Finansinspektionen's Regulations

Publisher: Gent Jansson, Finansinspektionen, Box 6750, 113 85 Stockholm.
Ordering address: Thomson Fakta AB, Box 6430, 113 82 Stockholm. Tel. +46 8-587 671 00, Fax +46 8-587 671 71.
Subscribe also by e-mail at www.fi.se.
ISSN 1102-7460

FFFS 2005:1
Published
23 February 2005

Finansinspektionen's (the Swedish Financial Supervisory Authority) General Guidelines Regarding Governance and Control of Financial Undertakings;

decided on 7 February 2005.

Finansinspektionen has issued the following general guidelines.

Chapter 1. Scope

§ 1 Through these general guidelines, Finansinspektionen wishes to promote a sound culture of governance and control, as well as adequate functions for governance and control of undertakings under the supervision of the Authority.

§ 2 The general guidelines cover operations in undertakings that are under the supervision of Finansinspektionen (hereinafter referred to as "undertakings") and should be applied by:

– individual undertakings and, where appropriate, within groups, groups of financial undertakings and financial conglomerates.

However, they shall not apply to:

– undertakings in their operations pursuant to the Investment Funds Act (SFS 2004:46); and
– financial institutions pursuant to Chapter 1 section 5 item 7 of the Banking and Financing Business Act (SFS 2004:297).

§ 3 Finansinspektionen has also issued general guidelines regarding the management of specific risk areas within various undertakings. These general guidelines are intended to supplement them.

Comply or explain

§ 4 These general guidelines are formulated in general terms and allow for alternative solutions. It should be possible to explain such solutions.

Definitions

§ 5 *Function* means one or more persons, units or divisions or, specifically appointed committees, charged with the task of performing one or more of the duties mentioned in these general guidelines.

Internal regulations means the policy and governance documents, guidelines, instructions or other written documents through which the issuer (board of directors, managing director or any other employee) governs the operations.

Internal governance and control means the process by which the undertaking's board of directors, managing director, management or other personnel create reasonable certainty that the undertaking's goals are fulfilled in the following areas:

- an appropriate and efficient organisation and management of the operations;
- reliable financial reporting;
- compliance with applicable laws, ordinances and other regulations.

Chapter 2. Governance

The board of directors' responsibility and duties

§ 1 An undertaking's board of directors shall bear the ultimate responsibility for the undertaking's organisation and management of its affairs. The nature of the board of directors' responsibility follows, *inter alia*, from the company law and business law legislation applied by the undertaking.

The board of directors should adopt a strategy and targets for the operations conducted by the undertaking. The board of directors should also follow up compliance with these targets.

Material changes relating to the operations and organisation should be decided upon by the board of directors.

§ 2 Where an undertaking is the parent undertaking in a group, the board of directors of the parent undertaking should endeavour to ensure that common internal rules are adopted in respect of the licensed operations which are conducted by undertakings within the group. The aforesaid should apply to the undertaking in a group of financial undertakings or a financial conglomerate which enjoys a superior position within the group or the conglomerate.

Where appropriate, the functions addressed in Chapter 3 (Risk management and Risk Control), Chapter 5 (Compliance with Regulations) and Chapter 6 (Independent Monitoring Functions) may be located centrally within a group, a group of financial undertakings or a financial conglomerate. The aforesaid shall apply provided that the functions possess expertise and resources relating to all licensed operations.

§ 3 In undertakings that are not covered by the Swedish Companies Act, the board of directors should also adopt, in internal regulations, rules of procedure for the board of directors and duties for the managing director or equivalent employee.

The managing director's responsibilities and duties

§ 4 An undertaking's managing director shall handle the day-to-day management of the undertaking's affairs in accordance with the board of directors' guidelines and instructions. The managing director shall also take the measures required in order that:

– the undertaking's accounts are maintained in accordance with law; and
– the administration of funds is conducted in a secure manner.

The nature of the managing director's responsibility follows, *inter alia*, from company law and business law legislation.

The managing director should ensure that the board of directors receives such objective, detailed and relevant information as required in order to take well-founded decisions and that the board of directors is regularly informed regarding developments in the undertaking's operations.

Internal information

§ 5 An undertaking should possess efficient information and communications systems for the dissemination of internal information. The reference here is, *inter alia*, to technical systems as well as organisation and routines for the internal communication and dissemination of information.

