Circolare della Commissione federale delle banche: Sorveglianza e controllo interno del 27 settembre 2006

Indice

I. Oggetto

La presente circolare contiene le prescrizioni relative alla „corporate governance“, alla sorveglianza dell'operato dell'impresa nonché al controllo interno e alla relativa sorveglianza da parte degli organi preposti in seno a banche, commercianti di valori mobiliari e gruppi finanziari (art. 3c cpv. 1 LBCR) nonché nei conglomerati finanziari dominati dal settore bancario o da quello del commercio di valori mobiliari (art. 3c cpv. 2 LBCR), qui di seguito tutti designati con il termine "istituti". **1**

Per controllo interno (sinonimo: sistema di controllo interno) si intende l'insieme delle strutture e dei processi di controllo interni che, a tutti i livelli dell'istituto, assicurano il suo buon funzionamento e la realizzazione degli obiettivi di politica commerciale. Il controllo interno non comprende esclusivamente le attività di controllo effettuate a posteriori, bensì anche quelle relative alla gestione e alla pianificazione. Un controllo interno efficace comprende in particolare le attività di controllo integrate nel processo di lavoro, le procedure concernenti la gestione e il rispetto delle norme applicabili (compliance), nonché un controllo dei rischi indipendente dalla gestione dei rischi e la funzione di compliance. La revisione interna verifica e valuta il controllo interno e contribuisce pertanto al suo costante affinamento. **2**

II. Campo di applicazione

La presente circolare si applica agli istituti di cui al numero marginale (di seguito nm.) 1, con le seguenti limitazioni: **3**

- Commercianti di valori mobiliari senza statuto di banca: i nm. da 18 a 40 non si applicano se vi è identità personale tra i membri del consiglio di amministrazione e la direzione operativa. I nm. da 41 a 53 si applicano per analogia. **4**

- Banchieri privati: i nm. da 18 a 40 non si applicano. I nm. da 41 a 53 si applicano per analogia. Le altre disposizioni possono subire deroghe o semplificazioni, previo accordo con la società di audit e con l'autorità di sorveglianza, nella misura in cui gli associati presentano i requisiti necessari in materia di responsabilità personale e gestione degli affari. **5**

- Filiali bancarie, commercianti di valori mobiliari, società figlie principalmente attive nel settore finanziario detenute direttamente o indirettamente da gruppi finanziari svizzeri o esteri o da conglomerati finanziari svizzeri o esteri dominati dal settore bancario o da quello del commercio di valori mobiliari: i nm. da 18 a 40 non si applicano, ma l'istituzione di un comitato di audit è auspicata. I nm. da 41 a 53 si applicano per analogia. **6**

- Succursali di istituti esteri: i nm. da 9 a 53 non si applicano. Le altre disposizioni si applicano per analogia. **7**

- Imprese che non sono principalmente attive nel settore finanziario, ma che appartengono a dei gruppi finanziari o a dei conglomerati finanziari dominati dal settore bancario o da quello del commercio di valori mobiliari: la circolare non si applica. In caso di dubbio, talune società del gruppo, su richiesta della società madre, possono essere esplicitamente esentate dalla sua applicazione. **8**

III. Consiglio di amministrazione

A. Compiti e responsabilità

a) Sorveglianza e controllo interno

Il consiglio di amministrazione, ovvero all'organo che esercita la direzione superiore, la vigilanza e il controllo, è responsabile per regolamentare, istituire, mantenere, sorvegliare e verificare regolarmente l'esistenza di un controllo interno adeguato. Il controllo interno deve essere adeguato alla dimensione, alla complessità, alla struttura e al profilo di rischio dell'istituto. **9**

Istituendo un controllo interno basato sull'analisi sistematica dei rischi e operando la relativa sorveglianza, il consiglio di amministrazione si assicura che tutti i rischi significativi ai quali l'istituto è esposto sono identificati, limitati e sorvegliati. Nei gruppi finanziari e nei conglomerati finanziari dominati dal settore bancario o da quello del commercio di valori mobiliari occorre in particolare tenere conto dei rischi risultanti dal raggruppamento di più imprese in un'entità economica unica. L'analisi sistematica dei rischi deve essere documentata per iscritto. **10**

Il consiglio di amministrazione deve discutere regolarmente con la direzione le sue valutazioni relative all'adeguatezza e all'efficacia delle misure di controllo interno. **11**

b) Ambito di controllo

Conferendo istruzioni alla direzione operativa, il consiglio di amministrazione deve fare in modo che i collaboratori di ogni grado gerarchico conoscano e comprendano quali sono le loro responsabilità e i loro compiti nell'ambito del processo del controllo interno. **12**

