



FINANSTILSYNET

THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Circular

Guidelines to the Regulations on Risk Management and Internal Control

CIRCULAR:

3/2009

DATE:

13.01.2009

TRANSLATION AS OF MARCH 2010

RECIPIENTS:

Sent to all entities under supervision

FINANSTILSYNET

P.O.BOX 1187 Sentrum

NO-0107 Oslo

About the regulations

The purpose of the Regulations of 22 September 2008 no. 1080 is to improve the institutions' risk management and internal control by elaborating on the responsibilities the board of directors and management have beyond what follows from the provisions of corporate law and special legislation. These Regulations replace the Regulations of 20 June 1997 no.1057 on Responsibility for Internal Control and on Documentation and Confirmation of Internal Control. The new Regulations do not entail wide-ranging material changes, but do take account of other regulatory changes and the development of the theoretical basis for risk management and internal control. In addition, their scope is expanded to encompass new types of institutions subject to the supervision by Finanstilsynet. The Circular replaces Circular 16/2003.

The Regulations and Circular are general in nature and not everything referred to will be equally relevant to everyone. The institutions' risk management and internal control shall be tailored according to the nature, scope and complexity of the institution's activities, cf. section 2. The job of risk management and internal control is a continuous process that will mature and be enhanced over time. Finanstilsynet assumes that institutions that have been subject to the previous regulations possess the relevant competence and experience as a consequence of implementing the relevant processes. The focus therefore will be on providing guidance to the new institutions that are subject to the Regulations, and to small institutions. The Regulations set minimum requirements for the institution's processes and documentation related to risk management and internal control. The Circular provides guidance on what Finanstilsynet will emphasise in its supervision.

Chapter 1 – Introductory provisions

Section 1 Scope

The scope of the Regulations has been expanded to also encompass:

- Debt collection agencies
- External accounting firms

The Regulations also apply to institutions subject to the regulations covering capital requirements. However, a dispensation has been included in section 6, paragraph three, to reduce unnecessarily additional burden for institutions regulated by the Financial Institutions Act. The intention is to introduce a similar solution in the insurance area when the Solvency II legislation is implemented.

The Regulations on Risk Management and Internal Control apply at a consolidated level to the parent company in a financial group. However, this does not reduce the responsibilities and obligations of subsidiaries and their boards of directors. The ultimate parent company bears responsibility for risk management in the group and must be familiar with the risk assessments made in the subsidiaries subject to the regulations.

Lawyers who perform estate agency or debt collection activities by virtue of their personal license do not fall under the scope of the regulations.

Section 2 Proportionality

The principle of proportionality is not new, but has been included to clarify that what is good, adequate risk management and internal control can vary. Each institution must itself conduct this assessment according to the nature, scope and complexity of the institution's activities.

The provision allows smaller institutions to be subject to less comprehensive requirements concerning the risk management and internal control process than those to which large institutions are subject. This may also apply to institutions with a limited range of products, e.g. monoline insurance companies.

Elements of an overall assessment could be:

- Number of employees
- Turnover
- Whether the market or products are subject to frequent changes
- How easy it is for the CEO and other managers to check that the activities are being operated in line with the applicable routines and regulations, and how extensive the control must be to maintain such an overview
- Whether the regulations stipulate special customer protection requirements
- What opportunity customers have to themselves check the quality of the service being offered

Chapter 2 – Responsibility for risk management and internal control

Section 3 The board of directors

Pursuant to the regulations, the board of the directors shall ensure that the risk management and internal control in the institution is adequate in scale and performed in a systematic manner. The board is free to choose a practical and clear manner of doing this.

The principles for risk management and internal control ought to concisely state how the institution should weigh factors of importance to ensure proper operation, such as the allocation of roles between the board and the management, and other controlling functions, organisational factors, systemic factors, and how authority may be delegated.

The board must ensure that measures are implemented to rectify or reduce weaknesses that are uncovered, and that account is taken of risk management and internal control when decisions about material changes to the activities are taken.

