

**POSITION PAPER**

**Towards Common Principles for Internal Control & Risk Management Systems at  
Listed Companies in Europe**

26 January 2010

## Table of Contents

<b>1.</b>	<b>DEFINITIONS – FOREWORD – MAIN CONCLUSIONS .....</b>	<b>4</b>
1.1	Definitions .....	4
1.2	Foreword .....	6
1.3	Main Conclusions.....	6
<b>2.</b>	<b>THE EUROPEAN APPROACH .....</b>	<b>9</b>
2.1	The Directives .....	9
2.2	A developed and a simplified model .....	10
<b>3.</b>	<b>SCOPE, OBJECTIVES AND LIMITATIONS OF ICRM SYSTEMS .....</b>	<b>11</b>
3.1	Overview of concepts.....	11
3.2	Contributing to company performance .....	11
3.3	Part of the management tools and processes .....	12
3.4	Two different types of risks.....	13
3.5	ICRM Systems are dynamic .....	14
3.6	Proportionate assessments of selected areas.....	14
3.7	Limitations of ICRM Systems .....	15
3.8	The terms “assurance” and “reasonable assurance” .....	15
<b>4.</b>	<b>THE EUROPEAN LEGAL PROVISIONS ON THE AUDIT COMMITTEE .....</b>	<b>16</b>
4.1	Exemptions under the 8 <sup>th</sup> Directive.....	16
4.2	The Audit Committee’s oversight function .....	17
4.3	The Audit Committee should receive information.....	17
<b>5.</b>	<b>RESPONSIBILITIES AND INTERACTION OF PARTIES INVOLVED IN ICRM .....</b>	<b>19</b>
5.1	Overview of responsibilities depending on parties involved .....	19
5.2	Senior Management: a steering and ongoing monitoring function .....	19
5.3	Management .....	21
5.4	Audit Committee: an overall monitoring for oversight purposes.....	21
5.5	Board .....	22
5.6	Internal Audit Department.....	23
5.7	Statutory Auditor: overall understanding .....	24

## **Appendices**

Appendix I: ICRM Systems - Summary of tasks- Developed model

Appendix II: ICRM Systems - Summary of tasks- Simplified model

Appendix III: ICRM Systems - Key interactions - Developed model

Appendix IV: ICRM Systems - Key interactions - Simplified model

Appendix V: ICRM Systems - Provisions of the European Directives

## 1. DEFINITIONS – FOREWORD – MAIN CONCLUSIONS

### 1.1 DEFINITIONS

*Note: Definitions herein are for the purpose of this position paper only.*

<b>Audit Committee</b>	audit committee of the company as under Article 41, paragraphs 1 (indent 1), 2, 3 and 4, of the 8 <sup>th</sup> Directive, or body performing equivalent functions as under Article 41, paragraph 5 of the 8 <sup>th</sup> Directive, as the case may be <sup>1</sup> .
<b>Board</b>	in a two-tier system, the supervisory body of the company and in a one-tier system, the administrative body or the board of directors of the company.
<b>Directives</b>	refers to the following European Directives: <ul style="list-style-type: none"><li>- Fourth Council Directive 78/660/EC of 25 July 1978 on the annual accounts of certain types of companies, or the “4<sup>th</sup> Directive”;</li><li>- Seventh Council Directive 83/349/EC of 13 June 1983 on consolidated accounts, or the “7<sup>th</sup> Directive”;</li><li>- Directive 2006/43/EC of the European Parliament and of the Council of 17 May 2006 on statutory audits of annual accounts and consolidated accounts, amending Council Directives 78/660/EEC and 83/349/EEC and repealing Council Directive 84/253/EEC, or the “8<sup>th</sup> Directive”.</li></ul>
<b>EU</b>	European Union.
<b>ICRM</b>	Internal Control and Risk Management.
<b>ICRM Systems</b>	ICRM systems and processes.
<b>Management</b>	persons other than Senior Management, who carry out management functions within the company.
<b>Senior Management</b>	senior management, executive management or the management board of the company, as the case may be. <sup>2</sup>

---

<sup>1</sup> In Italy, the Audit Committee’s function as described in this position paper is performed by an external “board of auditors” (*collegio sindacale*) and/or, as only recommended by the corporate governance code, by an “internal control committee” within the “board of directors”. For this reason, in Italy, the recommendations made in this position paper as regards the Audit Committee may not be applicable or refer either to the “board of auditors” or to the “internal control committee” or to both of them, as the case may be.

**Statutory Auditor** statutory auditor or audit firm, as the case may be.

---

<sup>2</sup> In Italy, the notion of Senior Management as meant in this position paper could include members of the board of directors.

