AIDA

associazione internazionale di diritto delle assicurazioni

XLIII Congresso della Sezione
Piemonte - Valle d'Aosta

IL SISTEMA DEI CONTROLLI INTERNI: ASSICURAZIONI E BANCHE

in collaborazione con IRSA
Istituto per la Ricerca e lo Sviluppo delle Assicurazioni

CAMERA DI COMMERCIO
INDUSTRIA ARTIGIANATO E AGRICOLTURA
DI TORINO

Torino, 26 novembre 2009
Centro Congressi Torino Incontra


AIDA
Sezione Piemonte - Valle d'Aosta

INDICE

INTRODUZIONE

IL SISTEMA DEI CONTROLLI INTERNI: PROFILI GENERALI

Prof. Avv. Paolo Montalenti
Ordinario di Diritto Commerciale
Università degli Studi di Torino
Presidente Sezione Piemonte - Valle d'Aosta AIDA

SOMMARIO:

1. *Centralità del sistema dei controlli interni per una buona* corporate governance*.*

La crisi finanziaria mondiale ha focalizzato l'attenzione di istituzioni, operatori, esperti e cittadini sulla banca, la finanza, i mercati finanziari, i riflessi sull'economia reale. I temi della *corporate governance* rischiano di sfumare in secondo piano. Ma agli interventi di emergenza dovranno seguire le scelte regolatorie di lungo periodo per riequilibrare il sistema. In questa prospettiva il tema dei *controlli interni*, in particolare per le società quotate, mantiene un ruolo centrale, che non deve essere offuscato.

Si può infatti osservare che l'attenzione dei regolatori e delle diverse istanze internazionali per l'elaborazione di proposte relative all'introduzione dei cd. *global legal standard*, o di *European legal standard*, si è concentrata sul tema della vigilanza e sulle ipotesi di coordinamento tra organi nazionali e/o di istituzione di strumenti di controllo sovranazionale sul funzionamento dei mercati finanziari.

Tuttavia, ad oggi, siamo ancora ai passi iniziali e non si intravedono a breve iniziative concrete di particolare incisività.

Se è vero che, grazie ai plurimi interventi di *bailout* delle banche, attuati nei singoli Paesi con strumenti giuridici diversi (dai prestiti agevolati all'ingresso nel capitale sociale sino al vero e proprio salvataggio), al fine di evitare il fallimento del sistema creditizio mondiale, la fase più drammatica della crisi

pare superata. E' vero anche però che la radice profonda della crisi – e cioè l'emissione di titoli relativamente ai quali erano vieppiù incerti sia il contenuto del diritto incorporato sia la capacità effettiva di rimborso dell'emittente – non è stata ancora estirpata. Significativa la circostanza che ad oggi paiono essere ancora in circolazione circa 1,4 miliardi di dollari di titoli cosiddetti "tossici".

Se dunque gli interventi sulla stabilità delle banche, con l'imposizione di più rigorosi coefficienti di patrimonializzazione e di limiti all'impiego della leva finanziaria, hanno prodotto immediati effetti di stabilizzazione del mercato, se l'introduzione di criteri più stringenti per la verifica del merito di credito ha migliorato il controllo sull'indebitamento del sistema industriale rispetto al sistema creditizio, è anche vero, tuttavia, che il controllo sul corretto rapporto tra impresa e finanziamento attraverso il mercato finanziario è, parrebbe, ancora da costruire.

Significativo il fatto che, considerato il fallimento delle certificazioni delle società di *rating*, per il noto intreccio di conflitti di interessi, assistiamo, in questo periodo, ad un grande successo dei *no rating bonds*. Lo strumento non deve essere valutato negativamente *per se*, in quanto può anche rappresentare un fisiologico apporto di mezzi freschi all'impresa sempreché la fiducia sulla bontà dei *business plan*, sulla solidità della società e sulla capacità di ripagamento del debito sia ben riposta e l'affidamento riposi dunque su dati e elementi attendibili.

Da tutto quanto sopra consegue che il buon funzionamento del mercato finanziario si fonda anzitutto su una buona *corporate governance* interna degli emittenti, su un rapporto equilibrato tra impresa (e cioè tra attività e programmazione strategica) e finanza, anziché su strumenti e operazioni meramente speculative fondate sull'irresponsabilità a catena dei vari intermediari e sulla traslazione del rischio soltanto sull'utilizzatore finale.

In altre parole l'anomalia del sistema si è cristallizzata nella circostanza che l'emittente ritiene assolto il proprio dovere di diligenza perché ha ottenuto la certificazione del revisore e la valutazione positiva della società di *rating*, l'intermediario collocatore perché ha fatto affidamento su certificazione dei revisori e *rating*, i fondi perché hanno confidato sulla veridicità delle attestazioni dei primi, gli intermediari finali perché non hanno assunto direttamente alcuna responsabilità sulla consistenza del titolo: i diversi soggetti del ciclo dell'intermediazione finanziaria ottengono finanza o commissioni; il rischio grava sull'investitore finale.

In conclusione, dunque, se la gestione dell'impresa non è condotta con effettivi criteri di legalità e correttezza amministrativa, se i piani strategici non sono fondati su elementi reali e realistici, se il rapporto con le fonti di finanziamento non è equilibrato, i rischi di *default* sul mercato finanziario crescono vertiginosamente. E pertanto l'istituzione di un sistema efficace di controlli interni[1] diventa il primo indispensabile presidio "anticipato" per il corretto funzionamento del sistema industriale e finanziario.

[1] Segnalo alcuni lavori in cui ho trattato il tema degli assetti organizzativi e del sistema dei controlli interni: *Consiglio di amministrazione e organi delegati: flussi informativi e responsabilità*, in *Le Società*, 1998, 899 ss; Corporate Governance, *consiglio di amministrazione, sistemi di controllo interno: spunti per una riflessione*, in *Riv. soc.*, 2002, 803 ss; *L'amministrazione sociale dal testo unico alla riforma del diritto societario*, in *AA.VV., La riforma del diritto societario*, Giuffrè, Milano, 2003, 65 ss.; *La società quotata*, in *Trattato di diritto commerciale*, diretto da G. Cottino, vol. IV, t. 2, Cedam, 2004, 227 ss.; *La responsabilità degli amministratori nell'impresa globalizzata*, in *Giur.*

Ma la costruzione di un sistema che sia al contempo efficiente al fine della prevenzione dei rischi e non eccessivamente invasivo nella operatività gestionale, nonché armonicamente costruito sia per ripartizione tra organi sia per coordinamento tra gli stessi, è una sfida di estrema difficoltà. L'evoluzione spesso caotica e non lineare degli istituti relativi al controllo nel nostro ordinamento ne è testimonianza.

comm., I, 2005, 435 ss; *Il sistema dei controlli interni nelle società di capitali*, in *Le Società*, 2005, 294 ss; *Gli obblighi di vigilanza nel quadro dei principi generali sulla responsabilità degli amministratori di società per azioni*, in *Liber amicorum Gian Franco Campobasso*, Utet, Torino, 2006, Vol. 2, 832 ss; *Sui controlli societari: funzioni da semplificare*, in *Il Sole 24-ore*, 27 novembre 2007.

Si veda ancora da ultimo *Organismo di vigilanza 231 e ordinamento societario: spunti di riflessione sul sistema dei controlli*, in *Giur. comm.*, 2009, 643 ss.

2. Il "reticolo" dei controlli.

Nell'ordinamento italiano gli interventi in materia di controlli, dalla c.d. "miniriforma delle società per azioni" (L. 216/1974) alla legge per la tutela del risparmio (L. 262/2005), sono stati numerosi ed anche correlati al contesto europeo e internazionale. Significativo, altresì, l'apporto del Codice di Autodisciplina. Ma il susseguirsi di plurimi interventi legislativi ha creato più che un sistema, un "reticolo" di controllori e una "sommatoria" di tipologie di controlli che suscitano non poche perplessità. E' stato davvero raggiunto un punto di equilibrio tra necessità di prevenire (irregolarità contabili e fiscali, conflitti di interessi, abusi di maggioranza, false informazioni al mercato ecc.) e rischio di imporre alle imprese vincoli o costi eccessivi? Ed ancora: si sono create sinergie positive o si sono prodotte invece sovrapposizioni e duplicazioni?
Il convincimento che si sta consolidando tra operatori ed esperti è oggi nel senso che il sistema richieda una significativa semplificazione e soprattutto una chiarificazione di ruoli e funzioni allo scopo di evitare gli eccessi di sovrapposizioni di competenze.
L'*overlapping* più che stimolare cooperazioni virtuose rischia di produrre "conflitti di competenza negativa".

3. Le diverse tipologie di controlli.

Il compito non è facile. La stessa espressione "controllo" è ormai difficile da decifrare, perché è utilizzata per indicare concetti e funzioni assai diversi: dall'influenza dominante su di una società controllata alla valutazione di merito delle scelte gestionali; dalla verifica di legalità al giudizio di correttezza istruttoria e procedurale; dal controllo preventivo sull'idoneità delle procedure e degli assetti organizzativi adottati al controllo successivo sul concreto funzionamento degli stessi; dalla vigilanza diretta sull'operatività delle funzioni d'impresa alla vigilanza indiretta effettuata attraverso l'assunzione di informazioni. Le categorie stesse – controllo di legalità, di legalità sostanziale, di correttezza contabile, di correttezza amministrativa, di *efficacia*, di efficienza, di merito – devono dunque essere rimeditate.
Pare cioè necessaria una rivisitazione sistematica delle partizioni concettuali tradizionali (controllo di legalità, controllo di legalità sostanziale, controllo di merito).
Il *controllo di merito* spetta ai soci nei confronti del consiglio di amministrazione ma anche a quest'ultimo, come *plenum*, nei confronti dei delegati. Si tratta di un controllo in forma di *potere di indirizzo, di condizionamento, di opposizione* (con la revoca dell'amministratore o della delega) non già di sorveglianza e verifica in funzione di eventuali iniziative sul terreno della responsabilità.
Infatti il *merito* della gestione, e cioè il contenuto delle scelte manageriali è assistito – il punto è pacifico anche nel nostro ordinamento – dalla c.d. *business judgement rule*: le operazioni gestorie degli amministratori non sono sindacabili, né dal collegio sindacale, né dal comitato *audit*, né dai revisori, né dal giudice se non in caso di *manifesta irrazionalità* oppure di *palese assenza*

di procedimenti di valutazione **dei profili economici, finanziari, tecnici dell'operazione.**
L'altro profilo del controllo è il *controllo sull'adeguatezza degli assetti organizzativi e sul rispetto dei principi di corretta amministrazione* (cfr. art. 2381, comma 3°, art. 2403, comma 1°, art. 149, comma 1° t.u.f.; art. 149, comma 4-*bis* e comma 4-*ter*, t.u.f.), controllo affidato, con compiti differenziati, sia all'organo di gestione come *plenum* sia all'organo di controllo a cui si aggiunge il comitato *audit*.
In conclusione la partizione pare oggi potersi schematizzare in *(i) controllo di merito (ii) controllo di adeguatezza organizzativa (iii) controllo di correttezza gestionale (iv) controllo di legalità.*
Ed è allora nell'ambito di questo paradigma concettuale che l'assegnazione delle funzioni ad uno più organi deve essere ripensata, interrogandosi se (i) debba trattarsi di competenza da assegnarsi ad un unico organo oppure (ii) da imputarsi a più organi in un'ottica "policentrica" (iii) oppure invece da razionalizzarsi con più precise attribuzioni di competenze e con specifiche regole di coordinamento.

4. Controlli diretti e controlli indiretti un punto critico.

Dall'esame della complessa e articolata disciplina del "reticolo" dei controlli, oltre ai profili critici già analizzati, derivanti, in particolare, dall'eccesso di competenze concorrenti e dalle vere e proprie sovrapposizioni di funzioni, si deve altresì segnalare che il "sistema" si fonda ormai sulla netta prevalenza dei controlli indiretti sui controlli diretti.
Ciò deriva, è indubbio, anche dalla oggettiva complessità della grande impresa moderna nella quale il potere, sia pure gerarchicamente organizzato, è fortemente articolato e diffuso, per cui ben si può affermare che anche la "direzione suprema degli affari" si estrinseca, da un lato, in linee direttrici generali, dall'altro nella verifica dell'efficienza e dell'efficacia dell'azione di altri soggetti (organi delegati, alta dirigenza, *managers*, responsabili di settore, amministratori di società controllate ecc.).
Analogo fenomeno si verifica nelle procedure di controllo per cui molte istanze procedono non già ad atti di ispezione e di vigilanza *diretta* bensì ad atti di accertamento presso le "istanze inferiori" volte a verificare il corretto svolgimento delle procedure di controllo e l'adeguatezza degli assetti organizzativi di cui le procedure stesse sono parti integranti.
L'amministratore delegato riceve i *report* del preposto al sistema di controllo interno, questi le informazioni dai propri sottoposti, il consiglio di amministrazione – per effettuare la valutazione di adeguatezza – le "attestazioni di conformità" dagli organi delegati, "validate" dal preposto al controllo interno e dal collegio sindacale (che sugli assetti organizzativi deve vigilare con atti di ispezione sì ma, anch'esso, prevalentemente, attraverso un'attività di sorveglianza indiretta).
In conclusione il sistema si presenta come una sorta di "piramide rovesciata" che ricomprende l'insieme delle funzioni di controllo indiretto e che poggia sul vertice, anch'esso rovesciato, dei controlli diretti su cui si regge, in definitiva, l'intera architettura.

Difficile dire se la materia debba essere in qualche modo regolata in via normativa: certo è però che il sistema presenta una evidente fragilità, in quanto se i controlli diretti (i cosiddetti "controlli di linea") dovessero fallire, l'intero sistema dei controlli si troverebbe ad essere inefficace. In altre parole: i controlli indiretti, proprio perché molteplici articolati e diffusi, contengono in sé maggiori risorse di *feedback* e quindi di "autocorrezione"; i controlli diretti, se non opportunamente presidiati, ad esempio con l'istituzione di "controllori dei controllori", i quali verifichino, periodicamente ma sistematicamente e direttamente, che i controlli diretti siano effettuati e che siano effettuati in modo adeguato, rischiano di minare la solidità e l'efficacia dell'intero sistema.
Un problema che la sovrapposizione di funzioni di controllo indiretto, di cui si è detto, può certamente acuire.

5. Il collegio sindacale.

Nella disciplina del Codice di commercio (artt. 183 e 184) e del Codice civile del 1942 la funzione del collegio sindacale poteva schematizzarsi secondo la triplice direttrice del controllo dell'amministrazione, della vigilanza sull'osservanza della legge e dell'atto costitutivo e del controllo contabile. Già in allora si pose la delicata questione, che sarebbe divenuta a dir poco annosa, relativa alla qualificazione dei poteri-doveri dell'organo di controllo e più precisamente l'interrogativo se il controllo sulla gestione dovesse configurarsi come mero controllo di legalità oppure anche di merito o se dovesse attestarsi sul crinale intermedio della legittimità sostanziale.
Venendo alla disciplina delle società quotate si può osservare come già il d.p.r. 31 marzo 1975, n. 186, in attuazione della L. 216/1974 abbia attribuito le funzioni di controllo contabile ad una società di revisione iscritta all'albo speciale; rimase però ancora aperto il problema se e, in caso affermativo, in quale misura, residuassero delle competenze in materia al collegio sindacale.
Il Testo Unico della Finanza sembrerebbe aver chiarito il tema là dove ha precisato che il collegio sindacale ha un dovere di vigilanza sul sistema amministrativo e contabile; vero è tuttavia che l'opinione prevalente in dottrina (che anche personalmente ho sostenuto) il collegio sindacale mantiene anche una funzione di controllo sintetico sulla correttezza contabile. Lo si evince da molteplici indici normativi, in particolare dalla disposizione (art. 153, comma 2° t.u.f.) che attribuisce al collegio sindacale il potere di fare proposte all'assemblea in ordine al bilancio e alla sua approvazione (più che dal generico rilievo che nella legge, del cui rispetto i sindaci sono garanti, rientrano anche le norme relative alla contabilità). Il legislatore ha opportunamente precisato che il collegio sindacale vigila anche sul rispetto dei principi di corretta amministrazione da intendersi, a mio avviso, come osservanza delle regole procedurali e sostanziali per una efficiente gestione dell'impresa, desumibili dalla prassi aziendale, particolarmente rilevanti in relazione ad operazioni societarie (acquisizioni, contratti di collaborazione commerciale, finanziamenti strutturati, ecc.) che assumono una complessità crescente nella realtà attuale dell'impresa.

A testimonianza della funzione anticipatrice della disciplina speciale (cioè della regolamentazione della società quotata) rispetto alla evoluzione del diritto comune, si può notare come con la riforma del diritto societario del 2003 la funzione dell'organo di vigilanza nella società azionaria "chiusa" sia stata sostanzialmente omologata a quella delle società aperte, ferma restando, nella prima, la possibilità di attribuire al collegio sindacale anche il controllo contabile.
Con la legge per la tutela del risparmio (L. 262/2005) al collegio sindacale di società quotata è stato attribuito altresì lo specifico compito di vigilare sulle modalità di concreta attuazione delle regole di governo societario previste dai codici di comportamento.
In materia, a ben vedere, molti problemi sono tuttora aperti.
In estrema sintesi a me pare che i nodi ancora da sciogliere siano i seguenti.
In primo luogo il permanere di un sia pur sintetico dovere di verifica contabile lascia un margine di incertezza su quale sia il grado di profondità dell'attività di vigilanza esigibile dai sindaci e su quale sia il dovere di spontanea attivazione in materia da parte del collegio stesso.
In secondo luogo pare difficile negare che il confine tra correttezza gestionale e controllo di merito è estremamente labile. Vero è che la correttezza può circoscriversi alla verifica della adozione di procedure, informative, istruttorie, deliberative, analiticamente articolate, strutturalmente precise e pertanto affidabili, mentre il merito attiene più precisamente alla opportunità e convenienza delle scelte. Vero è anche però che la *business judgement rule*, e cioè l'insindacabilità nel merito delle decisioni amministrative a meno che si rivelino manifestamente irrazionali, fa sì che la linea di demarcazione tra la valutazione della ofelimità di un'operazione economica e lo *screening* di correttezza si riveli, soprattutto in assenza di una precisa presa di posizione del legislatore, non particolarmente agevole.
E questa difficoltà dell'*actio finium regundorum* è acuita dalla introduzione, in via di autodisciplina, del Comitato *Audit*.

6. Il Comitato Audit.

Su ispirazione del diritto societario e finanziario statunitense e con un significativo parallelismo con le tendenze internazionali in materia di *corporate governance*, il Codice di Autodisciplina ha introdotto l'istituto degli amministratori indipendenti. Nel quadro della valorizzazione del loro ruolo, in particolare in relazione al sistema di controllo interno, ha previsto la istituzione di un Comitato per il controllo interno, composto esclusivamente da amministratori indipendenti, di cui almeno uno in possesso di un'adeguata esperienza in materia contabile e finanziaria. Adesso sono attribuibili compiti specifici di valutazione in materia di utilizzo dei principi contabili, di formulazione di pareri sui principali rischi aziendali e sul sistema di controllo interno, di disamina del piano di lavoro preparato dai preposti, di valutazione delle proposte delle società di revisione per l'affidamento dell'incarico e altri ulteriori compiti eventualmente affidati ad esso dal consiglio di amministrazione.

In particolare sono poi attribuiti al comitato di controllo interno specifiche funzioni in materia di operazioni con interessi degli amministratori e di operazioni con parti correlate.
Anche con riferimento a questo organo autoregolamentare incerta è la soluzione in punto di qualificazione della funzione del comitato e della correlativa responsabilità.
Si può ricordare che, secondo un'opinione diffusa, il *Comitato Audit* avrebbe una mera funzione consultiva rispetto al consiglio di amministrazione e che detto organo, nell' esercizio di tale funzione, non si esponga ad una forma autonoma di responsabilità.
Questa ricostruzione non pare condivisibile, anche alla luce del dettato del nuovo art. 2392 c.c. La norma sancisce che gli amministratori devono adempiere ai propri doveri legali e statutari con la diligenza necessaria; essi sono solidalmente responsabili verso la società dei danni derivanti dall'inosservanza di tali doveri, a meno che si tratti di funzioni delegate o anche soltanto *in concreto attribuite ad uno* o *più amministratori.* In sintesi, da quest'ultimo inciso dell'art. 2392 c.c. pare doversi evincere un'ipotesi autonoma di responsabilità propria a carico di tutti gli amministratori a cui sia stato affidato in concreto un compito specifico.
Ritengo, quindi, diversamente da quanto ebbi a sostenere prima della riforma del diritto societario, che il *Comitato Audit*, sia pure limitatamente all'ambito disegnato dall'esercizio delle sue funzioni di controllo, di supporto, o istruttorie in materia contabile, si esponga ad una responsabilità propria, affine a quella di un organo delegato. È un punto che va meditato e chiarito, perché non è certamente marginale.
Particolarmente delicata è poi la questione dell'inquadramento dei rapporti tra collegio sindacale e Comitato *Audit*. Non è chi non veda che, sia in materia contabile sia in materia di correttezza gestionale, di là dal diverso grado di analiticità della individuazione delle rispettive funzioni (nelle norme di legge per il primo, nel Codice di Autodisciplina per il secondo), le contiguità, ma anche le vere e proprie sovrapposizioni, sono numerose.
Si pone allora l'interrogativo, a cui non è agevole fornire risposta sicura, se ciò dia luogo ad una virtuosa sinergia cooperativa nel quadro di un sistema che ebbi a definire come sistema policentrico oppure invece se non vi sia un rischio di conflitti di competenza, in particolare di conflitti di competenza negativi. In definitiva: sinergia positiva o tendenziale duplicazione?

