Finansinspektionen's Regulatory Code

Publisher: Finansinspektionen, Sweden, *www.fi.se*
ISSN 1102-7460

FFFS 2014:5
Published
17 April 2014

Finansinspektionen's Regulations and General Guidelines regarding information security, IT operations and deposit systems;

decided on 11 April 2014.

Finansinspektionen prescribes[1] the following pursuant to Chapter 5, Section 2, point 4 of the Banking and Financing Business Ordinance (2004:329) and Chapter 6, Section 1, points 9 to 12 and 29 of the Securities Market Ordinance (2007:572), and provides the following general guidelines.

Chapter 1 Scope

Section 1 These regulations include provisions on how an undertaking is to manage information security, IT operations and deposit systems.

Section 2 The regulations apply to the following undertakings:

1. banking companies,
2. savings banks,
3. members' banks,
4. credit market companies,
5. credit market associations, and
6. investment firms.

Definitions

Section 3 In these regulations and general guidelines, the same definitions are used as in Chapter 1, Section 3 of Finansinspektionen's Regulations and General Guidelines (FFFS 2014:1) regarding governance, risk management and control at credit institutions and Finansinspektionen's Regulations (FFFS 2014:4) regarding the management of operational risks, unless otherwise stated in the regulations.

In addition, the following definitions apply:

1. *information security:* protection of the confidentiality, accuracy and accessibility of information,

2. *IT operation:* an undertaking's organisation, processes and staff to manage its IT systems.

3. *confidentiality:* the fact that information is not made available or disclosed to unauthorised persons,

[1] Cf. Directive 2009/14/EC of the European Parliament and of the Council of 11 March 2009 amending Directive 94/19/EC on deposit-guarantee schemes as regards the coverage level and payout delay (OJ L 68, 13.3.2009, p. 3, Celex 32009L0014)

4. *integrity:* property of information entailing that the information has not been amended without authorisation, by mistake or due to a malfunction,

5. *traceability:* the ability to unambiguously trace activities performed and the person or system function that has performed them, and

6. *availability:* the ability to use information to the expected extent and within the desired period.

Chapter 2 Information security

Information security management system

Section 1 A management system under Sections 2 to 9 shall be used to ensure that the information security work performed by an undertaking is structured and methodical.

Goals and direction

Section 2 An undertaking shall document goals and direction for its information security. The board of directors or managing director shall decide on goals and direction.

Responsibility for information security and coordination

Section 3 An undertaking shall ensure that there is a clear allocation of responsibility for information security within its operations.

Section 4 An undertaking shall appoint a person who is responsible for leading and coordinating the information security work.

Information classification

Section 5 An undertaking shall classify its information so that it is ascribed the right level of protection. This classification shall be based on the requirements imposed on the information's confidentiality, integrity and availability in its operations.

The undertaking shall document the classification under the first paragraph and appoint persons or functions who are responsible for the information processed within its operations.

Risk analysis

Section 6 An undertaking shall analyse the risks related to the undertaking's information security once a year as well as in the event of changes that can affect the information security. The undertaking shall decide how to manage risks identified based on these analyses and incidents that have occurred.

The undertaking shall document the risk analyses and its decisions on measures.

Internal rules

Section 7 An undertaking shall decide on the internal rules for its information security work.

The undertaking shall consider the nature, scope and complexity of its operations when formulating the internal information security rules.

General guidelines

The internal rules should specify requirements for

1. physical security,
2. protection of data communications and operations,
3. traceability in IT systems,
4. separating the production environment for IT systems from testing and development environments,
5. control of access to information,
6. security requirements for IT systems at the time of purchase, development, maintenance and decommissioning,
7. reporting and managing incidents related to information security, and
8. regular controls of the undertaking's IT system in relation to the protection level for information laid down under Section 5.

Section 8 In particular, an undertaking shall specify in the internal rules under Section 7 how the undertaking shall allocate, change and withdraw access permissions to IT systems. The undertaking shall regularly, though at least once a year, check that existing access permissions are restricted to needs based on work duties allocated.

