

Circolare 2017/2

Corporate governance – assicuratori

Corporate governance, gestione del rischio e sistema di controllo interno nel settore assicurativo

Riferimento:	Circ. FINMA 17/2 «Corporate governance – assicuratori»
Data:	7 dicembre 2016
Entrata in vigore:	1° gennaio 2017
Concordanza:	sostituisce le Circ. FINMA 08/32 «Corporate governance – assicuratori» e Circ. FINMA 08/35 «Revisione interna – assicuratori», entrambe del 20 novembre 2008
Basi legali:	LFINMA art. 7 cpv. 1 lett. b LSA artt. 14, 22, 27, 67, 68, 75, 76 OS artt. 12–14, 16, 96–98a, 191, 195–196, 204

Destinatari									
LBCR	LSA	LisFI			LinFI		LICol	LRD	Altri
Banche		Gestori patrimoniali	Trustee	Gestori di patrimoni collettivi	Sedi di negoziazione	Controparti centrali	SICAV	OAD	
Gruppi e cong. finanziari.		Direzioni dei fondi			Depositari centrali		Società in accomandita per ICC	Assoggettati OAD	
Altri intermediari		Società di intermed. mobiliare che tengono conti			Repertorio di dati sulle negoz.		SICAF	Società di audit	
Assicuratori	X	Società di intermed. mobiliare che non tengono conti			Sistemi di pagamenti		Banche depositarie	Agenzie di rating	
Gruppi e cong. assicurativi	X				Partecipanti		Rappresentanti di ICC esteri		
Intermediari assicurativi							Altri intermediari		

I. Scopo	nm.	1
II. Ambito di applicazione	nm.	2-5
III. Principi in materia di <i>corporate governance</i>	nm.	6-15
IV. Consiglio di amministrazione	nm.	16-27
A. Composizione	nm.	16-23
B. Comitati del consiglio di amministrazione	nm.	24-27
V. Sistema di gestione del rischio e sistema di controllo interno	nm.	28-56
A. Sistema di gestione del rischio	nm.	28
B. Sistema di controllo interno	nm.	29-36
C. Processi di <i>compliance</i>	nm.	37
D. Funzioni di controllo	nm.	38-56
a) Funzione preposta alla gestione del rischio	nm.	41
b) Funzione preposta alla <i>compliance</i>	nm.	42-43
c) Revisione interna	nm.	44-56
VI. Disposizione transitoria	nm.	57

I. Scopo

La presente circolare concretizza le disposizioni della Legge federale sulla sorveglianza delle imprese di assicurazione (LSA; RS 961.01) in materia di *corporate governance*, gestione del rischio e sistema di controllo interno (SCI). 1

II. Ambito di applicazione

La presente circolare si applica a tutte le imprese di assicurazione ai sensi dell'art. 2 cpv. 1 lett. a e b LSA nonché ai gruppi e ai conglomerati assicurativi ai sensi dell'art. 2 cpv. 1 lett. d in combinato disposto con gli artt. 65 e 73 LSA assoggettati alla vigilanza dei gruppi e dei conglomerati. 2

La presente circolare si applica per analogia alle filiali in Svizzera di imprese di assicurazione con sede all'estero (art. 2 cpv. 1 lett. b LSA) e di imprese di assicurazione autorizzate all'esercizio del ramo assicurativo C3 (riassicurazione mediante *captive*). 3

I nn. 16-27, che concernono il consiglio di amministrazione di un'impresa di assicurazione, si applicano per analogia all'organo amministrativo della società cooperativa. 4

Nell'applicazione di tali disposizioni occorre tenere conto delle peculiarità, delle dimensioni e della complessità dell'impresa di assicurazione come pure del principio di proporzionalità. 5

III. Principi in materia di *corporate governance*

L'impresa di assicurazione applica in particolare i seguenti principi in materia di *corporate governance* a tutta l'impresa: 6

- chiara assegnazione e documentazione di mansioni, competenze e responsabilità come pure dei canali di rendicontazione; 7
- chiara separazione tra attività operative e attività di controllo per mezzo di adeguate misure; 8
- messa a punto di processi di rendiconto interni ai fini di trasmettere delle informazioni a tutti i servizi rilevanti in seno all'impresa; 9
- documentazione di decisioni importanti (misure comprese); 10
- messa a punto, in tutta l'impresa, di un efficace sistema di gestione del rischio e di un efficace sistema di controllo interno (SCI), che comprenda le funzioni di controllo (gestione del rischio, *compliance*, revisione interna) e il controllo periodico della relativa adeguatezza effettuato da una terza parte indipendente (interna o esterna); 11
- definizione di principi, processi e strutture per il rispetto delle prescrizioni legali, normative e interne; 12