7. L'organo di vigilanza.

Il d. lgs. 231/2001 ha, come è noto, disciplinato la responsabilità amministrativa della persona giuridica e, per quanto qui rileva, ha introdotto l'onere (o l'obbligo?) di istituire un modello di prevenzione dei reati e un organismo di vigilanza[2].
Sotto il primo profilo si pone il problema, a cui credo si debba fornire risposta positiva, se il modello rientri negli assetti organizzativi. Anche la giurisprudenza di merito ha accolto questa impostazione ritenendo sussistente la responsabilità civile degli amministratori per mancata adozione del modello. Da ciò discende che, anche in relazione al modello 231, si pone il problema di competenze convergenti o parallele non limitate cioè all'organismo di vigilanza ma estese al dirigente preposto, agli organi delegati – per l'attuazione – al Consiglio di Amministrazione – per la valutazione – al Collegio Sindacale – per la vigilanza – e al Comitato Audit – per i profili di correttezza.
In conclusione, un'intrecciarsi di funzioni e di controlli particolarmente fitto.
In secondo luogo, l'organismo di vigilanza è un vero e proprio *nomen* privo di una specifica disciplina. Incerte le regole sulla composizione, non disciplinata l'organizzazione della vigilanza nei gruppi, assente la regolamentazione dei rapporti tra organismo di vigilanza e organi societari di controllo: molti, dunque, i problemi aperti.
Alcune soluzioni possono essere individuate in via interpretativa. Come ho cercato di dimostrare in altra sede, la responsabilità non trascende il perimetro della singola società, ma ciò non esclude la rilevanza di una contemplazione nel modello dei rapporti di gruppo.
L'organismo di vigilanza non può essere qualificato come organo societario ma deve rispondere a requisiti di efficacia, competenza, imparzialità e indipendenza; ciò non toglie che la composizione mista di *inside* e di esterni può costituire un punto di equilibrio tra conoscenza dell'impresa e imparzialità di valutazione.
Nomina e revoca devono attribuirsi al Consiglio di Amministrazione, dubbio restando se, per quest'ultima, debba sussistere una giusta causa.
La funzione dell'ODV, infine, non è la replicazione dei poteri-doveri di tutti gli organi di controllo; esso non è investito di una sorta di potere di supervisione trasversale e di carattere generale su tutti i settori e le funzioni dell'organizzazione d'impresa che possano essere in qualche misura investiti da fatti di reato: tra poteri-doveri di controllo, estensione dell'area di questi e reati da prevenire, deve sussistere un nesso di correlazione stretto.
Ma la supplenza dell'interprete in presenza di una forte variabilità operativa della prassi, nonché di interventi non marginali diretti a colmare i vuoti normativi, paiono suggerire l'opportunità di una chiarificazione legislativa.

8. Il coordinamento tra gli organi di controllo: un problema aperto.

[2] Su questi argomenti mi permetto di rinviare al mio *Organismo di vigilanza 231 e ordinamento societario: spunti di riflessione sul sistema dei controlli*, cit. nonché al mio *Organismo di vigilanza 231 e gruppi di società*, in AGE, 2009, in corso di stampa.

L'intensificarsi e l'espandersi del "reticolo" dei controlli solleva, come si è detto, numerosi interrogativi. E' stato davvero raggiunto un punto di equilibrio tra necessità di prevenire e rischio di imporre alle imprese vincoli o costi eccessivi?
In effetti regole insufficienti in materia di controlli alterano il corretto funzionamento dei mercati ma regole eccessivamente severe rischiano di rivelarsi comunque inidonee ad impedire qualsiasi "devianza" e contemporaneamente in grado o di stimolarne l'elusione o di incidere negativamente sull' efficienza e la redditività dell'impresa: l'esperienza, oggi oggetto di rimeditazioni, del Sarbanes-Oxley Act è significativa.
Ed ancora: si sono create sinergie positive o prodotte invece sovrapposizioni o duplicazioni?
Gli operatori si chiedono, infine, come coordinare l'intero meccanismo (sindaci, revisori, amministratori indipendenti, amministratori di minoranza, *leading indipendent director*, comitato audit, responsabile dei documenti contabili, organismo di vigilanza, preposto al controllo interno .... ecc.). E il problema si acuisce nei settori vigilati - banche e assicurazioni - ove si aggiungono le norme speciali, primarie e secondarie, e le Istruzioni dell'Organo di vigilanza.
Nel settore assicurativo, ad esempio, si è espressamente affrontato il problema.
Infatti il Regolamento ISVAP (20 marzo 2008, n. 20), disciplina la materia con particolare analiticità, collegando strettamente – in materia di controlli interni, di componenti del sistema, di flussi informativi, di gestione dei rischi, di esternalizzazione – le regole aziendalistiche con i precetti normativi.
Di particolare interesse la nozione di "Alta Direzione", che getta un ponte tra diritto societario e diritto dell'impresa; la disciplina delle funzioni di controllo - revisione interna, *risk management* e *compliance* - di cui si individuano analiticamente le articolazioni operative; le disposizioni in materia di gruppo assicurativo.
Il regolamento affronta con una disposizione specifica (art. 17), il tema - di rilievo sistematico generale - del *coordinamento tra organi di controllo.*
La norma secondaria ora ricordata stabilisce infatti che «l'organo di controllo, la società di revisione, la funzione di revisione interna, il *risk management* e di *compliance,* l'organismo di vigilanza di cui al decreto legislativo 8 giugno 2001, n. 231, l'attuario incaricato e ogni altro organo o funzione a cui è attribuita una specifica funzione di controllo collaborano tra di loro, scambiandosi ogni informazione utile per l'espletamento dei rispettivi compiti.
L'organo amministrativo definisce e formalizza i collegamenti tra le varie funzioni a cui sono attribuiti compiti di controllo».
In realtà si tratta di una norma per così dire "ottimistica" che rinvia alla autonomia privata la soluzione di uno dei punti critici più delicati in materia di amministrazione e controllo, area del diritto societario in cui il legislatore, primario e secondario, è intervenuto con particolare intensità, ma che ora suscita in operatori ed interpreti il grave interrogativo se la pluralità di

istanze di controllo stimoli sinergie virtuose o produca invece inefficienti sovrapposizioni o duplicazioni.

9. Ipotesi di lavoro per una semplificazione.

Immaginare soluzioni non è semplice. Nel rivisitare la materia bisogna anche evitare di gettare a mare i risultati di un percorso lungo e complesso attraverso il quale il nostro legislatore ha voluto, peraltro in sintonia con l'evoluzione dei principali ordinamenti, costruire un sistema di controlli articolati e pervasivi di cui società e mercati certamente necessitano per il loro ordinato funzionamento. Si tratta allora di ipotizzare interventi correttivi e non totali inversioni di rotta. Una linea che potrebbe essere percorsa è quella, a mio parere, di individuare le vere e proprie duplicazioni che rischiano di creare, effettivamente, conflitti di competenza negativa.
Il compito non è facile.
Formulo sinteticamente alcune ipotesi per le *società quotate*, prescindendo, allo stato, dalla questione se i problemi debbano trovare una soluzione in via normativa, di autodisciplina o di interpretazione condivisa:

- ***(i)*** **circoscrivere il controllo del collegio sindacale al *controllo di legalità sostanziale,* escludendo espressamente il controllo sulla contabilità e sui bilanci, il controllo sul merito delle scelte[3], il controllo sulla correttezza della gestione;**
- ***(ii)*** **confermare l'attribuzione al consiglio di amministrazione come *plenum* della funzione di *controllo sul merito della gestione* da parte degli organi delegati;**
- ***(iii)*** **attribuire soltanto al comitato *audit* il *controllo sulla correttezza della gestione e sulla adeguatezza delle procedure interne;***
- ***(iv)*** **limitare, in materia di procedure, la funzione del dirigente preposto alla redazione dei documenti contabili societari alla predisposizione di *adeguate procedure amministrative e contabili per la formazione dei bilanci*;**
- ***(v)*** **affidare invece alla società di revisione, oltreché, ovviamente, il controllo dei conti, la *verifica di adeguatezza delle procedure stesse*;**
- ***(vi)*** **attribuire al sistema di controllo interno, la *verifica sul rispetto effettivo delle procedure amministrative e contabili* (oggi assegnato al dirigente preposto) e sulle procedure interne, in senso ampio;**
- ***(vii)*** **assegnare espressamente all'ODV poteri circoscritti alla *verifica delle sole procedure relative alla prevenzione degli specifici reati* che nella specifica società potrebbero essere compiuti, con esclusione delle competenze di controllo sulla sicurezza già affidate ai soggetti competenti ai sensi della L. 626/1996 e s.m.;**
- ***(viii)*** **nel modello dualistico si dovrebbe prevedere che lo statuto debba stabilire le funzioni di alta direzione attribuite al *consiglio di sorveglianza*, introdurre l'obbligo di istituire il *comitato audit***

[3] Controllo di merito che oggi deve invece ritenersi attribuito, quanto meno in termini di efficienza delle scelte, anche al collegio sindacale: cfr. P. MONTALENTI, *La società quotata*, cit., 258 ss. In senso analogo P. MARCHETTI, *Controllo e gestione nel sistema dualistico*, in AA.VV., *Sistema dualistico e* governance *bancaria*, a cura di P. Abbadessa e F. Cesarini, 2009, Giappichelli, Torino, 158.

nell'ambito di questo organo, statuire espressamente che i rapporti tra consiglio di gestione e consiglio di sorveglianza siano disciplinati da un regolamento interno.

Si tratta, come è ovvio, di ipotesi di lavoro su cui riflettere: ciò che è sicuro è che semplificazione e razionalizzazione sono esigenze da tutti avvertite come non più differibili.

RELAZIONI

I CONTROLLI INTERNI NEL SISTEMA ASSICURATIVO E BANCARIO: PROFILI GENERALI

Prof. Andrea Vicari
Associato di Diritto delle Assicurazioni
Università degli Studi di Milano

1. *Il sistema di controllo interno della disciplina bancaria e assicurativa*

Il sistema di controllo interno è comunemente definito come l'insieme delle regole, delle procedure e delle strutture organizzative volte a consentire, attraverso un adeguato processo di identificazione, gestione e monitoraggio dei principali rischi, una conduzione dell'impresa sana, corretta e coerente con gli obiettivi prefissati ([4]).
Il sistema di controllo interno è disciplinato sia dalla disciplina bancaria sia dalla disciplina assicurativa ([5]).
Desidero subito segnalare come entrambe queste normative considerino essenziale lo sviluppo del sistema del controllo interno come un presidio che si affianca al patrimonio di vigilanza nell'obiettivo di garantire la sana e prudente gestione della società.
Secondo la Banca d'Italia, "gli strumenti di vigilanza prudenziale, tipicamente i coefficienti patrimoniali, nell'imporre una dotazione di capitale minima per fronteggiare i rischi, propongono modelli di misurazione semplificati, non sufficienti da soli ad assicurare uno sviluppo equilibrato dell'impresa"; conseguentemente si avverte "l'esigenza di affiancare agli strumenti prudenziali di tipo quantitativo indicazioni volte a favorire la definizione nelle banche di un sistema dei controlli interni efficiente ed efficace" (Istruzioni di Vigilanza per le Banche, Tit. IV, Cap.11, Sez I, § 1).
Analogamente per l'Isvap "la disciplina sulle riserve tecniche e sugli investimenti degli attivi a copertura delle riserve tecniche, diretta a contemplare requisiti e vincoli patrimoniali per fronteggiare i rischi, calcolati in via semplificata, non è in grado da sola di assicurare uno sviluppo equilibrato dell'impresa"; è necessario "che tali strumenti prudenziali di tipo quantitativo siano affiancati da requisiti qualitativi di gestione che assicurino una adeguata *governance* ed efficienti sistemi di controllo interno" (così la Circolare 577/D del 30 dicembre 2005; nello stesso senso si veda ora la relazione al Regolamento Isvap n. 20).
Vorrei, però, anche evidenziare come il presidio rappresentato dal sistema dei controlli interni può non solo affiancare il patrimonio di vigilanza

[4] Cfr. tra i molti PRICEWATERHOUSECOOPERS (a cura di), *Il sistema di controllo interno. Un modello integrato di riferimento per la gestione dei rischi aziendali*, 3ª ed., Milano, 2004; G. D'ONZA, *Il sistema di controllo interno nella prospettiva del* risk management, Milano, 2008. Nella letteratura di diritto societario specialmente P. MONTALENTI, Corporate Governance, *consiglio di amministrazione, sistemi di controllo interno: spunti per una riflessione*, in *Riv. soc*., 2002, p. 803 ss.; ID., *Organismo di vigilanza e sistema dei controlli*, in *Giur. comm.*, 2009, I, p. 643 ss.
[5] Per il diritto bancario v. V. PESIC, *Il sistema dei controlli interni nella banca. Obiettivi manageriali ed esigenze di vigilanza per il governo dei rischi*, Roma, 2009; per il diritto assicurativo v. E. PARRETTA, *Controllo interno e assicurazioni. L'attività di* internal auditor *nel sistema di* governance *delle imprese assicuratrici*, Milano, 2007.

nell'obiettivo di garantire la sana e prudente gestione della società, ma anche – a certe condizioni – parzialmente sostituirlo. Un efficace sistema di controlli interni può consentire il contenimento degli obblighi di patrimonializzazione per le banche e le assicurazioni, con ricadute positive sia per gli azionisti in termini di remunerazione del loro investimento nella società, sia per i clienti nella prospettiva della riduzione del costo medio degli affidamenti e dei premi (a ciò dedicherò la prima parte del mio intervento: §§ 2-4).
Ove sia raggiunta tale dimostrazione, si potranno adottare conseguentemente delle precise scelte interpretative della disciplina in tema di sistema di controllo interno, volte a rafforzarlo e a renderlo più efficiente (su questo aspetto concentrerò la seconda parte dell'intervento: §§ 5-9).

2. *L'aumento dei rischi nel settore bancario e assicurativo: recenti tendenze*

Come è noto, negli ultimi anni tanto le banche quanto le assicurazioni hanno affiancato a quelle tradizionali attività nuove e più rischiose.
(i) Il fenomeno è decisamente vistoso per le banche che esercitano attività finanziarie (ricordo incidentalmente che in Europa, a partire dal 2005, le banche svolgono in misura prevalente attività finanziarie rispetto all'attività bancaria tradizionale ([6])).
L'esercizio di tali attività ha incrementato (in particolare ed in via di semplificazione) il rischio operativo, corrispondente al rischio generato dall'esercizio di attività finanziaria diverso da quello di mercato e di controparte, comprensivo di quello connesso all'"innovazione finanziaria" ed all'"introduzione di nuovi prodotti, attività, processi e sistemi". La disciplina diretta a contenere questo rischio (Circolare della Banca d'Italia 263/2006, Tit. II, Cap. 5) richiede alle banche di mantenere genericamente (salve regole diverse per le banche di maggiori dimensioni e per attività particolari) un ammontare di patrimonio di vigilanza pari al quindici per cento del margine di intermediazione medio degli ultimi tre anni.
La scelta del Comitato di Basilea, e poi della Banca d'Italia (tendenzialmente più concentrate su altre tipologie di rischi) di non specificare un vero e proprio approccio per la stima del rischio di operativo, limitandosi a specificare alcuni requisiti minimi, è guidata, come è stato fatto osservare, da due obiettivi: in primo luogo, si prende atto che lo stato dell'arte in materia di modelli per tale tipologia di rischio è ancora incompleto ed in rapida evoluzione; in secondo luogo, l'indicazione di un architettura di massima, aperta al recepimento di possibili innovazioni metodologiche, dovrebbe funzionare come incentivo per le banche ad investire in nuovi strumenti per la misurazione del rischio operativo, senza sentirsi vincolate da alcun modello specifico ([7]).
(ii) L'aumento dei rischi è, tuttavia, evidente anche per le società assicurative, che hanno avviato negli ultimi anni nuove iniziative tanto nel ramo danni (ad esempio il collocamento delle polizze *long term care*), quanto, soprattutto,

[6] Cfr. F. PIEROBON, *Evoluzione dell'attività bancaria e crisi finanziaria*, in AA. VV., *Oltre lo shock. Quale stabilità per i mercati finanziari*, Milano, 2009, p. 77 ss.
[7] Cfr. A. RESTI, *Il nuovo accordo di Basilea sul capitale: genesi, contenuti, impatti*, 2005, reperibile sul sito www.carefin.it, p. 29.

nel ramo vita (mi riferisco, evidentemente, alle polizze a contenuto finanziario dei rami vita III e V, anche in relazione ai nuovi obblighi di trasparenza e di valutazione dell'adeguatezza e appropriatezza della clientela imposti dalla più recente disciplina Consob e Isvap).
Nuovi rischi nel settore assicurativo si riscontrano, tuttavia, oltre che dal lato della gestione tecnica, dal lato della gestione finanziaria (e cioè degli investimenti degli attivi a copertura delle riserve tecniche). In questo senso meritano di essere anzitutto ricordati i provvedimenti Isvap 297 del 1996 e 981/G del 1998, che hanno consentito alle imprese di investire in strumenti finanziari derivati (tali discipline impongono una serie di requisiti organizzativi che l'impresa deve possedere per operare in derivati, a fianco di limiti di carattere generale e specifico con riferimento all'utilizzo ed alla valutazione di tali prodotti).
Con il provvedimento Isvap 2530/2007 sono poi stati autorizzati gli investimenti degli attivi a copertura delle riserve tecniche, tra l'altro, in fondi di *private equity* e in *hedge fund*, con il limite del 5% delle riserve tecniche (e dell'1% verso il singolo fondo; non sono, peraltro, previste norme specifiche in tema di strutture particolari che l'impresa assicurativa deve organizzare per effettuare tali tipologie di investimento, come per i derivati).
In prospettiva, la proposta di direttiva di Solvency 2 supera i limiti quantitativi per gli investimenti degli attivi a copertura delle riserve tecniche (attualmente imposti dai Provvedimenti Isvap n. 147 e 148 del 1996) e recepisce, come noto, il *prudent person principle*, che obbliga le imprese, nella scelta degli attivi, al rispetto di principi generali di sicurezza, liquidità, redditività, diversificazione del portafoglio, ma senza che siano imposti – salvo casi eccezionali e su basi comunque temporanee – precisi limiti quantitativi agli attivi detenibili (emblematico risulta l'art. 131, rubricato "*freedom of investment*").
(iii) Infine, va ricordato come le disposizioni di recepimento della disciplina di Basilea 2 (e in prospettiva la proposta di direttiva Solvency 2) riconoscono per ciascuna banca ed assicurazione la possibilità (e la responsabilità) di definire il proprio profilo di rischio e di commisurare ad esso i mezzi patrimoniali necessari, consentendo alle banche e alle assicurazioni più evolute di avvalersi di metodi avanzati di misurazione dei rischi (ICAAP, ORSA).

