Eidgenössische Finanzmarktaufsicht FINMA
Autorité fédérale de surveillance des marchés financiers FINMA
Autorità federale di vigilanza sui mercati finanziari FINMA
Swiss Financial Market Supervisory Authority FINMA

Circolare 2017/1
Corporate governance – banche

Corporate governance, gestione del rischio e controlli interni presso le banche

Riferimento:	Circ. FINMA 17/1 «*Corporate governance* – banche»
Data:	22 settembre 2016
Entrata in vigore:	1° luglio 2017
Concordanza:	sostituisce la Circ. FINMA 08/24 «Sorveglianza e controllo interno – banche» del 20 novembre 2008
Basi legali:	LFINMA art. 7 cpv. 1 lett. b LBCR art. 3 cpv. 2 lett. a e c, 3*b*–3*f*, 4^{quinquies}, 6 OBCR art. 11 cpv. 2, 12 LBVM art. 10 cpv. 2 lett. a e cpv. 5, 14 OBVM art. 19, 20 OFoP art. 7–12

Destinatari																															
LBCR			LSA			LBVM	LInFi							LICol										LRD			Altri				
Banche	Gruppi e congl. finanziari	Altri intermediari	Assicuratori	Gruppi e congl. assicurativi	Intermediari assicurativi	Commercianti di val. mobiliari	Sedi di negoziazione	Controparti centrali	Depositari centrali	Repertori di dati sulle negoziazioni	Sistemi di pagamento	Partecipanti	Direzioni dei fondi	SICAV	Società in accomandita per ICC	SICAF	Banche depositarie	Gestori patrimoniali di ICC	Distributori	Rappresentanti di ICC esteri	Altri intermediari	OAD	IFDS	Assoggettati OAD	Società di audit	Agenzie di rating					
X	X					X																									

Laupenstrasse 27, 3003 Berna
Tel. +41 (0)31 327 91 00, fax +41 (0)31 327 91 01
www.finma.ch

Indice

I. Oggetto

La presente circolare esplica i requisiti posti a *corporate governance*, gestione del rischio, sistema di controllo interno (SCI) e revisione interna presso banche, commercianti di valori mobiliari, gruppi finanziari (art. 3*c* cpv. 1 LBCR) nonché presso conglomerati finanziari dominati dal settore bancario o da quello del commercio di valori mobiliari (art. 3*c* cpv. 2 LBCR), di seguito denominati con il termine «istituti». 1

II. Definizioni

Per *corporate governance* si intendono, di seguito, i principi e le strutture per mezzo dei quali un istituto viene gestito e controllato dai propri organi. 2

La gestione del rischio comprende le strutture organizzative come pure i metodi e i processi che servono a determinare le strategie di rischio e le misure di gestione del rischio nonché all'identificazione, all'analisi, alla valutazione, alla gestione, al monitoraggio e alla reportistica dei rischi. 3

La tolleranza al rischio comprende ponderazioni sia quantitative che qualitative per quanto concerne i rischi essenziali che l'istituto è disposto ad assumere per raggiungere i propri obiettivi commerciali strategici e tenuto conto della relativa pianificazione del capitale e liquidità. La tolleranza al rischio viene determinata sia per ogni categoria di rischio corrispondente sia a livello di istituto, se rilevante. 4

Il profilo di rischio comprende, a livello di istituto e per ogni categoria di rischio corrispondente, le posizioni di rischio di volta in volta assunte dall'istituto in un determinato momento. 5

Il SCI comprende l'insieme delle strutture e dei processi di controllo che a tutti i livelli dell'istituto costituiscono la base per il raggiungimento degli obiettivi di politica commerciale e il corretto funzionamento dell'istituto. Il SCI non comprende esclusivamente l'attività di controllo effettuata a posteriori, ma anche quella relativa alla pianificazione e alla gestione. Un efficace sistema di controllo interno comprende, fra l'altro, le attività di controllo integrate nelle varie fasi lavorative, adeguati processi concernenti la gestione del rischio e il rispetto delle norme applicabili (*compliance*), come pure istanze di controllo strutturate in base a dimensioni, complessità e profilo di rischio dell'istituto, in particolare una funzione indipendente di controllo dei rischi e di *compliance*. 6

