Standard 4.1

Establishment and maintenance of internal control and risk management

Regulations and guidelines

RAHOITUSTARKASTUS
FINANSINSPEKTIONEN
FINANCIAL SUPERVISION

TABLE OF CONTENTS

tel. +358 10 831 51
fax +358 10 831 5328
firstname.lastname@rahoitustarkastus.fi
www.rahoitustarkastus.fi

For further details, please contact:
Market and Operational Risk, tel. +358 10 831 5207

tel. +358 10 831 51
fax +358 10 831 5328
firstname.lastname@rahoitustarkastus.fi
www.rahoitustarkastus.fi

For further details, please contact:
Market and Operational Risk, tel. +358 10 831 5207

1 APPLICATION

Issued on 27 May 2003
Valid from 1 July 2003

(1) This standard comprises the key principles of internal control and risk management as well as provisions on the establishment and maintenance of those functions. It lays down binding rules for the following supervised entities of the Financial Supervision Authority (FSA):

- credit institutions
- investment firms
- holding companies
- the central body of cooperative banks as referred to in the Cooperative Bank Act
- parent companies of financial and insurance conglomerates, whose primary business is financial.

Issued on 27 May 2003
Valid from 1 July 2003

(2) Internal control and risk management shall cover all operations of the supervised entity. In the establishment and maintenance of those functions, account must be taken of the supervised entity's organisational structure and of its scale and variety of business. Special attention must be paid, if the entity in question is a group or if it is engaged in business in several countries.

Issued on 27 May 2003
Valid from 1 July 2003

(3) If the supervised entity's organisation is small, if the level of risk-taking specified in the business plan is low, if the scale of the risk-exposed business is small and the business simple or otherwise transparent, or if the senior management itself actively participates in the detailed decision-making of the everyday business, compliance with detailed rules as applicable may be sufficient. Compliance with binding rules on internal control only as applicable requires a specific decision by the board of directors concerning the observance of alternative control practices. The supervised entity shall always ensure that internal control and risk management are adequate and proportionate to risks involved in the business.

tel. +358 10 831 51
fax +358 10 831 5328
firstname.lastname@rahoitustarkastus.fi
www.rahoitustarkastus.fi

For further details, please contact:
Market and Operational Risk, tel. +358 10 831 5207

Issued on 27 May 2003
Valid from 1 July 2003

(4) However, the FSA recommends that all corporations subject to its supervision establish and maintain internal control and risk management in accordance with this standard.

Issued on 27 May 2003
Valid from 1 July 2003

(5) Here the general expression supervised entity is used of all corporations within the scope of the standard.

tel. +358 10 831 51
fax +358 10 831 5328
firstname.lastname@rahoitustarkastus.fi
www.rahoitustarkastus.fi

For further details, please contact:
Market and Operational Risk, tel. +358 10 831 5207

2 OBJECTIVES

Issued on 27 May 2003
Valid from 1 July 2003

(1) The establishment and maintenance of internal control and risk management plays an important role in the management of the entities supervised by the FSA. The entities must be managed in a professional manner and according to sound and prudent business principles.

Issued on 27 May 2003
Valid from 1 July 2003

(2) The objective of the regulation on establishment and maintenance of internal control and risk management is to ensure that

- the internal control of a supervised entity and of corporations within its consolidation group is adequate with regard to the nature and scale of the business
- the supervised entity and corporations within its consolidation group do not take such risks in their operations that those risks could essentially jeopardise the supervised entity's capital adequacy or consolidated capital adequacy
- the supervised entity's internal control methods enable recognition, assessment and limiting of the risks involved in the business
- the supervised entity complies with standards for operational conduct in its customer relations.

tel. +358 10 831 51
fax +358 10 831 5328
firstname.lastname@rahoitustarkastus.fi
www.rahoitustarkastus.fi

For further details, please contact:
Market and Operational Risk, tel. +358 10 831 5207

