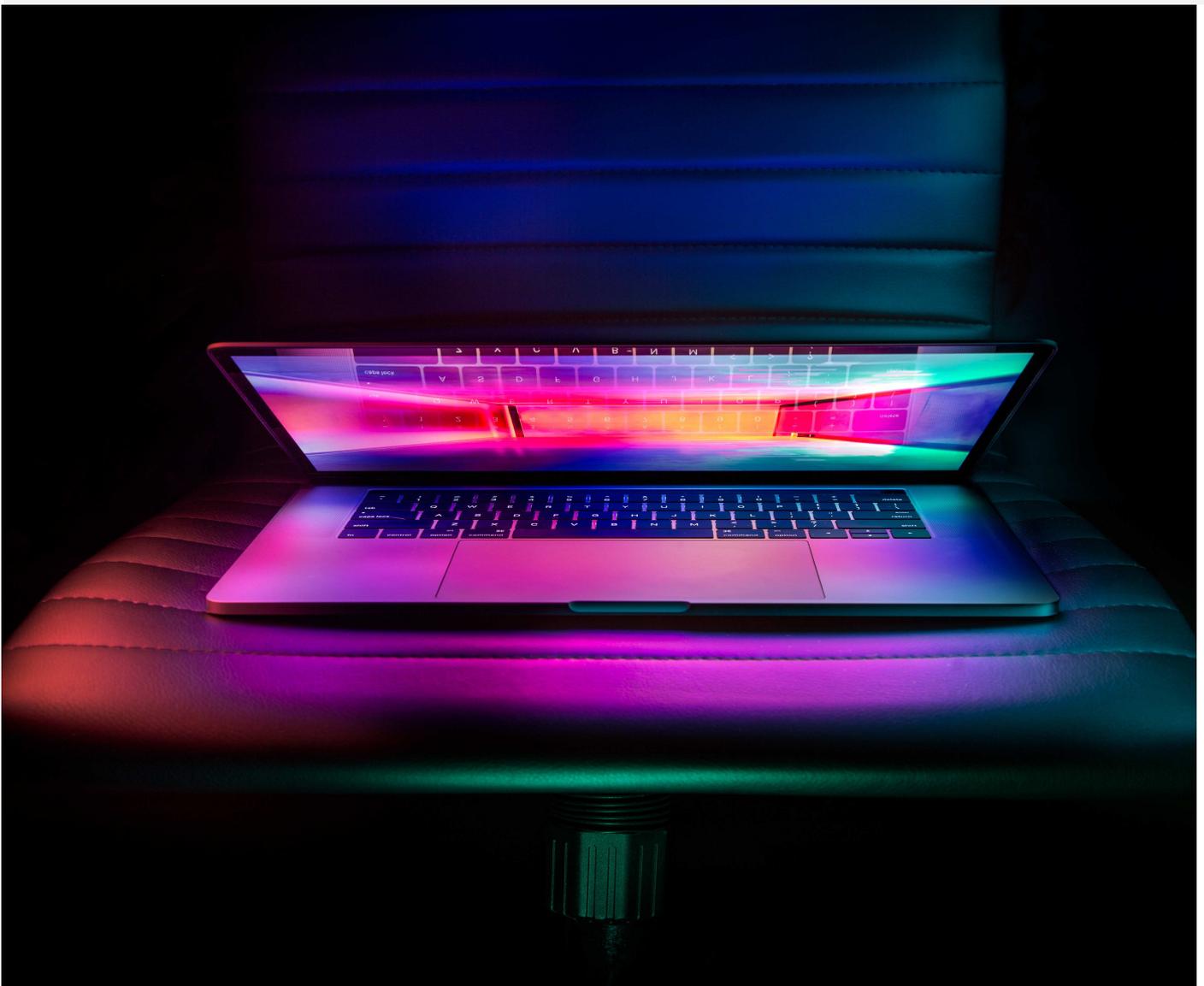


UN VALORE PER L'IMPRESA  
LA COMPLIANCE PER IL SETTORE FINANZIARIO



La funzione di conformità svolge un ruolo di rilievo nella creazione di valore aziendale, lavorando per garantire l'efficienza ed efficacia dei processi e dei sistemi aziendali coerentemente con quanto previsto dalle leggi nazionali ed europee, che sono in costante evoluzione. Questa azione contribuisce a preservare il buon nome della banca e la fiducia del pubblico.