Per *compliance* si intende il rispetto delle prescrizioni legali, normative e interne nonché l'osservanza degli standard e delle regole di condotta usuali sul mercato. 7

III. Ambito di applicazione (principio di proporzionalità)

La presente circolare si applica a tutti gli istituti di cui al nm. 1. I requisiti devono essere applicati nel singolo caso tenendo conto delle dimensioni, della complessità, della struttura e del profilo di rischio dell'istituto. Nel singolo caso, la FINMA può concedere agevolazioni o ordinare inasprimenti. 8

IV. Organo preposto all'alta direzione

A. Compiti e responsabilità

I compiti dell'organo preposto all'alta direzione comprendono in particolare le mansioni di seguito elencate. 9

a) Strategia commerciale e politica dei rischi

L'organo preposto all'alta direzione definisce la strategia commerciale ed emana principi sulla cultura d'impresa. Approva la strategia quadro per la gestione del rischio a livello di istituto ed è responsabile della regolamentazione, dell'istituzione e del monitoraggio di un efficace sistema di gestione del rischio come pure della gestione dei rischi complessivi. 10

b) Organizzazione

L'organo preposto all'alta direzione è responsabile di un'adeguata organizzazione aziendale ed emana i regolamenti necessari a tale scopo. 11

c) Finanze

L'organo preposto all'alta direzione si assume la responsabilità finale per quanto riguarda la situazione finanziaria e l'andamento dell'istituto. Esso approva o adotta la pianificazione del capitale e della liquidità, come pure il rapporto di gestione, il preventivo annuale, le chiusure intermedie e gli obiettivi finanziari annuali. 12

d) Risorse in termini di personale e altre risorse

L'organo preposto all'alta direzione è responsabile di un'adeguata allocazione di risorse all'interno dell'istituto, in termini sia di personale sia di dotazioni di vario tipo (p. es. infrastruttura, tecnologie informatiche), come pure della politica in materia di personale e di remunerazione. Esso decide in merito alla nomina e alla revoca dei membri dei comitati, dei membri della direzione generale, dei loro presidenti come pure del Chief Risk Officer (CRO) e del responsabile della revisione interna[1]. 13

[1] Il responsabile della revisione interna può essere nominato anche dal comitato di audit.

e) Monitoraggio e controllo

L'organo preposto all'alta direzione esercita l'alta vigilanza sulla direzione generale. Rientra nella sua sfera di responsabilità garantire un adeguato ambiente di rischio e di controllo in seno all'istituto e istituire un efficace sistema di controllo interno. Esso nomina e sorveglia la revisione interna, designa la società di audit in conformità al diritto in materia di vigilanza e ne valuta i rapporti. 14

f) Cambiamenti strutturali e investimenti sostanziali

L'organo preposto all'alta direzione decide in merito a modifiche sostanziali a livello dell'impresa e del gruppo, cambiamenti sostanziali presso importanti società affiliate e altri progetti di importanza strategica. 15

B. Membri dell'organo preposto all'alta direzione

a) Presupposti generali

L'organo preposto all'alta direzione dispone, nel suo complesso, di sufficienti competenze dirigenziali nonché delle conoscenze specialistiche necessarie e dell'esperienza richiesta nel settore bancario e finanziario. Esso presenta una sufficiente diversificazione affinché, oltre ai principali ambiti di attività, vengano rappresentati in maniera competente tutti gli ambiti centrali, come il settore finanze e contabilità e la gestione del rischio. 16

b) Indipendenza

L'organo preposto all'alta direzione è composto per almeno un terzo da membri indipendenti. In casi motivati, la FINMA può concedere delle deroghe, per esempio nel caso di gruppi finanziari svizzeri. 17

Un membro dell'organo preposto all'alta direzione è considerato indipendente nei seguenti casi: 18