Il consiglio di amministrazione deve fare in modo che l'eventuale pressione esercitata sui collaboratori di ogni grado gerarchico per il conseguimento degli obiettivi non porti allo sviamento dei meccanismi di controllo. Deve assicurarsi che i sistemi di remunerazione non incitino al non rispetto dei meccanismi di controllo. **13**

Il consiglio di amministrazione deve regolamentare la gestione dei conflitti di interesse. Se in un caso concreto un conflitto di interesse non può essere evitato, l'istituto deve adottare delle misure che ne permettano la gestione. **14**

c) Istituzione e sorveglianza della revisione interna

Il consiglio di amministrazione istituisce una revisione interna che gli è direttamente subordinata o che è subordinata al comitato di audit (o a un altro comitato). Per quanto concerne l'organizzazione, i compiti, le responsabilità nonché gli obblighi di rendiconto e di informazione si rinvia ai nm. da 54 a 79. **15**

Il consiglio di amministrazione o il comitato responsabile sorveglia e giudica l'efficacia della revisione interna e si assicura regolarmente che la stessa disponga delle risorse e delle competenze appropriate nonché dell'indipendenza e dell'obiettività adeguate per svolgere i propri compiti di controllo in seno all'istituto. **16**

B. Membri del consiglio di amministrazione

a) Requisiti generali

Per svolgere i propri compiti il consiglio di amministrazione deve soddisfare, quale gremio, i requisiti necessari a tal fine e segnatamente in termini di competenze professionali, di esperienza e di disponibilità. Valuta almeno una volta all'anno e documenta per iscritto il raggiungimento degli obiettivi e la propria modalità di lavoro. **17**

b) Indipendenza

I membri del consiglio di amministrazione organizzano i loro rapporti personali e professionali in modo da evitare, per quanto possibile, conflitti di interesse con l'istituto. In virtù dell'art. 8 cpv. 2 OBCR i membri del consiglio di amministrazione non possono in particolare far parte contemporaneamente della direzione operativa dell'istituto. **18**

Il consiglio di amministrazione deve essere composto, per almeno un terzo, da membri che soddisfano i requisiti di indipendenza esposti ai nm. da 20 a 24. I nomi di questi membri devono figurare nel rapporto annuale. Se meno di un terzo dei membri del consiglio di amministrazione dovessero soddisfare il requisito di indipendenza, il rapporto annuale deve contenere una giustificazione in merito. **19**

Un membro del consiglio di amministrazione presenta il requisito di indipendenza se soddisfa perlomeno i seguenti criteri: **20**

- non si occupa di altre funzioni in seno all'istituto e non se ne è occupato nel corso dei due anni precedenti; **21**
- non ha svolto la funzione di revisore responsabile dell'istituto presso la società di audit nel corso dei due anni precedenti; **22**
- non intrattiene con l'istituto relazioni d'affari che, per natura o importanza, potrebbero creare un conflitto d'interesse; e **23**
- non detiene una partecipazione qualificata (ai sensi dell'art. 3 cpv. 2 lett. c^{bis} LBCR e art. 10 cpv. 2 lett. d LBVM) dell'istituto e nemmeno rappresenta il detentore di una tale partecipazione. **24**

I membri del consiglio di amministrazione di banche cantonali o regionali designati o eletti dal cantone, dal comune o da altre corporazioni di diritto pubblico cantonali o comunali che controllano tali istituti sono considerati indipendenti ai sensi del nm. 24 se: **25**

- non appartengono al governo o all'amministrazione cantonale o comunale né ad altra corporazione di diritto pubblico cantonale o comunale, e **26**
- non ricevono istruzioni per la loro attività quale membro del consiglio di amministrazione da parte dell'organo che li ha eletti. **27**

C. Suddivisione dei compiti in seno al consiglio di amministrazione e dei suoi comitati

Il consiglio di amministrazione può istituire dei comitati incaricati di coadiuvarlo oppure assegnare dei compiti a taluni dei suoi membri. **28**

Un comitato di audit deve essere istituto se l'istituto raggiunge una certa dimensione oppure un certo grado di complessità (cfr. nm. 32-36). **29**