3. *Proposte di contenimento dei rischi mediante aumento degli obblighi di capitalizzazione*

A fronte dei rischi generati dalle nuove attività esercitate dalle banche e dalle assicurazioni e dagli spazi di autonomia gestionale aperti dalle nuove discipline, una diffusa opinione ritiene che l'attuale disciplina di Basilea 2 (e in prospettiva di Solvency 2) vada integrata con ulteriori norme (o interpretata con letture della regolamentazione) orientate a rafforzare gli obblighi di capitalizzazione delle banche e delle assicurazioni (per esemplificare, il rischio operativo ed il rischio di liquidità dovrebbero essere coperti con ulteriori presidi patrimoniali; dovrebbero essere applicate in modo particolarmente rigoroso la norme che facoltizzano le autorità di

vigilanza a richiedere alle banche e alle assicurazioni di detenere un patrimonio superiore a quello minimo regolamentare; etc.) ([8]).
Questo approccio accentua l'enfasi sull'adeguatezza del patrimonio di vigilanza come principale strumento idoneo a tutelare – in via preventiva ed astratta – la sana e prudente gestione della società. L'idea di fondo è quella per cui è opportuno che le banche e le assicurazioni si dotino di un ampio "cuscino" di patrimonio per fronteggiare, a prescindere da rischi specificamente individuati, rischi generici e non esattamente noti *a priori* ([9]).
Per converso, questa impostazione tende a valutare con un certo scetticismo il diverso approccio che valorizza, più che i vincoli patrimoniali, la costante revisione – principalmente *ex post* e in concreto – da parte delle autorità di vigilanza (e in prospettiva del mercato) delle specifiche attività delle banche e delle assicurazioni e che, conseguentemente, privilegia tecniche regolamentari orientate soprattutto ad assicurare l'adeguatezza e l'integrità dei sistemi di *corporate governance* e di controllo interno della singola banca e assicurazione.
Alla visione "patrimonialistica" può replicarsi, tuttavia, che una disciplina che imponga presidi di patrimonio senza che sia specificamente individuato quali rischi questo sia destinato a coprire e l'ammontare presumibile di tali rischi può rivelarsi inadeguata ed inefficiente. Viene, infatti, fatto notare che molte delle tipologie di rischi connesse all'esercizio dell'attività finanziaria non possono essere agevolmente mitigate né dalla previsione di un patrimonio minimo né dalla parametrazione dell'attività esercitata ad un determinato patrimonio ([10]).

4. *Alternative alla capitalizzazione delle banche e delle assicurazioni: il rafforzamento dei sistemi di controllo interno*

La soluzione ai problemi posti dalla limitatezza della disciplina dell'accordo di Basilea 2 (e, in prospettiva, di Solvency 2) non appare, dunque, quella di un

[8] Per questa tesi v. in luogo di molti A. USELLI, *La gestione dei rischi operativi nelle banche: problemi applicativi e implicazioni organizzative*, in *Banca, impresa, società*, 2005, p. 103 ss.; G. CAROSIO, *L'applicazione di Basilea 2 alla prova dei fatti*, intervento al seminario ABI, *Basilea 2 alla prova dei fatti. Gestione dei rischi, allocazione del capitale e relazione con le imprese*, Roma, 22 aprile 2008, p. 11.

[9] Si veda anche, emblematicamente, l'opinione del Governatore della Banca d'Italia: cfr. M. DRAGHI, *Un sistema con più regole, più capitale, meno debito, più trasparenza*, audizione del 21 ottobre 2008 alla VI Commissione del Senato della Repubblica, Finanze e Tesoro, nell'ambito dell'*Indagine conoscitiva sulla crisi finanziaria internazionale e sui suoi effetti sull'economia italiana*, p. 11 ss.; ID., *Restoring confidence with more transaparency*, intervista al *Wall Street Journal* del 2 febbraio 2009, ("what we want is a financial industry, and banking sector especially, where you have more capital, less debt, more rules and much stronger supervision"); ID., *Intervento* all'incontro AIAF – ASSIOM – ATIC FOREX di Bari, 19 gennaio 2008, p. 14 ("la tutela della stabilità richiede che le banche abbiano una capitalizzazione ben superiore a quella prevista dai requisiti minimi di Basilea 2 [e che] prevedano e mantengano margini di sicurezza sulle loro posizioni di liquidità"); ID., *Intervento* all'Assemblea Ordinaria dell'Associazione Bancaria Italiana, 9 luglio 2008, p. 8 (tutti gli scritti sono reperibili sul sito internet della Banca d'Italia).

[10] Con riferimento al rischio operativo, v. per il settore bancario, il documento del Basel Committee on Banking Supervision, *Sound practices for the management and supervision of operational risk*, reperibile sul sito www.bei.org, febbraio 2003; con riferimento al rischio operativo e di liquidità, per il settore assicurativo, v. il documento del Ceiops, *Report on issues regarding the risk management standards on assets*, 2008, reperibile sul sito www.ceiops.org, p. 20 e il documento dell'AIA, *A global framework for insurer solvency assessment*, reperibile sul sito www.actuaries.org, 2004, p. 130; nonché i documenti del CRO Forum, *Insurance risk management response to the crisis*, aprile 2009, e *Operational risk management*, maggio 2009, reperibili sul sito www.croforum.org.

ritorno verso l'approccio patrimoniale standardizzato (considerati i suoi costi e la sua tendenziale inadeguatezza rispetto ai nuovi rischi che le banche e le assicurazioni devono fronteggiare), ma quella della piena attuazione delle norme sui sistemi di controllo interno e dello sviluppo dei principi in tema di trasparenza.

I risparmi ottenuti a livello di obblighi di capitalizzazione potrebbero (e dovrebbero) essere utilmente impiegati dalle banche e dalle assicurazioni (oltre che per remunerare gli azionisti) rispettivamente per diminuire il costo medio dei finanziamenti erogati alle imprese (e dunque per favorire l'accesso delle stesse al credito bancario) nonché per ridurre i costi da riversare sui premi richiesti agli assicurati ([11]).

Fatta questa premessa, ne deriva che la soluzione dei (in parte nuovi) problemi che si pongono, a livello di identificazione e gestione dei rischi, alle banche e alle assicurazioni possono essere (e a mio avviso vanno) risolti – per venire al punto che in questa sede più interessa – mediante l'adozione di interpretazioni volte a rendere il più possibile efficiente il sistema della *governance* e dei controlli interni delle banche e delle assicurazioni.

Seguendo questa impostazione, ed esaminando i cinque componenti del sistema dei controlli interni tradizionalmente individuati dal *COSO Report* (ambiente di controllo, valutazione dei rischi, attività di controllo, informazione e comunicazione, monitoraggio), si possono dunque avanzare alcune considerazioni.

Anticipo subito che – per circoscrivere opportunamente l'ambito del mio intervento – mi limiterò all'analisi del tema del controllo interno solo dal punto di vista della gestione dei rischi, senza esaminare gli aspetti relativi all'informazione di bilancio e alla conformità alle norme (*compliance*).

Cercherò, inoltre, di condurre un discorso di valenza generale, riferito sia al settore bancario sia a quello assicurativo, senza tener conto degli specifici rischi di ciascuno.

Farò, infine, riferimento alle sole società che adottano il sistema di amministrazione e controllo tradizionale (consiglio di amministrazione e collegio sindacale) e alle sole società non sottoposte a vigilanza consolidata.

6. *Il "controllo" del consiglio di amministrazione*

(A) Lo sviluppo di un ambiente di controllo positivo e funzionale è fondamentalmente condizionato dal comportamento del consiglio di amministrazione. Nell'ambito del sistema dei controlli interni rilevanza centrale pare infatti assumere, prima ancora che l'efficacia dei controlli di secondo livello (*risk management*, *compliance*, etc.), il buon funzionamento del consiglio di amministrazione e dei suoi diretti ausiliari, ovvero il comitato per il controllo interno (a livello di assistenza) e l'*internal audit* (a livello di monitoraggio dell'efficienza dei controlli di secondo livello) ([12]).

[11] V. ad es. A. RESTI, *Il nuovo*, cit., p. 2 ss.; ID., *L'implementazione di Basilea 2: le nuove regole cambiano il gioco*, in *Bancaria* 1/2007, p. 30 ss.

[12] Come ha, infatti, evidenziato recentemente il Ceiops, *Lessons learned from the crisis: Solvency II and beyond*, 19 marzo 2009, reperibile sul sito www.ceiops.org, p. 3 s., la questione principale per la sana e prudente gestione degli intermediari non è (o non è soltanto) quella dei controlli di secondo livello, ma quella del buon funzionamento (oltre che del *risk management*) del consiglio di amministrazione. "is not just about risk measurement and quantification,

La disciplina bancaria e quella assicurativa – orientate ad rinforzare principalmente i poteri esecutivi dell'alta direzione – paiono, però, trascurare il ruolo ed il funzionamento del consiglio di amministrazione.

(i) Anzitutto, la formulazione della disciplina di settore in tema di competenze del consiglio di amministrazione appare spesso equivoca.

Le Istruzioni di Vigilanza della Banca d'Italia (Cap. V, Tit. 11, Sez. II, § 1.1) affermano che il consiglio di amministrazione "verifica che l'alta direzione definisca l'assetto dei controlli interni" e rimette all'alta direzione la "verifica nel continuo " del sistema. Il Regolamento Isvap n. 20 assegna al consiglio di amministrazione "la responsabilità ultima del sistema dei controlli interni" e rimette all'alta direzione il "mantenimento della funzionalità" del sistema.

Tali formulazioni di principio sembrano assegnare al consiglio di amministrazione un ruolo residuale in tema di sistema di controllo interno e, dunque, di gestione dei rischi assunti dalla banca e dell'assicurazione (anche se, per converso, in alcuni punti la disciplina assegna al consiglio di amministrazione un compito di "gestione dei principali rischi aziendali": v. ad es. l'art. 6 del Regolamento Isvap n. 20).

Non va, invece, dimenticato che tutte le decisioni fondamentali in tema di sistema di controlli interni sono in concreto riservate dalla disciplina al consiglio di amministrazione nella sua collegialità, con particolare riguardo alle decisioni e alla supervisione sul controllo di terzo livello, ovvero il controllo svolto dall'*internal audit*.

A tale proposito, si consideri che il consiglio di amministrazione deve nominare il responsabile della funzione, approvare il piano *audit* e le variazioni dello stesso, ricevere la reportistica e le comunicazioni urgenti dell'*internal audit*.

A riprova della centralità del consiglio di amministrazione nel sistema dei controlli interni, va segnalata, peraltro, una maggiore attenzione della disciplina assicurativa al consiglio; mentre in passato il programma di *audit* e la reportistica dovevano essere sottoposti all'alta direzione (v. l'art. 4.4 della Circolare Isvap n. 366/D del 3 marzo 1999), ora tanto il piano *audit* quanto la reportistica vanno sottoposti al consiglio di amministrazione (art. 15, comma 4, Regolamento Isvap n. 20). Va anche evidenziato che ora l'*internal audit* deve riportare "periodicamente", oltre che all'alta direzione e al collegio sindacale, al consiglio di amministrazione "la valutazione delle risultanze" della propria attività di revisione, che è una ricostruzione tendenzialmente analitica e di dettaglio (mentre le situazioni di particolare gravità vanno segnalate esclusivamente, oltre che al collegio sindacale, al consiglio di amministrazione).

(ii) In secondo luogo, la disciplina di settore va sempre coordinata con la disciplina del codice civile, che assegna (all'art. 2381 c.c.) al consiglio di amministrazione di "valutare" costantemente "l'adeguatezza dell'assetto organizzativo", agendo in "modo informato".

Come si vede, dunque, da un lato il codice civile assegna al consiglio di amministrazione il compito di valutare costantemente l'adeguatezza (tra l'altro) del sistema di controllo interno (e, dunque, di gestione dei rischi),

---

rather it is about effective governance and risk management"; "key success factors relate to model governance (checks and balances, proper documentation) and the involvement as well as proper understanding and steering by board and senior management, much more than to fine-tuning the ultimate risk metrics".

dall'altro la disciplina settoriale sembra assegnare all'alta direzione il compiuto di "verificare nel continuo" il medesimo sistema.
Sul punto si rende, dunque, necessario adottare interpretazioni equilibrate che, se da un lato devono valorizzare l'importanza assegnata all'alta direzione dalla disciplina di settore, dall'altro devono riservare al consiglio di amministrazione il giusto ruolo e consentire il corretto funzionamento del sistema dei controlli interni.
Ne deve conseguire, in altri termini, la costruzione di un sistema dove il consiglio di amministrazione (ripeto: non l'alta dirigenza) e l'*internal audit* collaborano attivamente per il corretto funzionamento del sistema dei controlli di secondo livello. Come è stato recentemente e opportunamente evidenziato, "i controlli diretti, se non opportunamente presidiati, ad esempio con l'istituzione di «controllori dei controllori», i quali verifichino, periodicamente ma sistematicamente e direttamente, che i controlli diretti siano effettuati e che siano effettuati in modo adeguato, rischiano di minare la solidità e l'efficacia dell'intero sistema" ([13]).
Questo implica, anzitutto, che il consiglio di amministrazione deve essere posto in condizione di affrontare le questioni connesse al sistema dei controlli interni con la dovuta attenzione e il necessario livello di approfondimento, potendo contare sul supporto di un adeguato lavoro istruttorio.
Tale attività istruttoria non può essere rimessa all'alta direzione ma va necessariamente svolta – a mio avviso – dal comitato per il controllo interno.
Si consideri emblematicamente il caso della sottoposizione da parte dell'*internal audit* dell'*audit plan* al consiglio di amministrazione: con tale proposta l'*internal audit* sta – come è stato evidenziato ([14])– di fatto "chiedendo l'autorizzazione ad analizzare parti dell'attività aziendali ritenute prioritarie ma anche a posticipare agli anni successivi la verifica di altre". Rispetto a queste decisioni del consiglio, è opportuno che l'attività istruttoria in merito all'iniziativa non venga effettuata dall'alta direzione il cui operato il consiglio di amministrazione sta sostanzialmente andando ad esaminare e che in merito a tali argomenti il consiglio medesimo abbia l'informazione necessaria messagli a disposizione da soggetti diversi dall'alta direzione.
Inoltre il comitato dovrebbe coadiuvare (verificando l'"effettivo funzionamento" del processo, ai sensi dell'art. 6, comma 2, Regolamento Isvap n. 20) l'alta direzione cui è assegnato (in particolare dall'art. 12, comma 1, Regolamento Isvap n. 20) il compito di assicurare mediante "adeguata reportistica" al consiglio di amministrazione la conoscenza completa dei fatti aziendali rilevanti (per quanto, infatti, ai sensi dell'art. 2381, comma 6, c.c. l'amministratore delegato debba riferire agli amministratori non esecutivi "in consiglio", appare comunque opportuno un controllo anche nella fasi precedenti la riunione consiliare sull'adeguatezza della reportistica).
(B) A fronte della complessità della materia bancaria, assicurativa e finanziaria, è altamente opportuno che gli amministratori siano selezionati in base a criteri di competenza e correttamente remunerati in relazione alle attività espletate; in questo senso, si impongono linee interpretative coerenti tanto in tema di disciplina sui requisiti di professionalità degli esponenti aziendali quanto in tema di remunerazione dei consiglieri di amministrazione.

[13] Cfr. P. MONTALENTI, *Organismo*, cit., p. 646 s.
[14] Cfr. E. PARRETTA, *Controllo*, cit., p. 100.

(i) Nel primo senso, può, ad esempio, evidenziarsi l'incongruenza di imporre al soggetto incaricato della funzione *audit* di "avere specifica competenza e professionalità per lo svolgimento dell'attività" e di "curare l'aggiornamento professionale" (v. l'art. 18 Regolamento Isvap n. 20) e di richiedere viceversa al consigliere di amministrazione della banca di aver solamente "maturato una esperienza complessiva di almeno un triennio attraverso l'esercizio di attività di amministrazione o di controllo ovvero compiti direttivi presso imprese" (art. 1, D.M. 161/1998).
La Raccomandazione della Commissione UE del 15 febbraio 2005 sul ruolo degli amministratori non esecutivi prescrive che, quando si propone la nomina di un amministratore, si dovrebbero segnalare le sue "particolari competenze pertinenti" per l'incarico nel consiglio d'amministrazione; ancor più incisivamente il recente *Ceiops Advice for Level 2 Implementing Measures on Solvency II: System of Governance* (già *Consultation Paper* n. 33) dell'ottobre 2009 conclude nel senso che il sistema di *governance* dell'impresa deve assicurare che i membri del consiglio di amministrazione posseggano "sufficienti qualificazioni professionali" nelle "aree rilevanti del *business*, in modo da assicurare di essere nel complesso in grado di fornire all'impresa un'amministrazione sana e prudente" (*fit and proper requirements*).
(ii) Le norme sulla remunerazione degli amministratori richiederebbero poi una revisione critica, considerato che le stesse favoriscono alti compensi per gli amministratori esecutivi ed il *top management* (al punto che alcuni *regulators* parlano oggi di *remuneration risk* ([15])) e conducono, invece, a molto più limitate (ma anche meno incentivanti) *fees* per gli amministratori non esecutivi e indipendenti ([16]).
(C) Per quanto riguarda il comitato per il controllo interno, la disciplina, in particolare assicurativa, definisce con chiarezza il ruolo dello stesso. A differenza del Codice di Autodisciplina delle società quotate, che assegna al comitato anche il compito di valutare (unitamente al dirigente preposto alla redazione dei documenti contabili societari ed ai revisori), il corretto utilizzo dei principi contabili (il che pone un problema anche di distinzione dei ruoli rispetto, in particolare, al collegio sindacale ([17])), la disciplina dell'Isvap (art. 6 Regolamento n. 20) riserva al comitato un ruolo tendenziale di "assistenza" al consiglio di amministrazione nelle sue principali attività connesse al sistema dei controlli interni.
La disciplina richiede che il comitato sia composto da amministratori non esecutivi, "preferibilmente indipendenti" (v. il citato art. 6). Se si considera, tuttavia, che a tale comitato
a porre il consiglio in condizione di decidere sulla base di informazioni adeguate), appare essenziale garantire che tale compito sia esercitato da soggetti in grado di svolgerlo in modo utile e distaccato. In ragione dell'importanza del ruolo appare, dunque, tendenzialmente necessario (e non

[15] V. il documento Ceiops, *Lesson learned from the crisis*, cit., p. 15.
[16] Il punto è attualmente oggetto di discussione a livello di *regulators*: v. anche il recente Provvedimento del Governatore della Banca d'Italia del 28 ottobre 2009, intitolato *Sistemi di remunerazione e incentivazione*; nonché l'intervento di A.M. TARANTOLA, *Il sistema dei conttrolli interni nella* governance *bancaria*, intervento al Convegno Dexia Crediop del 6 giugno 2008, p. 11 s.; a livello di *consultation papers* v. il *Ceiops Advice for Level 2 Implementing Measures on Solvency II: Remuneration Issue*, 2009, reperibile sul sito www.ceiops.org.
[17] Cfr. in sede di interpretazione dell'(attuale) punto 8.C.3(a) del Codice di Autodisciplina in particolare P. MONTALENTI, *Corporate*, cit., p. 828.

solo "preferibile") che le imprese costituiscano il comitato con amministratori indipendenti ([18]).

6. *Il controllo di "secondo livello" (*risk management*,* compliance, etc.*); i flussi informativi*

È questo un settore molto delicato, dove si intersecano le competenze di varie funzioni.
(A) A livello di individuazione dei rischi, appare opportuna la collaborazione tra varie funzioni: in particolare tra le funzione di *risk management*, di *compliance* e di *internal audit* nonché tra le stesse e il comitato per il controllo interno (che presta – come si è visto: art. 6 Regolamento Isvap n. 20 – un'attività di "assistenza" del consiglio di amministrazione nell'identificazione dei principali rischi aziendali).
A livello di controllo dei rischi, appare, invece, auspicabile quanto più possibile la separazione dei compiti e la formalizzazione degli stessi sia per le singole unità operative sia per le singole funzioni ([19]). L'art. 17 del Regolamento Isvap n. 20 prevede utilmente che le varie funzioni devono collaborare tra loro, sulla base di procedure formalizzate dal consiglio di amministrazione.
Risulta, in particolare, opportuno evitare all'*internal audit* l'esercizio di attività di controllo di secondo livello e mantenere nettamente separate la funzione di *internal audit* da quelle di *risk management* e di *compliance* (v. in questo secondo senso espressamente l'art. 23, comma 8, Regolamento Isvap n. 20 e il § 6 delle Disposizioni di Vigilanza della Banca d'Italia in tema di *compliance* del 10 luglio 2007 ([20])). Analogamente è preferibile garantire la separatezza tra *internal audit* e organismo di vigilanza *ex* d. lgs. 231/2001 ([21]).
Semmai si propone – nelle imprese di minori dimensioni – di accorpare, ove indispensabile per esigenze di economicità, alcune funzioni tra quelle di secondo livello, come il *risk management* e la *compliance* ([22]).
(B) Appare poi indispensabile la predisposizione di flussi informativi obbligatori e procedimentalizzati, non solo di tipo verticale (in particolare, verso il consiglio di amministrazione: v. l'art. 12, comma 1, Regolamento Isvap n. 20), ma anche orizzontale e trasversale tra singole unità e tra singole funzioni (senza lasciare, inoltre, la circolazione dell'informazione all'iniziativa discrezionale delle singole funzioni, come sembrerebbe presupporre l'art. 17, comma 1, del medesimo Regolamento, che dispone che le funzioni si

[18] Il Basel Committee on Banking Supervision, nel documento intitolato *Framework for international control systems in banking organizations*, settembre 1998, reperibile sul sito www.bei.org, *sub principle* 1, p. 11, si riferisce espressamente a "an independent audit committee to assist the board in carrying out its responsibilities".
[19] Cfr. Basel Committee on Banking Supervision, *Framework*, cit., *sub principle* 11.
[20] Cfr. sul punto C. CATANI, *La funzione di* compliance *nella disciplina assicurativa*, in *Assicurazioni*, I, 2008, p. 623 ss., ivi a p. 641.
[21] Cfr. ad es., per le banche, F. MAIMERI, *Controlli interni delle banche tra regolamentazione di vigilanza e modelli di organizzazione aziendale*, in *Riv. dir. comm.*, 2002, I, p. 609 ss., ivi a p. 623. Né può esservi duplicazione di ruoli con il dirigente preposto alla redazione dei documenti contabili, responsabile di predisporre adeguate procedure amministrative e contabili, sul quale, parimenti, si esercita il controllo dell'*internal audit*.
[22] Cfr. per questa possibilità ad es. C. CATANI, *La funzione*, cit., p. 643.