3 INTERNATIONAL FRAMEWORK

Issued on 27 May 2003
Valid from 1 July 2003

(1) This standard is based on the recommendations of the Basel Committee on Banking Supervision. According to the Basel Committee, shortcomings in the establishment and maintenance of internal control are among the reasons for the banking problems in the 1990s. Principle 14 in the recommendation called Core Principles for Effective Banking Supervision, issued in September 1997, contains requirements concerning credit institutions' internal control:

- clear segregation of authority and responsibilities
- segregation of certain functions among various individuals, ie functions involving committing the bank, paying away its funds, and accounting for its assets and liabilities
- reconciliation of these processes
- safeguarding of assets
- appropriate internal audit and other compliance functions to test adherence to these controls and to applicable laws and regulations.

Issued on 27 May 2003
Valid from 1 July 2003

(2) In September 1998, the Basel Committee issued a recommendation called Framework for Internal Control Systems in Banking Organisations. In the recommendation it emphasises that credit institutions' board of directors and senior management as well as internal and external audit shall pay increased attention to establishment of internal control and to ongoing evaluation of its functioning. The principles of the recommendation form the main contents of section 6 of this standard.

Issued on 27 May 2003
Valid from 1 July 2003

(3) In February 2002, IOSCO issued the recommendation Objectives and Principles of Securities Regulation. According to principle 23 of the recommendation, market intermediaries are required to comply with standards for internal organisation and operational conduct that aim to protect the interests of customers and ensure proper risk management. The corporation's board of directors and senior management shall bear the responsibility for the internal organisation and for the functioning and control of the operational conduct.

tel. +358 10 831 51
fax +358 10 831 5328
firstname.lastname@rahoitustarkastus.fi
www.rahoitustarkastus.fi

For further details, please contact:
Market and Operational Risk, tel. +358 10 831 5207

4 LEGAL BASIS

Issued on 27 May 2003
Valid from 1 July 2003

(1) The FSA's binding rules on establishment and maintenance of internal control and risk management are based on section 68, subsection 3 of the Credit Institutions Act (1607/1993) and section 29, subsection 3 of the Act on Investment Firms (579/1996). These rules also itemise the requirements of establishing and maintaining internal control and risk management applicable to parent companies of conglomerates as referred to in section 13 of the Act on the Supervision of Financial and Insurance Conglomerates (44/2002).

Issued on 27 May 2003
Valid from 1 July 2003

(2) In preparing these rules and regulations, account has been taken of Directive 2000/12/EC of the European Parliament and of the Council relating to the taking up and pursuit of the business of credit institutions (32000L0012, OJ L 126, 26.5.2000, p. 1) and of Council Directive 93/22/EEC on investment services in the securities field (31993L0022, OJ L 141, 11.6.1993, p. 27).

tel. +358 10 831 51
fax +358 10 831 5328
firstname.lastname@rahoitustarkastus.fi
www.rahoitustarkastus.fi

For further details, please contact:
Market and Operational Risk, tel. +358 10 831 5207

5 KEY PRINCIPLES OF INTERNAL CONTROL

5.1 Definition of internal control

Binding
Issued on 27 May 2003
Valid from 1 July 2003

(1) The supervised entity must be managed in a professional manner and according to sound and prudent business principles. This requires establishment and maintenance of an effective and reliable internal control.

Binding
Issued on 27 May 2003
Valid from 1 July 2003

(2) Internal control comprises economic and other control. In corporations, the board of directors, the senior management and the rest of the personnel execute the internal control. Internal control is by definition the sector of management and operations that seeks to ensure

- accomplishment of stated goals and objectives
- economic and effective use of resources
- adequate management of risks inherent in operations
- reliability and correctness of financial and other management information
- compliance with external rules and regulations and internal procedures as well as standards for operational conduct in customer relations
- adequate safeguarding of operations, data and assets of supervised entities and customers
- adequately and appropriately organised manually operated and IT-based systems to support the operations pursued.

