

Directives

of Federal Office of Private Insurance (FOPI)

1st January 2007

15/2006 – on Corporate Governance, Risk Management and the Internal Control System

Legal foundations: **Articles 14 and 22 ISA**
 Article 27 ISA
 Articles 67, 68, 75 and 76 ISA
 as well as the provisions contained in the associated ordinance

Decision of: **21 November 2006**

Enter into force: **on 1 January 2007**



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Swiss Federal Department of Finance FDF
Federal Office of Private Insurance FOPI

1 Legal foundations, purpose and scope

1.1 Legal foundations

This directive is based on the following legal foundations: article 14 and article 22 ISA (Insurance Supervision Act) with respect to corporate governance and risk management, article 27 ISA with respect to the internal control system, and articles 67, 68, 75, and 76 ISA with respect to insurance groups and conglomerates, as well as the provisions contained in the associated ordinance.

1.2 Purpose

This directive serves to concretise the provisions under supervision law relating to corporate governance (CG), risk management (RM), and the internal control system (ICS). In a consolidated and principle-based form, it lays down minimum standards with respect to CG, RM, and ICS for the insurance undertakings, groups, and conglomerates subject to supervision.

1.3 Scope

These provisions on corporate governance (CG), risk management (RM), and the internal control system (ICS) shall apply to insurance undertakings, groups, and conglomerates subject to Swiss insurance supervision by decree in accordance with article 2, paragraph 1(a) and (b) ISA and, by order, in accordance with article 2, paragraph 1(d) and article 65 or 73 ISA (hereinafter "undertakings"). For health insurance schemes offering products subject to the ICA (Insurance Contract Act), the rules set out in FOPI circular 11/2006 of the Health Insurance Division dated 1.11.2006 shall apply. The provisions of this directive shall apply analogously to Swiss branches of insurance undertakings with registered offices abroad. When applying these provisions, the complexity and size of the entity in question and the principle of proportionality shall be taken into account.

In the case of group and conglomerate supervision, implementation by the highest group company is sufficient, as long as the individual companies subject to supervision are included in the group-wide monitoring and control processes.

2 Definitions and objectives

2.1 Definition and objective of corporate governance

Corporate governance encompasses the principles and structures by which an undertaking is controlled and monitored. Corporate governance ensures a functional balance among the various organs of the undertaking (checks and balances), sufficient transparency of the internal processes, and a harmonisation of the objectives of the undertaking with the expectations of the various stakeholder groups. These include policyholders and beneficiaries, owners, the supervisory authority, and employees. From the perspective of supervision law, the protection of policyholders and beneficiaries is of particular importance.

2.2 Definition of risk management

Risk management encompasses the methods and processes for purposes of identification, assessment, risk strategies and risk control measures, and monitoring and reporting of risks.

2.3 Definition of the internal control system

The internal control system (ICS) encompasses the internally ordered procedures, methods, and measures that serve to ensure appropriate security with respect to the risks of business management, especially pertaining to the effectiveness of business processes, the reliability of financial reporting, and compliance with laws and regulations.

2.4 Objective of risk management and the internal control system

Appropriate risk management (article 22 ISA, articles 96-98, 195, and 196, paragraph 2 of the Supervision Ordinance, SO) and an effective internal control system (article 27 ISA) ensure that risk potentials can be recognised and assessed at an early stage, and that measures are introduced to prevent or hedge substantial risks and risk accumulations (article 96 SO).