Chapter 3. Internal governance and control

§ 1 Through sound internal control, an undertaking can ensure:

- an appropriate and efficient organisation and management of the operations;
- reliable financial reporting;
- efficient operation and management of information systems;
- a good ability to identify, measure, monitor and manage its risks;
- a good ability to comply with laws and ordinances, internal regulations, as well as generally accepted practice or generally accepted standards.

§ 2 The board of directors and managing director should endeavour to ensure that the organisation and management of the undertaking’s operations are characterised by sound internal control.

§ 3 In order to maintain sound internal control, the organisation should be adapted to the changes in internal and external risks that take place over time.

§ 4 An undertaking may achieve sound internal control by, for example:

- regularly following up on the operations and ensuring that controls are in place which guarantee that reporting appropriately reflects the operations;

- regularly monitoring that resources are used efficiently and in order to achieve the undertaking's goals;

- producing internal regulations, as well as documenting and updating them regularly;

- allocating responsibility and work in such a manner that the risk of conflicts of interest is avoided;

- ensuring that an employee does not handle a transaction alone throughout the entire processing chain (segregation of duties);

- ensuring, through controls, that information is provided in the event developments within a business area deviate from the undertaking's guidelines and targets;

- ensuring, through controls, that the reporting is complete and accurate, transactions are reported on time and that reported transactions are actually implemented;

- ensuring continuity in the operations and protecting the assets of the undertaking and the customers, through information security and physical security controls;

- ensuring that information and reporting systems guarantee current and relevant information regarding the institution's operations and risk exposure, etc.

Chapter 4. Management and control of risks

Business risks

§ 1 Risks which should be managed and controlled include, for example, the following:

- credit and counterparty risks;
- market risks (interest rate risks, currency risks, and price risks);
- liquidity risks;
- operational risks (risk of losses due to defective or inappropriate internal processes and routines, human error, defective systems or external events, including legal risks).

With respect to insurance companies and benevolent societies, there are also specific insurance risks such as:

- underwriting risks;
- provisions risks;
- reinsurance risks; and
- matching risks.

Internal regulations for management and control of risks

§ 2 The board of directors should ensure that the undertaking's management of risks (risk management) and follow-up of the undertaking's risks (risk control) are satisfactory.

For this purpose, internal regulations should be adopted regarding risk management and risk control. Compliance with these regulations should be ensured constantly.

How is risk control to be organised?

§ 3 The undertaking should contain a composite function for independent risk control. The function should inform the board of directors, management and other persons who require the information.

The information should provide a comprehensive and objective representation of the undertaking's risks and contain analyses of changes in the risks. The function

should also propose the changes in governance documents and processes which result from the observations regarding risk management.

The function should be answerable to the managing director. It may also be situated so that it is answerable to another senior officer who possesses sound knowledge of the undertaking's risks and is directly subordinate to the managing director. Such person shall not, however, be responsible for the day-to-day business operations.

The function should possess the resources necessary for its duties. The duties should not be carried out by employees who are engaged in the day-to-day business operations.

§ 4 The function may structure the work in different ways depending on the undertaking's operations. It may, for example, engage other functions in the undertaking to compile data for its reports and analyses. The function shall, however, at all times be responsible for the coordinated reporting and analyses of the undertaking's risks, and for ensuring that the underlying data is correct.

§ 5 Chapter 8 § 1 and Chapter 16, § 1 of the Insurance Operations Act (SFS 1982:713) regarding the duties and responsibility of the responsible actuary shall also apply with respect to insurance companies.

Chapter 5. Compliance

§ 1 *Compliance* means, in these general guidelines, compliance with laws, ordinances and internal regulations as well as generally accepted practices or generally accepted standards (hereinafter jointly referred to as "regulations") regarding the licensed operations.

Deficient compliance may result in increased operational risks, risks of legal sanctions, supervisory risks, economic losses and damage to reputation.

How is compliance to be ensured?

§ 2 The board of directors should ensure that a function (compliance) is in place which supports the operations being conducted in accordance with governing regulations. Where appropriate, the function should also monitor compliance.

The function should provide information regularly regarding the risks that may arise in the operations as a consequence of deficient compliance, assist in identifying and assessing such risks, and assist in the formulation of internal regulations. The function should also inform the board of directors, managing director and management with respect to compliance issues.

§ 3 The function should regularly ensure that the relevant personnel obtain information regarding new or amended regulations and, where required, training in the new regulations.

§ 4 The board of directors or managing director should issue internal regulations with respect to the function's area of responsibility, scope and implementation of the function's work as well as routines for information regarding observations.

§ 5 The function should be answerable to the board of directors or the Managing Director. It may also be so situated so that it is subordinate to another senior

officer in possession of sound knowledge regarding the undertaking's risks and operations in general, who is directly answerable to the managing director.

