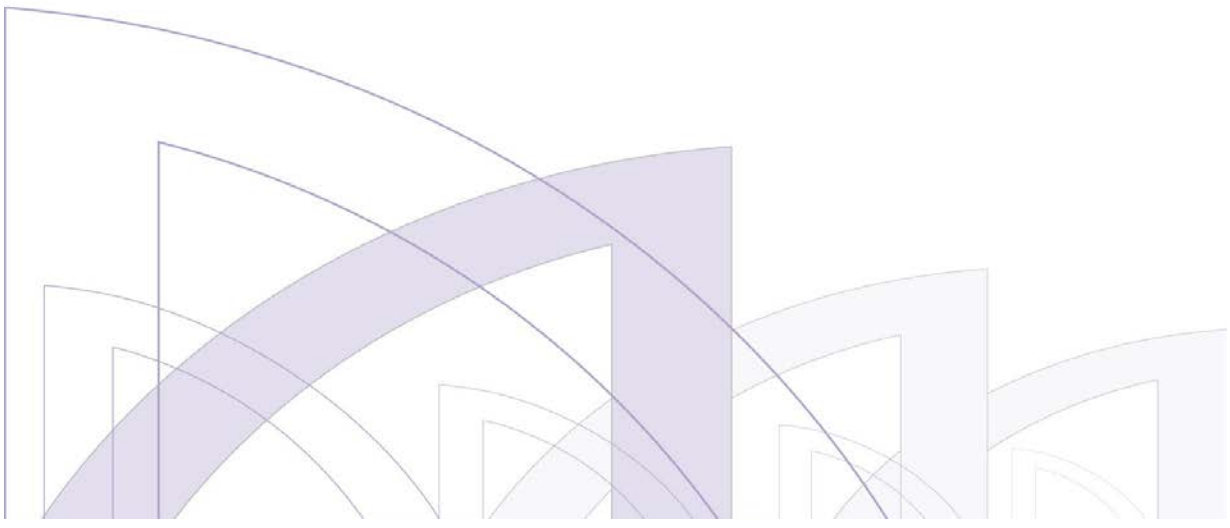
AUTORITÉ
DES MARCHÉS FINANCIERS

# Risk management and internal control systems

## Reference Framework

## Implementation Guide
## for small caps and midcaps



**CONTENTS**

## I- OBJECTIVES, PRINCIPLES AND CONTENT

### Introduction

This is an updated, revised version of the 2007 Reference Framework Implementation Guide adapted for small and medium capitalisation companies (small caps and midcaps), published by the AMF in 2008.

This update was made necessary by changes to the legislation and regulations since 2007, particularly the Act of 3 July 2008 and the Order of 8 December 2008 which transposed into French law the European directives imposing new requirements on listed companies in terms of internal control and risk management, and outlining the role of the audit committee in this respect.

In September 2009 the AMF therefore tasked a working group with adapting the 2007 Reference Framework and its version for small caps and midcaps published in 2008, in order to include a section on risk management.

### Objectives of this Guide

This Guide aims to achieve the following goals:
- help company chairmen, executive management and relevant managers in their task of devising risk management and internal control systems: principles, roles and responsibilities,
- facilitate the drafting of the “Chairman’s Report” on the internal control and risk management procedures implemented by the company.

### Principles

Like the Reference Framework, this Guide is not imposed on small caps and midcaps.

The purpose of the Guide and its questionnaires is to help companies identify the main risk management and internal control points that need to be implemented and/or improved. However, each company is responsible for its own organisational structure and its own risk management and internal control and system, which should be developed within the framework of sound governance and should comply with the specific regulations in force in certain sectors (banking, insurance) or on certain financial marketplaces. **This Guide must therefore be adapted to the company**. Depending on the company’s size, the complexity of its activity and processes, and its degree of internationalisation, it may draw greater inspiration from the application guide featuring in the Reference Framework published by the AMF in 2010.

### Content

This tool adapted to small caps and midcaps has two parts:
- general risk management and internal control principles, and
- two questionnaires, one on internal accounting and financial control, and the other on risk management.