- se non ricopre un'altra funzione all'interno dell'istituto e non l'ha ricoperta nel corso dei due anni precedenti; 19
- se, nel corso dei due anni precedenti, presso la società di audit dell'istituto non ha ricoperto la funzione di auditor responsabile competente per l'istituto in questione; 20
- se con l'istituto non intrattiene relazioni d'affari che, per natura o entità, potrebbero creare conflitti di interesse; e 21
- se non detiene una partecipazione qualificata (ai sensi dell'art. 3 cpv. 2 lett. c^{bis} LBCR e dell'art. 10 cpv. 2 lett. d LBVM) dell'istituto e non rappresenta il detentore di una tale partecipazione. 22

I membri dell'organo preposto all'alta direzione di banche cantonali o comunali designati o eletti da Cantoni, comuni o altri enti di diritto pubblico cantonali o comunali sono considerati indipendenti secondo il nm. 18-22 nei seguenti casi: 23

- se non appartengono al governo o all'amministrazione cantonale o comunale né a un altro ente di diritto pubblico cantonale o comunale; e 24
- se dall'organo che li ha designati o eletti non ricevono istruzioni per la loro attività quale membri dell'organo preposto all'alta direzione. 25

C. Principi della gestione del mandato

Ogni membro dell'organo preposto all'alta direzione dedica al proprio mandato tempo sufficiente e collabora attivamente alla conduzione aziendale strategica. Esercita il proprio mandato di persona e, al di fuori delle sedute ordinarie previste, si tiene costantemente a disposizione in caso di situazioni di crisi o di emergenze. 26

L'organo preposto all'alta direzione definisce il profilo richiesto ai suoi membri, al presidente e a eventuali membri del comitato come pure al presidente della direzione generale. Esso approva e valuta periodicamente il profilo richiesto agli altri membri della direzione generale, al CRO e al responsabile della revisione interna. Assicura inoltre la pianificazione della successione. 27

Almeno una volta all'anno, all'occorrenza con il coinvolgimento di un organo terzo, l'organo preposto all'alta direzione sottopone il proprio operato (raggiungimento degli obiettivi e modalità di lavoro) a un esame critico e ne documenta per iscritto l'esito. 28

L'organo preposto all'alta direzione disciplina la gestione dei conflitti d'interesse. Le relazioni d'interesse esistenti e passate devono essere notificate. Se un conflitto d'interesse non può essere evitato, l'istituto adotta gli opportuni provvedimenti per contenerlo o appianarlo in maniera efficace. 29

D. Suddivisione dei compiti e comitati

a) Ruolo del presidente

Il presidente presiede l'organo collegiale e rappresenta l'organo preposto all'alta direzione all'interno e all'esterno. Contribuisce in maniera decisiva a improntare la strategia, la comunicazione e la cultura d'impresa. 30

b) Comitati

Gli istituti delle categorie di vigilanza 1-3 devono istituire un comitato di verifica e un comitato di rischio. Gli istituti della categoria di vigilanza 3 possono riunire tali organi in un comitato misto. Gli istituti con rilevanza sistemica devono istituire almeno a livello di gruppo 31

un comitato di retribuzione e per le nomine. I comitati provvedono all'allestimento di un'adeguata reportistica all'attenzione dell'organo preposto all'alta direzione.

A livello di organico, il comitato di audit deve differenziarsi in maniera sufficiente da altri comitati. 32

La maggior parte dei membri del comitato di verifica e di rischio deve essere sostanzialmente indipendente (cfr. nm. 18-25). In linea di principio, il presidente dell'organo preposto all'alta direzione non deve rivestire la carica né di membro del comitato di audit né di presidente del comitato di rischio. I comitati dispongono complessivamente di sufficienti conoscenze ed esperienza nell'ambito di attività del corrispondente comitato. 33