## 1.2 FOREWORD

With the 4<sup>th</sup>, 7<sup>th</sup> and 8<sup>th</sup> Directives, companies listed in Europe now have a common legal framework for certain aspects of ICRM.<sup>3</sup> This position paper draws on the experience of companies to propose some common general principles on ICRM, based on a shared understanding of the objectives, scope and limitations of ICRM Systems.<sup>4</sup> This initiative follows the Statement of the European Corporate Governance Forum, which, in June 2006, pointed to the need to develop relevant principles on ICRM as experience was gained.<sup>5</sup>

The principles proposed in this position paper are adapted to the European context and are intended to offer an appropriate balance between the benefits that arise from adequate ICRM Systems and the possible burdens these systems could entail for companies. The principles relate to the roles of the players involved in ICRM Systems and their interactions, including with the company's Statutory Auditor.<sup>6</sup> These principles are derived from the Directives and are built around the issue of "monitoring the effectiveness of ICRM Systems"<sup>7</sup>. Far from giving a comprehensive view on ICRM, the principles developed in this paper should help listed companies fulfil the aim of the Directives and to enhance ICRM Systems and their oversight. The clarification of definitions and roles should contribute to improving the effectiveness of those systems, notably through better interaction and a common understanding shared by internal and external players. This position paper should be read against possible national legislation and corporate governance codes that may be applicable.

The European Issuers working group which co-operated on this position paper, involved representatives with various relevant backgrounds: Board, Senior Management, Management, internal control, internal audit, financial and legal. Delegates included representatives from both listed companies and national business organisations representing the same. The aim was to put forward a succinct, coherent and representative company's perspective rather than the views of individual functions or sector interests.

## 1.3 MAIN CONCLUSIONS

### 1.3.1. *EU approach*

The EU approach is rightly differing from the approach adopted in the United States with the Sarbanes Oxley law. Unlike the case in the US, public information in the EU on financial reporting related systems should remain a descriptive summary, while respecting the ongoing information requirements with regard to those incidents likely to have a significant effect on the price of the financial instruments offered to the

---

<sup>3</sup> Section 2 & 3.

<sup>4</sup> Section 2.

<sup>5</sup> See the statement of the European Corporate Governance Forum on [http://ec.europa.eu/internal\\_market/company/docs/ecgforum/statement\\_internal\\_control\\_en.pdf](http://ec.europa.eu/internal_market/company/docs/ecgforum/statement_internal_control_en.pdf).

<sup>6</sup> Section 5.

<sup>7</sup> Art. 41,2,b of the 8<sup>th</sup> Directive.

public. The role of the Statutory Auditor regarding internal control should consist in designing an appropriate statutory audit approach as opposed to expressing an opinion on its effectiveness.

### **1.3.2. Diversity of companies**

The aim of ICRM Systems is to ensure compliance with legal and regulatory requirements and the proper functioning of and compliance with internal processes, thereby facilitating internal information, oversight and decision making. ICRM Systems should be adapted to the company's organisation and proportionate to its characteristics, such as size, environment, activities, operations, needs and resources. As a consequence, the parties involved in ICRM, their roles and interactions could also vary. This position paper therefore describes two models: a developed model and a simplified model, which can be combined. Where the company has no audit committee as under Article 41, paragraphs 1 (indent 1), 2, 3 and 4, of the 8<sup>th</sup> Directive or has no internal audit department, their functions come respectively under the remit of the Board or of the departments practising internal control activities under the responsibility of the Senior Management. Under the European framework, Senior Management can fully continue to exercise its judgement to decide when and how to implement its ICRM Systems, based on costs and benefits and on the company's characteristics<sup>8</sup>.

### **1.3.3. The difference between the monitoring function of the Audit Committee and the monitoring function of the Senior Management**

#### *(a) Audit Committee*

The overall monitoring function of the Audit Committee is an oversight function that is different from the functions carried out by the Senior Management. The Board and the Audit Committee, which meet periodically, have a supervisory role, based on the information summaries they receive. They cannot carry out the ongoing monitoring of ICRM Systems or controls themselves, as such is the responsibility of Senior Management and Management. For the Audit Committee, the concept of monitoring the effectiveness of ICRM Systems denotes the high-level dynamic oversight process by which, based on the information summaries received, the Audit Committee is able to propose overall directions for Board consideration when deemed appropriate (setting directions is normally within the remit of the Senior Management). The overall monitoring function does not mean monitoring the management itself or the systems themselves. The aim is to best adapt those systems, the ongoing monitoring of controls by Senior Management and the control activities to the company's business and its continuously evolving external and internal environment. This includes overseeing the allocation of responsibilities within the company to avoid major loopholes in that area.