Se un istituto non dispone di un comitato di audit, il consiglio di amministrazione incarica uno o due suoi membri indipendenti che presentano i requisiti di cui al nm. 39, di norma ad esclusione del presidente del consiglio di amministrazione, di svolgere i compiti definiti nei nm. da 41 a 53. L'autorità di sorveglianza può concedere delle deroghe. Se i compiti menzionati sono conferiti al presidente del consiglio di amministrazione, il rapporto annuale deve contenere una giustificazione. **30**

I compiti e le competenze delegate a dei comitati o a delle persone singole nonché gli obblighi corrispondenti in materia di informazione, di coordinazione e di rapporto, devono essere regolamentati da parte del consiglio di amministrazione. La responsabilità per i compiti delegati permane comunque al consiglio di amministrazione in corpore. **31**

D. Comitato di audit

a) Criteri relativi all'istituzione di un comitato di audit

Gli istituti costituiscono un comitato di audit („audit committee"), se è dato almeno uno dei criteri di cui ai nm. da 33 a 36: **32**

- Bilancio > CHF 5 Mia. **33**
- Volume dei depositi (portafogli titoli e metalli preziosi depositati da clienti, ad esclusione di banche, secondo il reporting prudenziale AU 001 / AU 101) > CHF 10 Mia. **34**

- Mezzi propri necessari conformemente all'Ordinanza sui fondi propri (OFoP) > CHF 200 Mio. **35**

- Quotazione (titoli di partecipazione) **36**

Se un istituto non costituisce un comitato di audit, benché uno o più criteri esposti ai nm. da 33 a 36 sono dati, il rapporto annuale deve contenere una giustificazione. **37**

b) Requisiti concernenti i membri di un comitato di audit

La maggioranza dei suoi membri deve soddisfare i requisiti di indipendenza di cui ai nm. da 20 a 24. Se meno della metà dei suoi membri soddisfano tali requisiti, il rapporto annuale deve contenere una giustificazione. **38**

I membri del comitato di audit dispongono di buone conoscenze nonché di esperienza in materia finanziaria e contabile e hanno cognizione dell'attività di revisore interno ed esterno. **39**

Il presidente del consiglio di amministrazione non fa parte di norma del comitato di audit. Se l'istituto decide diversamente, il rapporto annuale deve contenere una giustificazione. **40**

c) Compiti di un comitato di audit

Il comitato di audit può assegnare dei mandati nell'ambito delle sue funzioni. **41**

aa) Sorveglianza e valutazione dell'integrità delle chiusure finanziarie

Il comitato di audit:

- analizza in modo critico le chiusure finanziarie e segnatamente i conti economici dell'istituto, eventuali conti di gruppo, i conti annuali e le chiusure intermedie pubblicate e verifica la tenuta regolare dei conti conformemente ai principi contabili applicati, valutando in particolare le poste significative a bilancio e fuori bilancio; **42**

- discute le chiusure finanziarie e la qualità delle procedure contabili con il membro della direzione responsabile per le finanze e per la contabilità, con il revisore responsabile nonché con il responsabile della revisione interna; **43**

- riporta al consiglio di amministrazione dei lavori effettuati conformemente ai nm. 42 e 43 e emette una raccomandazione nella quale indica se, a suo avviso, i conti possono essere sottoposti all'assemblea dei detentori di capitale. Una decisione in merito compete al consiglio di amministrazione in corpore. **44**

bb) Sorveglianza e valutazione del controllo interno nell'ambito dell'allestimento dei rendiconti economici

Il comitato di audit:

- sorveglia e valuta se il controllo interno nel corso dell'allestimento dei rendiconti economici è adeguato ed efficace; **45**

- si assicura che, in caso di modifiche sostanziali dal profilo del rischio dell'istituto, il controllo interno nell'ambito dell'allestimento dei rendiconti economici sia adeguato di conseguenza. **46**

cc) Sorveglianza e valutazione dell'efficacia della società di audit e della sua cooperazione con la revisione interna

Il comitato di audit:

- analizza, almeno annualmente e in caso di modifiche sostanziali del profilo di rischio dell'istituto, i rischi, la strategia di audit che ne deriva e la pianificazione dell'audit basato sui rischi della società di **47**

audit (Circ. CFB 05/1 “Audit”, Appendice 1);

- procede all’analisi critica dei rapporti di audit relativi all’audit dei conti annuali e dell’audit prudenziale (cfr. Circ. CFB 05/2 “Rapporto di audit”) e la discute con il revisore responsabile; **48**

- si assicura che le carenze riscontrate vengano corrette e che le raccomandazioni della società di audit vengano seguite; **49**