NTT DATA, sulla base della sua conoscenza dei processi e dei sistemi aziendali, è il partner ideale per supportare le analisi di Compliance e l'identificazione dei requisiti Business e IT, con un approccio concreto che concilia le esigenze delle funzioni di Business e IT nel rispetto delle norme vigenti.

## L'EVOLUZIONE DEL CONTESTO REGOLATORIO

In Italia, gli intermediari finanziari non sono più soggetti alla sola regolamentazione nazionale o regionale ma a un **sistema regolatorio sempre più ampio** e complesso in ambito europeo e internazionale.

La regolamentazione finanziaria internazionale ha tra i suoi macro obiettivi (cfr. IOSCO):

- la protezione degli investitori;
- l'efficienza e la trasparenza del mercato;
- la riduzione del rischio sistemico preservando l'integrità del mercato.

L'integrazione dei mercati richiede regole comuni da applicare con criteri omogenei, **evitando arbitraggi normativi e garantendo parità di condizioni** tra operatori tradizionali e nuovi operatori all'interno dei differenti paesi.

Negli ultimi anni, le Autorità hanno avviato un'intensa attività di definizione di norme considerabili internazionali, che impongono regole a entità finanziarie di altri paesi, ampliando così il perimetro normativo e la **collaborazione tra stati a livello mondiale**.

Alcuni esempi recenti sono il FATCA (Foreign Account Tax Compliance Act), che "impone" agli istituti finanziari di diversi stati nel mondo la comunicazione di informazioni relativamente ai conti e alle operazioni effettuate da cittadini USA; o il GDPR (General Data Protection Regulation), che impone regole in materia Privacy ai titolari e ai responsabili del trattamento stabiliti al di fuori dell'Unione Europea nel caso siano trattati dati di residenti UE.

L'internazionalizzazione offre **grandi opportunità ma comporta anche grandi rischi**.

Come vedremo, l'insuccesso in un mercato finanziario può avere un impatto significativo anche su altri mercati e su altre economie.

## LA PERCEZIONE DELLA COMPLIANCE: COSTO O VALORE?

Visti l'evoluzione e l'ampliamento del contesto regolatorio internazionale, la funzione di Compliance assume sempre più rilevanza all'interno delle aziende finanziarie e non. Eppure, ancora troppo spesso le attività di Compliance vengono percepite dai diversi Management aziendali come un freno alle attività del proprio Business, un ostacolo alla creatività del Marketing, un qualcosa di utile solo a rallentare i processi interni e il Time to Market dell'azienda.

Di seguito sono descritti solo alcuni degli esempi legati a una cattiva Governance e a una gestione dei rischi da parte di società, le quali, probabilmente, non consideravano la Compliance come un'attività in grado di generare **valore per l'impresa**, quanto piuttosto un **costo**.

### **1995: Collasso Barings Bank**

Un primo esempio è il collasso della Barings Bank, che ha rappresentato un fattore chiave di molti cambiamenti normativi alla fine degli anni '90. I derivati non autorizzati, negoziati a Singapore dal noto Broker inglese Nick Leeson, hanno causato perdite di oltre 800 milioni di sterline e, alla fine, il crollo della banca. Fondata nel 1806, Barings era il più vecchio e uno dei più noti nomi nel settore bancario internazionale. La causa del crollo è stata attribuita alla mancanza di sistemi e di controlli atti a gestire le attività di negoziazione e, in particolare, alla mancanza di un'appropriata supervisione delle negoziazioni da parte dei dirigenti.