- definizione di principi, processi e strutture per l'identificazione e la gestione di conflitti d'interesse e di abusi; 13
- definizione di principi concernenti il comportamento dei collaboratori atteso; 14
- messa a punto di processi tesi a garantire che le persone preposte all'alta direzione, alla vigilanza e al controllo nonché alla direzione dell'impresa di assicurazione dispongano in modo durevole della necessaria esperienza professionale, delle conoscenze specialistiche e dell'idoneità personale. 15

IV. Consiglio di amministrazione

A. Composizione

Oltre alle conoscenze necessarie in ambito assicurativo, collegialmente il consiglio di amministrazione deve disporre in particolare di esperienze professionali e di conoscenze sufficienti in materia di direzione, gestione strategica, gestione del rischio, finanza e contabilità. 16

Il consiglio di amministrazione è composto almeno da tre membri. Il numero di membri dipende dalle dimensioni, dalla complessità e dal profilo di rischio dell'impresa di assicurazione. 17

Il consiglio di amministrazione è composto almeno per un terzo da membri che adempiono i criteri di indipendenza qui di seguito. In casi motivati, la FINMA può concedere delle deroghe, per esempio nel caso di *captive* di riassicurazione o filiali di gruppi e agglomerati assicurativi assoggettati. 18

Un membro del consiglio di amministrazione è considerato indipendente se soddisfa almeno i seguenti criteri: 19

- non ricopre un'altra funzione in seno all'impresa di assicurazione e non l'ha ricoperta nel corso degli ultimi due anni; 20
- nel corso degli ultimi due anni non ha ricoperto la funzione di auditor responsabile presso la società di audit dell'impresa di assicurazione; 21
- non intrattiene con l'impresa di assicurazione relazioni d'affari che, per natura o entità, potrebbero creare conflitti d'interesse; e 22
- non detiene partecipazioni dell'impresa di assicurazione e non rappresenta alcun detentore di partecipazioni. Sono considerate detentori di partecipazioni le persone di cui all'art. 4 cpv. 2 lett. f LSA. 23

B. Comitati del consiglio di amministrazione

Se opportuno, il consiglio di amministrazione costituisce comitati del consiglio di amministrazione per l'effettivo esercizio dei suoi compiti. 24

Le imprese di assicurazione delle categorie di vigilanza 2 e 3 devono istituire un comitato di audit e un comitato di rischio. Le imprese di assicurazione della categoria di vigilanza 3 possono combinare il comitato di audit e il comitato di rischio in un unico comitato. 25

I comitati di audit e di rischio devono essere composti per almeno un terzo da membri indipendenti (cfr. nm. 19-23). In linea di principio, il presidente del consiglio di amministrazione non deve rivestire la carica né di membro del comitato di audit né di presidente del comitato di rischio. 26

Ogni comitato dispone collegialmente delle conoscenze e delle esperienze necessarie nel rispettivo ambito di attività. Il presidente di un comitato dispone di conoscenze specifiche nel proprio ambito di attività. 27

V. Sistema di gestione del rischio e sistema di controllo interno

A. Sistema di gestione del rischio

L'impresa di assicurazione dispone di un sistema di gestione del rischio secondo l'art. 96 OS, che deve essere documentato ai sensi dell'art. 97 OS. I sistemi dei limiti per le esposizioni ai rischi come pure i meccanismi di controllo di cui all'art. 97 cpv. 2 lett. e OS devono garantire che l'impresa di assicurazione operi nel quadro della sua capacità di rischio. I principi della gestione del rischio sono applicabili sia alle principali esternalizzazioni sia ad altre relazioni con terzi. 28

B. Sistema di controllo interno

L'impresa di assicurazione istituisce un sistema di controllo interno volto a garantire un'adeguata sicurezza per quanto concerne i rischi relativi alla gestione, in particolare in relazione all'efficacia dei processi operativi, all'affidabilità della rendicontazione finanziaria e all'ottemperanza delle norme legali e delle prescrizioni interne. I principi del sistema di controllo interno sono applicabili sia alle principali esternalizzazioni sia ad altre relazioni con terzi. 29

L'impresa di assicurazione definisce sufficienti attività di controllo a livello di impresa e di processi in modo tale da garantire il rispetto e l'esecuzione di procedure, metodi e misure ordinati dal consiglio di amministrazione e dalla direzione ai fini di contrastare i principali rischi correlati alla direzione. 30

Il consiglio di amministrazione, la direzione e gli altri collaboratori dispongono di tutte le informazioni necessarie per potere assumere le proprie responsabilità relative al sistema di controllo interno. 31

L'impresa di assicurazione documenta il proprio sistema di controllo interno. La documentazione deve essere costantemente aggiornata e comprendere in particolare: 32

- le direttive interne all'impresa concernenti il sistema di controllo interno e i processi a esso correlati; 33

- la descrizione dell'organizzazione a livello di struttura e processi, compresi i compiti, le competenze e le responsabilità; 34
- i requisiti sul piano del sistema di controllo interno (fra cui obiettivi, dotazione di risorse, sensibilizzazione dei collaboratori); 35
- descrizione delle attività di controllo consolidate. 36

