FINANSTILSYNET
Norway
This translation is for information purposes only. Legal authenticity remains with the official Norwegian version as published in Norsk Lovtidend.

Regulations on Risk Management and Internal Control

Legal authority: Laid down by Kredittilsynet (now Finanstilsynet) on 22 September 2008 pursuant to the Act of 7 December 1956 no. 1 on Supervision of Credit Institutions, Insurance Companies and Securities Trading, etc (Financial Supervision Act), section 4, no. 2, Act of 10 June 1988 no. 40 on Financing Activity and Financial Institutions (Financial Institutions Act), section 2-9b, Act of 5 July 2002 no. 64 on Registration of Financial Instruments (Security Register Act), section 4-4, and the Act of 29 June 2007 no. 74 on Regulated Markets (Stock Exchange Act), section 11.

Chapter 1 Introductory provisions

Section 1 Scope

These regulations apply to:

1. Financial institutions
2. Regulated markets
3. Investment firms
4. Management companies for securities funds
5. Pensions institutions
6. Clearing houses
7. Securities registers
8. E-money institutions
9. Insurance companies
10. Estate agents
11. Debt collection agencies
12. External Accounting firms

Section 2 Proportionality

Institutions shall tailor their risk management and internal control according to the nature, scope and complexity of the institution's activities.

Chapter 2 Responsibility for risk management and internal control

Section 3 The Board of Directors

The board of directors shall ensure the institution has appropriate systems for risk management and internal control, including:

1. ensuring a clear division of responsibilities between the board and the day-to-day management is stipulated in the instructions for the board and the chief executive officer,

2. ensuring the institution has a clear organisational structure,
3. stipulating goals and strategies for the institution, and general guidelines for its activities. These shall state the risk profile the institution shall have, and which limits to risk apply where this is relevant,
4. stipulating principles for the institution's risk management and internal control as a whole and within each individual area of activities,
5. ensuring the risk management and internal control are established pursuant to legislation and regulations, decisions, and instructions issued by Finanstilsynet, and guidelines issued by the board to the management, including through the review of reports prepared pursuant to section 8 and chapter 4,
6. ensuring the risk management and internal control are implemented and monitored, including through the review of reports prepared pursuant to section 8 and chapter 4,
7. deciding whether or not the institution should have an internal audit function pursuant to section 9,
8. evaluating its work and competence in relation to the institution's risk management and internal control at least once a year.

Section 4 The Chief Executive Officer

The Chief Executive Officer (CEO) shall:

1. ensure proper risk management and internal control are established based on an assessment of the relevant risks pursuant to guidelines stipulated by the board of directors,
2. continuously monitor changes to the institution's risks and ensure that the institution's risks are properly addressed in accordance with the board's guidelines,
3. provide the board with relevant and timely information that is of importance to the institution's risk management and internal control, including information about new risks,
4. ensure the institution's risk management and internal control are documented,
5. ensure the risk management and internal control are properly implemented and monitored.

Section 5 Outsourcing

Institutions remain responsible for risk management and internal control even when parts of the activities are outsourced. There must be a written agreement ensuring this. The agreement must ensure the institution access and control rights with respect to the outsourced activities.

The agreement shall ensure Finantilsynet access to information about and supervision of the activities where Finanstilsynet finds this necessary.

The institution shall ensure that the organisation possesses sufficient competence to manage the outsourcing agreement.

Chapter 3 Risk management and internal control

Section 6 Risk management

The institution shall continuously assess the material risks associated with its activities. If products or routines of material importance are changed or established, a risk assessment must be conducted before the activities commence.

A review of material risks must be conducted for each area of activities at least once a year, based on defined goals and strategies. Each area of activities must be subject to a systematic assessment of whether the institution's risk management and internal control are adequate to properly manage the institution's identified risks.

Institutions that carry out risk management and assess risks and capital requirements pursuant to the Act of 10 June 1988 no. 40 on Financing Activity and Financial Institutions (Financial Institutions Act), section 2-9 to and including section 2-9d, and the Regulations of 14 December 2006 no. 1506 (Capital Requirements Regulations) are deemed to have met the requirements in paragraphs one and two.

Section 7 Execution of internal control

The managers of each material area of activities shall continuously assess the execution of internal control.

A summary assessment must be conducted at least once a year to check whether the internal control has been adequately executed.

Section 8 Documentation and reporting

The assessments pursuant to section 6, paragraph two, and section 7, paragraph two, shall be documented. A summary containing conclusions regarding the risk situation and whether there is a need for new measures shall be produced for each area of activities.

The CEO shall, at least once a year, prepare an overall assessment of the risk situation, which shall be presented to the board of directors for their consideration.

As stipulated in section 6, paragraph three, an institution must also supplement the assessment pursuant to the Financial Institutions Act and Capital Requirements Regulations with an overall assessment pursuant to section 7.

The documentation shall be kept for at least three years and be made available to Finanstilsynet.

Chapter 4 Internal audit or independent confirmation

Section 9 Internal audit

The institutions listed in section 1, paragraph one, nos. 2, 6, and 7 shall establish an internal audit function. The same applies to those institutions listed in section 1, paragraph one, which have had aggregate total assets for their own account and customers’ account for more than 12 months in excess of NOK 10 billion or which form part of a financial group with aggregate total assets in excess of this figure.

The internal audit manager shall be appointed and dismissed by the board of directors, shall be entitled to attend board meetings, and shall submit a report on risk management and internal control at least once a year. The board shall approve the internal audit's resources and plans on an annual basis.

The internal audit shall be conducted in accordance with recognised standards and shall continuously monitor the institution's activities.

Section 10 Independent confirmation

In institutions that do not establish an internal audit function, the board of directors shall ensure the institution's appointed auditor submits an annual confirmation to the board that:

- risk assessments pursuant to section 6, paragraph two, have been conducted
- assessments pursuant to section 7, paragraph two, have been conducted
- there is documentation pursuant to section 8
- the institution's routines ensure that the overall assessment of the risk situation submitted to the board, cf. section 8, paragraph two, is based on the risk assessments that have been conducted.

Chapter 5 Dispensations

Section 11 Dispensations

Finanstilsynet may in special circumstances grant dispensations from the provisions of these regulations.

Chapter 6 Entry into force

Section 12 Entry into force, etc

These regulations enter into force on 1 January 2009. From the same date the Regulations of 20 June 1997 no.1057 on Responsibility for Internal Control and on Documentation and Confirmation of Internal Control are repealed. The requirements in these regulations shall be complied with by no later than 31 December 2009.

* * *