"scambiano ogni informazione utile per l'espletamento dei rispettivi compiti").

7. *Il controllo dell'*internal audit *e il problema dell'esternalizzazione della funzione*

Il monitoraggio del funzionamento dei controlli di secondo livello è funzionale a verificare che il sistema di tali controlli sia costantemente efficace. Esso è svolto principalmente dalla funzione di *internal audit*.
Rispetto a tale funzione vanno evidenziati – nella prospettiva considerata in questo scritto, volta a proporre linee interpretative che incrementino l'efficienza del sistema dei controlli interni – alcuni aspetti.

(A) La nomina da parte del consiglio di amministrazione consente, da un lato, di considerare "strategico e non semplicemente operativo il ruolo dell'*internal auditing* per il sistema del controllo interno" ([23]); dall'altro, di mettere al riparo la funzione da pressioni dell'alta direzione.
Questo secondo profilo, va, peraltro, costantemente assicurato, al fine di consentire all'*internal audit* di esercitare efficacemente il suo operato (in tal senso un indice interpretativo importante si ricava dall'art. 15 del Regolamento Isvap n. 20 per cui l'obbligo di segnalare le situazioni di particolare gravità è disposto in capo all'*internal audit* al consiglio di amministrazione e al collegio sindacale e non all'alta direzione; analogamente l'art. 8, comma 3, del medesimo Regolamento impone al collegio sindacale di vigilare sulla necessaria autonomia e indipendenza della funzione).
Si dovrebbe, dunque, evitare di assegnare all'*internal audit* compiti (anche in via di fatto) operativi che impongano al responsabile della funzione di soggiacere alle direttive dell'alta direzione ([24]). Significativo in questo senso appare, in ambito assicurativo, l'art. 46 della proposta di direttiva Solvency 2, che espressamente sancisce che la funzione di *internal audit* deve essere indipendente dalle funzioni operative ([25]).
Segnalo, infine, che in ambito bancario, al fine di garantire l'efficienza dell'*internal audit*, il Basel Committe ha manifestato l'esigenza che il personale impiegato in tale funzione risulti adeguatamente incentivato e remunerato ([26]).

(B) Si è discusso in dottrina se all'*internal audit* competano (o debbano competere) anche poteri ispettivi. Nella disciplina settoriale bancaria e

[23] Cfr. E. PARRETTA, *Controllo*, p. 95.
[24] Cfr. G. LEMME, *Amministrazione e controllo nella società bancaria*, Milano, 2007, p. 129. Merita di essere segnalato in questa direzione il cambiamento della disciplina dell'Isvap, ad esempio, in tema di gestione del registro reclami: mentre in precedenza le circolari Isvap n. 518D del 2003 e 542/S del 2003 assegnavano all'*internal audit* compiti operativi in tema di gestione del registro, ora il Regolamento Isvap n. 24 dispone che la gestione dei reclami compete ad una "specifica funzione aziendale", restando al responsabile dell'*audit interno*, "nell'ambito dell'attività di monitoraggio dell'efficacia ed efficienza del sistema dei controlli interni", solo di "verificare la correttezza delle procedure di gestione dei reclami" stessi.
[25] V. anche il *Ceiops Advice for Level 2 Implementing Measures on Solvency II: System of Governance*, cit., *sub* § 3.5.
[26] Cfr. Basel Committee on Banking Supervision, *Framework*, cit., *sub principle* 2, p. 12: "staff in control functions must be properly remunerated. … Senior management should institute compensation and promotion policies that reward appropriate behaviours and minimise incentives for staff to ignore or override internal control mechanisms".

assicurativa, tuttavia tali poteri sembrano non solo contemplati (v. art. 15 Regolamento Isvap n. 20), ma anche essenziali ([27]).

All'*internal audit* è riservata, infatti, quella che nella banche in passato veniva definita come attività di ispettorato e che nelle assicurazioni è sempre stata intesa come tale (si pensi alle ispezioni amministrative presso le agenzie).

Un indice interpretativo in questa direzione si ricava, ad esempio, dalla disciplina regolamentare dell'Isvap, dove si prevede che le imprese di assicurazione verificano l'adeguatezza della formazione e dell'aggiornamento professionale effettuati dalle reti distributive di cui si avvalgono, nonché l'osservanza delle regole generali di comportamento imposte alle stesse. Le verifiche svolte devono risultare da un rapporto annuale, redatto dall'unità organizzativa a ciò delegata e da inviare all'Isvap entro sessanta giorni dalla fine dell'anno solare, dopo essere stato sottoposto, "con eventuali osservazioni di merito", dal responsabile dell'*internal auditing* agli organi amministrativi della società. Come è stato correttamente osservato, da un lato, "l'aspettativa dell'Isvap non [è] quella di avere un mero controllo formale e documentale da parte del revisore interno", dall'altro "il riporto diretto del responsabile dell'*internal auditing* al consiglio di amministrazione e al *top management* permette che anche le problematiche emergenti in sede di [accertamenti di merito nonché di] ispezione amministrativa abbiano una debita attenzione presso i massimi vertici dell'azienda" ([28]).

(C) Un tema importante è quello relativo alla possibilità di esternalizzare la funzione di *internal audit*.

(i) In primo luogo, la possibilità di esternalizzazione della funzione dovrebbe essere sempre considerata l'opzione meno preferibile e comunque subordinata alla dimostrazione di precise esigenze di "economicità" o connesse alla sussistenza di un gruppo (v. Istruzioni di Vigilanza della Banca d'Italia per le banche, Tit. IV, Cap. 11, Sez. II, § 3 e Regolamento Isvap n. 20, art. 16) ([29]). Il referente del consiglio di amministrazione e del collegio sindacale per il controllo di terzo livello dovrebbe essere una struttura deputata a tale controllo in modo costante e sistematico e non in via episodica e dall'esterno.

In proposito merita di essere ricordato che il recente Regolamento congiunto Consob Banca d'Italia del 29 ottobre 2007 stabilisce (per gli intermediari che esercitano i servizi di investimento, ma con probabile valenza interpretativa più generale in tema di esercizio di attività finanziaria) che "l'esternalizzazione non può ridurre l'efficacia del sistema dei controlli" (art. 19); a sua volta il Regolamento Isvap n. 20 stabilisce che l'esternalizzazione non è ammessa se dalla stessa derivi un "ingiustificato incremento del rischio operativo" (art. 29).

Più recentemente, il citato *Ceiops Advice for Level 2 Implementing Measures on Solvency II: Systems of Governance* distingue tra *internal* ed

---

[27] Cfr. C. DE ROBBIO-C. PATALANO, *Il sistema dei controlli nelle nuove disposizioni di vigilanza*, in *Bancaria*, 12/1998, p. 79 ss., ivi a p. 83; E. PARRETTA, *Controllo*, p. 95.

[28] Cfr. E. PARRETTA, *Controllo*, cit., 118 s.

[29] Tendenzialmente critici rispetto alla esternalizzazione della funzione sono anche, per le società assicurative, S. MIANI-F. PICHER, *I controlli interni nelle imprese di assicurazione*, in AA. VV., *Rischi e controlli nelle banche e nelle assicurazioni*, Torino, 2003, p. 59 ss., ivi a p. 108; cauto, per il settore bancario, V. PESIC, *Il sistema*, cit., p. 222.

***external outsorcing*, suggerendo valutazioni meno rigorose solo per il caso in cui l'esternalizzazione avvenga a livello di società appartenenti al medesimo gruppo.**

(ii) In secondo luogo, si dovrebbe riflettere con attenzione circa l'opportunità di consentire l'esternalizzazione della funzione alle società di revisione. Per quanto la Banca d'Italia sembri ammetterlo (Istruzioni di Vigilanza per le banche, Tit. IV, Cap. 11, Sez. II, § 3), appaiono comunque attuali anche per le banche e le assicurazioni le osservazioni della Consob (con riferimento alle società per azioni quotate: v. la Comunicazione n. DEM/94875 del 27 dicembre 2000) per cui la funzione di *internal audit* non può essere affidata alle società di revisione, considerato che a tale funzione sono demandati compiti e responsabilità di notevole ampiezza (rispetto delle procedure interne, attività di supporto consultivo ai settori dell'organizzazione aziendale, etc.) che non possono essere utilmente svolte da società, quali quelle di revisione, con competenze limitate principalmente alla revisione contabile.

D'altra parte, la stessa Banca d'Italia pare privilegiare la possibilità di esternalizzare la funzione (non di *audit*, ma) di *compliance* a soggetti diversi dalle società di revisione (altre banche ovvero organismi associativi di categoria: v. le Disposizioni di Vigilanza della Banca d'Italia in tema di *compliance* del 10 luglio 2007, § 4).

Semmai alle società di revisione andrebbero assegnati incarichi mirati allo svolgimento di specifiche attività di verifica e di analisi di singoli aspetti del sistema di controllo interno, con principale attenzione ai profili amministrativo-contabili, sotto il diretto controllo della funzione (comunque istituita) di *internal audit* ([30]).

[30] V. in proposito anche il recente documento di ASSIREVI, *Tematiche di indipendenza relative ai servizi diversi dalla revisione: servizi relativi al sistema di controllo interno*, ottobre 2009, circa i compiti che la società incaricata della revisione contabile può esercitare in relazione al sistema di controllo interno della società revisionata.

8. *Il ruolo del collegio sindacale*

Delicata – come da più parti segnalato – è, infine, la ricostruzione dei rapporti tra *internal audit* e collegio sindacale.
La risposta al quesito circa la ricostruzione di tali rapporti va, probabilmente, assegnata intendendo il collegio sindacale come l'organo deputato ad esprimere una valutazione di adeguatezza e di efficacia del sistema di controllo interno e ad eseguire attività ispettive (*ex* art. 2403-*bis* c.c. e 151 t.u.f.) tendenzialmente episodiche e, per converso, l'*internal audit* come la funzione chiamata a realizzare le proprie verifiche (anche ispettive) su base stabile e sistematica ([31]).
In tal senso, appare esplicito l'art. 15 del Regolamento Isvap n. 20, per cui la funzione di *internal audit* è quella di comunicare "periodicamente", "a seguito dell'analisi sull'attività oggetto di controllo", al consiglio di amministrazione, all'alta direzione e al collegio sindacale "la valutazione delle risultanze e le eventuali disfunzioni e criticità".
Ne deriva, come è stato opportunamente notato, che il collegio sindacale, da un lato, si avvale – nell'espletamento della funzione di controllo – delle risultanze e dei dati forniti dall'*internal audit*, dall'altro è chiamato a svolgere "una ulteriore e finale attività di controllo sull'efficienza e sulla congruità dei dati forniti dal revisore esterno" ([32]). Inteso il rapporto in questa prospettiva, al collegio sindacale può essere riservata un'utile e non ripetitiva funzione di controllo, per così dire, di "quarto livello".
In questa direzione depone, di fatto, anche la disciplina dell'Isvap, che all'art. 8, comma 3, del Regolamento n. 20 stabilisce che al collegio sindacale spetta di "valutare l'operato della funzione di revisione interna" e di "verificarne la funzionalità".
Il ruolo del collegio sindacale diviene in questo senso cruciale: considerato che la funzione di *internal audit* risponde quasi sempre (secondo gli organigrammi aziendali) alla direzione generale, il collegio sindacale deve accertare costantemente che, da un lato, la funzione di *internal audit* si veda riconosciuta la necessaria autonomia e indipendenza dall'alta direzione e, dall'altro, essa eserciti effettivamente la propria attività nel rispetto di tali principi di autonomia e di indipendenza.

[31] Per l'auspicio di un tendenziale ridimensionamento del ruolo del collegio sindacale, al fine di evitare il rischio della duplicazione dei controlli, verso un più circoscritto "controllo di legalità sostanziale" v. P. MONTALENTI, *Organismo*, cit., p. 659.
[32] Cfr. S. MIANI-F. PICHER, *I controlli*, cit., p. 110.

TESTIMONIANZE

LA FUNZIONE *COMPLIANCE* NEL SETTORE BANCARIO: PROFILI OPERATIVI

Dott.ssa Rosalba Casiraghi
Membro del Consiglio di Sorveglianza e del Comitato di Controllo Intesa Sanpaolo S.p.A.
Presidente - NedCommunity

1. Ringrazio l'AIDA per l'invito a questo interessante congresso dedicato ad un tema di grande attualità, qual è quello del sistema dei controlli interni nel mondo assicurativo e bancario.

In questo contesto, porto la voce delle banche, una realtà che ho la possibilità di conoscere da un osservatorio per così dire "privilegiato", quale membro del Consiglio di Sorveglianza d'Intesa Sanpaolo.

2. Per precisare la situazione d'Intesa Sanpaolo, vorrei innanzi tutto dire qualche parola sul quadro normativo e sullo scenario di riferimento che hanno orientato le scelte del Gruppo, alla ricerca delle migliori e più efficaci modalità di presidio del rischio di conformità.

Credo che le scelte in questa materia assumano una valenza strategica per un'impresa bancaria, perché la *compliance* è chiamata a svolgere in azienda un ruolo estremamente importante e delicato, quello di preservare la fiducia di tutti gli stakeholder, a partire dal cliente. Ed è quasi superfluo sottolineare come la fiducia sia da sempre alla base del corretto funzionamento del sistema creditizio e finanziario e dell'economia nel suo complesso.

3. Con riferimento al contesto normativo, i capisaldi della funzione di conformità vanno ricercati nelle indicazioni del Comitato di Basilea, formalizzate nel documento *"Compliance and the compliance function in banks"* dell'aprile 2005. Esse hanno tracciato le linee guida a livello internazionale per affrontare il tema della *compliance* nell'ambito delle attività bancarie, fornendo istruzioni per l'istituzione della funzione aziendale atta al suo presidio.

A livello nazionale, il documento del Comitato di Basilea ha trovato trasposizione nelle Disposizioni di vigilanza di Banca d'Italia del 10 luglio 2007 in materia di funzione di conformità.

Inoltre la Direttiva 2006/73/CE, recante le modalità di esecuzione della Direttiva 2004/39/CE relativa ai mercati degli strumenti finanziari (cd. Direttiva Mifid), ha richiesto agli intermediari finanziari che prestano servizi d'investimento l'istituzione di una funzione deputata al controllo della conformità aziendale rispetto agli obblighi indicati nella Direttiva.

A livello nazionale, la previsione comunitaria è stata trasposta nel Regolamento congiunto di Banca d'Italia e CONSOB emanato il 29 ottobre 2007 ai sensi dell'art. 6 del Testo Unico della Finanza.

Come sapete, il mondo assicurativo si è mosso con un leggero ritardo rispetto al sistema bancario. E' del 26 marzo 2008 l'emanazione del Regolamento ISVAP n. 20, che ha introdotto anche per le compagnie di assicurazione alcune significative novità in materia di controlli interni ed istituito la funzione di Controllo di Conformità alle norme, anticipando le disposizioni che troveranno compimento con l'entrata in vigore delle disposizioni Solvency 2.

4. In particolare le Disposizioni di vigilanza di Banca d'Italia del 10 luglio 2007 rappresentano la normativa di riferimento per quanto riguarda:

- **la definizione del rischio di non conformità,**
- **il ruolo degli Organi di vertice della banca,**
- **i principali adempimenti della funzione di conformità, le aree di intervento e la struttura organizzativa,**
- **i requisiti del responsabile della *compliance*,**
- **i rapporti tra la *compliance* e le altre funzioni aziendali,**
- **le modalità di presidio per i gruppi bancari.**

***5.* Con riferimento al rischio di non conformità, esso viene definito come "il rischio di incorrere in sanzioni giudiziarie o amministrative, perdite finanziarie rilevanti o danni di reputazione in conseguenza di violazione di norme imperative (di legge o regolamenti) ovvero di autoregolamentazione (es. statuti, codici di condotta, codici di autodisciplina)".**

Relativamente alle norme da ricondurre sotto la responsabilità della *compliance*, Banca d'Italia indica in via generale come norme più rilevanti ai fini del rischio di non conformità quelle riguardanti 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.

Il Regolamento stabilisce inoltre alcuni criteri cui fare riferimento per garantire una efficace ed efficiente gestione del rischio di non conformità.

Ma soprattutto, Banca d'Italia pone particolare enfasi sul fatto che l'obiettivo di minimizzare il rischio di non conformità deve essere perseguito attraverso l'operare sinergico di tutte le componenti aziendali, a partire dagli Organi di Vertice. Al Consiglio di Amministrazione (o Consiglio di Gestione nel modello dualistico) e al Collegio Sindacale (o Consiglio di Sorveglianza) sono infatti attribuite rilevanti responsabilità nella supervisione complessiva del sistema di gestione del rischio della banca, ivi compreso il rischio di non conformità.

6. Per poter gestire adeguatamente il rischio di non conformità, l'Autorità di Vigilanza richiede l'istituzione di un'apposita funzione, con il compito specifico di verificare che le procedure interne siano coerenti con l'obiettivo di prevenire la violazione di norme applicabili alla banca.

Per svolgere correttamente i propri compiti tale funzione deve essere indipendente, dotata di risorse qualitativamente e quantitativamente adeguate ai compiti da svolgere e avere accesso a tutte le attività della banca, nonché a qualsiasi informazione rilevante.

Il responsabile della funzione di conformità, di conseguenza, non deve avere responsabilità dirette di aree operative né deve essere gerarchicamente dipendente da soggetti responsabili di tali aree e deve possedere requisiti adeguati di indipendenza, autorevolezza e professionalità. La sua nomina e la sua revoca sono di competenza, esclusiva e non delegabile, dell'Organo amministrativo, sentito l'Organo di controllo.

La funzione di conformità è tenuta a collaborare con le altre funzioni presenti in azienda - in particolare, revisione interna, controllo del rischio operativo, funzione legale, organizzazione, organismo di vigilanza individuato ai sensi della legge 231/2001 - allo scopo di sviluppare le proprie metodologie di gestione del rischio in modo coerente con le strategie e l'operatività aziendale.

Infine, con riferimento ai gruppi bancari, le Disposizioni di Vigilanza rimettono agli organi aziendali della capogruppo le decisioni strategiche a livello di gruppo in materia di gestione del rischio di non conformità. Le scelte effettuate devono tener conto della specifica operatività e dei connessi profili di rischio di non conformità di ciascuna delle società componenti il gruppo.

7. Le disposizioni delle Autorità di vigilanza sono maturate in un contesto di riferimento che, in questi anni, ha fatto emergere con enfasi la necessità di un forte presidio di *compliance*, richiedendo rapide risposte da parte delle Banche, in primis dei grandi gruppi con presenza internazionale.

8. Guardando allo scenario esterno, sono chiaramente individuabili i macro-trend in atto, che nel recente passato hanno aumentato la pressione sulle banche e sulle loro funzioni di controllo.

All'inizio di questo decennio casi, a tal punto noti da non dover essere più citati, avevano portato in evidenza l'esistenza di rischi operativi e reputazionali potenzialmente in grado di compromettere il legame di fiducia con la clientela. La recente crisi finanziaria mondiale ha ribadito i pericoli collegati con una crisi di fiducia, ingigantiti da una scala ormai divenuta mondiale.