c) Compiti del comitato di audit

I compiti del comitato di verifica comprendono in particolare: 34

- l'elaborazione di direttive generali concernenti la revisione interna e la reportistica finanziaria all'attenzione dell'organo preposto all'alta direzione; 35
- il monitoraggio e la valutazione della reportistica finanziaria e dell'integrità delle chiusure finanziarie, compresa la discussione in materia con il membro della direzione generale responsabile del settore finanze e contabilità, con il revisore responsabile e con il responsabile della revisione interna; 36
- il monitoraggio e la valutazione dell'efficacia dei controlli interni, segnatamente anche del controllo dei rischi e della funzione di *compliance* nonché della revisione interna, se tale compito non è svolto dal comitato di rischio; 37
- il monitoraggio e la valutazione dell'efficacia e dell'indipendenza della società di audit come pure della sua interazione con la revisione interna, compresa la discussione dei rapporti di audit con l'auditor responsabile; 38
- la valutazione della pianificazione dell'audit, della frequenza degli audit e dei risultati degli audit effettuati dalla revisione interna e dalla società di audit. 39

d) Compiti del comitato di rischio

Il comitato di rischio svolge in particolare i seguenti compiti: 40

- discutere la strategia quadro per la gestione del rischio a livello di istituto e presentare le corrispondenti raccomandazioni all'organo preposto all'alta direzione; 41
- valutare la pianificazione del capitale e della liquidità nonché la reportistica in materia all'attenzione dell'organo preposto all'alta direzione; 42
- valutare, almeno una volta all'anno, la strategia quadro per la gestione del rischio a 43

livello di istituto e disporre i necessari adeguamenti;

- controllare se l'istituto dispone di un'adeguata gestione del rischio mediante processi efficaci che tengono conto della situazione di rischio dell'istituto; 44

- monitorare l'applicazione delle strategie di rischio, in particolare verificare se sono in linea con la tolleranza al rischio indicata e con i limiti di rischio in conformità alla strategia quadro per la gestione del rischio a livello di istituto. 45

Il CRO e altri funzionari rilevanti inviano regolarmente al comitato di rischio rapporti esaustivi sui corrispondenti aspetti della strategia quadro relativa alla gestione del rischio a livello di istituto (in conformità al nm. 52-59) e sulla relativa osservanza. 46

V. Direzione generale

A. Compiti e responsabilità

La direzione generale deve provvedere affinché l'attività operativa sia in linea con la strategia commerciale nonché con le disposizioni e con le decisioni dell'organo preposto all'alta direzione. In particolare ha la responsabilità dei seguenti compiti: 47

- condurre le attività quotidiane, gestire a livello operativo i ricavi e i rischi, compresa la gestione della struttura del bilancio e della liquidità, come pure rappresentare l'istituto nei confronti di terzi in ambito operativo; 48

- presentare la richiesta per quanto concerne le operazioni che rientrano nell'ambito di competenza dell'organo preposto all'alta direzione o che sono vincolate all'approvazione di quest'ultimo come pure emanare prescrizioni che disciplinano l'attività operativa; 49

- organizzare e alimentare adeguati processi interni, un appropriato sistema di gestione dell'informazione (*Management Information System*), un sistema di controllo interno e un'adeguata infrastruttura tecnologica. 50

B. Requisiti posti ai membri della direzione generale

Per garantire adeguatamente il rispetto delle condizioni di autorizzazione nel quadro delle attività operative, i membri della direzione generale, in quanto organo collegiale e investiti di responsabilità funzionale, dispongono di sufficienti competenze dirigenziali, delle conoscenze specialistiche necessarie e di esperienza maturata nel settore bancario e finanziario. 51

VI. Strategia quadro per la gestione del rischio a livello di istituto

La strategia quadro per la gestione del rischio a livello di istituto è elaborata dalla direzione 52

generale e approvata dall'organo preposto all'alta direzione.

La strategia quadro comprende la politica di rischio, la tolleranza al rischio e i limiti di rischio basati su quest'ultima in tutte le categorie essenziali di rischio. 53