Whether this oversight function applies to ICRM Systems as a whole or only to ICRM Systems related to financial reporting, is a matter for Board consideration, corporate governance codes or legislation, as the case may be.

---

<sup>8</sup> See 2.2.

*(b) Senior Management*

Senior Management takes on the prime responsibility role in respect of ICRM. It has a central and unique role in that it performs both the steering function as well as the ongoing monitoring of the ICRM Systems.

The ongoing monitoring of controls by Senior Management consists in assessing whether ICRM Systems are suitable, operate as intended and are adjusted, over time, to changed conditions. The assessment of selected areas made in this context under the responsibility of Senior Management should be determined according to the company's priorities and may be effected over a number of years. The assessments should also be proportionate to the entity's characteristics and to the implications of the risks identified. A periodic assessment of the effectiveness of the whole of the ICRM Systems, or even of the control activities alone, cannot be envisaged; this would be overly cumbersome and costly and of limited relevance, if not misleading, in the ever-changing context in which the entity and its systems operate.

Senior Management should report to the Audit Committee on the main features of ICRM Systems and on key matters, including on the main incidents identified and the corrective actions decided or implemented.

*(c) Limitations*

No matter how well planned, designed and operated, the effectiveness of ICRM Systems can never be guaranteed, certified or be the subject of any assurance. Given the ever-changing environment and the dynamic nature and limitations of the ICRM Systems (e.g. for cost/benefit considerations), unavoidably some risks or weaknesses might not be prevented, detected or corrected. ICRM Systems can only contribute to reducing, but not eliminating risks and weaknesses altogether. ICRM Systems should not be mistaken for management decisions or for information systems or processes set up by companies to prepare and make decisions.

## 2. THE EUROPEAN APPROACH

### 2.1 THE DIRECTIVES

For listed companies, the Directives offer common European legal provisions concerning ICRM Systems:

#### *4<sup>th</sup> and 7<sup>th</sup> Directives*

The amended 4<sup>th</sup> and 7<sup>th</sup> Directives require listed companies in Europe to publish an annual corporate governance statement (as a specific section of the annual report or separately) containing a description of the main features of the company's ICRM Systems in relation to the financial reporting process or process for preparing consolidated accounts. Statutory Auditors are only required to express an opinion on the consistency of that description with the annual accounts for the same financial year.

#### *8th Directive*

Where public-interest entities are required to set up an Audit Committee, Article 41, paragraph 2 of the 8<sup>th</sup> Directive provides that

*"... the audit committee shall, inter alia: ...*

*(b) monitor the effectiveness of the company's internal control, internal audit where applicable, and risk management systems".*

In that case, Article 41, paragraph 4 provides that the Statutory Auditor

*"shall report to the audit committee on key matters arising from the statutory audit, and in particular on material weaknesses in internal control in relation to the financial reporting process".*

All relevant European provisions can be found in Appendix V.

EuropeanIssuers strongly supports the descriptive approach adopted in the EU. The oversight role of the Board of Directors and the role of the Statutory Auditor are adequate. The latter's role consists in checking the consistency of the corporate governance statement and, where applicable, alerting the Audit Committee to material weaknesses in internal control in relation to the financial reporting process identified in an audit of financial statements. It is a role of designing an appropriate statutory audit approach, based inter alia on the understanding of the audited company's internal control relevant to the statutory audit. The role does not imply that the Statutory Auditor has to express an opinion on effectiveness.

The European approach thus avoids the pitfalls of the US legislation. The application of Section 404 of the Sarbanes Oxley Act, due in particular to the costs it involves and its complexity, has led many companies, including European companies, to de-list in the United States. It is of prime importance that a US-type approach is not introduced to avoid such de-listing movement in the EU.

## 2.2 A DEVELOPED AND A SIMPLIFIED MODEL

Listed companies are diverse in the nature, size, location and complexity of their businesses and, accordingly, in the nature of the risks they run and in the relevant laws and regulations to which they are subject. This diversity is reflected in the needs, organisation and resources (governance, management structure, staff, etc.) of listed companies and determines the nature, scope, and sophistication of their processes, systems and controls.

The Directives offer the necessary flexibility by providing exemptions from having an Audit Committee. The Directives also recognise that companies do not always (need to) have an internal audit department. Moreover the Directives do not require companies to implement specific ICRM Systems, rightly leaving the appropriateness of such to the reasonable judgement of the Senior Management. In other words, the Directives do not set out precise systems.