Al tempo stesso, è in atto una crescente complessità del business, che presenta diversi aspetti:

- **un primo fattore di complessità risiede nello scenario esterno, nazionale ed internazionale. Le tensioni acuite dalla crisi finanziaria ed economica hanno reso l'opinione pubblica, i risparmiatori e le associazioni che li rappresentano più critici che in passato nei confronti di banche ed intermediari;**
- **un secondo fattore di complessità consiste nella crescente articolazione e stratificazione della normativa, da parte di un legislatore e di regulators, nazionali ed internazionali, che, al di là d'affermazioni di principio, stanno ancora mettendo a punto adeguati processi di coordinamento e semplificazione. Ne consegue un aumento dei costi di regolamentazione e dei rischi di conformità da fronteggiare;**
- **un ulteriore elemento di complessità deriva dall'evoluzione della vigilanza da *rule based a principle based,* per cui la disciplina fissa obiettivi e requisiti di principio lasciando liberi gli operatori di definire i propri modelli gestionali. Tale approccio, che ha l'indubbio pregio d'essere meno invasivo rispetto ad una normativa per regole, richiede alle banche ed agli intermediari una maggiore responsabilità e sistemi di controllo interno e d'autovalutazione robusti.**

Alla funzione di conformità è attribuito un ruolo cruciale nella gestione di questi elementi di complessità. La *compliance* ha, infatti, una funzione fondamentale nel miglioramento della relazione con la clientela, concorrendo a ristabilire un clima di maggiore fiducia, nella gestione di norme e regole sempre più articolate e nella strutturazione di solidi sistemi di controllo interni, insieme alle altre funzioni aziendali a ciò preposte.

9. Le risposte a queste sollecitazioni da parte delle Banche, a livello internazionale, sono state diverse. Particolarmente interessante è vedere come i grandi gruppi bancari abbiano ricercato modelli organizzativi idonei a garantire un efficace presidio della conformità tenendo conto delle proprie specificità.

Un primo elemento che emerge è che non si registrano strutture organizzate esclusivamente per normativa, ma prevalgono impostazioni per area di business / realtà geografica. Semplificando, si possono infatti individuare tre macro-modelli di riferimento:

- **un'impostazione divisionale, per aree di business. E' il modello tipicamente adottato da banche con limitata presenza internazionale, in quanto permette di implementare *policy* a livello di Gruppo in maniera più efficace ed efficiente;**
- **un'organizzazione geografica. E' la struttura che si ritrova più comunemente in gruppi bancari con poche business line ma una presenza geografica diffusa, in grado di rispondere con maggiore efficienza alla necessità di competenze e supporto regolatorio locali;**
- **una struttura ibrida. E' la *best practice* per banche universali con presenza internazionale, con necessità di bilanciare le due dimensioni della matrice**

per assicurare che l'organizzazione soddisfi i regolatori e al tempo stesso stabilisca una relazione di vera partnership con le divisioni di business.

Dico subito che Intesa Sanpaolo, che concentra la maggior parte delle sue attività sul territorio nazionale, ha articolato la sua funzione di conformità in strutture responsabili di specifiche aree di business; a queste si affiancano tuttavia ulteriori strutture "trasversali", una incaricata della *governance* e del controllo complessivo del Gruppo e l'altra focalizzata su particolari normative che assumono rilevanza "cross" su tutte le società controllate (antiriciclaggio, embarghi, D.Lgs. 231/01).

10. Nelle sue scelte strategiche in tema di *compliance*, credo di poter affermare che Intesa Sanpaolo abbia dimostrato di saper rispondere con serietà e convinzione alle sollecitazioni provenienti dalle Autorità di vigilanza, operando in un'ottica sostanziale e non formale.

11. Nel giugno del 2008 Intesa Sanpaolo ha varato un'importante riorganizzazione interna introducendo, tra l'altro, la figura del Chief Risk Officer, sotto la cui responsabilità è stata costituita la Direzione Centrale Compliance.

L'area del Chief Risk Officer rappresenta, per così dire, la seconda linea di difesa nell'ambito del sistema dei controlli della Banca, in quanto comprende, oltre alla Compliance, le strutture del Risk Management e del Legale. In linea con le Disposizioni di Vigilanza, si è così ottenuta una piena separazione tra i controlli di secondo livello e quelli di terzo livello, affidati all'Auditing, che risponde direttamente al Consiglio di Gestione e al Consiglio di Sorveglianza. Il sistema dei controlli è completato, ovviamente, dai controlli di primo livello, la cui responsabilità è in capo alle strutture operative.

12. All'indomani della sua costituzione, la Direzione Compliance ha avviato un Progetto finalizzato all'individuazione di un Modello di *compliance* in grado di garantire un'efficace gestione del rischio di non conformità a livello di Gruppo. In aderenza alle disposizioni normative, tale modello è stato formalizzato nelle "Linee Guida di *Compliance* di Gruppo" approvate nel marzo scorso dagli Organi Sociali della Banca.

Le Linee Guida innanzitutto definiscono ruoli e responsabilità a tutti i livelli aziendali, attribuendo:

- **ai Consigli di Sorveglianza e di Gestione la supervisione complessiva della gestione dei rischi di non conformità, attraverso l'approvazione delle politiche di gestione, la costituzione della funzione di conformità e la valutazione almeno annuale dell'adeguatezza della stessa funzione;**
- **al CEO la responsabilità di un'efficace attuazione degli indirizzi deliberati dal Consiglio di Gestione e dal Consiglio di Sorveglianza verso le strutture coinvolte;**

- **alla Compliance tutti i compiti attribuiti alla funzione di conformità dalle Disposizioni di vigilanza di Banca d'Italia e dal Regolamento congiunto di Banca d'Italia e CONSOB con riferimento agli ambiti normativi considerati a maggiore rilevanza dalle Autorità di Vigilanza o per i quali si è reputato comunque necessaria una gestione accentrata del rischio di non conformità. Sono poi stati individuati specifici ambiti normativi, comunque rilevanti ai fini del rischio di non conformità, per i quali i compiti attribuiti alla Compliance sono svolti da altre strutture aziendali, dotate di adeguata indipendenza oltre che delle necessarie competenze;**
- **infine, le Linee Guida prevedono la collaborazione di diverse strutture aziendali per lo sviluppo di metodologie di gestione del rischio, la definizione dei processi, la diffusione della cultura di *compliance*.**

13. Gli ambiti normativi ricondotti sotto la responsabilità della Direzione Compliance vengono presidiati in via diretta o indiretta. E' da evidenziare che, per gli ambiti normativi presidiati indirettamente, i compiti propri della Compliance sono svolti da altre strutture aziendali, fermo restando l'accentramento presso la Compliance dei ruoli di:

- **definizione delle linee guida e delle regole metodologiche di presidio e di valutazione del rischio di non conformità,**
- **coordinamento delle iniziative di *compliance* anche ai fini delle scelte di priorità in relazione al rischio relativo,**
- **verifica dell'effettiva applicazione di linee guida e regole metodologiche da parte delle strutture preposte al presidio,**
- **produzione di un'informativa integrata delle relative risultanze agli Organi Sociali.**

14. Le Linee guida definiscono poi i principali macro processi che descrivono le modalità di presidio e controllo del rischio di non conformità:

- **l'identificazione e la valutazione periodica del rischio di non conformità e dei relativi presidi che costituiscono il primo momento logico del modello di gestione e risultano funzionali all'individuazione e programmazione degli interventi di gestione;**
- **il monitoraggio della normativa esterna e sua traduzione in linee guida, processi e procedure interne;**
- **la prestazione di consulenza e assistenza al Vertice aziendale e alle altre strutture della Banca e la valutazione preventiva della conformità alla normativa vigente dei progetti innovativi, delle operazioni e dei nuovi prodotti e servizi da avviare alla commercializzazione;**
- **la verifica dell'adeguatezza e dell'effettiva applicazione dei processi e delle procedure interne e degli adeguamenti organizzativi suggeriti per la prevenzione del rischio di non conformità;**

- **la diffusione di una cultura aziendale improntata ai principi d'onestà, correttezza e rispetto dello spirito e della lettera delle norme attraverso l'istituzione di canali di comunicazione e strumenti di formazione efficaci, identificando i fabbisogni formativi relativi alle materie di competenza e predisponendo i contenuti delle iniziative di formazione per tutte le risorse della Banca;**
- **la gestione delle relazioni con le Autorità di Vigilanza inerenti alle tematiche di conformità e coordinamento delle attività necessarie per l'evasione delle risposte alle richieste che le Autorità inoltrano alla Banca, nonché la gestione degli eventi di non conformità;**
- **le attività operative di tenuta dei registri e di effettuazione delle segnalazioni e comunicazioni richieste dalla normativa;**
- **la predisposizione delle relazioni destinate agli Organi sociali comprendenti, su base annuale, l'identificazione e la valutazione dei rischi di non conformità e la programmazione degli interventi di gestione e, a consuntivo su base semestrale, la descrizione delle attività effettuate, delle criticità rilevate e dei rimedi individuati.**

15. Le Linee guida disegnano altresì il Modello di presidio a livello di Gruppo. Esse prevedono che la Direzione Compliance svolga nei confronti delle controllate un ruolo d'indirizzo e controllo, mirato a garantire un efficace ed efficiente presidio dei rischi di non conformità.

Il modello di governo sul Gruppo contempla due diverse modalità di presidio, declinate per tenere conto dell'articolazione operativa e territoriale di Intesa Sanpaolo. In particolare è previsto:

- **per le Banche Rete e le Società italiane specificamente individuate, la cui operatività è connotata da un elevato livello d'integrazione con la Capogruppo, l'accentramento delle attività di presidio della conformità presso la Direzione Compliance (cosiddette società in *service*);**
- **per le altre Società italiane, specificamente individuate in relazione all'esistenza di un obbligo normativo o a motivo della loro rilevanza, nonché per le Banche e le Filiali estere, la costituzione di una funzione di conformità interna e la nomina di un Compliance Officer locale, cui sono attribuite le responsabilità in materia di *compliance* (società in *governance*). I Compliance Officer locali dipendono funzionalmente dalla Direzione Compliance.**

16. Un'ulteriore attività cui è stata attribuita massima rilevanza è stata la definizione delle modalità di valutazione dei rischi e dei presidi, primo passo per individuare le aree su cui concentrare le azioni di mitigazione da porre in essere e definire le priorità d'intervento.

Ricordo brevemente che il rischio di non conformità è costituito da due componenti, quell'operativa e quella reputazionale:

- **la prima è rappresentata dal rischio di incorrere in sanzioni giudiziarie o amministrative e perdite finanziarie rilevanti in conseguenza di violazione di norme imperative o d'autoregolamentazione,**
- **la seconda, dal rischio di sostenere un aggravio delle perdite finanziarie derivanti da comportamenti di non conformità connessi ad una perdita di reputazione della banca.**

17. Senza entrare in dettagli tecnici, sottolineo soltanto che, per sua natura, il rischio di *compliance* non è di facile quantificazione. Ci si è dunque posti l'obiettivo di ordinare, in termini relativi - sotto forma di *cluster* - il rischio attribuibile agli ambiti normativi di competenza della *compliance*.

Preciso che, parlando di rischio, mi riferisco al cosiddetto "rischio residuo", ovvero del rischio che permane dopo aver considerato gli interventi adottati a fini di mitigazione dello stesso.

L'analisi è partita da dati quantitativi, rappresentati dalle perdite operative registrate negli ultimi anni, opportunamente corrette per tener conto della evoluzione di scenario prevista in base ad un giudizio manageriale di tipo qualitativo.

Sempre con il supporto di giudizi qualitativi, formulati dagli "specialisti" aziendali, sono stati valutati sia i rischi reputazionali sia il livello di adeguatezza dei presidi posti in essere, ovvero dell'insieme degli interventi di carattere normativo, procedurale, organizzativo, informatico adottati a mitigazione del rischio di *compliance*.

18. Il risultato del lavoro effettuato si può rappresentare graficamente attraverso una matrice.

Sull'asse delle ordinate sono riportati i quartili emersi dalla valutazione del rischio potenziale mentre in ascissa sono indicati i livelli di presidio dai più elevati (presidio adeguato) a quelli che richiedono interventi di rafforzamento.

In tal modo si trovano nel quadrante in alto a destra le normative che presentano un elevato rischio potenziale associato a un livello di presidio non soddisfacente e che quindi richiedono interventi prioritari.

La matrice ha consentito quindi di individuare gli ambiti normativi sui quali indirizzare in via prioritaria le risorse disponibili sia della Compliance sia delle altre Strutture aziendali, per quanto di competenza.

19. Il risultato del *risk assessment* ha costituito la base di lavoro per la prima Relazione annuale di *compliance* e, soprattutto, del Piano degli interventi 2009, approvato dagli Organi Sociali a inizio anno.

Le azioni di mitigazione per gli ambiti giudicati a più alto rischio residuo sono poi dettagliate nel Tableau de Bord di Compliance, che consente alla funzione di conformità di monitorare in via continuativa lo stato d'avanzamento delle

attività, portando prontamente all'attenzione degli Organi sociali eventuali criticità emerse.

20. Voglio chiudere con un breve cenno ad un ulteriore strumento realizzato dalla Banca per la gestione dei rischi: il Reporting integrato dei rischi operativi e reputazionali.

Esso riepiloga, in un unico documento, le principali criticità e necessità di intervento riscontrate a livello di Gruppo, consentendo di concretizzare le sinergie tra tutte le strutture aziendali coinvolte nel sistema dei controlli, come auspicato dalla Banca d'Italia.

La gestione del Reporting viene infatti effettuata congiuntamente dalla Compliance, dal Risk Management e dall'Organizzazione e coinvolge, per quanto di competenza, la Governance Amministrativo Finanziaria (responsabile dei controlli ex D.Lgs. 262/05). Un fattivo supporto viene anche da parte dell'Internal Auditing.

Tale strumento presenta un'indubbia valenza per consentire ai Vertici aziendali le scelte di priorità dei piani d'intervento e l'allocazione delle risorse, e il monitoraggio nel continuo dell'evoluzione delle azioni di mitigazioni programmate.

21. il Reporting integrato rappresenta:

- **le perdite operative registrate nel periodo, con indicazione dei più significativi scostamenti rispetto alle attese,**
- **alcuni indicatori sintetici riferiti al presidio della *business continuity* (in termini di rilevanza e livello di copertura) e della normativa aziendale (grado di formalizzazione dei processi),**
- **le evidenze delle criticità/necessità di intervento ad alta rilevanza e le connesse azioni di mitigazione, i cui dettagli sono sviluppati nel prosieguo del documento.**

<u>Conclusione</u>

Parlavo prima di complessità. Credo che per fronteggiare il difficile scenario di riferimento le banche debbano necessariamente far leva, in primo luogo, su una *governance* solida, basata in particolare su un sistema dei controlli coerente ed integrato.

Pur nel rispetto dei singoli mandati, ritengo fondamentale che tutte le strutture di controllo attivino un costante flusso d'informazioni, tengano aperto un dialogo continuo, ricercando tutte le possibili sinergie che consentano il più efficace ed efficiente presidio del rischio nel suo complesso, al di là delle definizioni con cui lo si è identificato.

A questo riguardo, molto rimane ancora da fare, ma la strada su cui ci siamo avviati è certamente adeguata a fornire un ulteriore elemento per il rafforzamento all'azienda ed il potenziamento della solidità complessiva.

Agenda

- **Contesto normativo – La funzione di conformità nella normativa nazionale**
- **Il contesto di riferimento - Elementi di benchmarking**
- **Il caso Intesa Sanpaolo**

INTESA SANPAOLO

Contesto normativo

Contesto normativo - Disposizioni di Vigilanza (1/3)

Banca d'Italia Disposizioni di Vigilanza
La funzione di conformità (compliance)
10 luglio 2007

- **Il rischio di non conformità alle norme**
  - Definizione
  - Norme più rilevanti
  - Principali criteri per una efficace ed efficiente gestione del rischio
- **Ruolo degli organi di vertice della banca**
  - Responsabilità della supervisione complessiva del sistema di gestione del rischio di non conformità
  - Responsabilità della efficacia della gestione del rischio
- **La funzione di conformità alle norme**
  - Principali adempimenti
  - Aree di intervento
  - Organizzazione
- **Il responsabile della funzione di conformità alle norme**
- **Rapporti con altre funzioni aziendali**
- **La funzione di conformità nelle strutture di gruppo**

Contesto normativo - Disposizioni di Vigilanza (2/3)

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 violazione di norme imperative ovvero di autoregolamentazione
- Tra le **norme più rilevanti** ai fini del rischio di non conformità sono indicate quelle riguardanti 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
- Principali criteri per una **efficace ed efficiente gestione del rischio:**
  - chiara e formalizzata **individuazione e distinzione di ruoli e responsabilità** ai diversi livelli dell'organizzazione della banca
  - **istituzione di un'apposita funzione** incaricata della gestione del rischio di non conformità
  - nomina di un **responsabile della conformità** all'interno della banca
  - predisposizione di un **documento interno** che indichi responsabilità, compiti, modalità operative, flussi informativi, programmazione e risultati

Ruolo degli organi di vertice della banca

- Responsabilità della **supervisione complessiva** del sistema di gestione del rischio di non conformità
- Responsabilità della **efficacia della gestione del rischio**

Contesto normativo - Disposizioni di Vigilanza (3/3)

Funzione di conformità	Deve **verificare che le procedure interne siano coerenti** con l'obiettivo di **prevenire la violazione di norme** di eteroregolamentazione e autoregolamentazione applicabili alla banca
Il responsabile della funzione di conformità	**Non deve avere responsabilità dirette di aree operative** né deve essere gerarchicamente dipendente da soggetti responsabili di tali aree e deve possedere **requisiti adeguati di indipendenza, autorevolezza e professionalità**
Rapporti con altre funzioni aziendali	La funzione di conformità collabora con le altre funzioni presenti in azienda allo scopo di **sviluppare le proprie metodologie di gestione del rischio.** L'adeguatezza ed efficacia della funzione di conformità devono essere sottoposte a **verifica periodica da parte della revisione interna**
Gestione del rischio di Gruppo	**Le decisioni strategiche a livello di gruppo** in materia di gestione del rischio di non conformità sono rimesse agli **organi aziendali della capogruppo**. Le attività relative alla funzione di conformità **possono essere accentrate**, al fine di conseguire economie di scala, anche attraverso la costituzione di unità specializzate all'interno del gruppo medesimo

- **Contesto normativo – La funzione di conformità nella normativa nazionale**
- **Il contesto di riferimento - Elementi di benchmarking**
- **Il caso Intesa Sanpaolo**

Analisi internazionale - Il contesto di riferimento

- Contesto di crisi e crescente complessità del business
- Aumento requisiti normativi
- Crescente vigilanza dei regolatori
- Crescenti costi di failure

Best practice internazionali

Organizzazione divisionale

Tipicamente adottato in **banche con limitata presenza internazionale**

Permette di implementare policy a livello di Gruppo in maniera più efficace ed efficiente

Organizzazione geografica

Struttura comune in **banche con poche business line** ma **presenza geografica diffusa**

Risponde alla necessità di competenze e supporto regolatorio locali

Organizzazione ibrida

Best practice per banche universali con presenza internazionale

Necessità di bilanciare le due dimensioni della matrice per assicurare che l'organizzazione:

- soddisfi i regolatori
- stabilisca una relazione di vera partnership con le divisioni di business