Nella strategia quadro occorre tenere conto dei seguenti aspetti: 54

- categorizzazione unitaria[2] dei rischi essenziali per garantire la coerenza con gli obiettivi della gestione del rischio; 55
- precisazione della potenziale perdita derivante dalle categorie essenziali di rischio; 56
- definizione e impiego degli strumenti e delle strutture organizzative che servono a identificare, analizzare, valutare, gestire e monitorare le categorie essenziali di rischio nonché ad allestire la reportistica; 57
- elaborare una documentazione che consenta di verificare adeguatamente la determinazione della tolleranza al rischio come pure dei corrispondenti limiti di rischio; 58
- determinare l'aggregazione dei dati sui rischi e la relativa reportistica presso gli istituti delle categorie di rischio 1-3. Gli istituti di rilevanza sistemica devono in particolare riportare informazioni sull'architettura dei dati e sull'infrastruttura informatica, che consentano un'analisi e una valutazione dei rischi aggregata e attuale come pure l'aggregazione dei dati sui rischi e la reportistica concernente tutte le categorie essenziali di rischio dell'istituto, sia in condizioni normali che in situazioni di stress. 59

VII. Sistema di controllo interno

Nel quadro del sistema di controllo interno vi sono almeno due istanze di controllo: le unità operative orientate a generare utili e le istanze di controllo da esse indipendenti. 60

A. Unità operative orientate a generare utili

Le unità operative orientate a generare utili svolgono la loro funzione di controllo nel quadro delle attività quotidiane mediante la gestione del rischio, in particolare mediante monitoraggio, gestione e reportistica diretti. 61

B. Istanze di controllo indipendenti

Le istanze di controllo indipendenti monitorano i rischi e controllano che le prescrizioni legali, normative e interne vengano rispettate. A livello specifico dell'istituto possono essere istituite diverse istanze di controllo indipendenti, ma che assumano almeno i compiti e le 62

[2] In base a natura, tipologia e livello e in linea con le definizioni ai sensi del diritto in materia di vigilanza in conformità all'OFoP.

responsabilità del controllo dei rischi (nm. 69-76) e della funzione di *compliance* (nm. 77-81).

Il sistema di remunerazione delle istanze di controllo indipendenti non deve creare incentivi che generano conflitti di interesse con le mansioni di dette unità. 63

a) Costituzione e subordinazione gerarchica

Nel quadro dei loro compiti, le istanze di controllo indipendenti dispongono di diritti illimitati di informazione, accesso e consultazione; rispetto alle unità operative orientate a generare utili, esse devono godere di autonomia strutturale nell'organizzazione globale rispettivamente nel sistema di controllo interno. Devono disporre di risorse e di competenze adeguate. 64

L'istituto designa uno o più membri della direzione generale a cui affidare la competenza per le istanze di controllo indipendenti. 65

L'istituto fa in modo che le istanze di controllo indipendenti dispongano di un accesso diretto all'organo preposto all'alta direzione. 66

In quanto istanze di controllo indipendenti, gli istituti delle categorie di vigilanza 1-3 dispongono di un controllo dei rischi e di una funzione di *compliance* autonomi. Esse designano un CRO che sia competente, oltre che per il controllo dei rischi, anche per altre istanze di controllo indipendenti. 67

Il CRO designato dagli istituti di rilevanza sistemica è membro della direzione generale. 68

b) Compiti e responsabilità del controllo dei rischi

Il controllo dei rischi garantisce una sorveglianza e una reportistica completa e sistematica delle posizioni di rischio singole come pure aggregate. In quanto parte integrante delle analisi quantitative e qualitative, tale controllo comprende lo svolgimento di *stress test* e di analisi di scenario in un contesto di condizioni commerciali sfavorevoli. 69

Presso gli istituti delle categorie di vigilanza 1-3, il controllo dei rischi garantisce inoltre un'applicazione adeguata delle disposizioni concernenti l'aggregazione e la reportistica relative ai dati sui rischi in conformità al nm. 59. 70

Il controllo dei rischi sorveglia il profilo di rischio dell'istituto, in particolare dal punto di vista della conformità alla tolleranza al rischio stabilita nella strategia quadro per la gestione del rischio a livello di istituto e ai limiti di rischio. 71

Al controllo dei rischi compete inoltre l'elaborazione e l'esercizio di adeguati sistemi di monitoraggio dei rischi, la definizione e l'utilizzo di basi e metodi per l'analisi e la valutazione dei rischi (p. es. metodi di valutazione e di aggregazione, convalida di modelli) nonché la sorveglianza dei sistemi per il rispetto delle prescrizioni ai sensi del diritto in 72

materia di vigilanza (in particolare disposizioni in materia di fondi propri, di ripartizione dei rischi e di liquidità).