The function should possess resources sufficient for its duties. It should also have personnel who possess sound knowledge of the undertaking's risks and the regulations applied by the undertaking.

§ 6 The work of the function may be structured in different ways depending on the undertaking's operations. It may vary between different undertakings and between, for example, the local and central levels in an undertaking.

The ambition should be that the undertaking achieves, as far as possible, an independent position in relation to the direct commercially driven operation. The work of the function may, where appropriate, be performed by consultants.

§ 7 Finansinspektionen's regulations regarding rules of conduct on the securities markets shall also apply with respect to securities companies.

Chapter 6. Independent Monitoring Function (Internal audit)

§ 1 The board of directors should ensure that a function is in place which monitors and evaluates the internal control (including the risk control and the compliance function). In undertakings with an internal audit function, the duties shall be performed by such function.

The function should possess sufficient resources for its duties. It should also have personnel who possess:

– sound knowledge of the undertaking's risks and the regulations applied by the undertaking; and
– particular expertise in auditing and evaluating the development, operation and management of the undertaking's information systems.

§ 2 The function should be directly answerable to the board of directors. Organisationally, it should be entirely separated from the operations that are audited. The independence of the function thus entails that it should not participate in the operative business.

§ 3 The board of directors should, in internal regulations, determine the function's responsibilities, work duties and reporting routines.

§ 4 The function should monitor that the scope and focus of the operations are in accordance with the board of directors' internal regulations. The function should also audit and evaluate the undertaking's organisation and routines. The head of the function should be present at board meetings at which the function's reports are considered.

§ 5 The audit may, where appropriate, be performed by consultants.

§ 6 The function's work should be documented.

Chapter 7. Engagement agreements

§ 1 An undertaking may outsource parts of the operations to an external service provider, whether within or outside the undertaking's own group or group of

undertakings. The board of directors and managing director shall, however, at all times be responsible for the outsourced activities.

§ 2 The board of directors or managing director should draw up internal regulations as to which licensed operations, or operations that have a natural connection with financial operations or their support functions, may be outsourced and the manner in which such shall take place.

The internal regulation should state at least the following:

- the demands which are imposed regarding the undertaking's order placement expertise;
- the manner in which risks associated with outsourcing are to be managed;
- that the undertaking shall ensure that the service provider protects confidential information with respect both to the undertaking and its customers;
- the manner in which the undertaking shall govern and monitor performance of the engagement and review the outsourced activities;
- the demands which must be imposed regarding expertise of the service provider and internal controls and quality, as well as the service provider's possibilities to perform the engagement in the long term.
- that the undertaking and service provider shall prepare and maintain contingency plans for unforeseen events, including crisis and catastrophe planning, which shall be tested regularly;
- that it must be ensured that Finansinspektionen is able, in the future, to exercise effective supervision over the undertaking as well as that the undertaking's obligations towards Finansinspektionen or the undertaking's customers are not breached;
- that contingency plans and strategies shall be prepared regarding the manner in which the engagement might be discontinued and the activities resumed by the undertaking without significant disruption in important activities;
- that a written agreement shall be prepared which regulates the service level, the parties' rights and obligations, as well as other issues pursuant to these general guidelines.

§ 3 Upon outsourcing of activities within a group or group of undertakings, particular attention should be paid to issues of bias and conflicts of interest. The board of directors should ensure that all such issues are identified and that the undertaking has internal regulations in place which address issues of bias and conflicts of interest.

§ 4 Where an undertaking intends to outsource a significant part of the licensed operations, or activities that have a natural connection with financial operations or their support functions, the undertaking should notify such in advance to Finansinspektionen.

§ 5 Chapter 6, § 7 of the Banking and Financing Business Act (SFS 2004:297) shall also apply with respect to banks and credit market undertakings.

Chapter 8, § 8 of the Insurance Operations Act (SFS 1982:713) shall also apply with respect to insurance companies.

Finansinspektionen's general guidelines regarding securities operations (FFFS 2002:5) shall also apply with respect to securities companies.

These general guidelines shall enter into force on 1 May 2005, at which time the following statutes shall be repealed:

1. Finansinspektionen's general guidelines (FFFS 1999:12) regarding governance, internal information and internal controls within credit and securities institutions as well as investment fund companies;

2. Finansinspektionen's general guidelines (FFFS 2000:3) regarding governance, internal information and internal controls within insurance companies and benevolent societies.

INGRID BONDE

Hans Schedin