To the extent that the institution utilises systems or "package solutions" from industry organisations, chain management or other external suppliers, the board must conduct its own genuine assessment of the adaptations necessary for its own institution.

The board is required to consider the need to establish an internal audit function in the institution (section 9). Where an institution has not found it necessary to establish an internal audit function, Finanstilsynet may in the course of its supervision ask the board to justify its decision not to do so.

Some institutions are subject to provisions regarding risk management and internal control in other legislation. Depending on the scope and complexity of the activities, the requirements relating to risk assessments pursuant to the other legislation may fulfil some of the requirements in these Regulations. If so, this should be evident from the board's principles for risk assessment and internal control, or other board decisions.

The division of work and independent control can be a challenge in small institutions. The board should consider whether there is a need for special control measures if it is difficult to ensure adequate independence and separation between executing and controlling functions.

The boards of institutions that carry out intermediary activities, provide advice or manage customer funds must ensure that the institution's risk management and internal control encompass safeguarding the customers' interests, including the institution's compliance with general conduct of business rules or customer protection provisions.

Section 4 The Chief Executive Officer

The CEO is responsible for establishing a sound internal control environment at all levels of the institution. The CEO should involve himself or herself in the entire risk management process. In smaller institutions the CEO will often participate in the actual process. In larger institutions the CEO will be responsible for initiating the process, involving himself or herself in the overall risk assessment, actively assessing whether the management and control system is appropriate, and ensuring that line managers actively participate.

The CEO will need to ensure the board of directors receives sufficient information about the main features of the institution's risk management and internal control system. The board's principles should state how extensive the reporting should be, and what should be reported when and how.

When it comes to professional estate agency, the CEO of the estate agent is exempted from the obligations pursuant to section 4. These obligations are assigned to the institution's professional manager, cf. the Regulations of 23 November 2007 no. 1318, section 2-8. No equivalent dispensation has been granted for external accounting firms that utilise the dispensation in the Regulations on External Accountants, section 1-3.

Section 5 Outsourcing

If an institution outsources, it must ensure, either itself or through a formalised cooperation with a firm other than the supplier, that the organisation possesses sufficient competence to

manage the outsourcing agreement. This might, for example, apply to settlement functions and IT systems.

Chapter 3 – Risk management and internal control

Section 6 Risk management

The purpose of section 6 is to contribute to a satisfactory risk assessment process and raise awareness of risk in the institution. The risk assessment is the basis for assessing the need for new and changed control measures and shall be carried out before changes are made in the organisation, new products are launched, or the institution expands into new markets. It is also important that risk assessments are carried out in the event of major internal or external unforeseen events.

What is risk management?

An institution's risk management is what the institution through its strategy, organisation, routines and proper operation does to achieve its goals, secure its own and its customers' assets, and ensure reliable reporting and compliance with laws and regulations. This entails more than what has traditionally been perceived as internal control.

There are a number of recognised frameworks for risk management. These constitute important theoretical bases but are not expected to be familiar to everyone. The most commonly used in Norway are the so-called COSO frameworks. COSO has issued a number of reports about and frameworks for risk management and internal control (www.coso.org).

As a consequence, risk management is not a clearly defined term, and its meaning can vary over time. One definition of (enterprise) risk management is provided in COSO 2:

"Enterprise risk management is a process, effected by the entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.." (*Enterprise Risk Management - Integrated Framework, published by COSO, September 2004*)

According to COSO 2, the key components of enterprise risk management are:

- Internal control environment - the internal control environment provides the starting point for the employees' attitude to risk. It also encompasses the risk management philosophy and appetite for risk, integrity and ethical values, and the environment in which they operate.
- Objective setting - objectives must exist before the management can identify potential events that could affect the achievement of them. Comprehensive risk management