This position paper proposes two models<sup>9</sup>:

- a “developed model” including both an Audit Committee and an internal audit department;
- a “simplified model” without audit committee as under Article 41, paragraphs 1 (indent 1), 2, 3 and 4, of the 8<sup>th</sup> Directive and without an internal audit department, which shows how their absence impacts on the interaction between the persons and bodies involved in the company’s ICRM Systems. The functions attributed to the aforesaid audit committee are then carried out by the Board, while those that may be attributed to an internal audit department are organised at Management level.

Depending on a company’s characteristics and on the relevant requirements, a company may want to choose either one of these models or a combination of the two.

---

<sup>9</sup> See Appendices III and IV.

### **3. SCOPE, OBJECTIVES AND LIMITATIONS OF ICRM SYSTEMS**

#### **3.1 OVERVIEW OF CONCEPTS**

The roles and interactions within a company as described in this position paper can only be fully understood, if the basic concepts including the concepts of “ICRM” and “ICRM Systems” are clear.

ICRM Systems are based on a control environment and include:

- risk management systems, which can be described as “systems for determining and analysing the main identifiable risks in relation to the company’s activities, for ensuring that controls and procedures exist and for informing management and those in charge of governance<sup>10</sup> about those risks, thus enabling them to make informed management decisions”;
- information processes enabling all relevant players within the company to exercise their control responsibilities;
- control activities (policies and procedures, which should be proportionate to the implications of the processes concerned, can be found everywhere in the organisation, at every organisational level and in every function, be they controls focusing on prevention or detection, manual or computerised controls, or controls by virtue of the reporting structure);
- ongoing monitoring of controls and risk management systems by management in general<sup>11</sup>.

In this section, we elaborate on:

- the scope of ICRM Systems as part of the management tools and processes which contribute to company performance,
- their objectives: facilitating internal information, oversight and decision making in a dynamic manner and
- their inherent limitations

#### **3.2 CONTRIBUTING TO COMPANY PERFORMANCE**

For a company to optimize its performance and appropriately report on its financial position, it is important that its internal systems are suited for different objectives:

- identifying the risks it may face,

---

<sup>10</sup> The expression “those in charge of governance” designates the Audit Committee and/or the Board.

<sup>11</sup> See 5.2 and 5.3.

- making relevant data available for decision making and for external information,
- controlling compliance with laws, regulations and management guidelines,
- monitoring the company's performance,
- adapting its strategy and systems as appropriate.

ICRM Systems are part of a broader set of systems set up to reach those objectives, which include information, decision making, control<sup>12</sup> and performance monitoring systems and processes.

Systems, processes and controls should not be implemented or performed at any price, but only if they have an added value , taking into account the specific situation of the company.

The nature, scope and sophistication of processes and systems will vary depending on the characteristics of the company: e.g. nature, size, location, complexity of the business, nature of the risks to which the entity is subject and relevant laws and regulations. Costs and benefits of those processes and systems will also be an important factor. As a consequence, companies cannot have sophisticated or costly systems in every domain and at all times, as this would adversely affect their performance and competitiveness. Acting with discernment, exercising sound judgement and reacting quickly are key to the company's performance and competitiveness and to the proper functioning of the company's processes and systems.

### **3.3 PART OF THE MANAGEMENT TOOLS AND PROCESSES**

ICRM Systems are only one, although necessary, component of sound company management. They complement but do not replace:

- strategic vision and managerial skills: e.g. the ability to summarize, decide, organise and manage according to circumstances;
- a company's management activities: e.g. the gathering of information, organisation, directional guidelines, instructions, individual decisions;
- the control of a company's management activities and decisions in respect of which other functions or tools exist, e.g. hierarchical oversight and appraisals, management control, cost accounting.

ICRM Systems should not be mistaken for management decisions or for information systems or processes set up by companies to prepare and make decisions and follow their impacts, assess their relevance, assess the company's situation and performance and report thereon.

---

<sup>12</sup> Control of the company's management.

As far as possible, the persons involved in ICRM Systems should not assess their own work and should be able to take an independent view on the company's systems, functions, activities and operations. For instance, to avoid the independence of the internal audit department, if any, being undermined, they should not become involved in the company's decision making or have conflicting interests.

### 3.4 TWO DIFFERENT TYPES OF RISKS

ICRM Systems aim at determining the main identifiable risks for companies and providing information for oversight and decision making purposes. As risks are often inherent in business opportunities, ICRM Systems should not be based on the premise that all risks could or should be avoided or reduced.

In this respect, a distinction should be drawn between:

- (a) *risks associated with business activities in general;*
- (b) *risks that may materially affect the process of preparation and presentation of the financial statements.*

For both types of the above risks, some significant risks might not be identified or properly assessed because of the limitations inherent to ICRM Systems<sup>13</sup>.