Il controllo dei rischi viene incluso in maniera adeguata nello sviluppo di categorie di prodotti, servizi, ambiti commerciali o di mercato nuove/i o ampliate/i, oppure nel caso di transazioni essenziali o complesse. 73

Il controllo dei rischi partecipa attivamente al processo decisionale concernente i limiti di rischio e garantisce che questi ultimi siano in particolare in linea con la tolleranza al rischio e armonizzati con i risultati degli *stress test* nonché che vengano posti in modo tale da costituire per la direzione generale un efficace strumento di gestione operativa. 74

Il controllo dei rischi presenta alla direzione generale almeno a ritmo semestrale e all'organo preposto all'alta direzione almeno una volta all'anno un rapporto sullo sviluppo del profilo di rischio dell'istituto e la sua attività in conformità ai nm. 69-78. Una copia di tali rapporti viene messa a disposizione della revisione interna e della società di audit. 75

In caso di sviluppi particolari, il controllo dei rischi informa senza indugio la direzione generale e la revisione interna e, qualora si verifichino fatti di ampia portata, informa in via aggiuntiva l'organo preposto all'alta direzione. 76

c) Compiti e responsabilità della funzione di *compliance*

I compiti e le responsabilità della funzione di *compliance* comprendono almeno le attività di seguito elencate: 77

- valutare, una volta all'anno, il rischio di *compliance* connesso all'attività dell'istituto ed elaborare un piano di intervento orientato al rischio, che deve essere approvato dalla direzione generale. Il piano di intervento deve altresì essere messo a disposizione della revisione interna; 78

- comunicare tempestivamente alla direzione generale i cambiamenti di rilievo intervenuti nella valutazione del rischio di *compliance*; 79

- presentare ogni anno all'organo preposto all'alta direzione un rapporto sulla valutazione dei rischi di *compliance* e l'attività della funzione di *compliance*. Una copia del rapporto viene messa a disposizione della revisione interna e della società di audit; 80

- comunicare tempestivamente alla direzione generale e all'organo preposto all'alta direzione gravi violazioni della *compliance* rispettivamente fatti di ampia portata e supportare la direzione generale nella scelta delle istruzioni da impartire o delle misure da adottare. La revisione interna deve essere opportunamente informata al riguardo. 81

VIII. Revisione interna

A. Costituzione

In linea di principio, ogni istituto deve costituire una revisione interna. 82

Se la costituzione di una revisione interna propria dell'istituto non è considerata adeguata, i compiti della revisione interna possono essere affidati: 83

- alla revisione interna della società madre o alla revisione interna di un'altra società del gruppo, se si tratta di una banca, di un commerciante di valori mobiliari o di un altro intermediario finanziario (p. es. un'impresa di assicurazione) sottoposto a vigilanza statale (per le banche estere nel quadro dell'art. 4^{quinquies} LBCR); 84
- a una seconda società di audit indipendente da quella dell'istituto; o 85
- a una società del gruppo o a un terzo indipendente, a condizione che la società di audit ne confermi le competenze professionali e disponga di adeguate risorse tecniche e in termini di personale. 86

B. Subordinazione gerarchica e organizzazione

La revisione interna è subordinata all'organo preposto all'alta direzione o al relativo comitato di audit e svolge in maniera indipendente i compiti di controllo e di sorveglianza che le vengono assegnati. Essa gode di un illimitato diritto di consultazione, informazione e verifica all'interno dell'istituto e delle imprese che rientrano obbligatoriamente nel perimetro di consolidamento in conformità al nm. 98. 87

La revisione interna deve essere costituita in base alle dimensioni, alla complessità e al profilo di rischio dell'istituto e dal punto di vista organizzativo rappresenta un'unità autonoma e indipendente rispetto all'attività operativa. 88

La revisione interna deve soddisfare le esigenze qualitative dell'Associazione Svizzera di Revisione Interna (ASRI). L'attività della revisione interna si basa sugli *International Standards for the Professional Practice of Internal Auditing* dell'Institute of Internal Auditors (IIA). 89

