Circular 2017/2
Corporate governance – insurers

Corporate governance, risk management and internal control system at insurers

Reference:	FINMA Circ. 17/2 "Corporate governance – insurers"
Date:	7 December 2016
Entry into force:	1 January 2017
Concordance:	former FINMA Circ. 08/32 "Corporate governance – insurers" and FINMA Circ. 08/35 "Internal audit – insurers", both dated 20 November 2008
Legal framework:	FINMASA Article 7 para. 1 let. b ISA Articles 4, 14, 22, 27, 67, 68, 75 and 76 ISO Articles 12-14, 16, 96-98*a*, 191, 195-196 and 204

Adressees

BankA			ISA			FinIA						FMIA						CISA						AMLA		Other	
Banks	Financial groups and congl.	Other intermediaries	Insurers	Insurance groups and congl.	Intermediaries	Portfolio managers	Trustees	Managers of collective assets	Fund management companies	Investment firms (proprietarian trading)	Investment firms (non propriet. trading)	Trading venues	Central counterparties	Central securities depositories	Trade repositories	Payment systems	Participants	SICAVs	Limited partnerships for CISs	SICAFs	Custodian banks	Representatives of foreign CISs	Other intermediaries	SRO	SRO-supervised institutions	Audit firms	Rating agencies
			X	X																							

Laupenstrasse 27, 3003 Bern
Phone +41 (0)31 327 91 00, Fax +41 (0)31 327 91 01
www.finma.ch

Contents

I. Purpose

The purpose of this circular is to clarify the provisions of the Insurance Supervision Act (ISA; SR 961.01) on corporate governance, risk management and internal control systems (ICS). 1

II. Scope of application

This circular applies to all insurance companies as defined in Article 2 para. 1 lets. a and b ISA and to insurance groups and insurance conglomerates which are subject to group/conglomerate supervision under Article 2 para. 1 let. d in conjunction with Articles 65 and 73 ISA. 2

The circular applies by analogy to domestic branches of insurance companies domiciled abroad (Art. 2 para. 1 let. b ISA) and insurance companies licensed to operate in insurance class C3 (reinsurance through captives). 3

Margin numbers 16-27 regarding the board of directors of an insurance company apply to the governing body of cooperatives. 4

When applying these provisions, it is important to take account of the specificities, size and complexity of the insurance company in question and give due consideration to the principle of proportionality. 5

III. Corporate governance principles

The insurance company must implement the following corporate governance principles throughout its organisation: 6

- clear allocation and documentation of duties, powers, responsibilities and reporting channels; 7
- clear separation of operational activities and control activities; 8
- establishment of internal reporting processes to share information with all relevant units/individuals in the company; 9
- documentation of key decisions (and associated measures); 10
- establishment of effective company-wide risk management and an effective internal control system (ICS) including the control functions (risk management, compliance, internal audit), and periodic reviews of their appropriateness by an independent (internal or external) party; 11
- definition of principles, processes and structures for compliance with legal, regulatory and internal requirements; 12
- definition of principles, processes and structures for identifying and dealing with abuses and conflicts of interest; 13

- definition of principles relating to the conduct expected of employees; 14

- establishment of processes to ensure that individuals responsible for overall direction, supervision and control as well as the executive management of the insurance company have and maintain the required professional experience, specialist knowledge and personal aptitude. 15

IV. Board of directors

A. Composition

The board of directors as a body must have sufficient knowledge of the insurance business and the requisite experience and knowledge of business management, strategic management, risk control, and finance and accounting. 16

The board of directors must have at least three members. The actual number of members will depend on the size, complexity and risk profile of the insurance company. 17

At least one third of the members of the board must meet the following independence criteria. FINMA may approve exceptions where there is good reason for doing so (e.g. for reinsurance captives or for subsidiaries of insurance groups and of conglomerates supervised by FINMA). 18

Members of the board of directors are deemed to be independent if they: 19

- are not and have not in the previous two years been employed in some other function within the insurance company; 20

- have not been employed in the previous two years by the insurance company's audit firm as lead auditor of the regulatory audit responsible for the insurance company; 21

- have no commercial links with the insurance company which, in view of their nature and scope, would lead to conflicts of interest; and 22

- are not a shareholder of the insurance company and do not represent any shareholder. The definition of a shareholder can be found in Article 4 para. 2 let. f ISA. 23

B. Committees of the board of directors

Where appropriate, the board of directors forms committees to enable it to fulfil its mandate effectively. 24

Insurance companies in supervisory categories 2 and 3 establish an audit committee and a risk committee. A combined risk and audit committee can be formed by insurance companies in supervisory category 3. 25

At least one third of the members of the audit and risk committees must be independent (see margin nos. 19-23). The chair of the board of directors may not be a member of the audit committee or the chair of the risk committee. 26