### **2003: Cirio, Parmalat e titoli di stato argentini**

Il crack della Cirio-Parmalat è forse lo scandalo finanziario più noto nel nostro paese, anche perché coinvolse e sconvolse moltissimi risparmiatori che avevano investito in titoli spazzatura, venduti dalle banche senza avvertimenti particolari circa i relativi rischi. Anzi, molti dei titoli che poi si rivelarono spazzatura figurarono fino all'ultimo nell'elenco di quelli privi di rischio indicati dall'ABI.

### **2007: Crisi economica legata ai mutui Subprime USA**

La crisi che ha sconvolto il mercato internazionale è stata generata negli Stati Uniti, tra il 2004 e il 2006, dall'aumento dei tassi di interesse dall'1% al 5,35%. Ciò ha causato il calo dei prezzi delle abitazioni e livelli record di insolvenza sui mutui e, in particolare, dei mutui Subprime, ovvero mutui concessi nei confronti di soggetti potenzialmente insolventi. La rapida diffusione della crisi in tutto il mondo è derivata dalla cartolarizzazione dei Subprime e dal loro successivo impacchettamento in prestiti meno rischiosi, venduti dalle banche. Questi passaggi hanno comportato l'impossibilità di calcolare l'effettivo rischio e la reale esposizione delle banche americane. I risultati sono stati disastrosi: le banche hanno iniziato a essere sempre più riluttanti nel concedere nuovi prestiti per l'incertezza di una corretta valutazione del merito creditizio, provocando il dilagare della crisi di liquidità globale.

### **2008: Monte dei Paschi**

La più grave e la più lunga crisi bancaria italiana, tuttora non risolta, ha assorbito risorse per più di 30 miliardi di euro, imponendo alla fine l'ingresso nel capitale dello

stato come socio di maggioranza. La causa, ben nota, fu l'azzardato acquisto di Banca Antonveneta, per il quale, tuttavia, Monte dei Paschi aveva ottenuto l'autorizzazione dalle autorità di controllo, pur in assenza di una Due Diligence.

**2011: Lo scandalo della Libor**

Il tasso di offerta Inter-Bank di Londra (LIBOR) è alla base di molti milioni di contratti finanziari e prestiti a livello globale. Questo scandalo è venuto alla ribalta quando Barclays Bank è stata multata per 59,5 milioni di sterline nel giugno 2012 dalla FSA, con l'accusa di aver manipolato il tasso per migliorare le posizioni di Trading della banca e/o la sua affidabilità creditizia complessiva. È stato poi scoperto che questa pratica era comune sin dal 1991.

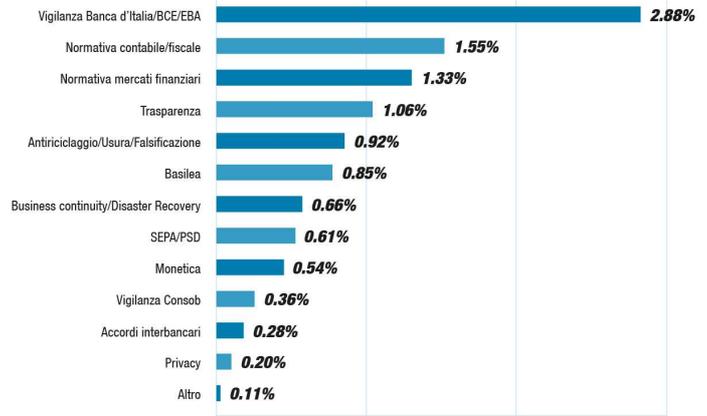
Oggi, i requisiti normativi come quelli definiti dalla Direttiva MiFID, ma non solo, richiedono agli intermediari finanziari l'implementazione di presidi a tutela del consumatore, utili a ridurre il rischio che eventi catastrofici come quelli sopra citati si ripresentino.