## II - GENERAL RISK MANAGEMENT AND INTERNAL CONTROL PRINCIPLES

Risk-taking is inherent to any enterprise. There can be no growth or value creation in a company without risk-taking. However, if risks are not properly managed and controlled, they can affect the company's ability to attain its objectives. Risk management and internal control systems play a key role in directing and guiding the company's various activities by preventing and managing risks on an ongoing basis.

### 1. General risk management principles

A) Definition

Risk management is the business of every stakeholder in a company. It should be comprehensive and cover all of the company's activities, processes and assets.

Risk management is a dynamic system, defined and implemented under the company's responsibility.

Risk management encompasses a set of resources, behaviours, procedures and actions adapted to the characteristics of each company and enabling managers to keep risks at an acceptable level for the company.

Risk is the possibility of an event occurring that could affect the company's personnel, assets, environment, objectives or reputation.

B) Goals of risk management

Risk management is a lever for managing the company that helps:

**a) Create and preserve the company's value, assets and reputation:**
Risk management serves to identify and analyse the main potential threats and opportunities for the company. The aim is to anticipate risks instead of submitting to them passively, and thus preserve the company's value, assets and reputation.

**b) Secure decision-making and the company's processes to attain its objectives:**
Risk management aims to identify the main events and situations that could have a significant impact on the attainment of the company's objectives. Controlling these risks facilitates the attainment of these objectives.
Risk management is an integral part of the company's decision-making and operating processes. It is an oversight and decision-making aid.
Risk management gives managers an objective and comprehensive outlook on the company's potential threats and opportunities. It enables managers to take measured and informed risks and provides a basis for their decisions regarding the attribution of human and financial resources.

**c) Encourage consistency between the company's actions and its values:**
Many risks reflect a lack of consistency between the company's values and day-to-day decision-making and actions. These risks mainly threaten the company's credibility.

**d) Ensure that the company's employees have a shared vision of the main risks** and raise awareness of the risks inherent in their activity.

C) Components of the risk management system

It is up to each company to create a risk management system that is appropriate to its specific circumstances.

The risk management system includes:

**1) An organisational framework**

**2) A three-stage risk management process in the company's internal and external context:**

- Risk identification: this stage identifies and centralises the main risks threatening the attainment of the company's objectives. A risk is a threat or a missed opportunity. It involves an event, one or more sources and one or more consequences. Risk identification is part of an ongoing approach.
- Risk analysis: in this stage, the potential financial, personal, legal and reputational consequences of the main risks are examined and the likelihood of their occurrence is assessed. This is an ongoing approach.

- Risk management procedures: in this stage, the most appropriate action plan or plans for the company are chosen. Several measures can be considered to maintain acceptable risk levels: reducing, transferring, eliminating or accepting a risk. The choice is made by weighing the opportunities against the cost of risk management measures, with due consideration of their potential effects on the occurrence and/or consequences of the risk.

**3) Ongoing oversight of the risk management system:**
The risk management system is subject to supervision and periodic reviews. Monitoring the system contributes to ongoing improvements.
The objective is to identify and analyse the main risks and to learn the lessons of risks that occurred.

A risk management questionnaire can be found in Chapter III.1 "*Risk management questionnaire*".

**2. Coordination of risk management with internal control**

Risk management and internal control systems complement each other in controlling the company's activities:

- The risk management system aims to identify and analyse the company's main risks. Risks that exceed the acceptable levels set by the company are dealt with and, as the case may be, are subject to plans of action. These plans may include the implementation of controls, a transfer of the financial consequences (through insurance or an equivalent mechanism) or a change to the organisational structure. The controls to be implemented are part of the internal control system. In this way the internal control system contributes to the management of the risks incurred in the company's activities;
- The internal control system relies on the risk management system to identify the main risks that need to be controlled;
- In addition, the risk management system itself needs to include controls that are part of the internal control system and aimed at ensuring the proper functioning of the risk management system.

The coordination and balance between the two systems depend on the control environment, which constitutes their shared foundation, and, more specifically: the company's own risk and control culture, management style and ethical values.

**3. General principles of internal control**

A) Definition

Internal control is a system that the company defines and implements under its own responsibility. It aims to ensure:

- compliance with laws and regulations,
- implementation of the instructions and directions given by executive management or the executive board,
- proper functioning of the company's internal processes, especially those relating to the protection of its assets,
- reliability of financial information,

More generally, it contributes to control over its activities, the efficiency of its operations and efficient use of its resources.