- giudica l’operato e la remunerazione della società di audit e si assicura della sua indipendenza; **50**

- valuta la cooperazione tra la società di audit e la revisione interna. **51**

dd) Valutazione del controllo interno che non concerne l’allestimento dei rendiconti economici e della revisione interna

Il comitato di audit:

- valuta il buon funzionamento del controllo interno che non verte sull’allestimento dei rendiconti economici, come la funzione di compliance e il controllo dei rischi, nella misura in cui tale giudizio non viene dato da altri comitati del consiglio di amministrazione; **52**

- deve essere informato sui risultati dei controlli effettuati dalla revisione interna e mantenere dei contatti regolari con il relativo responsabile, anche se la revisione interna è subordinata, conformemente ai nm. da 28 a 31, al consiglio di amministrazione in corpore o ad un altro comitato appartenente a quest’ultimo. **53**

IV. Revisione interna

A. Istituzione

Ogni istituto deve costituire una revisione interna (cfr. art. 9 cpv. 4 OBCR e art. 20 cpv. 2 OBCR). **54**

In casi specifici l’autorità di sorveglianza può, dopo consultazione con la società di audit, esentare un istituto dall’obbligo previsto al nm. 54. **55**

Se l’istituzione di una revisione interna dell’istituto non appare adeguata, i compiti della revisione interna possono essere assegnati: **56**

- alla revisione interna della società madre o alla revisione interna di un’altra società del gruppo, trattandosi di una banca, di un commerciante di valori mobiliari o di un’altro intermediario finanziario (ad esempio una compagnia assicurativa) sottoposto a sorveglianza statale (per le banche estere nell’ambito dell’art. $4^{quinquies}$ LBCR), **57**

- ad una seconda società di audit indipendente da quella dell’istituto, o **58**

- ad un terzo indipendente, a condizione che la società di audit confermi la sua qualifica professionale. **59**

B. Subordinazione gerarchica e organizzazione

La revisione interna è subordinata direttamente al consiglio di amministrazione o a uno dei suoi comitati ed esegue i compiti di revisione e sorveglianza che le sono assegnati. La revisione interna rende conto del proprio operato principalmente all’istanza del consiglio di amministrazione alla quale è direttamente sottoposta. **60**

La revisione interna del gruppo o del conglomerato finanziario si estende almeno a tutte le imprese che devono essere consolidate conformemente agli articoli 3b a 3g LBCR, agli articoli 10 cpv. 5 e 14 LBVM nonché agli articoli 6 a 10 OFoP. Nella misura in cui delle società del gruppo dispongono di dipartimenti di revisione autonomi, questi devono essere subordinati dal punto di vista funzionale alla revisione interna del **61**

gruppo o del conglomerato finanziario.

Il responsabile della revisione interna è designato dal consiglio di amministrazione. **62**

La revisione interna lavora indipendentemente dalla gestione quotidiana. **63**

La revisione interna dispone di un diritto di controllo illimitato in seno all'istituto e alle sue imprese che devono essere consolidate ai sensi del nm. 61. Ha un diritto di accesso illimitato a tutti i libri contabili, documenti, verbali e altre annotazioni nonché ai supporti di dati e ai sistemi. Ogni e qualsiasi informazione necessaria allo svolgimento dei suoi compiti deve essere messa a sua disposizione. **64**

Le basi necessarie per la revisione interna, come ad esempio un regolamento vertente sulla sua organizzazione, i suoi compiti e le sue responsabilità, devono essere emesse, a dipendenza dei rapporti di subordinazione diretta, dal consiglio di amministrazione o dal comitato responsabile. Accessoriamente la revisione interna stessa definisce le proprie modalità di lavoro (ad esempio la metodologia, i tipi di audit, la formazione e il perfezionamento professionali). **65**

La revisione interna deve corrispondere alle esigenze qualitative dell'Associazione svizzera di audit interno (ASAI). Eventuali deroghe devono essere giustificate nel rapporto annuale. Il lavoro della revisione interna si fonda sugli "Standards for the Professional Practice" dell'Institute of Internal Auditors (IIA). **66**

La revisione interna deve essere costituita in funzione delle dimensioni, della complessità e del profilo di rischio dell'istituto e rappresenta dal punto di vista organizzativo un'unità autonoma. Deve disporre di personale e di risorse materiali (ad esempio di mezzi informatici) sufficienti per svolgere il proprio mandato. Nel complesso i quadri devono disporre di conoscenze approfondite nei settori di attività nei quali l'istituto opera. In modo generale occorre assicurare che la regolarità della gestione e l'adeguatezza dei sistemi di controllo interni vengano valutati da revisori qualificati. **67**