- Event identification - internal and external events that affect an institution's goal achievement must be identified, and one differentiates between risks and opportunities. Opportunities are channelled back to the management's strategy and objectives setting processes.
- Risk assessment - risks are analysed and one assesses their likelihood and consequences as a basis for deciding how they should be managed. Both inherent and residual risk are assessed.
- Risk response - the management chooses forms of risk management - to avoid, accept, reduce or share risk - and develops an action plan to bring the risk into line with the institution's risk tolerance and appetite for risk.
- Control activities - guidelines and routines are established and implemented to ensure that the risk management is carried out in an effective manner.
- Information and communication - relevant information is identified, captured and communicated in a form, and at an early enough point in time, that enables the employees to address their responsibilities. Effective communication also takes place in the broader sense, both vertically and horizontally in the institution.
- Monitoring - the comprehensive risk management process is monitored and changed as needed. The monitoring is carried out through ongoing management activities, free standing evaluations and internal audits.

In small institutions the fact that there are few employees will constitute a risk in itself. The risk factors in particular include:

- Vulnerability through loss of competence
- Lack of competence to control specialists in own institution
- Dependency on individuals
- Problems achieving adequate division of work and independent control
- The CEO himself or herself participating in the activities
- The control system and management function not growing in line with the activities

How should risk management be implemented?

A comprehensive assessment of risks and associated control measures shall be carried out at least once a year. There is no requirement that this be done on specific dates or that the analyses of the individual areas must be carried out at the same time.

The special provision in the last paragraph of section 6 for institutions subject to the capital adequacy regulations should reduce the need to carry out processes that are almost the same pursuant to two different regulations. Banks that are authorised to provide investment services pursuant to the Securities Trading Act are however covered by section 6 with respect to these activities. In other words this part of the activities in the bank is not covered by the dispensation.

Section 7 Execution of the internal control

Internal control is a process, carried out by the board of directors, management and other staff, designed to provide a reasonable assurance regarding the achievement of company objectives. All managers should actively get involved in the assessment of whether the established risk management and internal control are being executed as expected within their own areas of responsibility. It is not enough just to build, for example, on the conclusions reached by compliance departments or the internal audit. The individual manager is free to choose his or her preferred working method. Reports from the internal audit unit and statements from the external auditor may be very useful in this work, but the cooperation should not be so extensive that it diminishes the independence of these functions.

Compliance and monitoring require managers at all levels of the organisation to implement and monitor the control measures adopted within their particular areas of responsibility. This is with a view to being able to intervene when controls fail or prove inadequate. The regulations impose no particular requirements as to how monitoring should be carried out, although keywords could be personal presence, making enquiries at meetings with colleagues, making spot checks and other special enquiries, scrutinising key figures and ratios, measuring deviations in IT systems and following up auditor's reports.

A systematic plan for monitoring must be in place and the plan must be reviewed regularly. The CEO must be prepared to brief the board, control committee, internal audit unit, external auditor or Finanstilsynet.

Small institutions do not need complicated systems to carry out satisfactory internal control. Nonetheless, some routines and controls must be in place. For example, these could include having:

- substitutes
- routines for countersignatures on received invoices and payments from client accounts
- written procedures for key areas
- check lists for executed actions in the procedures for key areas
- written control routines stating control points, documentation, responsibility for implementation, deadlines/frequency, etc, which state which controls should be carried out (e.g. which points in a matter should be checked), what should be checked (e.g. case files, journals, etc), who should carry out the checks and their frequency (e.g. at least three cases per month, all journals at the end of every month, etc)
- check lists for implemented control actions stating deviations, how deviations have been followed up, and measures/changes to routines to prevent repetition and that these have been reported up the line

Section 8 Documentation and reporting

The aim of this requirement is to ensure that sufficient information about the execution of risk management and internal control, including observed failures and weaknesses, is reported to the management and board of directors. A systematic programme for monitoring and reporting which includes managers at all levels of the organisation must be established in order to achieve this. Even if significant flaws and errors are rectified immediately, these

should be reported so that the personnel responsible for the control can assess whether the implemented measures are appropriate and whether the internal control is functioning as expected.