By helping prevent and control the risk of non-attainment of the company's stated objectives, the internal control system plays a central role in the company's conduct and oversight measures.

However, internal control cannot provide an absolute guarantee that the company's objectives will be achieved.

B) Components of internal control

The internal control system is devised by the executive management or the executive board. Appropriate communication measures are carried out to ensure that it is implemented by the company's personnel.

Internal control will be more relevant if it is built on rules of conduct and integrity upheld by the governance bodies and communicated to all employees. It must not be a purely formal system where serious breaches in business ethics could occur on the sidelines.
The internal control system is adapted to the circumstances of each company and should comprise:
- **an organisational structure** in which responsibilities are clearly defined, adequate resources and competencies are provided, and appropriate information systems, operating procedures or methods, tools and practices are implemented;
- **in-house dissemination of relevant and reliable information** allowing each member of personnel to discharge their responsibilities;

- **a risk management system** designed to identify, analyse and manage the main risks threatening attainment of the company's objectives. The risk management system is described in Section II.1. General risk management principles.
- **control activities** proportionate to the implications of each individual process and designed to reduce the risks that could affect the company's ability to achieve its objectives;
- **On-going monitoring** of the internal control system together with a regular review of its operation. This monitoring could be based on the company's internal auditing procedures if they exist, and may lead to changes in the internal control system.

### 4. Scope of risk management and internal control

It is up to each company to implement risk management and internal control systems that are appropriate for its situation.
In a group, the parent company shall ensure that its subsidiaries have risk management and internal control systems. These systems should be adapted to the subsidiaries' specific characteristics and to the relations between them and the parent company.
When a parent company has a substantial equity interest and significant influence over an affiliate, it should assess the possibility of acquainting itself with and examining its affiliate's measures with regard to risk management and internal control.

### 5. Risk management and internal control players

Risk management and internal control are the business of entire company, from the governing bodies to employees.

#### a) Executive management or the executive board

Executive management is responsible for designing and implementing internal control and risk management systems that are appropriate to the size of the company, its business and its organisational structure. This task includes:

- carrying out ongoing monitoring of internal control and risk management systems with the aim of ensuring their integrity and improving them by adapting to changes in the organisation and environment of the company,
- initiating any remedial measures that become necessary to correct problems identified and ensuring that these measures are carried out,
- ensuring that appropriate information is reported in a timely manner to the board of directors or the supervisory board.

#### b) Board of directors or supervisory board

The board is informed of the key characteristics of the internal control and risk management systems chosen and implemented by executive management.

The board may use its general powers as needed to have any audits or verifications that it deems timely carried out or to take any other action that it deems appropriate in this regard.

#### c) Audit committee

The audit committee's role and duties are dealt with in detail in the document entitled "Audit Committees: Working Group Report", published by the AMF in 2010 and available on the AMF website (www.amf-france.org).

For small-caps and midcaps[1] two options exist: either set up an audit committee or obtain the exemption provided for in article 823-20 4 of the Commercial Code.

#### d) Risk manager

When the position exists, the risk manager, or the person in charge of risk management, is responsible for deploying and implementing the overall risk management process as defined by executive management. For this purpose, the risk manager establishes a structured system that is both permanent and adaptable for the purpose of identifying, analysing and managing the main risks. The risk manager runs the risk management system and provides methodological support to the company's operational and functional divisions.

[1] Companies listed in Euronext compartments B and C. These criteria are likely to be amended in the future revision of the Prospectus Directive.

**e) Internal audit**

When there is one, the internal audit department is responsible, within the scope of its duties, for assessing the operation of the internal control system, for monitoring it regularly, and for making recommendations to improve it.

**f) Employees**

Management in each entity ensures that the company's risk management policy is applied. It is responsible for applying this policy and ensures that exposure to these risks complies with the executive management's risk management policy.

**g) Statutory auditors' role**

Statutory auditors' legal duties do not include participation in risk management and internal control systems. They learn about the systems, rely on internal audit work, when internal audit exists, to obtain a better understanding and formulate an opinion about the appropriateness of this work in full independence.