Il sistema di remunerazione dei collaboratori della revisione interna non deve creare incentivi che generano conflitti di interesse. 90

C. Compiti e responsabilità

La revisione interna svolge verifiche e valutazioni indipendenti concernenti l'adeguatezza e l'efficacia dell'organizzazione aziendale e i processi operativi, e in particolare concernenti il sistema di controllo interno e la gestione del rischio dell'istituto. 91

La revisione interna svolge almeno una volta all'anno una valutazione globale dei rischi dell'istituto, tenendo adeguatamente conto degli sviluppi esterni (p. es. contesto economico, modifiche a livello normativo) e dei fattori interni (p. es. progetti importanti, orientamento dell'attività). 92

In base alla valutazione del rischio e alle esigenze di verifica che emergono altrimenti, la revisione interna fissa gli obiettivi di verifica e la relativa pianificazione per il successivo periodo di audit e li sottopone, congiuntamente alle modifiche sostanziali, all'approvazione dell'organo preposto all'alta direzione o al relativo comitato di audit. 93

La revisione interna provvede che la direzione generale e la società di audit siano informate sulla valutazione dei rischi e gli obiettivi di verifica. 94

La revisione interna riferisce, tempestivamente e per iscritto, all'organo preposto all'alta direzione o al relativo comitato di audit e alla direzione generale in merito a tutte le constatazioni significative emerse in fase di audit. 95

Almeno una volta all'anno la revisione interna redige un rapporto scritto sui risultati significativi delle verifiche e sulle principali attività svolte durante il periodo di audit considerato e lo sottopone per informazione, corredato delle corrispondenti conclusioni, all'organo preposto all'alta direzione o al relativo comitato di audit, alla direzione generale e alla società di audit. 96

Inoltre, la revisione interna o un'altra istanza indipendente in seno all'istituto (p. es. funzione di *compliance* o controllo dei rischi) informa l'organo preposto all'alta direzione o il relativo comitato di audit almeno a ritmo semestrale sulle misure adottate per colmare le lacune sostanziali e sullo stato di avanzamento dell'attuazione delle raccomandazioni della revisione interna e della società di audit. 97

IX. Strutture del gruppo

La presente circolare si applica per analogia ai gruppi e ai conglomerati finanziari («gruppi»). 98

I gruppi devono disciplinare i compiti e le competenze delle unità investite della responsabilità generale della conduzione del gruppo. Le disposizioni, tenuto conto dell'attività e dei rischi essenziali a livello di gruppo e di singolo istituto, devono garantire una gestione efficiente e unitaria del gruppo, consentire lo scambio di informazioni, tenere conto delle strutture giuridiche e organizzative nonché definire i compiti e le responsabilità come pure la necessaria indipendenza dei relativi livelli gerarchici. Occorre in particolare tenere conto dei rischi che risultano dal raggruppamento di più imprese in un'unica entità economica. 99

X. Entrata in vigore e disposizioni transitorie

I seguenti requisiti devono essere applicati al più tardi entro un anno dall'entrata in vigore: 100

- l'applicazione della regola che prevede l'indipendenza di un terzo dei membri dell'organo preposto all'alta direzione in conformità al nm. 17; 101
- l'istituzione di un comitato di audit e, separatamente, di un comitato di rischio per gli istituti delle categorie di vigilanza 1-3 in conformità al nm. 31; 102
- l'allestimento e l'approvazione di una strategia quadro per la gestione del rischio a livello di istituto in conformità al nm. 52 segg.; 103
- la creazione di una funzione di CRO a sé stante, segnatamente come parte integrante della direzione generale per gli istituti di rilevanza sistemica in conformità ai nm. 67 e 68. 104

L'adempimento delle ulteriori disposizioni concernenti l'aggregazione e la reportistica relativa ai dati sui rischi in conformità al nm. 59 per le banche di rilevanza sistemica è fissato al momento temporale successivo fra: 105

- entrata in vigore della presente circolare, e
- un periodo transitorio di tre anni in seguito alla designazione di banca di rilevanza sistemica in conformità all'art. 8 cpv. 3 LBCR.