#### (a) *Risks associated with business activities*

Risks associated with business activities in general can be balanced against opportunities and therefore are not always mitigated or avoided. Indeed entrepreneurship consists in making judgements and decisions on business opportunities and associated risks (often under time pressure). It implies risk-taking. In a competitive economy, there is no performance or profit without risk and no company without risk. By identifying risks and supplying relevant information on them, ICRM Systems enable appropriate judgement to be exercised by management in general when balancing risks and opportunities.

#### (b) *Risks that may affect the financial statements*

Financial statements should give a true and fair view of the assets, liabilities, financial position and profit or loss of the issuer, to the best knowledge of the persons responsible with the issuer. Hence, it is important to identify risks which may materially affect the financial

---

<sup>13</sup> See 3.7.

statements so that those risks can be reduced to an acceptably low level and material misstatements can be prevented, detected and corrected on a timely basis. Those risks could not possibly be balanced against opportunities.

The Statutory Auditor is concerned only with risks that may affect the preparation and presentation of the financial statements and not with risks associated with business activities as a whole<sup>14</sup>.

### **3.5 ICRM SYSTEMS ARE DYNAMIC**

ICRM Systems encompass a range of activities. They aim at ensuring that laws and regulations, management guidelines and instructions are complied with, that internal processes are functioning correctly and financial information is reliable.

ICRM Systems are necessarily dynamic, as they need to be adapted by the company to its own situation and evolution, especially with regard to the preparation of financial statements.

Given the ever-changing environment, and the need to implement corrective actions where required, ICRM Systems need to be updated, adapted and adjusted regularly.

### **3.6 PROPORTIONATE ASSESSMENTS OF SELECTED AREAS**

It is appropriate for a company to use its best endeavours to monitor and regularly adapt ICRM Systems. Assessments of selected areas, made in this context, should be proportionate, determined according to priorities and may be effected over a number of years. In contrast, making a periodic (e.g. annual) assessment of the effectiveness of the entirety of systems, or even of the control activities alone, cannot be envisaged. Such would be overly cumbersome and costly, compared to its benefits, and would be of very limited relevance due to the dynamic nature of the company and its systems.

---

<sup>14</sup> See ISA (international standard on auditing) 200 Objective and General Principles Governing an Audit of Financial Statements” paragraph 22.

### 3.7 LIMITATIONS OF ICRM SYSTEMS

The likelihood that the ICRM's objectives will be achieved does not depend solely on the will of the company or its management in general. ICRM Systems are affected by limitations inherent to every internal system and process, including by the exercise of judgement and by deficiencies occurring because of technical failure or human error, as well as by external uncertainties. This is especially so given the ever-changing environment.

It is unavoidable that some risks or weaknesses might not be prevented or detected. No matter how well planned, designed and operated, ICRM Systems might still have their own deficiencies or weaknesses and at any rate, they can only reduce but not altogether eliminate risks and weaknesses. Moreover, whether an act complies with laws and regulations (an internal control objective) is eventually a matter for determination by a court of law.

In addition, companies must look at the cost/benefit ratio and cannot afford to develop systems and processes at any price, even if this entails assuming a certain degree of risk.

### 3.8 THE TERMS "ASSURANCE" AND "REASONABLE ASSURANCE"

The terms "assurance" or "reasonable assurance"<sup>15</sup> are not used in this position paper and should be avoided with regard to ICRM Systems as they are misleading, for three main reasons:

- They do not properly reflect the existence of inherent limitations and the fact that some risks are balanced against opportunities<sup>16</sup>; they may wrongly be understood as possibly guaranteeing the effectiveness of ICRM Systems or the achievement of company business objectives;
- They may suggest that an assessment of the whole of the systems is carried out, rather than partial assessments on selected areas according to the priorities defined;
- They may suggest that assessments are periodic, whereas those partial assessments are carried out when and where needed, generally over a number of years.

---

<sup>15</sup> Under the ISAs, *"the objective of a reasonable assurance engagement is a reduction in assurance engagement risk to an acceptably low level in the circumstances of the engagement as the basis for a positive form of expression of the practitioner's conclusion."*

<sup>16</sup> See 3.4.

## 4. THE EUROPEAN LEGAL PROVISIONS ON THE AUDIT COMMITTEE

This section focuses on the role of the Audit Committee in ICRM as it can be derived from the Directives.<sup>17</sup>

### 4.1 EXEMPTIONS UNDER THE 8<sup>TH</sup> DIRECTIVE

The 8<sup>th</sup> Directive offers the flexibility necessary to take into account the characteristics of the entity and its legal environment. It is appropriate to provide for exemptions from having an audit committee as under Article 41, paragraphs 1 (indent 1), 2, 3 and 4 as well as from having an internal audit department.