Il sistema di remunerazione dei collaboratori della revisione interna non deve comprendere elementi suscettibili di generare conflitti di interesse. In particolare la remunerazione (ad esempio i salari, bonus, onorari e premi) non deve dipendere dal risultato di prodotti o di transazioni specifiche. **68**

C. Compiti e responsabilità

a) Valutazione dei rischi, pianificazione delle revisioni e dei rapporti

La revisione interna fornisce delle basi decisionali importanti, che permettono di valutare se l'istituto dispone di un sistema di controllo interno efficace ed adeguato al suo profilo di rischio. **69**

La revisione interna procede almeno annualmente ad una valutazione globale dei rischi dell'istituto, considerando in giusta misura le evoluzioni esterne (ad esempio il contesto economico, le modifiche di regolamentazioni) e dei fattori interni (ad esempio progetti importanti, riorientamento dell'attività). **70**

Sulla base di tale valutazione, la revisione interna fissa gli obiettivi di audit principali per il periodo di audit successivo. **71**

La revisione interna deve inoltre assicurarsi che tutte le attività dell'istituto che comportano un rischio vengano sottoposte, nell'ambito di una pianificazione pluriannuale, ad un audit effettuato dalla stessa revisione interna oppure dalla società di audit. **72**

La revisione interna rende conto tempestivamente e per iscritto al consiglio di amministrazione o al comitato responsabile e alla direzione operativa delle sue valutazioni dei rischi e dei suoi obiettivi di audit, sottoponendo questi ultimi nonché la pianificazione dell'audit all'approvazione del consiglio di amministrazione o del comitato responsabile. Trasmette una copia dei documenti alla società di audit. **73**

Durante il periodo di audit la revisione interna valuta se sono avvenute delle modifiche sostanziali del profilo di rischio e se le stesse richiedono un adeguamento della pianificazione dell'audit. In caso affermativo, la revisione interna sottopone tempestivamente le modifiche sostanziali della pianificazione annuale al consiglio di amministrazione o al comitato responsabile della sua approvazione. Informa inoltre la società **74**

di audit delle modifiche intervenute.

La revisione interna rende conto al consiglio di amministrazione e alla direzione, tempestivamente e per iscritto, di tutte le constatazioni importanti riscontrate nell'ambito di un audit. **75**

Almeno annualmente la revisione interna redige un rapporto scritto sui risultati essenziali degli audit effettuati e sulle sue principali attività durante il periodo e lo sottopone per informazione, con le conclusioni che ne derivano, al consiglio di amministrazione o al comitato responsabile. Tale rapporto sarà pure trasmesso alla direzione e alla società di audit. **76**

La revisione interna informa inoltre almeno semestralmente il consiglio di amministrazione o il comitato responsabile delle misure adottate a seguito delle carenze riscontrate e dello stato di avanzamento della messa in atto delle raccomandazioni della revisione interna e della società di audit. La trasmissione di questa informazione come pure del relativo "audit tracking" possono anche essere effettuate da un'altra istanza indipendente in seno all'istituto, come ad esempio da quella che esercita la funzione di compliance o del controllo dei rischi. **77**

b) Ripartizione dei compiti tra la revisione interna e la società di audit

La revisione interna e la società di audit coordinano le loro attività nell'ambito della determinazione dei loro rispettivi obiettivi e delle loro strategie di audit. Le stesse difendono così i loro rispettivi punti di vista e su tale base possono fissare un approccio comune. La revisione interna permane responsabile della realizzazione dei suoi obiettivi di audit. **78**

La revisione interna trasmette tempestivamente i propri rapporti alla società di audit. La società di audit ha il diritto di consultare i documenti di lavoro della revisione interna. La società di audit mette invece a disposizione i suoi rapporti di audit alla revisione interna. **79**

V. Direzione operativa

A. Compiti e responsabilità

La direzione operativa applica le istruzioni del consiglio di amministrazione in materia di istituzione, di mantenimento e di regolare sorveglianza del controllo interno. **80**

La direzione operativa:

- elabora le procedure appropriate per identificare, misurare, valutare, analizzare e controllare i rischi corsi dalla banca. Ciò comprende in particolare la concretizzazione delle attività di controllo integrate nel processo di lavoro conformemente ai nm. 87 a 96, la funzione di compliance definita ai nm. 100 a 112 nonché il controllo dei rischi previsto ai nm. 113 a 125; **81**