3 Provisions on corporate governance

3.1 General principles of corporate governance

The undertakings shall take the following principles of corporate governance into account and shall take measures necessary for their implementation:

- Clear documentation of the existing corporate governance structures and reporting processes, e.g. in articles of associations, organisational rules and regulations, and the rules and regulations of appointed committees (cf. article 4, paragraph 2(a) and (b) ISA and article 191 SO);
- Compliance with the legal foundations and regulatory demands relevant to the activities of the undertaking;
- Integrity and ethical conduct as well as a culture of accountability, such as by
 - issuing directives or instructions that require employees of the undertaking to act in an ethical manner;
 - establishing appropriate compensation and incentive systems that serve the long-term interests and the long-term fulfilment of the goals of the undertaking and that promote ethical conduct;
 - recruiting employees based on the requisite qualifications.
- Compliance with principles for preventing conflicts of interest and abuses. For this purpose, the undertakings shall issue internal directives, such as relating to capital in-

vestments and hedging instruments. For the latter, the code of conduct for occupational pensions shall serve analogously as a minimum standard;

- Appointment of a compliance function, if reasonable given the size and complexity of the undertaking's business;
- Periodic sensitisation of employees according to level with respect to corporate governance, e.g. through training;
- Independence of the internal auditing office as an important control function for monitoring business activities (article 27, paragraph 1, sentence 2 ISA);
- Creation of an appropriate environment in which the responsible actuary can fulfil his responsibilities (cf. article 4, paragraph 2(h), articles 23-24 ISA, article 99 SO, and articles 2-4 SO-FOPI).

3.2 Board of directors

For the board of directors, the following corporate governance principles shall apply (for cooperative societies, these principles shall apply analogously to the governing body):

- In particular, the board of directors is responsible for overall direction, organisation, and supervision of the undertaking (article 716a, paragraph 1 of the Code of Obligations (CO), cf. also articles 894 et seq. CO) and must be composed in such a way that it as a whole can fulfil these responsibilities (article 12, paragraph 1, first half sentence SO). Inter alia, this also requires appropriate availability;
- As a whole, the board of directors must have both general expertise and the necessary strategic insurance knowledge so that it can fulfil its responsibilities of supervising and directing the activities of the undertaking, especially in order to understand and assess the transactions, processes, and risks of the undertaking (article 12, paragraph 1, second half sentence SO);
- The members of the board of directors must vouch for sound and proper business conduct by having appropriate expertise (see above) and appropriate experience (fitness) and by enjoying a good reputation (properness) (articles 14 and 67 ISA);
- The members of the board of directors shall ensure that their personal and professional arrangements avoid conflicts of interest with the undertaking to the extent possible;
- In principle, the chairman of the board of directors may not simultaneously serve as chief executive officer (prohibition of dual function under article 13 SO);
- As part of its statutory organisational authority, the board of directors shall appoint board committees depending on the size and complexity of the undertaking's business for the purpose of improving monitoring and control (e.g. an audit committee, a nomination or compensation committee);
- The board of directors shall take measures to ensure that the principles of this directive are implemented in the undertaking.

3.3 Executive board

For the executive board, the following principles of corporate governance shall apply (for cooperative societies with similar organisational structures, they shall apply analogously):

- The members of the executive board must vouch for sound and proper business conduct by having appropriate expertise and appropriate experience (fitness) and by enjoying a good reputation (properness) (articles 14 and 67 ISA);
- The members of the executive board must have the requisite knowledge and experience to manage the areas delegated to them (article 14, paragraph 1 SO);
- The executive board of the undertaking must immediately inform the supervisory authority of any occurrences relevant to supervision (article 47, paragraph 3 ISA; see also FOPI directive 10/2006 concerning the independent duty of insurance undertakings to provide information, dated 12.10.2006, in force since 1.11.2006);
- The members of the executive board shall ensure that their personal and professional arrangements avoid conflicts of interest with the undertaking to the extent possible.