Article 41 of the 8<sup>th</sup> Directive requires public-interest entities to have an Audit Committee, whose functions are performed without prejudice to the responsibility of the Board or other members who are appointed by the general meeting of shareholders of the audited entity.

However, in certain circumstances set out in Article 41, paragraphs 1 (indent 2) and 6 of the 8<sup>th</sup> Directive respectively, Member States may provide for exemptions:

- They may exempt public-interest entities from the obligation to have an Audit Committee. In particular, for “small and medium-sized enterprises” which meet the criteria of the Prospectus Directive<sup>18</sup>, they may permit the functions assigned to the Audit Committee to be performed by the Board as a whole;

---

<sup>17</sup> The Italian regime is as follows: the corporate governance system adopted by 96% of Italian listed companies provides for two mandatory bodies: i) a “board of directors” and ii) an external “board of auditors” (*collegio sindacale*). i) The “board of directors”, appointed by the general shareholders’ meeting, considers the adequacy of the company’s organisational structure and of the company’s administrative and accounting system. The “board of directors” has full responsibility for its own activity. ii) The “board of auditors” (*collegio sindacale*) is also appointed by the general shareholders’ meeting and is different from the Statutory Auditor which performs the control on financial statements. The “board of auditors” is independent from the “board of directors” and it is composed by independent auditors. Among other tasks, it monitors the adequacy of the company’s internal control system. While performing their activity, the members of the “board of auditors” are competent to carry any inspections and checks, individually as well as collectively. As regards this aspect of the role of the “board of auditors”, the Italian regime goes beyond what is required by the 8<sup>th</sup> Directive and beyond the recommendations made in this position paper.

At the same time, listed companies that voluntarily comply with the Italian “Corporate Governance Code” may appoint an “internal control committee” which is therefore an optional body under the remit of the “board of directors”. The “internal control committee” only advises the “board of directors” on its evaluations and decisions relating to the internal control system: thus, the “board of directors” retains full responsibility for the activity of the “internal control committee”, given that this body is not mandatory by Law.

<sup>18</sup> According to Article 2(1)(f) of Directive 2003/71/EC, “Companies which, according to their last annual and consolidated accounts, meet at least two of the following criteria: an average number of employees during the financial year of less than 250, a total balance sheet not exceeding EUR 43 000 000 and an annual net turnover not exceeding EUR 50 000 000”.

- They may allow or decide that the provisions of Article 41, paragraphs 1 to 4 relating to the audit committee shall not apply to any public-interest entity that has a body performing equivalent functions to an audit committee, established and functioning according to provisions in place in the Member State in which the entity to be audited is registered.

We should also note that Article 41, paragraph 2 (b) of the 8<sup>th</sup> Directive does not require public-interest entities to have an internal audit department.

#### **4.2 THE AUDIT COMMITTEE'S OVERSIGHT FUNCTION**

The Audit Committee does preparatory work for the Board and acts under the Board's collective responsibility. The Audit Committee must therefore not be considered as a separate company body. The Board determines the sphere of activity of the Audit Committee. Whether or not the Audit Committee monitors ICRM Systems that do not relate to financial reporting is a matter for Board consideration, corporate governance codes or national law, as the case may be.

Monitoring the effectiveness of a company's ICRM Systems is only one of the functions of the Audit Committee under the 8<sup>th</sup> Directive. Its other functions include monitoring the financial reporting process, monitoring the statutory audit of the annual and consolidated accounts, reviewing and monitoring the independence of the Statutory Auditor and making a recommendation for its appointment<sup>19</sup>. When these functions are carried out by a body performing equivalent functions, for instance the Board, it will by definition carry out wider functions, possibly including the determination of the course of the company's business. The responsibility of the Audit Committee to monitor ICRM Systems cannot prevail over these other functions within the company. In addition, the Audit Committee's members, given the nature of their role, do not and cannot carry out these functions on a permanent basis.

Consequently, the Audit Committee should concentrate on overseeing the functions performed in this field by the company's Senior Management.

#### **4.3 THE AUDIT COMMITTEE SHOULD RECEIVE INFORMATION**

Only the Statutory Auditor is explicitly mentioned as a source of information for the Audit Committee by the 8<sup>th</sup> Directive. This source is only used in exceptional circumstances. Indeed: *"the Statutory Auditor shall report to the Audit Committee on key matters arising from the statutory*

---

<sup>19</sup> Article 41 paragraphs 2 to 4.

*audit, in particular on material weaknesses in internal control in relation to the financial reporting process.*"<sup>20</sup> However, in general the Audit Committee obtains information summaries from the Senior Management and may obtain information summaries from the internal audit department, if any, either directly or indirectly via Senior Management<sup>21</sup>.