- costituisce e documenta una struttura organizzativa che definisce chiaramente le responsabilità, le competenze, gli obblighi di rendiconto, il potere di dare istruzioni e decisionale nonché i flussi d'informazione; **82**

- assicura che tutte le informazioni importanti sullo sviluppo dell'attività vengano raccolte, trasmesse ed elaborate (sistema di gestione nell'informazione); **83**

- verifica regolarmente l'adeguatezza del controllo interno; **84**

- rende conto periodicamente al consiglio di amministrazione dell'efficacia del controllo interno e informa immediatamente il consiglio di amministrazione e la revisione interna in caso di constatazioni rilevanti. **85**

B. Separazione delle funzioni e attività di controllo

La direzione operativa assicura che vi sia una separazione adeguata delle funzioni ed evita l'attribuzione di responsabilità conflittuali. Nel caso in cui la separazione delle funzioni non può essere completamente **86**

realizzata a seguito delle dimensioni dell'istituto, attribuisce una particolare attenzione al conseguente potenziamento delle competenze gestionali dei collaboratori responsabili.

Attività di controllo sono da prevedere quale parte integrante dei processi lavorativi, ad esempio sotto forma di: **87**

- controlli di svolgimento: constatano gli scarti per rapporto agli obiettivi in un momento in cui eventuali correzioni possono ancora essere facilmente apportate; **88**

- controlli del risultato: confrontano gli obiettivi fissati ai risultati effettivamente raggiunti. Vi si ricorre quando l'apporto diretto di correzioni non è più necessario e/o possibile; **89**

- verifiche del comportamento: vengono utilizzate per verificare il comportamento di individui o di unità organizzative. Vengono in particolare effettuate quando non sono riscontrabili dei risultati quantitativi. **90**

Le attività di controllo applicabili sono in particolare le seguenti: **91**

- controlli di attività: dei rapporti adeguati al livello gerarchico sul rendimento economico e sulla situazione in materia di rischi e di controllo devono essere trasmessi regolarmente ai vari gradi funzionali, che li verificano criticamente; **92**

- controlli concreti: avvengono, ad esempio, tramite l'applicazione del „principio di verifica a quattro occhi", una limitazione dell'accesso tecnico ad averi in contanti o ad oggetti di valore, nonché con l'allestimento periodico di inventari; **93**

- verifica del rispetto dei limiti prescritti; **94**

- verifica del rispetto delle competenze e delle autorizzazioni, segnatamente delle autorizzazioni relative all'accesso ai sistemi informatici e ai dati base, nonché alle loro mutazioni („golden-keyholders"); **95**

- verifica e controllo della concordanza, ad esempio delle transazioni e delle posizioni contabili. **96**

C. Compliance (rispetto delle norme)

Per compliance si intende il rispetto delle norme legislative, dei regolamenti e delle prescrizioni interne nonché il rispetto delle norme e delle regole deontologiche in uso nel settore interessato. **97**

Il rischio di compliance corrisponde al rischio di violazione delle prescrizioni, delle norme e delle regole deontologiche nonché alle relative sanzioni, alle perdite finanziarie o al danno reputazionale che ne può derivare. **98**

Compete alla direzione operativa prevedere dei sistemi e dei processi interni appropriati per assicurare la compliance in seno all'istituto. Adotta tutte le misure e disposizioni operative necessarie a questo scopo, assicurandosi in particolare che vengano emesse le necessarie istruzioni e che tutti i collaboratori siano implicati nell'applicazione della compliance, a prescindere dal loro grado gerarchico. Negli istituti che operano su scala internazionale occorre in particolare assicurarsi che le istruzioni concernenti più Stati siano compatibili con il diritto locale. **99**

D. Funzione compliance

a) Istituzione e subordinazione gerarchica

Ogni istituto deve dotarsi di una funzione compliance che, nell'ambito della propria attività, gode di un diritto illimitato all'informazione con relative possibilità di accesso e consultazione. La funzione compliance è integrata nell'organizzazione globale dell'istituto, ma è indipendente dalle sue attività operative che generano utili. **100**

La funzione compliance deve disporre di risorse e di competenze adeguate alla dimensione dell'istituto, alla complessità della sua attività e della sua organizzazione nonché al suo rischio di compliance. **101**

L'istituto designa un membro della direzione quale responsabile della funzione di compliance e fa pertanto in modo che questa possa accedere liberamente alla direzione. **102**