4 Provisions on risk management and the internal control system

4.1 General principles

- The undertaking shall guarantee and document risk management procedures appropriate to its business with respect to all significant risks (article 22 ISA, articles 96 and 97 SO);
- The undertaking shall implement and document an effective internal control system appropriate to its business (article 27 ISA);
- The undertaking shall define the scope and utility of the internal structures and processes as well as of the internal organisation, accountability, and division of labour between risk management and the internal control system;
- The undertaking shall periodically verify the processes used in risk management and the internal control system and shall implement important adjustments in a timely manner;
- The undertakings shall ensure sufficient resources for risk management and the internal control system and shall define the reporting process. The undertaking shall sensitise employees according to level with respect to the tasks and responsibilities relating to risk management and the internal control system, e.g. through training;
- The undertaking shall define risk strategies appropriate to its size and complexity, taking into account its appetite and tolerance for risk. Risk tolerance is limited by the economic loss of value that the undertaking is willing to bear or that it can bear due to appropriate measures. Risk tolerance depends on the available resources (capital, human resources, information technology) and dictates the risk limits. Risk appetite encompasses the risk that an undertaking wants to assume, given its possibilities;
- The processes of risk management and the internal control system comprise the following elements:
 - Risk identification and assessment (4.2);
 - Risk control measures and control activities (4.3);
 - Information and documentation (4.4);
 - Monitoring for purposes of identifying deficiencies and corrective measures (4.5).

4.2 Risk identification and assessment

- The undertaking shall take appropriate measures with respect to risk identification and assessment;
- An important part of the process of risk identification consists in classifying the significant risks;
- Risk identification and assessment must be performed regularly;
- The significant risks must be identified and assessed;
- The methods of risk identification and assessment must be reviewed regularly and adjusted as needed;
- Risk identification and assessment must take current scientific developments into account, especially with regard to economic and actuarial methods;
- Risk identification and assessment must include a prospective analysis.

4.3 Risk control measures and control activities

- The undertaking shall take appropriate measures with respect to risk control measures and control activities (such as directives and controls on underwriting, investments, re-insurance, technical reserves, claims management, etc.);
- The risk control measures must be compatible with the internally defined risk appetite and risk tolerance;
- The control activities must ensure that the defined measures are complied with. Periodically, a report shall be compiled on significant non-compliance with limits and measures as well as on the implementation of corrective measures;
- The significant risks must be monitored;
- The methods of the risk control measures and control activities shall be reviewed regularly and adjusted as needed;
- The provisions concerning risk control measures and control activities must take current scientific developments into account, especially with regard to economic and actuarial methods;
- An appropriate separation of functions between operational and control activities must be ensured to prevent conflicts of interest.

4.4 Information and documentation

- The goals of risk management and the internal control system must be communicated within the company in a form appropriate to the time and the addressee;
- The information shall be submitted to the appropriate decision-makers. Information and escalation processes must be defined;
- Employees must be provided with all necessary information, so that they can fulfil the requisite responsibilities in risk management and the internal control system;
- Documentation of risk management and the internal control system:
 - Risk management and the internal control system must be documented;

- In particular, the documentation must encompass:
 - Organisation including tasks, competences, and responsibilities;
 - Demands on risk management and the internal control system;
 - Risk strategy including risk tolerance;
 - Procedures for identifying significant risks and explanation of the methods, instruments, and processes for identifying, assessing, and monitoring these risks;
 - Explanation of the applicable limit systems for risk exposures and of the control mechanisms;
 - Internal directives on risk management, the internal control system, and the related processes.
- In the event of changes, the documentation must be brought up to date.
- Internal risk reporting (article 96, paragraph 2(e) SO):
 - Internal risk reporting shall reflect the current risk situation and risk concentrations, indicating the methods, instruments, and procedures that have led to these assessments;
 - Internal risk reporting shall be submitted in a timely manner to the appropriate decision-makers;
 - The report shall contain statements on the effectiveness and the weaknesses of risk management and the internal control system.
- Internal and external transparency:
The undertaking shall regularly inform the various stakeholder groups on:
 - Corporate governance;
 - The type of risk management and the internal control system.

4.5 Monitoring for purposes of identifying deficiencies and corrective measures

The undertakings shall evaluate the availability and functioning of the components of risk management and the internal control system, as well as the progress made over time with respect to quality.

5 Entry into force and transitional provisions

This directive shall enter into force on 1 January 2007. The provisions of this directive must be implemented by 31 December 2007.

Federal Office of Private Insurance

Herbert Lüthy
Director