Finansinspektionen's Regulatory Code

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

FFFS 2014:4
Published
17 April 2014

Finansinspektionen's Regulations and General Guidelines regarding the management of operational risks;

decided on 11 April 2014.

Finansinspektionen prescribes 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 13 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 its operational risks.

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.

Section 3 However, Sections 15 to 23 of Chapter 5 and Section 4, point 1 of Chapter 6 do not apply to investment firms.

Section 4 The regulations contain provisions relating to the following:

– Scope (Chapter 1),

– Governance and responsibility (Chapter 2),

– Identification and measurement (Chapter 3),

– Reporting (Chapter 4),

– Management of operational risks in operations (Chapter 5), and

– Further requirements for the management of operational risks within investment services and activities and foreign exchange trading (Chapter 6).

Definitions

Section 5 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 2007:16) governing investment services and activities, unless otherwise stated in the regulations.

In addition, the following definitions apply:

1. *contingency plan:* a plan describing the measures that an undertaking is to take to deal with serious and extensive interruptions, disruptions or crises,

2. *incident*: an event that has or is at risk of having an adverse effect on the undertaking's operations, assets or reputation,

3. *continuity plan:* a plan describing how operations are to be maintained in the event of an interruption or a major operational disruption,

4. *operational risk:* the same as in Article 4.1 (52) of Regulation (EU) No 575/2013 of the European Parliament and Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012,[1]

5. *process*: a chain of consecutive activities that produces a result based on a certain input of resources, and

6. *recovery plan:* a plan describing the priorities and procedures according to which an undertaking shall revert to normal operations following an interruption or major operational disruption.

Chapter 2 Governance and responsibility

Section 1 An undertaking shall determine a risk appetite for its operational risks. The undertaking shall have limits for its operational risks within the framework of its risk appetite.

The undertaking shall use its products, services, functions, processes and IT systems as a basis for setting limits. It should be possible to use qualitative or quantitative measures to assess these limits. The undertaking shall document its risk appetite and limits.

The board of directors shall decide on and regularly evaluate and if necessary update the risk appetite for operational risks. The managing director shall decide on and regularly evaluate and if necessary update the limits for operational risks.

Section 2 An undertaking shall have internal rules for the management of operational risks specifying

1. the main operational risks to which the undertaking is exposed,

2. first the methods and processes used to identify, measure and manage operational risks that also take into account infrequent incidents of a serious nature, and second procedures for managing the risk that these methods may potentially yield erroneous results, and

3. the undertaking's procedures for determining and monitoring the risk appetite and limits under Section 1.

[1] Cf. Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012 (OJ L 176, 27.6.2013, p. 1, Celex 32013R0575).

If the undertaking uses risk transfer in the course of its management of operational risks, the principles for this should be specified in its internal rules.

The board of directors shall decide on the internal rules.

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

Outsourcing agreements

Section 3 Provisions regarding outsourcing agreements are provided in Chapter 9 of Finansinspektionen's Regulations (FFFS 2007:16) governing investment services and activities, and Chapter 10 of Finansinspektionen's Regulations and General Guidelines (FFFS 2014:1) regarding governance, risk management and control at credit institutions.

Chapter 3 Identification and measurement

Section 1 An undertaking shall identify operational risks in its products, services, functions, processes and IT systems.

Section 2 An undertaking shall have methods to identify and measure its operational risks. These methods shall be documented.

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

Section 3 An undertaking shall regularly measure the operational risks under Section 1 by assessing the likelihood of them occurring and what impact they would have. The undertaking shall also determine the measures to be taken to manage these risks.

Risk indicators

Section 4 An undertaking shall determine and document indicators and thresholds for its operational risks that provide a warning when risks increase.

The undertaking shall regularly review and, if necessary, update these indicators and thresholds.

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

General guidelines

Examples of indicators that the undertaking should consider:

1. frequent reorganisations or major operational changes,
2. high staff turnover,
3. large number of vacant posts,
4. large number of customer complaints,
5. that the number of incidents has increased or the type of incidents has changed, and
6. that the internal audit function has reported deficiencies in the internal rules.

Incidents

Section 5 An undertaking shall have internal rules to manage incidents arising in its operations.

Section 6 An undertaking shall document and analyse an incident when it occurs. The undertaking shall also document the losses that have arisen in conjunction with the incident. The undertaking shall have procedures in place to ensure that this information is correct. This does not apply to an incident reported anonymously.

The undertaking shall use the information in the first paragraph when identifying and measuring operational risks under Section 3.

Chapter 4 Reporting

Section 1 When reporting operational risks to the board of directors and managing director, an undertaking shall specify

1. indicators for operational risks under Chapter 3, Section 4,
2. breaches of risk appetite and risk limits under Chapter 2, Section 1, and
3. serious incidents.

The undertaking shall also report the results from tests of the contingency, continuity and recovery plans to the board of directors at least once a year.