Il sistema di remunerazione (ad esempio stipendi, bonus, onorari e premi) dei collaboratori del compliance non deve comprendere elementi suscettibili di generare conflitti di interesse. In particolare la remunerazione non deve dipendere dal risultato di prodotti o di transazioni specifiche. **103**

La funzione compliance può costituire un dipartimento con altre funzioni interne, ad esempio con il servizio giuridico o con il controllo dei rischi, in assenza di conflitti di interesse. I compiti di ciascuna funzione devono tuttavia essere definiti e assegnati in modo inequivocabile. **104**

In particolare negli istituti in cui l'attività e l'organizzazione non presentano un grado di complessità rilevante e il rischio di compliance è ridotto, la funzione compliance può essere svolta da collaboratori che lavorano a tempo parziale o da collaboratori che svolgono parallelamente anche un'altra funzione interna, purché la stessa non presenti un conflitto d'interessi. Tale funzione può anche essere oggetto di outsourcing ed essere assicurata sulla base di un mandato esterno. **105**

In un istituto di piccole dimensioni, nei quali l'integrazione e l'indipendenza della funzione di compliance elencate al nm. 100 e l'assenza dei conflitti di interesse richiesta al nm. 105 non possono essere integralmente garantite, in considerazione delle dimensioni, i compiti della funzione compliance devono essere svolti altrimenti in maniera fidata. Spetta alla società di audit giudicare ciò e prendere posizione in merito nel rapporto sull'audit prudenziale. **106**

b) Compiti e responsabilità

I compiti, le responsabilità e l'obbligo di informare competono alla funzione compliance e devono essere previsti in un regolamento approvato dalla direzione o dal consiglio di amministrazione. **107**

I compiti della funzione di compliance comprendono di norma:

- l'assistenza e la consulenza della direzione operativa e dei collaboratori in ambito di applicazione e sorveglianza del compliance; **108**
- la valutazione del rischio di compliance legato all'attività dell'istituto e l'elaborazione di un piano di azione basato sul rischio, che deve essere approvato dalla direzione operativa. Il piano d'azione deve essere messo a disposizione della revisione interna; **109**
- il supporto della direzione operativa nella formazione e informazione dei collaboratori in ambito di compliance; **110**
- l'informazione tempestiva della direzione operativa in merito ai cambiamenti di rilievo del rischio di compliance, l'accertamento di violazioni rilevanti in ambito di compliance e le inchieste condotte in merito nonché l'appoggio fornito alla direzione operativa nella scelta delle istruzioni da fornire o delle misure da adottare. La revisione interna deve essere informata di conseguenza; **111**
- la trasmissione annuale di un rapporto al consiglio di amministrazione sulla valutazione del rischio di **112**

compliance e sull'attività della funzione di compliance definita ai nm. 108 a 111. Una copia del rapporto deve pure essere messa a disposizione della revisione interna e della società di audit.

E. Controllo dei rischi (Risk Control)

a) Istituzione e subordinazione gerarchica

Ogni istituto deve dotarsi di un controllo dei rischi che, nell'ambito dei suoi compiti, gode di un diritto illimitato di informazione, con le relative possibilità di accesso e consultazione. Lo stesso è da integrare nell'organizzazione globale dell'istituto indipendentemente dalle sue attività operazionali che generano utili. **113**

Il controllo dei rischi deve disporre delle risorse e delle competenze adeguate alla dimensione dell'istituto, alla complessità della sua attività e della sua organizzazione nonché al suo profilo di rischio. **114**

L'istituto designa un membro della direzione operativa quale responsabile del controllo dei rischi e fa pertanto in modo che quest'ultimo possa accedere liberamente alla direzione. **115**

A dipendenza delle differenti categorie di rischio alle quali l'istituto è esposto (ad esempio rischi di mercato, di credito, operazionali), il controllo dei rischi può consistere in più dipartimenti o funzioni indipendenti, che tuttavia devono tutte rendere conto al membro della direzione responsabile del controllo dei rischi. **116**

Il sistema di remunerazione (ad esempio stipendi, bonus, onorari e premi) dei collaboratori del controllo dei rischi non deve comprendere elementi suscettibili di generare conflitti di interesse. In particolare la remunerazione non deve dipendere dal risultato di prodotti o di transazioni specifiche. **117**

Il controllo dei rischi può costituire un dipartimento con altre funzioni interne, ad esempio con la funzione compliance, in assenza di conflitti di interesse. I compiti di ciascuna funzione devono tuttavia essere definiti e assegnati in modo inequivocabile. **118**