Binding
Issued on 27 May 2003
Valid from 1 July 2003

(3) Risk management forms an integral part of internal control. Risk management refers to the recognition, assessment/measurement, limiting and monitoring of risks involved in or essentially related to the business. Risk management is used to diminish the probability of contingent losses or the

tel. +358 10 831 51
fax +358 10 831 5328
firstname.lastname@rahoitustarkastus.fi
www.rahoitustarkastus.fi

For further details, please contact:
Market and Operational Risk, tel. +358 10 831 5207

threat that such losses pose to the supervised entity's reputation.

5.2 Board of directors' responsibility for establishment and maintenance of internal control

Binding
Issued on 27 May 2003
Valid from 1 July 2003

(4) The supervised entity's board of directors is responsible for the establishment and maintenance of adequate and functioning internal controls. At least once a year it shall approve the requisite level of risk-taking based on the entity's risk-bearing capacity and reassess them as part of the business plan. The board of directors also approves significant operating principles for the risk management, at the same time bearing ultimate responsibility for ensuring that the internal control and risk management are comprehensive and functioning.

Binding
Issued on 27 May 2003
Valid from 1 July 2003

(5) A parent company's board of directors must ascertain the compliance with principles of internal control in all corporations controlled by the company. In particular, the parent company's board of directors must ascertain that no corporation controlled by the company takes such risks in its operations that those risks could essentially jeopardise the supervised entity's capital adequacy or consolidated capital adequacy. The responsibility of the parent company's board of directors does not diminish the responsibility of a subsidiary's board of directors concerning the establishment and maintenance of internal control and risk management in its own corporation.

Binding
Issued on 27 May 2003
Valid from 1 July 2003

(6) In its decisions about the organisational structure, the supervised entity's board of directors shall ensure that the structure provides the required conditions for effective internal controls. This requires that authority and responsibilities as well as reporting relationships are clearly assigned in the organisation and duties appropriately differentiated. Reliable reporting requires that it is executed independently of the business. The monitoring of compliance with external rules and regulations and internal procedures must be reliably and independently established and maintained. In addition, the supervised entity must have an internal audit function that effectively and variedly monitors the functioning of internal controls and also reports its key findings directly to the board of directors.

Binding
Issued on 27 May 2003
Valid from 1 July 2003

(7) The supervised entity's board of directors shall regularly control the corporation's performance and the risks involved in its operations. In order to limit material risks, procedures shall be laid down in writing and limits set for measurable risks.

tel. +358 10 831 51
fax +358 10 831 5328
firstname.lastname@rahoitustarkastus.fi
www.rahoitustarkastus.fi

For further details, please contact:
Market and Operational Risk, tel. +358 10 831 5207

5.3 Independent risk management assessment

Binding
Issued on 27 May 2003
Valid from 1 July 2003

(8) A risk-management assessment function independent of the risk-taking business and risk management must be established for monitoring the risk-taking. It shall maintain, develop and prepare risk management principles for approval by the board of directors and lay down procedures for risk assessment and measurement. It must continuously ensure that each risk remains within approved limits and that the procedures for measuring each risk are appropriate. The procedures must also comprise assessment of effects of exceptional situations (stress tests). In addition, the risk management assessment must ensure that the total effect of all material business risks on the performance of the supervised entity and its consolidation group and on the regulatory capital be reported to the board of directors and senior management.

Justifications
Issued on 27 May 2003
Valid from 1 July 2003

(9) If the supervised entity's organisation is small, if the level of risk-taking specified in the business plan is low and if the scale of the risk-exposed business is small and the business simple or otherwise transparent, eg when the senior management itself actively participates in the detailed decision-making of the everyday business, compliance as applicable with the requirement of organising an independent risk-management assessment function may be sufficient. A guiding principle in this respect can be how the board of directors can ascertain the functioning of risk management and internal controls.

5.4 Outsourcing of operations and use of agent

Binding
Issued on 27 May 2003
Valid from 1 July 2003

(10) Transfer of business activities to an agent or other outsourcing of operations (outsourcing) does not release the supervised entity from its liabilities and obligations.

Binding
Issued on 27 May 2003
Valid from 1 July 2003

(11) If a supervised entity plans to outsource some of its operations, it must be convinced that the outsourcing does not impair its risk management, other internal controls or actual business.