**COSTI IT PER LA COMPLIANCE BANCARIA**

Un'analisi svolta sulla spesa IT nel settore Banking (cfr. "Rilevazione sull'IT nel sistema bancario italiano ABI-CIPA"), mostra come la quota **riservata alla Compliance del Cash Out IT** dei principali 23 gruppi bancari italiani (pari a **4.634 milioni di euro circa**), risulti essere pari al **13,8%** e in **crescita rispetto agli ultimi anni**.



Analizzando la ripartizione del Cash Out IT nei vari **ambiti normativi** di interesse, si osserva che la maggior quota del Cash Out IT è destinata agli ambiti di **Vigilanza Banca d'Italia/BCE/EBA** (2,83%), seguiti a distanza da quelli per la Normativa **contabile/fiscale** (1,55%), per la Normativa **mercati finanziari** (1,33%) e per la **Trasparenza** (1,06%), mentre i rimanenti ambiti hanno assorbito quote inferiori all'1%.



**LA COMPLIANCE NELLE BANCHE**

**La Funzione**

La Compliance ha la missione di **assicurare l'adeguatezza delle procedure interne a prevenire la violazione di norme di etero regolamentazione** applicabili all'insieme dei processi aziendali.

La funzione assiste gli Organi Sociali e le Unità Organizzative nel perseguimento degli obiettivi in materia di conformità, promuovendo la diffusione di una **cultura aziendale** improntata ai principi di onestà, correttezza e rispetto dello spirito e della lettera delle norme.

**La Funzione presiede pertanto il rischio di non conformità alle norme**, vale a dire *il rischio di incorrere in sanzioni giudiziarie o amministrative, perdite finanziarie rilevanti o danni di reputazione in conseguenza di violazioni di norme imperative (legge, regolamenti) ovvero di autoregolamentazione (ad es. statuti, codici di condotta, codici di autodisciplina).*

Il **Rischio di non conformità** è dunque definito dalla contemporanea esistenza di due condizioni:

- presenza di violazioni di norme imperative (leggi o regolamenti), di settore (codici di autodisciplina, standard provenienti da organismi di settore, Best Practice) o interne (statuti, codici di condotta, procedure);
- sanzioni giudiziarie o amministrative, perdite finanziarie rilevanti o danni di reputazione conseguenti ai comportamenti di cui sopra.

Vi sono connessioni tra il **rischio di non conformità** e i **rischi operativi** e **reputazionali**. Infatti, il rischio di non conformità è riconducibile al **rischio operativo** per la parte relativa alle perdite, mentre è riconducibile al **rischio reputazionale** per i danni di reputazione.

## Principi e modalità

Le Disposizioni di Vigilanza (Banca d'Italia, Circolare n. 285/2013) richiedono un modello basato sulle peculiarità di ciascun intermediario in termini di dimensioni, caratteristiche individuali, complessità operativa, secondo i principi di:

- **proporzionalità;**
- **gradualità.**

La funzione di conformità alle norme presiede, secondo un **approccio Risk Based**, alla gestione del rischio di non conformità con riguardo a tutta l'attività aziendale, verificando che le procedure interne siano adeguate a prevenire tale rischio.

Per le norme più rilevanti ai fini del rischio di non conformità, quali quelle che riguardano l'esercizio dell'attività bancaria e di intermediazione, la gestione dei conflitti di interesse, la trasparenza nei confronti della clientela e, più in generale, la disciplina posta a tutela del consumatore, e per quelle norme per cui non siano già previste forme di presidio specializzato all'interno della banca, **la funzione è direttamente responsabile della gestione del rischio di non conformità.**

Con riferimento ad altre normative, per le quali siano già previste forme specifiche di **presidio specializzato** (ad es. normativa sulla sicurezza sul lavoro e in materia di trattamento dei dati personali), la banca può **graduare i compiti della Compliance**. Di tali compiti è **comunque responsabile**, in collaborazione con le funzioni specialistiche incaricate, almeno della definizione delle metodologie di valutazione del rischio di non conformità e dell'individuazione delle relative procedure, e procede alla verifica dell'adeguatezza delle procedure medesime a prevenire il rischio di non conformità.