As a body each committee has the knowledge and experience required to perform its role. The chair of a committee must have specific knowledge in their area of responsibility. 27

V. Risk management system and internal control system

A. Risk management system

The insurance company has a risk management system which meets the requirements set out in Article 96 ISO and which is documented in accordance with Article 97 ISO. The purpose of the risk exposure limit systems and control mechanisms defined in Article 97 para. 2 let. e ISO is to ensure that the insurance company operates within the parameters of its risk capacity. Risk management principles apply to major outsourcing arrangements and other relationships with third parties. 28

B. Internal control system

The insurance company establishes an internal control system to ensure that there is an appropriate level of assurance regarding the risks of the business, particularly as regards the effectiveness of business processes, the reliability of financial reporting, and compliance with legal norms and internal regulations. Internal control system principles apply to major outsourcing arrangements and other relationships with third parties. 29

The insurance company defines sufficient control activities at both company and process level with the aim of ensuring that the processes, methods and measures which have been set out by the board of directors and the executive board to control key business risks are complied with and implemented. 30

The board of directors, the executive board and other employees of the company receive all the information they require to meet their responsibilities regarding the internal control system. 31

The insurance company documents its internal control system. The documentation is kept up-to-date and comprises in particular: 32

- internal company guidelines on the internal control system and the associated processes; 33
- a description of the system's organisational and operational structure, including the relevant duties, powers and responsibilities; 34
- the requirements to be met by the internal control system (e.g. goals, provision of resources, awareness-raising among employees); 35
- a description of the established control activities. 36

C. Compliance processes

The insurance company identifies its key legal and regulatory obligations and makes an assessment of its key compliance risks. 37

D. Control functions

The insurance company ensures that each control function meets its responsibilities objectively and independently. 38

The compensation system for employees of control functions must be set up in such a way that potential conflicts of interest with the business units which these employees monitor or control are kept to a minimum. 39

The control functions have unrestricted access to all the individuals and information sources they need in order to meet their responsibilities. 40

a) Risk management function

The head of the risk management function regularly makes an independent assessment of the insurance company's key risks and of the appropriateness of the risk management system, and reports periodically (at least annually) about this assessment to the board of directors. 41

b) Compliance function

The compliance function assesses the appropriateness of the principles, processes and (control) structures which the insurance company has established to comply with legal, regulatory and internal requirements; it also assesses how the company deals with compliance breaches. 42

The head of the compliance function periodically (at least annually) makes an independent assessment of the insurance company's key compliance risks and reports about the assessment to the board of directors. 43

c) Internal audit

Internal audit reports directly to the board of directors or its audit committee. It is organisationally and operationally independent of the insurance company's other control functions and has an unlimited right of inspection, information and audit within the insurance company. 44

Internal audit is established in accordance with international professional standards for internal auditing[1] and applies these standards in its activities. 45

Internal audit performs its activities on the basis of a periodic, risk-based audit plan. For this purpose, internal audit determines all of the company's relevant business areas, functions 46

[1] International Standards for the Professional Practice of Internal Auditing from The Institute of Internal Auditors (IIA)

and processes (the auditable entities) and carries out a risk assessment of the auditable entities at least annually. If the insurance company's risk profile changes significantly during the audit period, internal audit reviews its audit plan and updates it accordingly. The board of directors or its audit committee approves the audit plan and any material amendments to it.

Internal audit produces a report at least annually for the attention of the board of directors. This report covers the following in particular: 47

- implementation of the audit plan, as approved by the board of directors, and any activities which go beyond the scope of the plan; 48

- implementation status of agreed improvements; 49

- any factors which negatively affect the independence, objectivity or effectiveness of internal audit. 50

Internal audit reports in writing to the board of directors or its audit committee in a timely and objective manner on all material audit findings. Serious shortcomings must be reported immediately. 51

Internal audit makes its report to the board of directors and its individual audit reports available to the audit firm appointed by the insurance company under Article 28 ISA. 52

The complete or partial outsourcing of the internal audit function is subject to the approval requirement stated in Article 4 para. 2 let. j ISA. The internal audit function can be outsourced to: 53

- the internal audit function of a group company, provided that the supervised insurance company is included in group-wide control and management processes; 54

- an audit firm which has been approved by the Federal Audit Oversight Authority (FAOA) and which is independent of the audit firm already appointed by the insurance company under Article 28 ISA; 55

- an external service provider which is independent of the audit firm already appointed by the insurance company under Article 28 ISA; 56

VI. Transitional provision

Margin numbers 17-23 and 25-27 must be implemented by 31 December 2019 at the latest. FINMA may approve exceptions in cases where there is good reason to do so. 57