Important guidelines, routines and control measures must be available in writing. The fact that a risk assessment has been conducted must be documented.

The institution is also free to choose its preferred method of documentation. The documentation shall reflect work procedures, control routines and material risk assessments in a way that enables the board and CEO to decide whether the institution has assessed risks and control measures in each area of activities. It should state how the managers at the different levels have participated in the process.

Chapter 4 – Internal audit or independent confirmation

Section 9 Internal audit

The internal audit unit shall, independent of the management, carry out systematic risk assessments and inspections of the internal control to ensure it is working in an appropriate and satisfactory manner. The board of directors shall approve the allocation of resources to the internal audit unit and annual plans for their activities.

This function is an important aspect of the board's monitoring of risk management and internal control. It is especially relevant in large, complex organisations and also in smaller institutions with a high level of operational risk. Internal audits entail a strengthening of internal control, and might also be considered in institutions which are not required to have an internal audit.

Internal audit is an independent discipline, with its own standards, methods and ethical rules. The Institute of Internal Auditors Norway prepares standards within this field. The internal audit function may be entirely or partially outsourced. The institution's external auditor cannot be an internal auditor since this would contravene the Auditors Act, section 4-5, paragraph two.

The internal audit requirement is triggered as soon as the assets under management have exceeded the NOK 10 billion threshold for more than 12 months, unless the institution can prove that the assets under management will fall below this threshold within the next 6 months.

With regard to debt collection agencies, the portfolio of claims will not be deemed part of the assets under management pursuant to the regulations. Nonetheless, pursuant to section 3, paragraph one, no. 7 the board must decide whether or not the institution should have an internal audit function.

If the institution chooses to outsource the internal audit function, it must ensure that the requirements in section 5 are met.

Section 10 Independent confirmation

This provision applies to institutions that have not established an internal audit unit. The intention is to ensure that the board of directors receives an independent confirmation from a body that does not itself participate in the institution's internal control. The confirmation shall be issued by the institution's appointed auditor.

The auditor is not required to confirm the quality of the institution's risk assessments and documentation of routines and control measures, but that the institution actually has carried out such assessments and that the documentation exists. As far as the provision's last bullet point is concerned, the auditor shall check that the routines the institution has established for implementing the internal control process ensure there is agreement between the risk assessments carried out in the line and the reporting that takes place to the board of directors.

Section 11 Dispensations

The dispensation provision has been retained even though it is not used very often. Finanstilsynet stresses that a restrictive practice will be exercised. For example, it will not be possible to receive a dispensation just because an institution is small or was only recently established.

Section 12 Entry into force

The regulations enter into force on 1 January 2009. All the requirements stipulated in the regulations must be carried out at least once during 2009.

[Regulations on Risk Management and Internal Control](#) (pdf) (English translation of FOR-2008-09-22-1080 Forskrift om risikostyring og internkontroll)

Bjørn Skogstad Aamo

Anne Merethe Bellamy

Contact persons:

External Accountants:

Knut Lykke, ph: +47 22 93 98 40, e-mail: knut.lykke@finanstilsynet.no

Banks:

Morten Thorbjørnsen, ph: +47 22 93 98 92, e-mail: morten.thorbjornsen@finanstilsynet.no

Insurance:

Ellen Jakobsen, ph: +47 22 93 98 24, e-mail: ellen.jakobsen@finanstilsynet.no

Investment firms:

Leif Roar Johansen, ph. +47 22 93 98 10, e-mail: leif.roar.johansen@finanstilsynet.no

Real Estate Agents:

Eva Marie Hansen, ph: +47 22 93 97 75, e-mail: eva.marie.hansen@finanstilsynet.no

Debt Collection Agencies:

Linda Marie Vestheim-Vigeland, ph: +47 22 93 97 32,

e-mail: linda.marie.vestheim-vigeland@finanstilsynet.no