They certify the financial statements and, as part of their task, they may identify material risks and major internal control weaknesses that could have a significant impact on financial and accounting disclosures.

They present their observations about the chairman's report and about internal control procedures relating to the way accounting and financial reporting is drawn up and managed, and they certify that other information required by law has been produced.

**6. Limitations of risk management and internal control**

No matter how well-conceived and rigorously applied risk management and internal control systems are, they cannot provide an absolute guarantee that the company's objectives will be reached.
The probability of reaching these goals depends on more than just the company's will. Every system and process has its limitations. These limitations stem from many factors, such as uncertainties in the outside world, the use of sound judgment or problems that may arise from technical and human failures or from ordinary errors.
Risk management choices are made by weighing the opportunities against the cost of risk management measures, with due consideration of their potential effects on the occurrence and/or consequences of the risk in order to avoid taking needlessly expensive actions.

## III. QUESTIONNAIRES ON GENERAL PRINCIPLES

The two questionnaires below are tools intended to facilitate the design and implementation of internal control and risk management systems, as well as reporting and disclosure with regard to these systems. Their main purpose is to allow companies to identify control points that need to be improved, in particular as regards reporting internal control and risk management procedures to shareholders and to the market, and to facilitate the drawing-up of the Chairman's Report required by law.

These questionnaires should be adapted to the specific features of each company. To help managers in this adaptation, the company should use the risk management and internal control application guide published by the AMF in 2010 and available on the AMF website (www.amf-france.org).

The application guide addresses the following principles and key points:

I – Risks relating to accounting and financial organisation and reporting

II – Control objectives

III – Oversight of the accounting and financial organisational structure
- Principles and key analysis points
- Role of the executive management
- Role of the Board of Directors or the Supervisory Board

IV – Processes contributing to the preparation of the accounting and financial information to be published
- Principles and key analysis points

### 1. Risk management questionnaire

**Note that if the board of directors has set up an audit committee, then the role attributed to the board in the following questions could just as easily be played by the audit committee.**

**Organisational framework for risk management**

- *Has the company established risk management objectives?*
- *Have risk management responsibilities been defined and notified to the people concerned?*
- *Is the person in charge of risk management adequately qualified to perform his duties with regard to operational staff and managers?*
- *Have policies and procedures for managing the main risks been defined, approved by executive management and implemented in the company?*
- *Does the company have a "common language" for dealing with risk (uniform definitions, criteria for risk identification, analysis and monitoring, etc.)?*
- *Has the company identified its legal and regulatory obligations with regard to risk disclosure?*
- *Does the company provide internal information to the people concerned:*
  - *about risk factors?*
  - *about risk management systems?*
  - *about current actions and the people in charge of them?*

**Risk identification**

- *Is there a process for identifying risks that threaten attainment of the company's objectives? Has an appropriate structure been set up for this purpose?*
- *Have systems been established to identify the main risks affecting the process of preparing the financial statements?*

**Risk analysis**

- *Does the company analyse the potential impact of the main risks identified (quantified or not, financial or non-financial impact) and the estimated degree of risk control?*
- *Has the company's past experience with risks or that of similar entities been taken into consideration?*
- *Are several functions in the company involved in analysing the potential consequences and probabilities?*
- *Does executive management share risk analysis with the persons concerned?*
- *Does the risk analysis consider internal and external changes affecting the company?*

**Managing the main risks**

- *Do major risks give rise to specific actions? Has the responsibility for such actions been defined? Where appropriate, is implementation of these actions monitored?*
- *Does the company have a crisis management plan?*

**Oversight and review of risk management**

- *Does the management receive information about the key characteristics of actions taken to manage the company's main risks (type of actions taken or hedges established, insurance, exclusions and the amount of coverage, etc.)?*
- *Have specific resources been allocated to implementation and supervision of the risk management procedures?*
- *Is there a mechanism that makes it possible, when necessary, to adapt risk management procedures to changes in risks and the external environment, as well as to changes in the company's objectives and business activities?*
- *Is there a system for identifying and correcting the main weaknesses in the risk management system used by the company?*
- *Has the board of directors or, where appropriate, the supervisory board, been informed of the main thrust of risk management policies? Is the Board updated periodically on the main risks identified and the key characteristics of the risk management system, including the resources allocated and ongoing improvements?*