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

Chapter 5 Management of operational risks in operations

Processes

Section 1 An undertaking shall determine and specify in a list its operating processes that are of material significance.

This list shall be regularly reviewed and updated if necessary.

Section 2 An undertaking shall document the processes under Section 1 and appoint a person or function to be responsible for each such process.

Section 3 An undertaking shall specify in internal rules how to document the processes under Section 1 and how operational risks in these processes is to be managed.

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

General guidelines

The undertaking should describe the following in the process documentation under Section 2

1. which rules affect the design of the process,
2. the process's main activities and their relationship(flowcharts),
3. the information used in the activities under 2,
4. the quality requirements imposed on the information under 3,
5. which IT systems support the process,
6. at which point controls are carried out and decisions made in the process,
7. stakeholders to the process, e.g. staff, customers, public authorities, sub-contractors and other undertakings, and
8. the output of the process, e.g. a service, product or other output.

Section 4 An undertaking shall have procedures in place to analyse whether there are activities in the processes under Section 1 where there is a risk of significant losses due to, for example, mistakes, manipulation of information and also the potential to hide erroneous assessments and losses.

The undertaking shall introduce the necessary controls in the processes if it identifies such activities.

The procedures under the first paragraph shall be documented.

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

Staff

Section 5 An undertaking shall have procedures in place for how to manage operational risks with regard to its staff, stating how the undertaking

1. verifies essential information, taking particular account of the risk of conflicts of interest in conjunction with the undertaking employing new staff,

2. ensures that it has sufficient staff in relation to the work duties,

3. evaluates whether it has any staff with such expertise or that occupy such a function that they are difficult to replace at short notice, and appoints replacements for such staff,

4. determines requirements for expertise and knowledge for staff and also ensures that their expertise and knowledge are maintained,

5. determines and updates job descriptions, mandates and limits,

6. deals with the duty of confidentiality regulated in Chapter 1, Section 10 of the Banking and Financing Business Act (2004:297) and Chapter 1, Section 11 of the Securities Market Act (2007:528), and

7. identifies and manages operational risks that may arise in conjunction with staff internally changing work duties or organisational unit.

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

Legal risks

Section 6 An undertaking shall specify in internal rules how it manages legal risks. The internal rules shall specify how the undertaking

1. ensures that its operations comply with laws, statutes and other regulations,
2. ensures and follows up the accuracy and validity of contracts entered into or other legal documents concluded,
3. archives contracts and other legal documents, and
4. manages and follows up legal processes.

The internal rules under the first paragraph shall also specify which person or function is responsible for the management of 1 to 4.

Security work

Section 7 An undertaking shall have internal rules for security work that include information about which assets and values are to be protected. The undertaking shall specify measures to be taken to protect these assets and values and also the extent of these measures.

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

General guidelines

The undertaking should use scenarios or simulations in its security work to increase awareness of how different types of threat, impropriety and criminal act may arise in the undertaking's operations.

Section 8 Provisions on information security are provided in Chapter 2 of Finansinspektionen's Regulations and General Guidelines (FFFS 2014:5) regarding information security, IT operations and deposit systems.

IT systems

Section 9 Provisions on how an undertaking is to manage IT systems are provided in Chapter 3 of Finansinspektionen's Regulations and General Guidelines (FFFS 2014:5) regarding information security, IT operations and deposit systems.

Approval process

Section 10 An undertaking shall have a process in place to approve new or materially altered products, services, markets, processes and IT systems and also in the event of major changes to the undertaking's operations and organisation.

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

Section 11 An undertaking shall describe the approval process under Section 10 in internal rules. The internal rules shall also specify

1. what the undertaking means by new or materially altered, existing products, services, markets, processes, IT systems and major changes to the undertaking's operations and organisation, and also

2. the functions and units that are to participate in the process.

When producing the internal rules, the undertaking shall consider the nature, scope and complexity of the operations when applying the first paragraph.

Section 12 An undertaking shall ensure that the approval process under Section 10 has the following components:

1. controls to ensure compliance with applicable rules,

2. analysis of whether the undertaking's risk levels may increase or if new risks may arise and whether this could affect the undertaking's capital requirements,

3. controls to ensure that there are sufficient staff and access to expertise, internal rules, tools and processes in business units and also support and control functions to be able to understand and monitor the risks, and

4. documentation of approval decisions stating the considerations on which the decision was based.

Section 13 The risk control function shall determine whether the process under Section 10 is to apply if this has not been specified in the internal rules under point 1 of Section 11.

Section 14 When an undertaking decides on a new product, service, market, process or IT system, it shall determine which person or function is to be responsible for managing the risks associated therewith.

Continuity management

Section 15 An undertaking shall specify the following in its internal rules for continuity management:

1. the methods and procedures that the undertaking is to follow to have properly functioning continuity management. These methods and procedures shall include contingency, continuity and recovery plans,

2. officers responsible (roles and positions) for steering operations and for deciding on measures in the event of an interruption or major operational disruption, and

3. principles for managing and making decisions on measures depending on the type and scope of interruption or major operational disruption.