Sotto il profilo organizzativo, tenuto conto dei molteplici profili professionali richiesti per l'espletamento di tali adempimenti, le varie fasi in cui si articola l'attività della funzione di conformità alle norme possono essere affidate a **risorse appartenenti ad altre strutture organizzative** (ad 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.

## Il processo di Compliance

NTT DATA è in grado di offrire supporto agli intermediari finanziari in relazione a tutte le fasi del processo di Compliance.



In particolare, NTT DATA opera per:

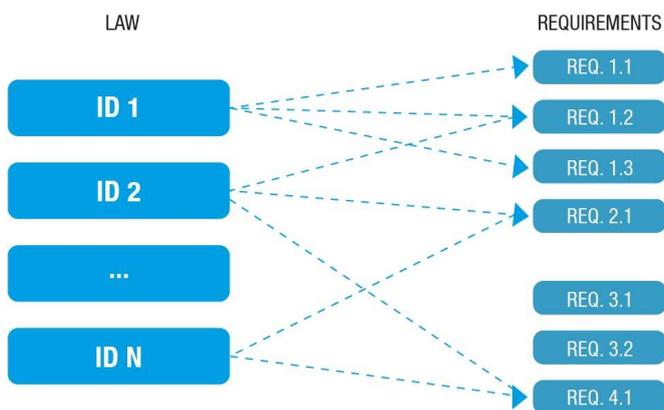
- fornire indicazioni inerenti le novità normative aventi impatto sulla banca/società;
- prestare consulenza ed assistenza nell'interpretazione delle norme e in tutti gli ambiti in cui assume rilevanza il rischio di non conformità;
- valutare preventivamente la conformità alla normativa esterna, al fine di verificarne gli impatti e stabilire le necessarie azioni da intraprendere per garantire la conformità (Gap Analysis);
- verificare l'adeguatezza dei processi e delle procedure, al fine di valutare se i medesimi risultino adeguatamente definiti, disciplinati e conformi alla normativa (Risk Assessment);
- formare le unità operative e interessate per materia, fornendo linee guida per il recepimento delle evoluzioni normative;
- svolgere verifiche settoriali e/o tematiche in considerazione di espressi obblighi normativi (es. verifiche MiFID, remunerazioni, trasparenza, conflitti di interesse, ecc.) e, più in generale, in tutti gli ambiti su cui si dovesse ritenere necessario ed opportuno lo svolgimento di specifici controlli, sulla base delle risultanze dell'attività di Risk Assessment.

## APPROCCIO NTT DATA

NTT DATA unisce la conoscenza dei processi aziendali di Business, maturata presso importanti intermediari finanziari (in particolare su normative di settore in ambito pagamenti, Privacy, trasparenza, etc.), a quella dei processi IT e alle esperienze maturate in qualità di System Integrator.

Queste caratteristiche le consentono di supportare i clienti in modo efficace ed efficiente, con un approccio E2E, favorendo:

- analisi analitiche;
- valutazioni di dettaglio;
- proposte di intervento/raccomandazioni più puntuali.



NTT DATA supporta pertanto le funzioni di Compliance nelle analisi delle normative per l'identificazione di requisiti sia di Business che IT.

Il mix di competenze espresse da NTT DATA favorisce la stesura dei requisiti, che vanno oltre l'approccio "a silos" che contraddistingue ancora alcuni ambiti operativi, favorendo invece la collaborazione e lo scambio tra Business e IT.

In concreto, nel caso di **nuove normative**, NTT DATA definisce i requisiti normativi e conduce le conseguenti attività di Assessment, accertando i Gap rilevati in ambito organizzativo, di processo e sui sistemi informativi.

Analizzata la situazione corrente, durante l'Assessment di Business e IT, l'attività prosegue con la definizione degli interventi, suddividendoli in specifici cantieri operativi e differenziati per aree tematiche.