---

<sup>20</sup> Article 41 paragraph 4 of the 8<sup>th</sup> Directive.

<sup>21</sup> See 5.2 and 5.6.

## **5. RESPONSIBILITIES AND INTERACTION OF PARTIES INVOLVED IN ICRM**

### **5.1 OVERVIEW OF RESPONSIBILITIES DEPENDING ON PARTIES INVOLVED**

The parties involved in ICRM vary from one company to another, depending in particular on the company's characteristics and legal environment<sup>22</sup>. In this section, we describe the responsibilities of the various parties involved in ICRM as well as the key interactions between those parties, including, where relevant, the company's Statutory Auditor.

The following responsibilities may be identified:

- organisation of the systems;
- day-to-day running of the systems/day-to-day administration of controls;
- internal control activities;
- ongoing monitoring of controls;
- overall monitoring for internal oversight purposes;
- internal information.

The responsibilities of the different parties involved in ICRM are schematised in Appendices I "Developed model" and II "Simplified model".

The key interactions of the different parties involved in ICRM are schematised in Appendices III "Developed model" and IV "Simplified model".

### **5.2 SENIOR MANAGEMENT: A STEERING AND ONGOING MONITORING FUNCTION**

Senior Management takes on the prime responsibility role in respect of ICRM. The role of Senior Management is central to ICRM Systems and therefore of the utmost importance. Its role encompasses a steering, an ongoing monitoring and an information function. Senior Management receives support of the internal audit department, if any, which reports the results of its activities to Senior Management.

---

<sup>22</sup> See 2.2.

### **5.2.1 Steering function**

Senior Management is in charge of steering the design, implementation and maintenance of ICRM Systems that are most suitable for the company's specificities and activities. This includes the setting of overall and specific directions, the determination of priorities and taking necessary corrective actions.

### **5.2.2 Ongoing monitoring function**

The ongoing monitoring by Senior Management consists in considering regularly whether the ICRM Systems are suitable for the company's business and its characteristics, whether they operate as intended over time and whether they are adjusted as appropriate due to changed conditions.

More specifically, it can involve:

- assessing risk management processes on a timely basis according to defined priorities;
- assessing internal controls on a timely basis and on areas selected according to defined priorities (in the internal audit work plan, where applicable);
- considering the analysis of the main identified incidents and the conclusions of the performed controls;
- ensuring, based on the information received, that necessary corrective actions are undertaken and implemented.

The ongoing monitoring may be permanent, i.e. through controls built into the normal recurring activities or periodic through separate, regular reviews of selected areas, including reviews carried out by the internal audit department, if any.

#### *Information function*

Senior Management ensures that appropriate information is delivered to the Audit Committee and, where required, to the public<sup>23</sup>.

---

<sup>23</sup> See Directive 2003/6/EC of the European Parliament and of the Council of 28 January 2003 on insider dealing and market manipulation ("Market Abuse Directive").

### **5.3 MANAGEMENT**

ICRM depends also on the support of Management, which is directly involved in the administration of controls and in the day-to-day running of the systems. Management also coordinates the activities of the company's employees involved in ICRM activities.

### **5.4 AUDIT COMMITTEE: AN OVERALL MONITORING FOR OVERSIGHT PURPOSES**

#### ***5.4.1 Overall monitoring for internal oversight purposes***

The Audit Committee performs an overall monitoring function of the effectiveness of ICRM Systems, which should not duplicate the ongoing monitoring performed by Senior Management<sup>24</sup>.

The function of the Audit Committee is an internal oversight function, based on essential information received. Indeed the members of the Audit Committee generally do not carry out these functions with the company on a permanent basis. Nor could the monitoring function prevail over their other functions with the company. Such could be counter-productive and even detrimental to the company. Furthermore, as the ongoing monitoring of controls is a component of the ICRM Systems, it is even more relevant to ensure an independent and overall, but not ongoing, monitoring of those systems by the Audit Committee, based on the essential information received from various sources.

The overall monitoring of the ICRM Systems by the Audit Committee consists in ensuring that ICRM Systems, considered appropriate by Senior Management, are in place and that they are subject to proper ongoing monitoring and controls. This is done through the high level process described below.

#### ***5.4.2 Monitoring the effectiveness of ICRM Systems***

The concept of "monitoring the effectiveness of ICRM Systems" refers to the high level, dynamic process of improvement by which, based on essential information that it receives, the Audit Committee is able to propose overall directions for Board consideration, when it deems it appropriate. As indicated above, setting directions is normally within the remit of Senior Management.

The Audit Committee receives information from the Senior Management, receives information from the internal audit department, if any, and receives information from the Statutory Auditor, where the situation requires so<sup>25</sup>.