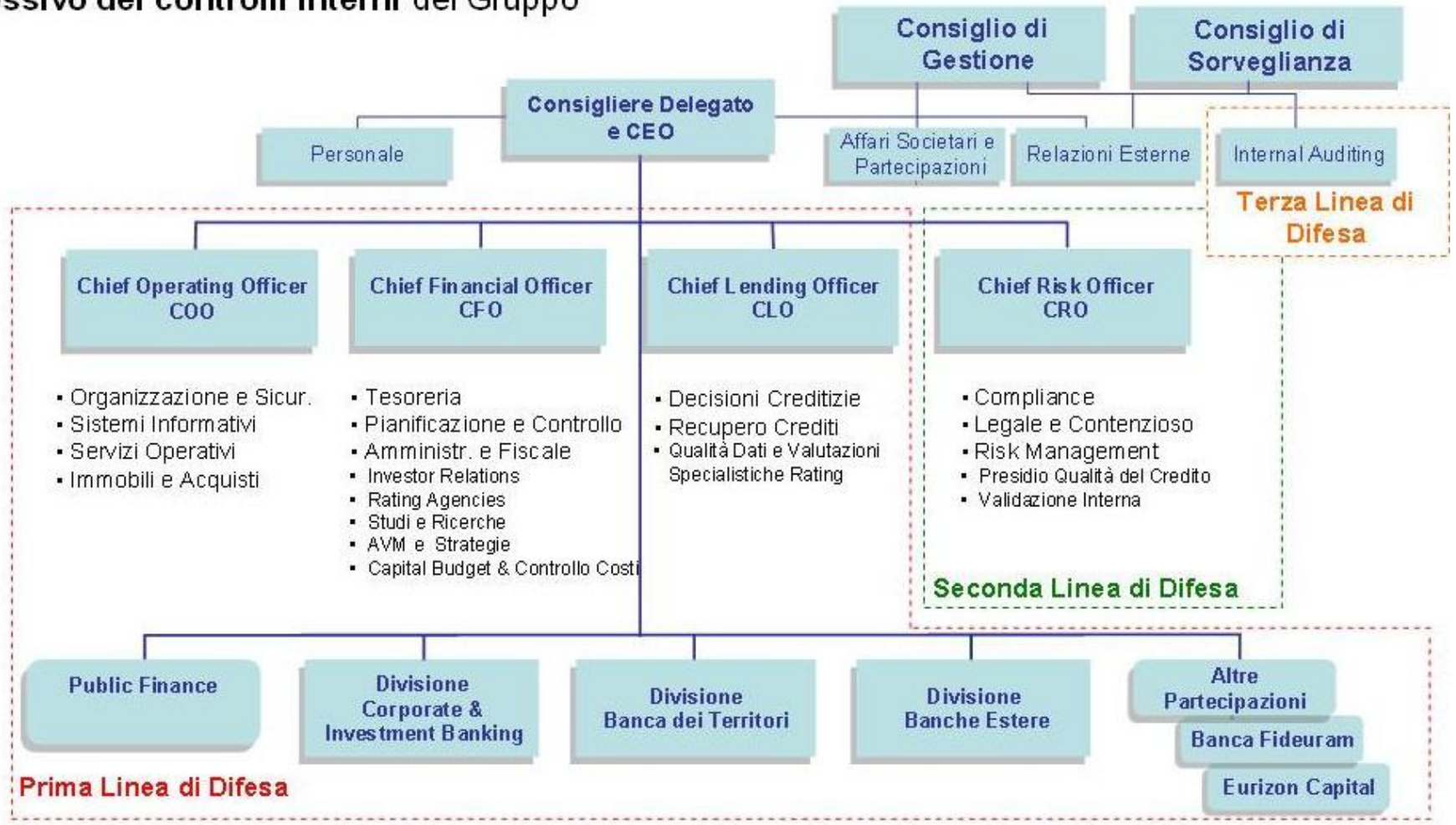
Fonte: Interviste, McKinsey

Agenda

- **Contesto normativo – La funzione di conformità nella normativa nazionale**
- **Il contesto di riferimento - Elementi di benchmarking**
- **Il caso Intesa Sanpaolo**

Intesa Sanpaolo - Struttura organizzativa

In Intesa Sanpaolo il sistema di presidio del rischio di compliance è parte integrante del **sistema complessivo dei controlli interni** del Gruppo



Responsabilità

In Intesa Sanpaolo le **Linee Guida di Compliance di Gruppo**, redatte in stretta coerenza con le indicazioni contenute nelle Disposizioni di Vigilanza e nel Regolamento congiunto di Banca d'Italia e Consob, definiscono il sistema di presidio del rischio di compliance

Principi guida - ambiti normativi

- **Presidi diretti** - ambiti normativi presidiati direttamente dalla Direzione Compliance
  - servizi d'investimento
  - intermediazione assicurativa e previdenziale
  - market abuse
  - conflitti di interesse
  - operazioni personali
  - sollecitazione all'investimento
  - trasparenza delle condizioni contrattuali
  - credito alle famiglie
  - usura
  - pratiche commerciali scorrette
  - sistemi di pagamento
  - responsabilità amministrativa degli Enti
  - antiriciclaggio
  - embarghi
  - banca depositaria
- **Presidi indiretti** - ambiti normativi con compiti di compliance attribuiti ad altre strutture
  - operazioni con parti correlate
  - obbligazioni degli esponenti del Gruppo bancario
  - tutela della concorrenza
  - tutela della privacy
  - internal dealing
  - insider list sui titoli Intesa Sanpaolo e di Società del Gruppo
  - tutela ambientale
  - sicurezza sul lavoro

Linee guida - macro processi di compliance

Le Linee guida definiscono i principali **macro processi** che descrivono **le modalità di presidio del rischio di non conformità**

Principi guida - Modello di governo sul Gruppo

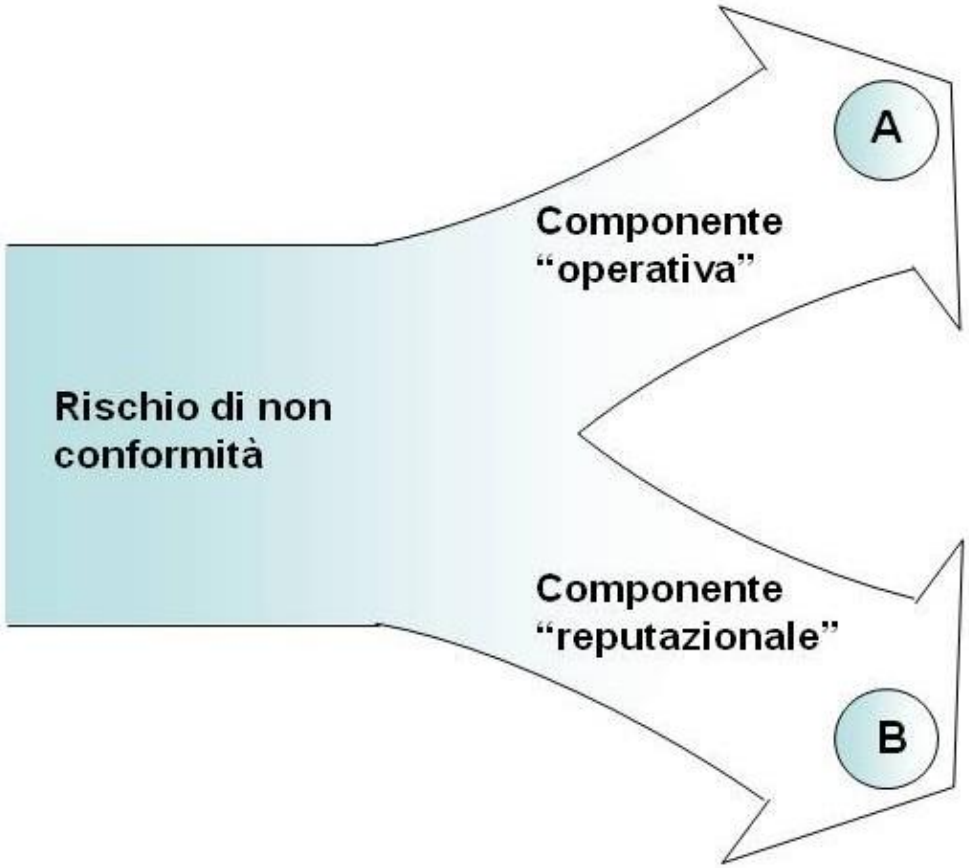
Società con accentramento del presidio della conformità presso la Capogruppo

- Banche Rete in service che hanno adottato sistema informativo target
- Società italiane con operatività fortemente integrata con quella di Capogruppo

Società e Filiali estere con funzioni di conformità interne e Compliance Officer locale

- Banche Rete in governance
- Altre Banche e Società Italiane
- Banche della Divisione Banche Estere
- Banche estere della Divisione Corporate e IB
- Filiali estere di Capogruppo

Valutazione del rischio di compliance



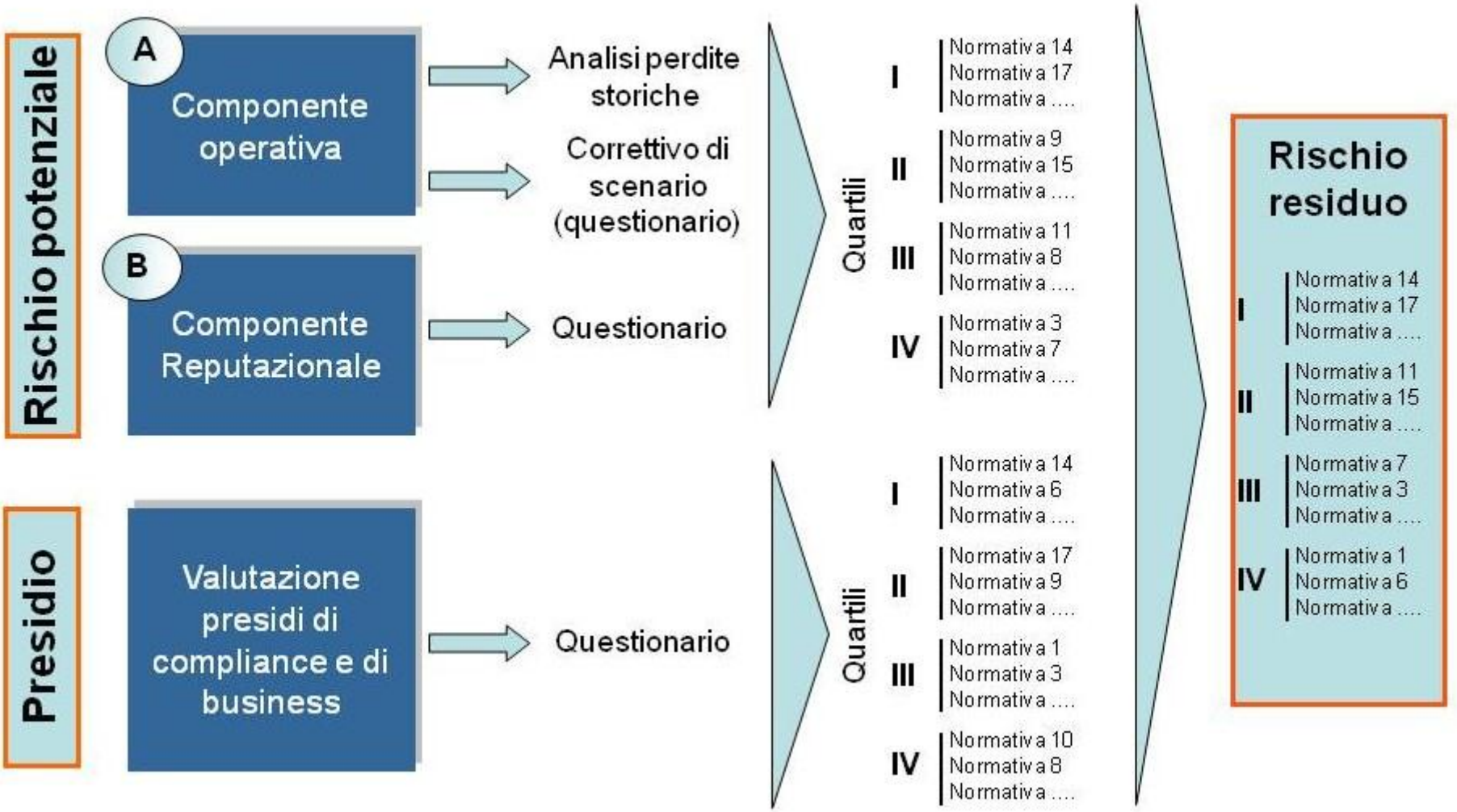
Rischio di incorrere in **sanzioni** giudiziarie o amministrative e **perdite finanziarie** rilevanti in **conseguenza** di **violazione** di **norme** imperative (di legge o regolamenti) o di **autoregola-mentazione** (es., statuti, codici di condotta, codici di auto-disciplina di categoria)

+

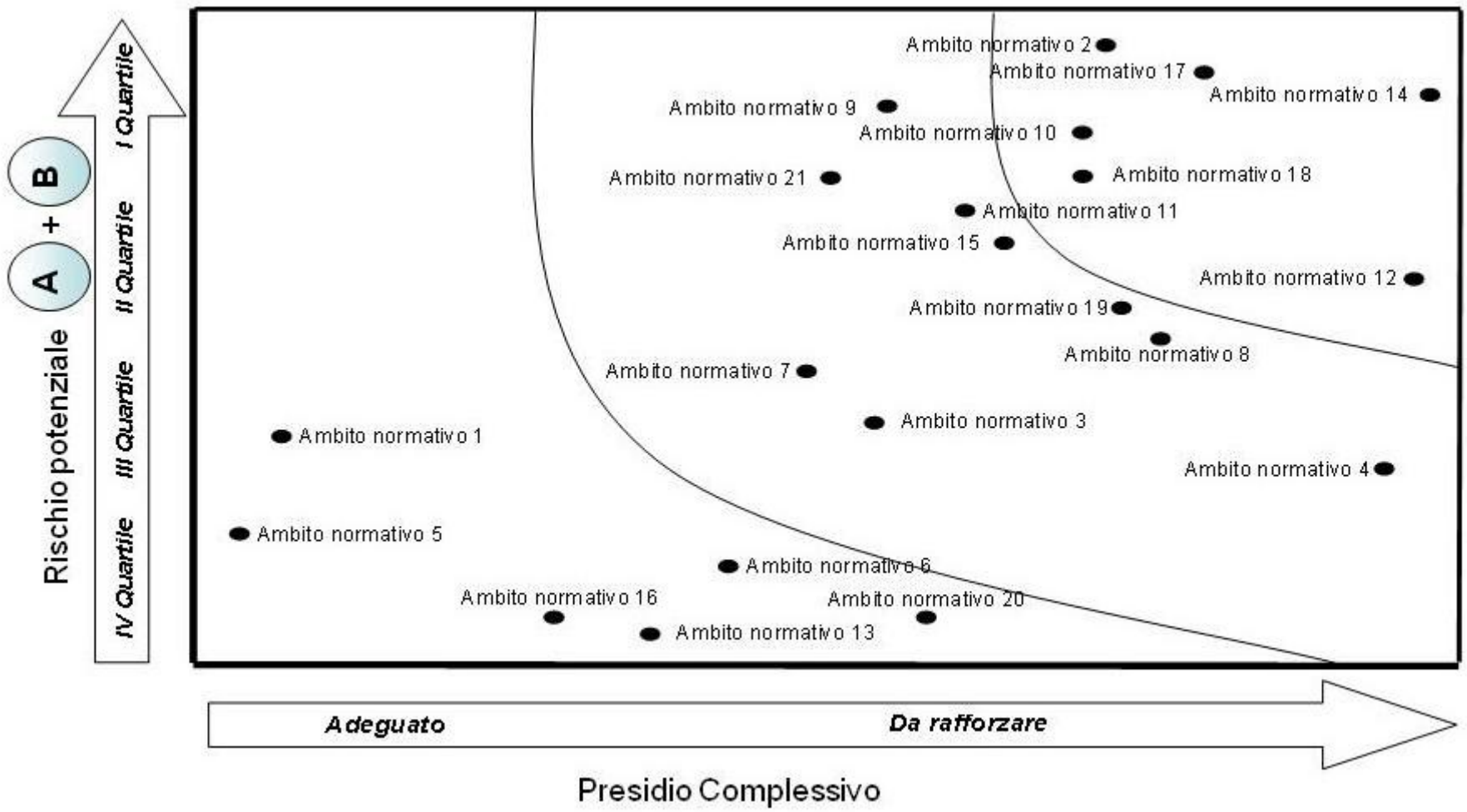
Rischio di sostenere un **aggravio** delle **perdite** finanziarie derivanti da comportamenti di **non conformità** (addizionali rispetto alla perdita conseguente l'evento stesso), connessi ad una **perdita** di **reputazione** della banca

Fonte: Elaborazioni Circ. Bankit, Libro bianco dell'ABI sulla Funzione Compliance

Valutazione dei rischi e dei presidi

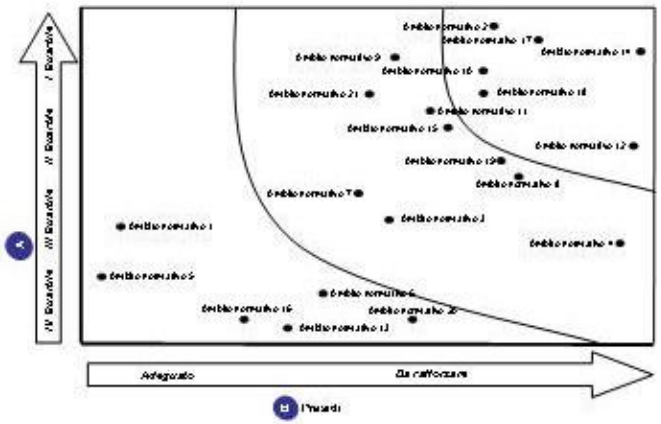


Matrice rischi/presidi



Relazione annuale e Tableau de Bord Compliance

Risk Assessment → Relazione annuale → Tableau de Bord di Compliance



Reporting integrato

- Vista integrata delle evidenze ad alta criticità e del **presidio dei rischi operativi e reputazionali del Gruppo**
- Strumento di indirizzo e monitoraggio del piano degli interventi prioritari
- Contenuto del Reporting:
  - **perdite operative** ripartite per processo
  - **indicatori sintetici** riferiti al presidio della business continuity e della normativa aziendale
  - evidenze delle **criticità/necessità di intervento** ad alta rilevanza e connesse **azioni di mitigazione**
- Strutture coinvolte: Direzioni Compliance, Risk Management, Organizzazione e Sicurezza, Amministrazione e Fiscale e Direzione Internal Auditing

Reporting integrato - cruscotto indicatori

Processi	Perdite Operative				Business continuity (1)		Normativa		Numero evidenze ad alta criticità per categoria di rischio				Numero azioni di mitigazione in ritardo e/o critiche !
	Numero eventi di perdita (1° sem.)	Importi (€/000)			Grado di rilevanza (luglio 09)	Grado di copertura dei sistemi (luglio 09)	Grado di formaliz-zazione processi target (giugno 09)	Trend (2)	Compliance	Informativa Finanziaria	Business Continuity	Altri Rischi Operativi e Reputazionali	
		Perdite registrate (1° sem.)	Stima annua da analisi di scenario	Rapporto tra perdite registrate e perdite stimate									
Indirizzo e controllo	n	€	€	%	n	n	%	⇨	n	n	n	n	n
Gestione risorse													
Servizi di supporto al business													
Gestione Finanza													
Gestione Credito													
Gestione Operations													
Sviluppo e vendita prodotti													
Totali													

(1) Valori indicati su una scala da 1 a 4 per il grado di rilevanza da 0 a 4 per il grado di copertura dei sistemi

(2) Trend rispetto inizio anno: ⇧ aumento superiore al 30%; ⇗ aumento compreso tra il 10% e il 30%; ⇨ invariato o variazione compresa tra +/- 10%; ⇘ diminuzione compresa tra il 10% e il 30%; ⇩ diminuzione superiore al 30%

LA FUNZIONE *COMPLIANCE* NEL SETTORE ASSICURATIVO: PROFILI OPERATIVI

Dott. Vittorio Frigerio
Partner Responsabile Settore Assicurativo
Deloitte & Touche S.p.A.

Agenda

Funzione di compliance: principali riferimenti internazionali

Rischio operativo, di compliance, legale, reputazionale

Regolamento ISVAP N. 20 del 26 marzo 2008

Focus sulle principali analogie e differenze nella disciplina degli intermediari

Collocazione organizzativa della funzione di compliance

Modello organizzativo

Perimetro della funzione

Reportistica/flussi informativi

Interrelazioni con le altre funzioni

Appendice

Funzione di compliance: principali riferimenti internazionali

L'istituzione della funzione di compliance nel settore assicurativo, in linea con i più recenti orientamenti internazionali, riveste un duplice ruolo:

- ✓ **migliorare il generale sistema dei controlli interni e quindi la governance;**
- ✓ **agevolare la graduale transizione verso il nuovo regime di Solvency II.**

Rigorosi *requirments* in materia di *governance* sono il prerequisito di un regime di solvibilità efficiente. Il presidio di alcune tipologie di rischio (e.g. rischio reputazionale) non possono essere affrontati se non fissando requisiti di governance.

Un solido sistema di *governance* è pertanto di importanza fondamentale per l'adeguata gestione dell'impresa di assicurazione.

Per ottemperare a queste esigenze la direttiva *Solvency* II prevede l'istituzione di una funzione di verifica permanente dell'osservanza della normativa vigente.