Binding
Issued on 27 May 2003
Valid from 1 July 2003

(12) The outsourcing may neither impair the access to information granted to the supervised entity's management nor the possibilities to manage and monitor the outsourced operations. It may not prevent the access to information and right of disclosing such information to others which is required in supervision executed by authorities, in risk management and in other internal controls. The supervised entity shall also apply the key principles of internal control and risk management to outsourced operations.

tel. +358 10 831 51
fax +358 10 831 5328
firstname.lastname@rahoitustarkastus.fi
www.rahoitustarkastus.fi

For further details, please contact:
Market and Operational Risk, tel. +358 10 831 5207

Binding
Issued on 27 May 2003
Valid from 1 July 2003

(13) The selected provider of outsourced services must be economically viable and have sufficient expertise, and it must know and commit itself to comply with binding rules of the supervised entity on outsourced operations and sound banking and securities trading practices.

Binding
Issued on 27 May 2003
Valid from 1 July 2003

(14) A written plan must be prepared for the outsourcing projects and the supervised entity's board of directors must approve the significant projects of the plan. The plan must show how the business to be outsourced is included in the supervised entity's risk management and other internal controls, eg how reliable reporting is ensured, how the monitoring of compliance with external rules and regulations and internal procedures has been arranged and how the internal audit works in the case of outsourced operations.

Binding
Issued on 27 May 2003
Valid from 1 July 2003

(15) A written contract shall be prepared on the outsourcing. The supervised entity shall have the right to cancel the outsourcing contract, and it shall prepare a back-up plan in case that the service provider performs poorly or fails absolutely to provide the service. The contract shall contain a clause stating that the operations may not be further outsourced to a third party without the supervised entity's consent.

tel. +358 10 831 51
fax +358 10 831 5328
firstname.lastname@rahoitustarkastus.fi
www.rahoitustarkastus.fi

For further details, please contact:
Market and Operational Risk, tel. +358 10 831 5207

6 MAJOR ELEMENTS OF INTERNAL CONTROL

6.1 Management policy and control culture

Binding
Issued on 27 May 2003
Valid from 1 July 2003

(1) As a minimum requirement, the board of directors must

- bear the primary responsibility for internal control and its functioning
- have at their disposal broad professional skills and experience of recognising risks in the operating environment
- approve the supervised entity's business plan and as part of that the level of risk-taking according to risk-bearing capacity, as well as once a year make sure that the business plan is up to date
- approve the principles of risk management and ensure that they contain a procedure for the start-up of new business activities and for introducing new products
- ascertain the functioning of risk management and of its compliance with legislation and authority regulations/standards
- approve the operating principles of internal audit and the audit plan
- decide on the organisational structure
- decide on the reporting and on other internal control procedures, through which it monitors the operations, operating performance and risks involved in the operations.

Binding
Issued on 27 May 2003
Valid from 1 July 2003

(2) As a minimum requirement, the senior management must

- ensure that the practical measures of internal control are taken
- set quantitative and qualitative objectives for each business area, in accordance with the business plan approved by the board of directors, and monitor their accomplishment
- develop and maintain procedures that are based on the risk

tel. +358 10 831 51
fax +358 10 831 5328
firstname.lastname@rahoitustarkastus.fi
www.rahoitustarkastus.fi

For further details, please contact:
Market and Operational Risk, tel. +358 10 831 5207

management principles approved by the board and through which risks are recognised, assessed/measured, monitored and limited; these procedures must be documented
- maintain an organisational structure in which authority, responsibilities and reporting relationships are clearly and comprehensively assigned in writing
- organise an independent risk-management assessment function.

Binding
Issued on 27 May 2003
Valid from 1 July 2003

(3) In their operations, the board of directors and senior management must

- promote the formation of a corporate culture that accepts internal control as a normal and necessary part of corporate operations
- ensure that the employees are skilled, that they are suitable for and committed to their job, and that they understand the importance of internal control and their own contribution to it.