In alcuni casi, questa attività di Compliance si tramuta in un supporto all'attività di redazione dei requisiti di Business e IT. In queste circostanze, una volta

analizzati e classificati i requisiti di Business e IT, vengono svolti approfondimenti ad hoc per le singole aree tematiche individuate.

NTT DATA dispone di un proprio strumento per consentire la valutazione dei livelli di conformità alla norma, favorendo la definizione degli interventi per l'adeguamento mediante una sistematica comparazione, requisito per requisito, tra la nuova normativa e quella attualmente in vigore e applicata (ad es. PSD vs PSD2), in modo da identificare i singoli punti distintivi oggetto di modifica da parte del legislatore.

Nel caso di **normative consolidate**, NTT DATA può predisporre e/o eseguire:

- test di impianto e funzionamento, volti a verificare l'aderenza della normativa interna alle leggi in vigore nazionali, europee o agli standard internazionali;
- verifiche di Compliance, con l'obiettivo di analizzare la reale aderenza dei processi e sistemi in uso presso l'azienda rispetto alle normative interne esistenti.

## Key Takeaways

- Gli intermediari sono soggetti ad un **sistema regolatorio sempre più ampio** e complesso in ambito europeo e internazionale.
- **L'internazionalizzazione** del contesto regolamentare fa sì che vi siano parità di condizioni e si evitino arbitraggi normativi.
- La poca attenzione alla Compliance ha portato a **Crack finanziari** senza precedenti.
- Il sistema dei controlli interni e, in particolare, la Compliance, svolgono un ruolo chiave nella creazione di **valore per l'impresa**.
- La spesa per Compliance sale al 13,8% del Cash Out IT. La Compliance si conferma una **voce di spesa consistente**, con impatto sulle Funzioni IT e di Business.
- **NTT DATA** non è solo un **centro di eccellenza** in attività di sviluppo e/o integrazione IT ma rappresenta un punto di riferimento anche per attività di **adeguamento normativo** per tutti gli aspetti di People, Process e System.

## Contatti



**Chiara Scattone**  
Associate Manager  
Consulting

*Responsabile della Practice di Consulting Compliance e Audit, lavoro ormai da circa 15 anni nell'ambito bancario e finanziario, occupandomi di questioni di carattere normativo e di Compliance, nonché di processi e del sistema di controlli interni. Il tema della Compliance e dei controlli nel mondo bancario è da sempre oggetto di conflitto e di dibattito, pur rimanendo di primissima importanza per la sopravvivenza dell'azienda e per la creazione di valore, anche sociale.*



**Andrea Viola**  
Senior Consultant  
Consulting

*In 7 anni di esperienza nella consulenza in ambito Finance, ho avuto modo di svolgere attività sia di Business che IT. Ho svolto diversi progetti in ambito Compliance e Audit su attività di pianificazione, Assessment e verifiche ex post, con riferimento ad alcune delle principali tematiche normative, quali i servizi di pagamento (PSD2), antiriciclaggio, servizi di investimento (MiFID), trasparenza e Privacy (GDPR).*

### Fonti:

<sup>1</sup> Rilevazione sull'IT nel sistema bancario italiano.

<sup>2</sup> Banca d'Italia, Circolare n. 285/2013.

## NTT DATA

NTT DATA Italia è parte della multinazionale giapponese NTT DATA, uno dei principali player a livello mondiale nell'ambito della Consulenza e dei Servizi IT. Digitale, Consulenza, Cyber Security e System Integration sono solo alcune delle principali linee di business. La nostra missione è creare valore per i nostri clienti attraverso l'innovazione. NTT DATA conta su una presenza globale in oltre 50 paesi, 110.000 professionisti e una rete internazionale di centri di ricerca e sviluppo a Tokyo, Palo Alto e Cosenza. NTT DATA è presente in Italia con oltre 3000 dipendenti e 8 sedi: Milano, Roma, Torino, Genova, Treviso, Pisa, Napoli e Cosenza. [www.nttdata.com/it](http://www.nttdata.com/it)