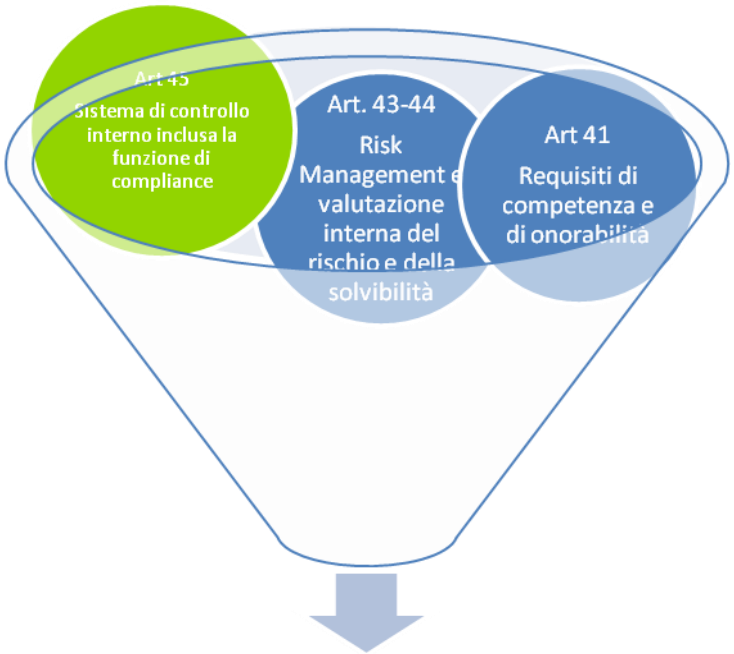
I compiti assegnati alla funzione di verifica permanente sono:

- ✓ **la valutazione del possibile impatto di qualsiasi variazione del quadro giuridico sulle operazioni dell'impresa interessata nonché l'identificazione e la valutazione del rischio di mancata osservanza della normativa vigente;**

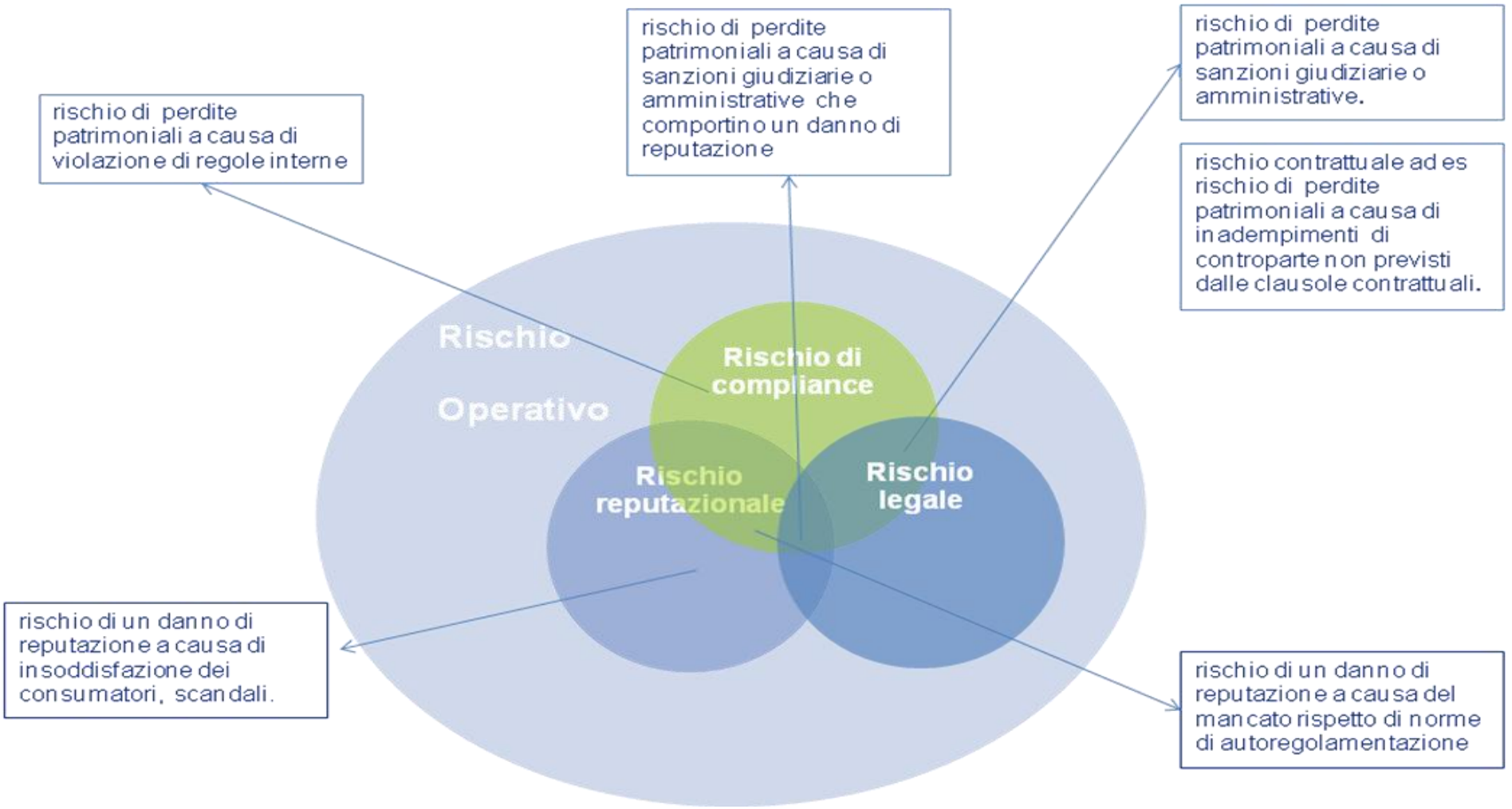
- ✓ **la consulenza all'organo amministrativo o direttivo in merito al rispetto delle disposizioni legislative, regolamentari e amministrative adottate in applicazione della presente direttiva.**

Funzione di compliance: principali riferimenti internazionali

Nell'ambito della normativa Solvency II la funzione di compliance è inserita nel cosiddetto Pillar 2 alla base del sistema di *governance* complessivo:



Rischio operativo, di compi anche, legale, reputazionale



Regolamento ISVAP N. 20 del 26 marzo 2008

Principi sottostanti all'istituzione della funzione di compliance

- **Obiettivi: valutare che l'organizzazione e le procedure interne siano adeguate rispetto all'obiettivo di prevenire il rischio di incorrere in sanzioni giudiziarie o amministrative, perdite patrimoniali o danni di reputazione, in conseguenza di violazioni di leggi, regolamenti o provvedimenti delle Autorità di vigilanza ovvero di norme di autoregolamentazione.**

- **Focus su rapporti con consumatore: nella identificazione e valutazione del rischio di non conformità alle norme, le imprese pongono particolare attenzione al rispetto delle norme relative alla trasparenza e correttezza dei comportamenti nei confronti degli assicurati e danneggiati, all'informativa precontrattuale e contrattuale, alla corretta esecuzione dei contratti, con particolare riferimento alla gestione dei sinistri e, più in generale, alla tutela del consumatore.**

- **Istituzione: formalizzata in una specifica delibera dell'organo amministrativo, che ne definisce le responsabilità, i compiti, le modalità operative, la natura e la frequenza della reportistica agli organi sociali e alle altre funzioni interessate.**

- **Caratteristiche: proporzionalità, indipendenza, adeguatezza qualitativa e quantitativa delle risorse, separatezza dalle funzioni operative e dalle altre funzioni di controllo.**

- **Attività:**
-
  - **a) identifica in via continuativa le norme applicabili all'impresa e valuta il loro impatto sui processi e le procedure aziendali;**
  - **b) valuta l'adeguatezza e l'efficacia delle misure organizzative adottate per la prevenzione del rischio di non conformità alle norme e propone le modifiche organizzative e procedurali finalizzate ad assicurare un adeguato presidio del rischio;**
  - **c) valuta l'efficacia degli adeguamenti organizzativi conseguenti alle modifiche suggerite;**
  - **d) predispone adeguati flussi informativi diretti agli organi sociali dell'impresa e alle altre strutture coinvolte.**

- **Responsabile della funzione: nominato e revocato dall'organo amministrativo; deve essere in possesso di adeguati requisiti di professionalità, indipendenza ed autorevolezza.**
- **Esternalizzazione: possibile quando per le ridotte dimensioni e per le caratteristiche operative, l'istituzione di una specifica funzione di compliance non risponda a criteri di economicità.**

Focus dulle principali analogie e differenze nella disciplina degli intermediari

PRINCIPALI COMPITI ASSEGNATI

Servizi Bancari Banche
(Provvedimento Banca d'Italia del 10/7/2007)

Principali adempimenti

- 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 diretti agli organi aziendali e alle strutture coinvolte (gestione del rischio op. e revisione interna);

- la verifica dell'efficacia degli adeguamenti organizzativi (strutture, processi, procedure anche operative e commerciali) suggeriti per la prevenzione del rischio di conformità.

Altri adempimenti

-Valutazione ex ante della conformità dei nuovi progetti e prevenzione conflitti di interesse

-Valutazione coerenza del sistema premiante (incentivazione)

- Consulenza/assistenza ai vertici aziendali

-Formazione

Servizi e attività di investimento Banche /SIM/ SGR
(Regolamento Congiunto Banca d'Italia-Consob)

Principali adempimenti

-controllare e valutare regolarmente l'adeguatezza e l'efficacia delle procedure adottate per la prestazione dei servizi e delle misure adottate per rimediare a eventuali carenze nell'adempimento degli obblighi da parte dell'intermediario

-fornire consulenza e assistenza ai soggetti rilevanti incaricati dei servizi ai fini dell'adempimento degli obblighi posti dalle disposizioni di recepimento della direttiva 2004/39/CE e delle relative misure di esecuzione.

Assicurazioni
(Regolamento Isvap n.20)

Principali adempimenti

a) identifica in via continuativa le norme applicabili all'impresa e valuta il loro impatto sui processi e le procedure aziendali;

b) valuta l'adeguatezza e l'efficacia delle misure organizzative adottate per la prevenzione del rischio di non conformità alle norme e propone le modifiche organizzative e procedurali finalizzate ad assicurare un adeguato presidio del rischio;

c) valuta l'efficacia degli adeguamenti organizzativi conseguenti alle modifiche suggerite;

d) predispone adeguati flussi informativi diretti agli organi sociali dell'impresa e alle altre strutture coinvolte.

Collocazione organizzativa della funzione di compliance

- **La collocazione organizzativa della funzione di compliance nell'organigramma aziendale deve realizzare i seguenti principi dettati dal Regolamento n. 20:**
  - **separatezza dalle funzioni operative e dalle altre funzioni di controllo;**
  - **indipendenza;**
  - **libero accesso a tutte le attività dell'impresa e a tutte le informazioni pertinenti;**
  - **risorse qualitativamente e quantitativamente adeguate.**

- **I requisiti sopra indicati comportano una collocazione della funzione di compliance preferibilimente in staff all'organo amministrativo.**

- **Nella prassi operativa, in caso di funzione di compliance posta a diretto riporto dell'organo amministrativo, si è posto il problema di trovare un interlocutore per la risoluzione di problematiche day by day.**

- **Dall'esame delle relazioni annuali sul governo societario (2008) delle principali società quotate emerge che:**
  - **Fondiaria-Sai: la funzione di Compliance riporta al Consiglio d'Amministrazione;**
  - **Generali: la funzione riporta al Consiglio d'Amministrazione per il tramite del Comitato per il Controllo Interno,**

– **Cattolica: la funzione riporta al Presidente del Consiglio d'Amministrazione.**

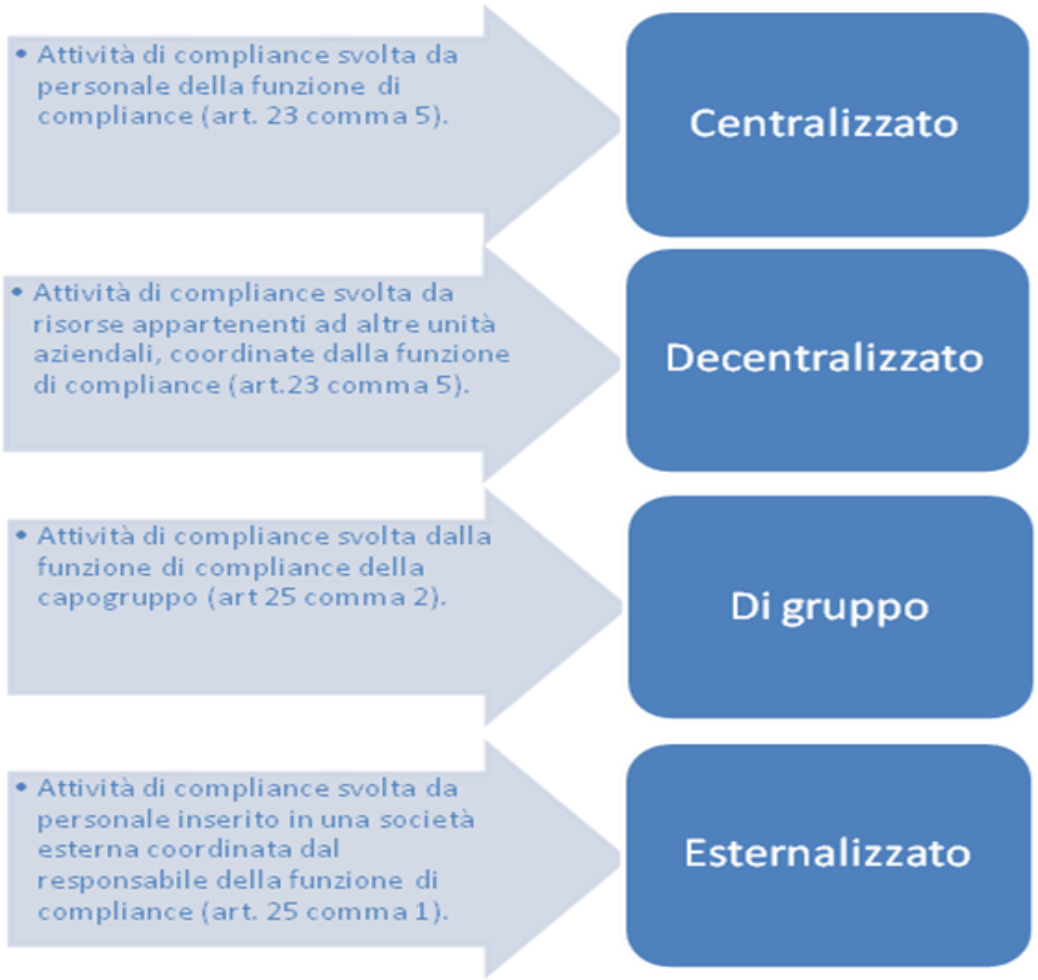
Modello organizzativo

Modello organizzativo

La scelta del modello organizzativo della funzione di compliance deve basarsi sui criteri di:

- proporzionalità alle caratteristiche strutturali ed operative dell'impresa;
- coerenza con le dimensioni aziendali e con l'assetto organizzativo e strategico dell'impresa.

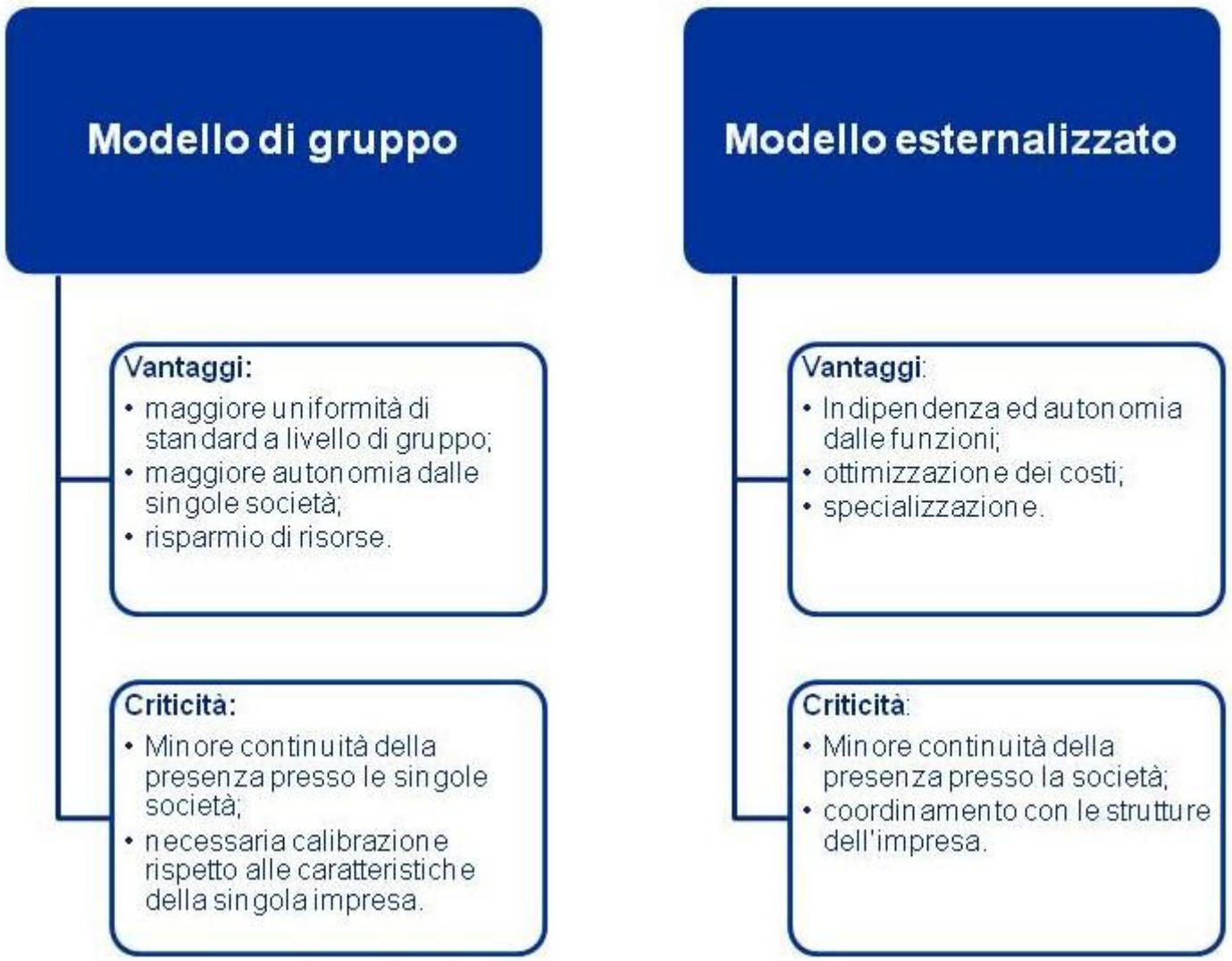
Dal dettato normativo sono individuabili i modelli organizzativi illustrati a fianco.



Modello centralizzato

Modello decentralizzato

Modello organizzativo



Modello organizzativo

Dalle prime esperienze nel campo della compliance delle compagnie di assicurazione emerge che:

Le società singole o appartenenti a gruppi di matrice bancaria	Le società appartenenti a gruppi assicurativi internazionali	Le società appartenenti a gruppi nazionali
• generalmente hanno istituito una funzione di compliance adottando un modello decentralizzato o esternalizzato a seconda dell'economicità della scelta.	• generalmente dotate di una funzione di compliance preesistente all'introduzione del regolamento 20, hanno previsto un sistema di riporto gerarchico all'organo amministrativo e dei riporti funzionali alla struttura di compliance gruppo.	• generalmente prevedono una funzione di compliance di gruppo per le società assicurative e funzioni di compliance decentralizzate per le società prodotto non assicurative.

Modello organizzativo

Dall'esame delle relazioni annuali sul governo societario (2008) delle principali società quotate emerge che:

- **GRUPPO GENERALI: istituzione di una funzione di gruppo collocata presso la Capogruppo. Le attività di compliance vengono svolte nell'ambito del modello di Compliance di Gruppo che prevede:**

  - **Controlli di primo livello inseriti nell'ambito delle singole unità operative; identificati a livello delle principali macro aree funzionali (Danni, Vita , Finanza…) degli Incaricati Compliance di Business Unit che assicurano un presidio del rischio di non conformità per le relative aree di competenza;**

  - **La funzione di compliance che costituisce un presidio aggiuntivo ed indipendente del complessivo Sistema dei Controlli Interni e di Gestione dei Rischi, focalizzato sul rischio di non conformità.**

- **Gruppo Unipol: la funzione di Compliance è accentrata nella Capogruppo; da questo accentramento sono escluse UGF Banca S.p.A. e le società del relativo Gruppo Bancario.**

- **Gruppo Fondiaria-Sai: la funzione di Compliance è accentrata nella Capogruppo.**

Perimetro della funzione

- **Il perimetro di operatività della funzione di Compliance è costituito dall'insieme di norme il cui rispetto deve essere presidiato dalla funzione.**

- **Il perimetro normativo della funzione di Compliance è molto esteso in quanto indicativamente correlato ad una qualsiasi norma sia esterna che interna (cfr art. 22 Regolamento Isvap n. 20).**

- **La normativa non contiene una descrizione delle norme cui le compagnie devono attenersi tuttavia il Regolamento Isvap n. 20 sottolinea l'importanza della tutela del consumatore intesa come rispetto delle norme relative alla trasparenza, correttezza dei comportamenti vs assicurati e danneggiati, informativa precontrattuale e contrattuale**

Reportistica / flussi informativi

Deloitte.