Section 9 An undertaking shall ensure that the internal rules under Section 7 are regularly evaluated and shall update them if so required.

Chapter 3 IT operations

Security

Section 1 An undertaking shall ensure that its IT systems are sufficiently secure in relation to the nature of the information processed in the systems.

General guidelines

When assessing whether IT systems are sufficiently secure, the undertaking should base this on the classification of information made under Chapter 2, Section 5.

Goals and strategy

Section 2 An undertaking shall have overall goals and strategies for its IT operations that are documented.

The managing director shall decide on the undertaking's overall goals and strategies under the first paragraph and regularly evaluate and update them if so required.

Responsibility

Section 3 An undertaking shall ensure that it is clear who is responsible for the various parts of the undertaking's IT operations. The undertaking shall appoint a person or function to be responsible for the undertaking's system requirements for each IT system.

Processes

Section 4 An undertaking shall have appropriate processes for managing its IT systems. The undertaking shall document the processes and describe the circumstances of importance for managing its IT systems in a controlled way.

The undertaking shall consider the nature, scope and complexity of the operations when applying the first paragraph.

General guidelines

The processes that the undertaking is to document should encompass:

1. purchases, development, maintenance and decommissioning,
2. operation, including back-ups, and restoring systems and recovering data,
3. incident management,
4. change management, and
5. testing.

Documentation of IT systems

Section 5 An undertaking shall have documentation for each individual IT system that is of importance to the operation. These systems shall be specified in a list that is to be regularly reviewed and updated if so required.

Outsourcing agreements

Section 6 Provisions regarding outsourcing agreements are provided in Chapter 10 of Finansinspektionen's Regulations and General Guidelines (FFFS 2014:1) regarding governance, risk management and control at credit institutions and Chapter 9 of Finansinspektionen's Regulations (FFFS 2007:16) governing investment services and activities.

Chapter 4 Deposit systems

Scope

Section 1 The provisions of this chapter apply to undertakings that receive or intend to receive deposits encompassed by a deposit guarantee scheme under the Deposit Guarantee Scheme Act (1995:1571).

Deposit systems

Section 2 When processing its information about depositors and their deposits, an undertaking shall use IT systems that enable the undertaking to automatically compile data about depositors and their deposits in accordance with the Swedish National Debt Office's Regulations (RGKFS 2011:2) regarding the obligation of institutions to submit information about depositors and their deposits.

Risk analysis

Section 3 An undertaking shall annually analyse the risks relating to the IT systems used by the undertaking to process its information about depositors and their deposits. This analysis shall include the protection of the information's integrity and the system integrity of the IT system. The analysis shall also encompass the information's confidentiality and accessibility.

System integrity in this chapter means that an IT system can maintain its intended function and thereby be protected against undesirable impact, modification or examination.

Functions and procedures

Section 4 An undertaking shall ensure that IT systems under Section 2 have technical functions and that there are administrative procedures to ensure

1. access controls,
2. that activities in the IT system and changes to the IT system are traceable,
3. system integrity,
4. the integrity of information,
5. that the system's operation can be recovered following an interruption, and
6. that information is available in accordance with the Swedish National Debt Office's Regulations (RGKFS 2011:2) regarding the obligation of institutions to submit information about depositors and their deposits.

The undertaking shall also decide on the required technical functions and administrative procedures based on the risk analyses it is to perform under Section 3.

Documentation

Section 5 In addition to the requirements specified in Chapter 3, Section 5, an undertaking shall document the undertaking's technical functions and administrative procedures under Section 4.

This documentation shall be regularly reviewed and updated if so required.

Audit and reporting

Section 6 The undertaking's internal audit function shall perform an annual audit of the undertaking's deposit system as well as the technical functions and administrative procedures that are of importance to the security of the system. If the undertaking does not have an internal audit function, it shall assign the annual audit to another party who has special expertise within the area of security.

The audit shall be documented and reported to the undertaking's board of directors.

General guidelines

The undertaking's audit should be based on established security principles.

These regulations and general advice shall enter into force on 1 June 2014.

MARTIN ANDERSSON

Anders Lindgren