C. Processi di *compliance*

L'impresa di assicurazione identifica i propri obblighi legali e regolamentari fondamentali ed effettua una stima dei propri rischi di *compliance* principali. 37

D. Funzioni di controllo

L'impresa di assicurazione provvede affinché ogni funzione di controllo svolga i propri compiti in modo obiettivo e indipendente. 38

La remunerazione dei collaboratori delle funzioni di controllo deve essere strutturata in modo tale da ridurre al minimo eventuali conflitti d'interesse con le unità operative da essi sorvegliate o controllate. 39

Le funzioni di controllo hanno accesso illimitato a tutte le persone e informazioni di cui necessitano per lo svolgimento dei loro compiti. 40

a) Funzione preposta alla gestione del rischio

Il responsabile della funzione preposta alla gestione del rischio effettua regolarmente una stima indipendente dei rischi importanti dell'impresa di assicurazione e dell'adeguatezza del sistema di gestione del rischio. Egli presenta periodicamente (almeno una volta all'anno) un resoconto all'attenzione del consiglio di amministrazione. 41

b) Funzione preposta alla *compliance*

La funzione preposta alla *compliance* valuta l'adeguatezza dei principi, dei processi e delle strutture (di controllo) allestiti dall'impresa di assicurazione volti all'osservanza delle prescrizioni legali, regolamentari e interne come pure valuta il modo in cui l'impresa di assicurazione gestisce eventuali violazioni delle norme in materia di *compliance*. 42

Il responsabile della funzione preposta alla *compliance* effettua periodicamente (almeno una volta all'anno) una stima indipendente dei rischi di *compliance* importanti dell'impresa di assicurazione e presenta un resoconto al consiglio di amministrazione. 43

c) Revisione interna

La revisione interna è direttamente subordinata al consiglio di amministrazione o al relativo comitato di audit. A livello organizzativo e operativo è indipendente dalle altre funzioni di controllo dell'impresa di assicurazione. Essa gode di un illimitato diritto di consultazione, di informazione e di verifica all'interno dell'impresa di assicurazione. 44

La revisione interna è strutturata in conformità agli standard internazionali per la pratica professionale della revisione interna ¹ ; nel quadro della propria attività, essa rispetta tali standard.	45
La revisione interna svolge le proprie attività sulla base di una pianificazione dell'audit periodica e orientata al rischio. A tale scopo essa determina tutti gli ambiti di attività, le funzioni e i processi principali dell'impresa di assicurazione (gli oggetti da sottoporre ad audit) ed effettua almeno una volta all'anno una valutazione del rischio di tali oggetti. Se durante il periodo di audit si verificano modifiche sostanziali al profilo di rischio dell'impresa di assicurazione, la revisione interna esamina la pianificazione dell'audit e, all'occorrenza, la adegua. Il consiglio di amministrazione o il relativo comitato di audit approva il piano di audit e le modifiche sostanziali apportate.	46
La revisione interna redige almeno una volta all'anno un rapporto all'attenzione del consiglio di amministrazione, includendo in particolare i seguenti punti:	47
• l'attuazione del piano di audit approvato dal consiglio di amministrazione come pure le attività svolte in via complementare al piano di audit;	48
• lo stato di attuazione delle misure di miglioramento adottate;	49
• le circostanze che pregiudicano l'indipendenza, l'oggettività o l'efficacia della revisione interna.	50
La revisione interna redige tempestivamente e in modo oggettivo all'attenzione del consiglio di amministrazione o del relativo comitato di audit un rapporto scritto contenente tutte le constatazioni importanti stabilite nell'ambito di un audit. Le carenze gravi devono essere comunicate senza indugio.	51
La revisione interna mette il proprio rapporto all'attenzione del consiglio di amministrazione come pure i singoli rapporti a disposizione della società di audit secondo l'art. 28 LSA.	52
L'esternalizzazione integrale o parziale dei compiti della revisione interna è soggetta all'obbligo di approvazione secondo l'art. 4 cpv. 2 lett. j LSA. I compiti della revisione interna o parti di essi possono essere affidati:	53
• alla revisione interna della società al vertice di un gruppo, purché l'impresa di assicurazione assoggettata alla vigilanza sia integrata nei processi di controllo e di gestione del gruppo;	54
• a una società di audit abilitata dall'Autorità federale di sorveglianza dei revisori ASR che sia indipendente dalla società di audit già incaricata dall'impresa di assicurazione in conformità all'art. 28 LSA;	55
• a un prestatore esterno di servizi che sia indipendente dalla società di audit già incaricata dall'impresa di assicurazione in conformità all'art. 28 LSA.	56

¹ Standard internazionali per la pratica professionale della revisione interna emanati dall'Institute of Internal Auditors (IIA).

VI. Disposizione transitoria

I nn. 17, 18–23 e 25–27 devono essere applicati entro il 31 dicembre 2019 al più tardi. In casi motivati la FINMA può concedere deroghe. 57