In particolare negli istituti in cui l'attività e l'organizzazione non presentano un grado di complessità rilevante e il rischio è ridotto, il controllo dei rischi può essere svolto da collaboratori che lavorano a tempo parziale o da collaboratori che svolgono parallelamente anche un'altra funzione interna, purché la stessa non presenti un conflitto d'interessi. **119**

In un istituto di piccole dimensioni, nei quali l'integrazione e l'indipendenza del controllo dei rischi elencate al nm. 113 e l'assenza dei conflitti di interesse richiesta al nm. 119 non possono essere integralmente garantite, in considerazione delle dimensioni, i compiti del controllo dei rischi devono essere svolti in maniera fidata tramite altri mezzi. Spetta alla società di audit giudicare e prendere posizione su questo aspetto nel rapporto sull'audit prudenziale. **120**

b) Compiti e responsabilità

I compiti, le responsabilità e l'obbligo di informare competono al controllo dei rischi e devono essere previsti in un regolamento approvato dalla direzione o dal consiglio di amministrazione. **121**

Il controllo dei rischi sorveglia, quale funzione di controllo indipendente, il profilo di rischio assunto dall'istituto. Fornisce le informazioni necessarie alla sorveglianza dei rischi e elabora le basi sulle quali si fondano la politica di rischio dell'istituto („risk policy"), la sua propensione al rischio („risk appetite") e i limiti di rischio che devono essere approvati dalla direzione operativa o dal consiglio di amministrazione. **122**

Compete in particolare al controllo dei rischi di strutturare e applicare i sistemi adeguati di sorveglianza dei rischi e di adattarli in funzione dei nuovi affari e dei nuovi prodotti, di definire e applicare le basi e i metodi per valutare i rischi (ad esempio i metodi di valutazione e aggregazione, l'efficacia dei modelli) nonché la sorveglianza dei sistemi adeguati per considerare le disposizioni in materia di fondi propri, di ripartizione dei rischi e di liquidità. **123**

Il controllo dei rischi trasmette almeno una volta per semestre un rapporto alla direzione operativa riguardo ai rischi e alle posizioni di rischio. In caso di sviluppi particolari della situazione informa immediatamente **124**

la direzione operativa e la revisione interna.

Il controllo dei rischi informa almeno annualmente il consiglio di amministrazione riguardo alla situazione **125**
di rischio dell'istituto e riguardo alla sua attività conformemente ai nm. 122 a 124. Una copia del rapporto informativo viene messa a disposizione della revisione interna e della società di audit.

c) Delimitazione per rapporto alla gestione dei rischi

La gestione dei rischi ha lo scopo di gestire e limitare in modo completo e sistematico i rischi sulla base **126**
delle conoscenze economiche e statistiche. Comprende l'identificazione, la misura, la valutazione, la gestione e l'allestimento di rapporti sulle posizioni-rischio individuali o aggregate. La gestione dei rischi è assicurata a livello organizzativo appropriato per mezzo di metodi adeguati che tengono conto delle particolarità dell'istituto.

VI. Audit e valutazione da parte della società di audit

Le società di audit verificano il rispetto della presente circolare conformemente alla Circ. CFB 05/1 "Au- **127**
dit" e espongono il risultato delle loro verifiche nel rapporto di audit (Circ. CFB 05/02 "Rapporto di audit").

VII. Entrata in vigore

Data dell'entrata in vigore: 1° gennaio 2007. **128**

Sostituisce: Circ. CFB 95/1 "Revisione interna" del 14 dicembre 1995 e le direttive dell'ASB sul controllo **129**
interno del giugno 2002.

VIII. Disposizioni temporali

Gli istituti adempiono le prescrizioni della presente circolare entro il 1° gennaio 2008. In merito ai requisiti **130**
di indipendenza del consiglio di amministrazione e del comitato di audit (audit committee) è accordato un termine transitorio fino al 1° gennaio 2009.

Basi giuridiche:

- LBCR: art. 3 cpv. 2 lett. a; art. 3b-h; art. 4^{quinquies}
- OBCR: art. 8 cpv. 2, art. 9; art. 44 lett. o
- OFoP: art. 6-11
- LBVM: art. 10 cpv. 2 lett. a; cpv. 5; art. 14
- OBVM: art. 19; art. 20; art. 26; art. 29 cpv. 1
- OBVM-CFB: art. 8 cpv. 1