6.2 Risk management

Binding
Issued on 27 May 2003
Valid from 1 July 2003

(4) Risk management must be used to ensure that material risks, which could adversely affect the achievement of the supervised entity's business objectives, are recognised, assessed/measured and monitored as part of the daily management of business operations. Risk management shall cover all material business risks: both internal and external, both measurable and non-measurable, both risks controllable by the supervised entity and risks that cannot be controlled, ie risks that the supervised entity only can protect itself against. For measurable risks the supervised entity shall establish measurement methods and for the management of non-measurable risks it shall develop appropriate assessment methods. Risk management procedures must be continuously maintained and developed to ensure that all new and material but so far unrecognised risks also become embraced by the risk management.

6.3 Daily control and segregation of duties

Binding
Issued on 27 May 2003
Valid from 1 July 2003

(5) Internal control shall be part of the supervised entity's daily activities. An effective internal control requires that an appropriate control structure be set up in the supervised entity with control activities defined at every business level. The daily control activities include management reviews, appropriate measurements applicable to each business area and unit, physical controls, checking for compliance with agreed exposure limits and operating principles/instructions and follow-up on non-compliance, a system of approvals and authorisations, and different verification and reconciliation measures.

tel. +358 10 831 51
fax +358 10 831 5328
firstname.lastname@rahoitustarkastus.fi
www.rahoitustarkastus.fi

For further details, please contact:
Market and Operational Risk, tel. +358 10 831 5207

Binding
Issued on 27 May 2003
Valid from 1 July 2003

(6) An effective internal control requires that there is appropriate segregation of duties among various individuals and measures taken to ensure that nobody in the supervised entity's personnel, as a representative of the entity, monitors its own business or the business of related entities or otherwise influences and/or participates in decision-making concerning such business. Possible dangerous combinations of duties in an individual's job description or conflicts of interest shall be recognised and, if possible, eliminated.

6.4 Reporting and communication

Binding
Issued on 27 May 2003
Valid from 1 July 2003

(7) An effective internal control requires that the supervised entity, as a basis for its decision-making, is provided with adequate and comprehensive information, such as the entity's internal financial and operational data and data on compliance with external regulations and internal procedures as well as external data on the business environment and market developments. The information shall be reliable, material, timely, and provided in the agreed format.

Binding
Issued on 27 May 2003
Valid from 1 July 2003

(8) An effective internal control also requires that the supervised entity has reliable information systems in place that cover all significant activities. The systems shall be secure, monitored independently and supported by adequate contingency arrangements.

Binding
Issued on 27 May 2003
Valid from 1 July 2003

(9) The flow of necessary information shall be free upward, downward and laterally through the organisation to ensure an effective internal control. The organisational structure shall facilitate the upward flow of information so that the board of directors and senior management get the information they need (on operating performance, risks, deviations, observations of effective control etc.). The downward flow of information shall ensure that the personnel has knowledge of the policies and procedures, approved by the board of directors, that are necessary for executing its duties and that it also is provided with other information needed for executing its duties.

6.5 Monitoring and audit of the functioning of internal control

Binding
Issued on 27 May 2003
Valid from 1 July 2003

(10) The effectiveness of internal control shall be monitored and developed on an ongoing basis. Material risks shall be monitored as part of the daily business operations. In addition, the effectiveness of internal control shall be evaluated periodically through an internal audit independent of business operations and risk management. At agreed intervals, the internal control

shall also be audited as part of a greater whole.

Binding
Issued on 27 May 2003
Valid from 1 July 2003

(11) The functioning of internal control shall be audited effectively and variedly. The internal audit shall be independent of business operations and carried out by appropriately trained and competent staff. Internal audit shall report on the functioning of internal control directly to the board of directors and senior management.

Binding
Issued on 27 May 2003
Valid from 1 July 2003

(12) Internal control deficiencies and development issues identified in business operations and by internal audit or other control personnel shall be documented and reported to the appropriate management level and addressed promptly. Serious matters shall always be reported all the way to senior management and the board of directors. Summarising reports shall also be prepared on identified issues and corrective measures so that the supervised entity's board of directors and senior management can obtain an overall picture of the functioning of internal control.