**Financial and accounting disclosure**

- *Has a schedule been established that summarises the group's periodic market disclosure requirements for accounting and financial information? Does this schedule specify:*
  - *the nature and deadline for each periodic disclosure requirement,*
  - *the people responsible for preparing the disclosures.*
- *Are there people responsible and procedures in place for identifying and meeting market disclosure requirements?*
- *Has a procedure been established for checking information prior to disclosure?*

**2. Internal accounting and financial control questionnaire**

**Role of governance bodies[2]**
**Note that if the board of directors has set up an audit committee, then the role attributed to the board in the following questions could just as easily be played by the audit committee.**

- *Have the accounting principles that have a material impact on the presentation of the company's financial statements been formally validated by executive management, reviewed by the statutory auditors and presented to the board of directors or the supervisory board?*
- *With regard to preparation of the financial statements, has the executive management explained and substantiated the main accounting options and choices made to the board and have they been reviewed by the statutory auditors?*
- *Has a process been established for validating planned changes in accounting principles with due consideration of the economic aspects of the transactions? Does this process provide for consultation with the statutory auditors and notification of the board?*
- *Does the board receive the statutory auditors' assurance that they had be given access to all the information required for the performance of their duties, especially in the case of consolidated companies?*
- *Does the Board receive the statutory auditors' assurance that they have made enough progress on their work at the cut-off date to be able to present all their material observations?*
- *Are the earnings components, balance-sheet presentation, financial position presentation and the notes to the financial statements explained to the board each time the published financial statements are prepared?*
- *Has the Board been informed of the existence of a management control function which produces data that are periodically reconciled with the published financial information?*

[2] In this questionnaire, "governance bodies" means the board of directors or the supervisory board.

- *Has management periodically informed the board of cash position monitoring, especially at times of major tension?*
- *Are any restrictions on cash flows within the group stemming from special clauses or the percentage of equity held clearly specified to the board?*

**Accounting and financial reporting structure**

- *Does the accounting and financial reporting function have access to the information needed to prepare the financial statements from the entities covered by the statements?*
- *Does the group have an accounting principles manual that specifies the accounting treatment for the most significant transactions?*
- *If financial statements are published in accordance with several sets of accounting standards at the individual company or consolidated level, have procedures been established for explaining the main restatements?*
- *Are there accounting procedures manuals and instructions describing the breakdown of responsibilities for execution and control of accounting tasks, as well timetables for execution? As part of the preparation of the consolidated financial statements, are there dissemination procedures to ensure that the manuals and instructions are followed by subsidiaries?*
- *Have the people responsible for preparing the financial statements and financial information, and the various persons who participate in the preparation of the financial statements been identified?*
- *Has a process been established to identify the resources required for the smooth operation of the accounting function? Does it give due consideration to foreseeable developments?*

**Information system**

- *Have information procedures and systems been developed to meet requirements with regard to the reliability, availability and relevance of accounting and financial information? Have the roles and responsibilities of the players been defined?*
- *Are the information systems used for accounting and financial information adapted as the company's needs change? Has request and incident management been implemented?*
- *Have data back-up systems been established? Are they tested periodically?*
- *Have continuity of service measures been established in conjunction with users' needs? Are they tested periodically?*
- *Are record retention requirements with respect to information, data and computer processing used directly or indirectly to prepare accounting records and financial statements met?*

**Control activities**

- *Are regular audits and spot checks conducted to ensure compliance in practice with the manual of accounting principles and the manual of accounting procedures?*
- *Have procedures been established to identify and resolve new and unforeseen accounting problems in the accounting principles manual and/or the accounting procedures manual?*
- *Do internal control activities for accounting and financial reporting include procedures to protect assets (risk of negligence, errors and internal or external fraud)?*
- *Does the internal control system for accounting and financial reporting include specific audits of accounting aspects that are identified as critical, such as recognition of assets, recognition of earnings, accruals and inventory valuation?*
- *Are the procedures for preparing the group's financial statements applied in every consolidated entity? If there are exceptions, are there adequate procedures for dealing with them?*