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

The managing director shall decide on the internal rules.

Section 16 An undertaking shall determine the longest period permitted for an interruption for each process under Chapter 5, Section 1.

Impact analysis and recovery planning

Section 17 An undertaking shall regularly analyse the impact of such interruptions or major operational disruptions that may occur in the undertaking's operations and also in the operations that the undertaking has engaged another party to perform.

Section 18 The impact analysis under Section 17 shall be conducted at all business units and support functions considering their interdependence. An undertaking shall use the analysis as a basis for

1. determining the undertaking's priorities and goals in order to revert to normal operations after an interruption or major operational disruption, and

2. producing contingency, continuity and recovery plans.

The plans under 2 shall be documented.

Section 19 An undertaking shall ensure that its main data centre is at a sufficient geographical distance from the location where the undertakings stores its back-up copies.

General guidelines

If the undertaking has an alternative data centre, it should ensure that this is not dependent on the same physical infrastructure as the main data centre, and that data together with back-up copies that are stored at both data centres cannot be destroyed simultaneously.

Communication and training

Section 20 An undertaking shall have procedures to manage its internal and external communications in conjunction with an interruption or major operational disruption. When planning its communications, the undertaking shall also consider that an interruption or disruption may have a significant impact on the activity of subsidiaries or branches or affect the financial system in some other way.

Section 21 An undertaking shall regularly train and inform its staff about how to use contingency, continuity and recovery plans.

Updating and testing of plans

Section 22 An undertaking shall regularly update and test its contingency, continuity and recovery plans so that they are adapted to its operations and the priorities for reverting to normal operations under Section 18.

The undertaking shall appoint a person or function to be responsible for updating and testing each such plan.

Section 23 An undertaking shall determine the following in its internal rules for continuity management under Section 15:

1. what kinds of test it will perform under Section 22, and
2. how often the tests are to be performed.

Contingency, continuity and recovery plans for processes under Chapter 5, Section 1 and also the IT systems supporting these processes shall be tested at least once a year.

Chapter 6 Further requirements for the management of operational risks within investment services and activities and foreign exchange trading

Section 1 The provisions of this chapter shall, in addition to those stated in Chapters 1 to 5, be applied at undertakings authorised to provide investment services and perform investment activities under Chapter 2, Section 1, points 2–3 of the Securities Market Act (2007:528) and by undertakings that engage in foreign exchange trading under Chapter 7, Section 1, point 12 of the Banking and Financing Business Act (2004:297).

Segregation of duties

Section 2 An undertaking shall ensure that the work duties of staff who initiate and execute business transactions and staff whose work involves supporting, verifying and monitoring these transactions are kept separated.

Staff

Section 3 An undertaking shall ensure that staff who deal with business transactions for a period of at least ten consecutive working days in a twelve-month period are not able to

1. initiate and execute business transactions,
2. approve or confirm business transactions, or
3. process payments linked to business transactions.

Transaction management

Section 4 An undertaking shall ensure that

1. there is a complete and documented verification chain for each transaction and that this verification chain ensures traceability that enables follow up in relation to each trader,

2. there are documented procedures and controls throughout the entire chain from the opening of a business relationship to the settlement of transactions executed,

3. terms and conditions for the transaction are documented and confirmed before trading starts,

4. staff who initiate and execute business transactions, provide the support functions with the information and documentation required as soon as possible after the finalisation of a transaction so that they can reconcile, confirm, settle and verify the transaction,

5. procedures are established to manage and report transactions that have been executed incorrectly,

6. procedures are established to manage and report unconfirmed transactions as well as to review them on a daily basis, and

7. reconcile transactions, payments and positions on a daily basis.

Reconciliation under 7 shall also include amendments and cancellations

Managing collateral

Section 5 An undertaking shall have procedures in place] to manage and control the collateral provided in conjunction with transactions and positions.

Section 6 An undertaking shall ensure that procedures are established for verifying the availability within counterparty limits before these are used in conjunction with trading.

Monitoring and control

Section 7 In the event of material deviations or unreasonable results during trading, an undertaking shall analyse whether these have been caused by mistakes, irregularities or other occurrences in its operations.

Section 8 An undertaking shall review and reconcile all of its accounts on an ongoing basis.

Section 9 An undertaking shall verify the value of its net positions and the transactions that give rise to them.

Section 10 An undertaking shall determine and regularly follow up limits for its positions. The undertaking shall set the limits so that they can be followed up and controlled.

Section 11 An undertaking shall check at least on a quarterly basis that access permissions for the IT systems that are used in its operations are restricted to needs based on work duties allocated.

_____

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

MARTIN ANDERSSON

Agnieszka Arshamian