6.6 Prudential systems

Binding
Issued on 27 May 2003
Valid from 1 July 2003

(13) The supervised entity shall have adequate and appropriately designed manual and IT systems consistent with the nature and complexity of its activities. The systems shall form the basis for the operational activities.

Binding
Issued on 27 May 2003
Valid from 1 July 2003

(14) The activities, assets and information of the supervised entity shall be arranged in an adequately prudential manner and the data processing and communication shall also be prudent.

tel. +358 10 831 51
fax +358 10 831 5328
firstname.lastname@rahoitustarkastus.fi
www.rahoitustarkastus.fi

For further details, please contact:
Market and Operational Risk, tel. +358 10 831 5207

7 REPORTING TO THE FSA

Justifications
Issued on 27 May 2003
Valid from 1 July 2003

(1) The establishment and maintenance of internal control and risk management does not involve a separate, regular obligation of reporting to the FSA.

Binding
Issued on 27 May 2003
Valid from 1 July 2003

(2) However, in its financial statements the supervised entity shall regularly provide information on the establishment and maintenance of internal control and risk management. The contents of the information to be provided in the financial statements are detailed in the section *Accounting and financial statements.*

tel. +358 10 831 51
fax +358 10 831 5328
firstname.lastname@rahoitustarkastus.fi
www.rahoitustarkastus.fi

For further details, please contact:
Market and Operational Risk, tel. +358 10 831 5207

8 DEFINITIONS

Issued on 27 May 2003
Valid from 1 July 2003

(1) Here the **board of directors** refers to a body that sets the general operational framework for the corporation and bears the ultimate responsibility for the organisation's activities, for its decisions on business plans and objectives and for the functioning of its internal control.

Issued on 27 May 2003
Valid from 1 July 2003

(2) **Senior management** refers to a body that is responsible for the daily operative management of the supervised entity and the execution of the decisions made by the board of directors.

Issued on 27 May 2003
Valid from 1 July 2003

(3) A **function independent of the business operations** neither participates in the business management nor carry responsibility for the business profitability. In the organisational structure a function independent of the business operations does not even have an administrative reporting relationship to the business or the management of it.

tel. +358 10 831 51
fax +358 10 831 5328
firstname.lastname@rahoitustarkastus.fi
www.rahoitustarkastus.fi

For further details, please contact:
Market and Operational Risk, tel. +358 10 831 5207

9 FURTHER INFORMATION

Please find the necessary contact information in the list of Persons responsible for standards provided on the FSA website. For further information, please contact:

- Market and Operational Risk, tel. +358 10 831 5207

10 OBSOLETE GUIDELINES AND REGULATIONS

Issued on 27 May 2003
Valid from 1 July 2003

(1) This standard renders the following regulations and guidelines obsolete:

- Regulation on risk management and other aspects of internal control in credit institutions (108.1)
- Guideline on risk management and internal control principles as well as internal audit function of credit institutions (108.2) with the exception of provisions on data processing and internal audit (details on those will be provided in standards to be completed at a later date)
- Guideline on risk management and other aspects of internal control in stock exchange (202.13) with the exception of provisions on data processing and internal audit (details on those will be provided in standards to be completed at a later date)
- Regulation on risk management and other aspects of internal control in investment firms (203.27)
- Guideline on risk management and internal control principles as well as internal audit function of investment firms (203.28) with the exception of provisions on data processing and internal audit (details on those will be provided in standards to be completed at a later date)
- Guideline on risk management and other aspects of internal control in central securities depository (206.4) with the exception of provisions on data processing and internal audit (details on those will be provided in standards to be completed at a later date).

tel. +358 10 831 51
fax +358 10 831 5328
firstname.lastname@rahoitustarkastus.fi
www.rahoitustarkastus.fi

For further details, please contact:
Market and Operational Risk, tel. +358 10 831 5207