- **L'organo di controllo, la società di revisione, la funzione di revisione interna, di risk management e di compliance, l'organismo di vigilanza l'attuario incaricato e ogni altro organo o funzione a cui è attribuita una specifica funzione di controllo collaborano tra di loro, scambiandosi ogni informazione utile per l'espletamento dei rispettivi compiti (art. 17 Reg. 20 ISVAP).**

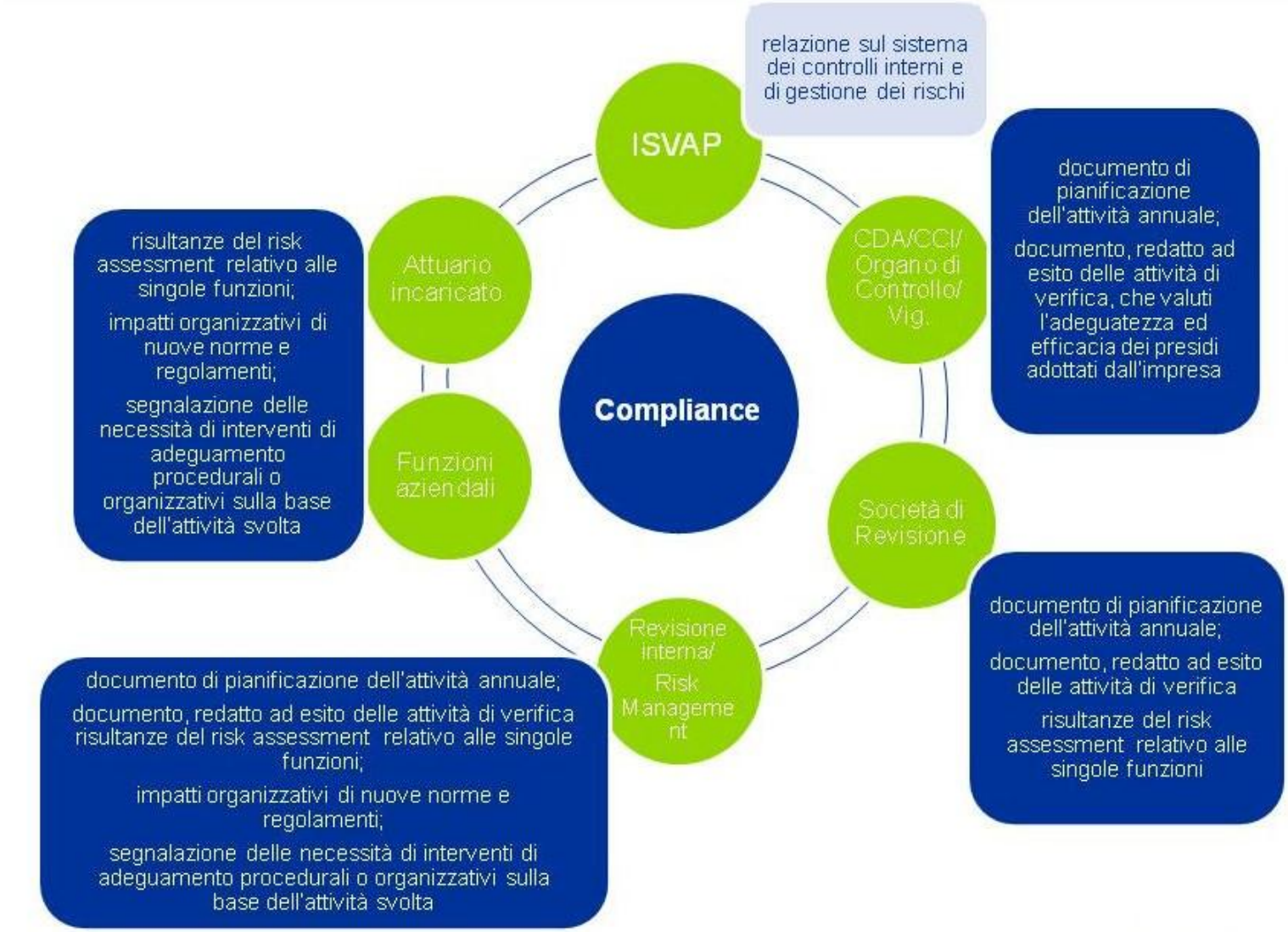
- **La delibera dell'organo amministrativo che istituisce la funzione di compliance definisce la natura e la frequenza della reportistica agli organi sociali ed alle altre funzioni interessate (art. 23 Reg. 20 ISVAP).**

- **Il responsabile della funzione predispone, almeno una volta l'anno, una relazione all'organo amministrativo sulla adeguatezza ed efficacia dei presidi adottati dall'impresa per la gestione del rischio di non conformità alle norme (art. 24 Reg. 20 ISVAP).**

- **Unitamente al bilancio di esercizio, le imprese trasmettono all'ISVAP una relazione sul sistema dei controlli interni e di gestione dei rischi, che illustri le iniziative eventualmente intraprese nell'esercizio o le modifiche apportate, le attività di revisione**

interna svolte, le eventuali carenze segnalate e le azioni correttive adottate (art. 28 Reg. 20 ISVAP).

Reportistica / flussi informativi



Reportistica / flussi informativi

Dalle relazioni annuali delle compagnie quotate emergono le seguenti informazioni relative alla reportistica nei confronti degli organi sociali:

- **Gruppo Generali: il responsabile della funzione riporta con cadenza almeno annuale al Consiglio d'Amministrazione anche per il tramite del Comitato per il Controllo Interno, predisponendo una relazione sui presidi adottati dall'impresa per la gestione del rischio di non conformità alle norme. In particolare, la relazione illustra sia le valutazioni effettuate sulle aree di rischio di non conformità sia le misure adottate per rimediare ad eventuali carenze rilevate. La funzione sottopone all'esame ed approvazione del Consiglio d'Amministrazione, previa presentazione al Presidente del Comitato per il Controllo Interno, il compliance plan delle attività pianificate .**

  Le valutazioni della Funzione sono svolte su aree di rischio di non conformità prescelte, di regola, sulla base di un perimetro normativo di riferimento, individuato in funzione di una serie di driver (priorità, frequenza ….) e dell'evoluzione normativa in atto.

- **Gruppo Fondiaria-Sai: la funzione di compliance di Gruppo predispone annualmente un proprio piano di intervento che viene sottoposto al Consiglio d'Amministrazione di Fondiaria-Sai.**

Interrelazioni con le altre funzioni

Deloitte.

- **Revisione Interna**
- **Risk management**
- **Funzione legale**
- **Funzione Organizzazione**

Interrelazioni con le altre funzioni

In merito al collegamento tra la funzione di compliance e le funzioni di revisione interna e risk management richiesto dall'art. 23 Regolamento ISVAP n. 20, la relazione Fondiaria-Sai riporta:

- **Il responsabile della funzione di Compliance di Gruppo, inoltre, coordina un apposito Comitato di Compliance e di Coordinamento Funzioni di Governance, avente come membri permanenti i responsabili della funzione di Audit e della funzione di Risk Management, nonché di altre funzioni accentrate a livello di Gruppo.**

- **Tale Comitato è un contesto formalizzato e regolamentato attraverso il quale, preservando al contempo le caratteristiche di autonomia ed indipendenza proprie delle funzioni coinvolte, si intende perseguire, in relazione al sistema di controllo interno e di gestione dei rischi del Gruppo FONDIARIA-SAI, i seguenti obiettivi:**

  - **consentire alla funzione di compliance di individuare le principali iniziative da intraprendere,**
  - **garantire il coordinamento funzionale delle strutture coinvolte nel processo di governance,**
  - **garantire il coordinamento, pur nel rispetto delle specifiche autonomie, dei piani delle singole strutture,**

- favorire l'interscambio delle conoscenze e delle problematiche gestite dalle singole strutture,
- definire e concordare linee guida di intervento con relativa definizione dei livelli di priorità.

Appendice

Principali analogie e differenze nella disciplina degli intermediari

Principali compiti assegnati

Reporting

Il perimetro di competenza

La funzione di compliance: costituzione e nomina del responsabile

Principali analogie e differenze nella disciplina degli intermediari

PRINCIPALI COMPITI ASSEGNATI

Servizi Bancari Banche (*Provvedimento Banca d'Italia del 10/7/2007*)	*Servizi e attività di investimento Banche / SIM / SGR* (*Regolamento Congiunto Banca d'Italia-Consob*)	Assicurazioni (Regolamento Isvap n.20)
Principali adempimenti - 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 diretti agli organi aziendali e alle strutture coinvolte (gestione del rischio op. e revisione interna); - la verifica dell'efficacia degli adeguamenti organizzativi (strutture, processi, procedure anche operative e commerciali) suggeriti per la prevenzione del rischio di conformità.	**Principali adempimenti** -controllare e valutare regolarmente l'adeguatezza e l'efficacia delle procedure adottate per la prestazione dei servizi e delle misure adottate per rimediare a eventuali carenze nell'adempimento degli obblighi da parte dell'intermediario -fornire consulenza e assistenza ai soggetti rilevanti incaricati dei servizi ai fini dell'adempimento degli obblighi posti dalle disposizioni di recepimento della direttiva 2004/39/CE e delle relative misure di esecuzione.	**Principali adempimenti** a) identifica in via continuativa le norme applicabili all'impresa e valuta il loro impatto sui processi e le procedure aziendali; b) valuta l'adeguatezza e l'efficacia delle misure organizzative adottate per la prevenzione del rischio di non conformità alle norme e propone le modifiche organizzative e procedurali finalizzate ad assicurare un adeguato presidio del rischio; c) valuta l'efficacia degli adeguamenti organizzativi conseguenti alle modifiche suggerite; d) predispone adeguati flussi informativi diretti agli organi sociali dell'impresa e alle altre strutture coinvolte.
Altri adempimenti -Valutazione ex ante della conformità dei nuovi progetti e prevenzione conflitti di interesse -Valutazione coerenza del sistema premiante (incentivazione) - Consulenza/assistenza ai vertici aziendali -Formazione		

Principali analogie e differenze nella disciplina degli intermediari

REPORTING

Servizi Bancari Banche (*Provvedimento Banca d'Italia del 10/7/2007*)	*Servizi e attività di investimento Banche /SIM/ SGR* (*Regolamento Congiunto Banca d'Italia-Consob*)	Assicurazioni (Regolamento Isvap n.20)
Reporting -Riferire di iniziativa o su richiesta, almeno una volta all'anno, al consiglio di amministrazione e al collegio sindacale sull'adeguatezza della gestione del rischio di non conformità attuata dalla banca; -Fornire tempestiva informazione al consiglio di amministrazione e al collegio sindacale su ogni violazione rilevante della conformità alle norme (es. violazioni che possono comportare un alto rischio di sanzioni regolamentari o legali, perdite finanziarie di rilievo o danno di reputazione).	**Reporting** -La funzione di controllo di conformità presenta agli organi aziendali, con periodicità almeno annuale, le relazioni sull'attività svolta. Le relazioni illustrano, per ciascun servizio prestato dall'intermediario, le verifiche effettuate e i risultati emersi, le misure adottate per rimediare a eventuali carenze rilevate nonché le attività pianificate. Le relazioni riportano altresì la situazione complessiva dei reclami ricevuti, sulla base dei dati forniti dalla funzione incaricata di trattarli, qualora differente dalla funzione di controllo di conformità.	**Reporting** -Il responsabile della funzione predispone, almeno una volta l'anno, una relazione all'organo amministrativo sulla adeguatezza ed efficacia dei presidi adottati dall'impresa per la gestione del rischio di non conformità alle norme

Principali analogie e differenze nella disciplina degli intermediari

IL PERIMETRO DI COMPETENZA

Servizi Bancari Banche (Provvedimento Banca d'Italia del 10/7/2007)	*Servizi e attività di investimento Banche / SIM / SGR* (Regolamento Congiunto Banca d'Italia-Consob)	**Assicurazioni** (Regolamento Isvap n.20)
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 imperative (di legge o di regolamenti) ovvero di autoregolamentazione (es. statuti, codici di condotta, codici di autodisciplina)	**Rischio di non conformità alle norme** Non definito esplicitamente (mancato rispetto delle disposizioni contenute nelle Direttive MIFID)	**Rischio di non conformità alle norme** Il rischio di incorrere in sanzioni giudiziarie o amministrative, perdite patrimoniali o danni di reputazione, in conseguenza di violazioni di leggi, regolamenti o provvedimenti delle Autorità di vigilanza ovvero di norme di autoregolamentazione.
Norme rilevanti da presidiare (perimetro minimale) 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.	**Norme rilevanti da presidiare (perimetro minimale)** Osservanza degli obblighi posti dalle disposizioni di recepimento della direttiva 2004/39/CE e delle relative misure di esecuzione (servizi e attività di investimento / gestione collettiva del risparmio)	**Norme rilevanti da presidiare (perimetro minimale)** Trasparenza e correttezza dei comportamenti nei confronti degli assicurati e danneggiati, all'informativa precontrattuale e contrattuale, alla corretta esecuzione dei contratti, con particolare riferimento alla gestione dei sinistri e, più in generale, alla tutela del consumatore.

Principali analogie e differenze nella disciplina degli intermediari

LA FUNZIONE DI COMPLIANCE: COSTITUZIONE E NOMINA DEL RESPONSABILE

Servizi Bancari Banche *(Provvedimento Banca d'Italia del 10/7/2007)*	*Servizi e attività di investimento Banche / SIM / SGR* *(Regolamento Congiunto Banca d'Italia-Consob)*	**Assicurazioni** **(Regolamento Isvap n.20)**
Nomina del responsabile Requisiti di indipendenza, autorevolezza e professionalità Nomina / revoca di competenza esclusiva del CdA, sentito il Collegio Sindacale	**Nomina del responsabile** Il responsabile non è gerarchicamente subordinati ai responsabili delle funzioni sottoposte a controllo ed è nominato dall'organo con funzione di gestione, d'accordo con l'organo di supervisione strategica, sentito l'organo con funzioni di controllo	**Nomina del responsabile** Requisiti di indipendenza, autorevolezza e professionalità. La nomina e la revoca sono di competenza dell'organo amministrativo (CdA)
Regolamento / Procedure della Funzione Il CdA, sentito il Collegio sindacale, approva le politiche di gestione del rischio di non conformità, inclusa la costituzione della funzione. Predisposizione di un documento interno che indichi responsabilità, compiti, modalità operative, flussi informativi, programmazione e risultati dell'attività svolta dalla funzione di conformità	**Regolamento/ Procedure della Funzione** Gli intermediari adottano procedure adeguate al fine di prevenire e individuare le ipotesi di mancata osservanza degli obblighi posti dalle disposizioni di recepimento della direttiva 2004/39/CE e delle relative misure di esecuzione, minimizzare e gestire in modo adeguato le conseguenze che ne derivano, nonché consentire alle autorità di vigilanza di esercitare efficacemente i poteri loro conferiti dalla relativa normativa.	**Regolamento/Procedure della Funzione** L'istituzione della funzione di compliance è formalizzata in una specifica delibera dell'organo amministrativo, che ne definisce le responsabilità, i compiti, le modalità operative, la natura e la frequenza della reportistica agli organi sociali e alle altre funzioni interessate.

Principali analogie e differenze nella disciplina degli intermediari

REQUISITI ORGANIZZATIVI MINIMI

Servizi Bancari Banche (*Provvedimento Banca d'Italia del 10/7/2007*)	*Servizi e attività di investimento Banche / SIM / SGR* (*Regolamento Congiunto Banca d'Italia-Consob*)	Assicurazioni (Regolamento Isvap n.20)
Indipendenza Nominato un responsabile indipendente; Presenza di adeguati presidi per prevenire i conflitti di interesse 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).	**Indipendenza** a) I responsabili della Funzione non sono gerarchicamente subordinati ai responsabili delle funzioni sottoposte a controllo. Essi riferiscono direttamente agli organi aziendali. b) i soggetti rilevanti che partecipano alle funzioni aziendali di controllo non partecipino alla prestazione dei servizi che essi sono chiamati a controllare; c) le funzioni aziendali di controllo siano tra loro separate, sotto un profilo organizzativo; d) il metodo per la determinazione della remunerazione dei soggetti rilevanti che partecipano alle funzioni aziendali di controllo non ne comprometta l'obiettività.	**Indipendenza** - Adozione di adeguati requisiti di indipendenza - Le imprese valutano se costituire la Funzione in forma di specifica unità organizzativa o mediante il ricorso a risorse appartenenti ad altre unità aziendali. In tale ultimo caso l'indipendenza va garantita attraverso la presenza di adeguati presidi per garantire separatezza di compiti e prevenire conflitti di interesse. - E' garantita la separatezza della funzione di compliance dalle funzioni operative e dalle altre funzioni di controllo.
Risorse qualitativamente e quantitativamente adeguate ai compiti da svolgere	**Risorse** Dispongono delle risorse e delle competenze necessarie per lo svolgimento dei loro compiti	**Risorse** Quantitativamente e professionalmente adeguate per lo svolgimento delle attività

Principali analogie e differenze nella disciplina degli intermediari

REQUISITI ORGANIZZATIVI MINIMI segue

Servizi Bancari Banche (Provvedimento Banca d'Italia del 10/7/2007)	*Servizi e attività di investimento Banche /SIM/ SGR* (Regolamento Congiunto Banca d'Italia-Consob)	Assicurazioni (Regolamento Isvap n.20)
Rapporti con altre funzioni aziendali Collabora con le altre funzioni presenti in azienda (es. revisione interna, controllo del rischio operativo, funzione legale, organizzazione, organismo di vigilanza individuato ai sensi della legge 231/2001, ecc.) allo scopo di sviluppare le proprie metodologie di gestione del rischio in modo coerente con le strategie e l'operatività aziendale, disegnando processi conformi. Specifica attenzione è posta nell'articolazione dei flussi informativi tra le due funzioni; in particolare il responsabile della revisione interna informa il responsabile della conformità per le eventuali inefficienze nella gestione del rischio emerse nel corso delle attività di verifica di propria competenza	**Rapporti con altre funzioni aziendali** Le funzioni aziendali di controllo siano tra loro separate, sotto un profilo organizzativo	**Rapporti con altre funzioni aziendali** Il collegamento tra la funzione di compliance e le funzioni di revisione interna e di risk management è definito e formalizzato dall'organo amministrativo. La funzione di compliance è comunque separata dalla funzione di revisione interna ed è sottoposta a verifica periodica da parte della stessa.
Revisione della Funzione -Almeno una volta l'anno il consiglio di amministrazione, sentito il collegio sindacale, valuta l'adeguatezza e a tal fine può avvalersi di un comitato costituito al suo interno; - Assoggettatamento a verifica della funzione di revisione interna	**Revisione della Funzione** Assoggettatamento a verifica della funzione di revisione interna	**Revisione della Funzione** Assoggettatamento a verifica della funzione di revisione interna

Principali analogie e differenze nella disciplina degli intermediari

REQUISITI ORGANIZZATIVI MINIMI segue

Servizi Bancari Banche (*Provvedimento Banca d'Italia del 10/7/2007*)	*Servizi e attività di investimento Banche / SIM / SGR* (*Regolamento Congiunto Banca d'Italia-Consob*)	Assicurazioni (Regolamento Isvap n.20)
Outsourcing E' prevista la possibilità di esternalizzare la funzione di compliance a strutture di gruppo ovvero a terzi dotati di requisiti idonei in termini di professionalità e indipendenza. Per l'esternazzzazione della funzione si rende necessaria l'adozione di adeguati presidi organizzativi e contrattuali (nomina di un responsabile sulle attività esternalizzate / referente)	**Outsourcing** Gli intermediari agiscono con la competenza e la diligenza dovute quando concludono, applicano o pongono termine ad un qualsiasi accordo con il quale esternalizzano ad un fornitore di servizi funzioni operative essenziali o importanti o qualsiasi attività o servizio di investimento. Gli intermediari adottano in particolare le misure necessarie per assicurare che siano soddisfatte le condizioni minime previste dalla normativa.	**Outsourcing** E' prevista la possibilità di esternalizzare la funzione di compliance a strutture di gruppo ovvero a terzi dotati di requisiti idonei in termini di professionalità e indipendenza. Per l'esternazzzazione della funzione si rende necessaria l'adozione di adeguati presidi organizzativi e contrattuali (nomina di un responsabile sulle attività esternalizzate / referente)