---

<sup>24</sup> See 5.2.

<sup>25</sup> See 2.1, 5.6 and 5.7

The Audit Committee is informed about the main features and significant updates of the company's existing ICRM Systems, including the allocation of responsibilities<sup>26</sup>.

In addition, the Audit Committee is informed of the main results of the ongoing monitoring and control activities<sup>27</sup>, in particular on the main incidents identified and on the related corrective actions decided or implemented by the Senior Management. The internal audit department, if any, may communicate the main results of its activities to the Audit Committee.

The aim is to best adapt or adjust ICRM Systems and the ongoing monitoring of such systems by Senior Management and thus ensure that the control activities are suited to the company's business and the continuous evolution of its external and internal environment. This includes overseeing the allocation of responsibilities within the company to avoid major loopholes in that area.

Finally, the Audit Committee ensures that the public has been properly informed of those incidents identified that are likely to have a significant effect on the prices of the financial instruments offered to the public<sup>28</sup>.

Monitoring the effectiveness of ICRM Systems does not mean monitoring the management itself or the systems themselves<sup>29</sup>. Moreover, this concept does not preclude the existence of limitations inherent to ICRM Systems. As said above<sup>30</sup>, it does not imply a public, overall or periodic<sup>31</sup> assessment of those systems, neither does it imply an assurance or the expression of such assurance by or within the entity.

## 5.5 BOARD

When there is an audit committee as under article 41 paragraphs 1 (indent 1), 2, 3 and 4, the Board, in order to carry out its ultimate oversight responsibilities may obtain information from four main sources:

- the aforesaid audit committee;
- Senior Management;

---

<sup>26</sup> See Appendices I and II.

<sup>27</sup> Activities, performed under the responsibility of the Senior Management, to ensure the design, implementation, improvement and update of the internal control and risk management systems, including the setting of overall and specific directions as well as the determination of priorities.

<sup>28</sup> See Directive 2003/6/EC of the European Parliament and of the Council of 28 January 2003 on insider dealing and market manipulation ("Market Abuse Directive"). This does not imply that the information is given by the audit committee or body performing equivalent functions.

<sup>29</sup> See 3.3.

<sup>30</sup> See 3.8.

<sup>31</sup> E.g. annual.

- the internal audit department, if any;
- the Statutory Auditor, as regards internal control in relation to the financial reporting process (for instance, on material weaknesses in the financial reporting process arising from the statutory audit).

The terms and conditions of communication between the Statutory Auditor and those in charge of governance (i.e. the Board and the Audit Committee, if any) are determined by the Board.<sup>32</sup>

In a one-tier system, the terms and conditions of communication between Senior Management and the Internal Audit Department, if any, on the one hand, and those in charge of governance, on the other hand, are determined by the Board.

In a two-tier system, the terms and conditions of communication between the internal audit department, if any, and those in charge of governance may be determined by the Board and/or the Senior Management.

The Board (and the Audit Committee, if any) may also wish to interview those responsible for key functions, including the person in charge of internal audit, if any, in the presence or, in some cases, without the presence of Senior Management.

## **5.6 INTERNAL AUDIT DEPARTMENT**

Based on its characteristics (see above), a company may decide to establish an internal audit department as part of its ICRM Systems.

The objectives and activities of the internal audit department vary and depend on the characteristics of the company.

The internal audit department plays a major role in the ongoing monitoring function<sup>33</sup>. The internal audit department may also be assigned other specific activities in relation to ICRM Systems' objectives, e.g. reviewing compliance with laws and regulations; ensuring that directional guidelines and instructions are applied and internal processes are functioning correctly; examining financial information. In establishing its work plan, the internal audit department takes into account the risks to which the company is subject. To that end, it liaises with the relevant people at management level.

In general, the internal audit department reports the results of its activities (including its recommendations), or the main results, as the case may be, to Senior Management, the Audit Committee or the Board, as appropriate and as the case may be.

---

<sup>32</sup> Except for the case where the Statutory Auditor is required to report key matters arising from the statutory audit, according to Article 41, paragraph 4 of the 8<sup>th</sup> Directive.

<sup>33</sup> See 5.2.

## 5.7 STATUTORY AUDITOR: OVERALL UNDERSTANDING

### 5.7.1 *Providing a basis for designing and implementing statutory audit procedures*

The purpose of a statutory audit is to enhance confidence in the financial statements. This is achieved through the expression of an opinion by the Statutory Auditor on whether the financial statements are prepared, in all material respects, in accordance with the applicable financial reporting framework<sup>34</sup>. Ensuring that financial information<sup>34</sup> is reliable is one of the objectives of internal control. However, pursuing that objective does not imply other internal control activities (e.g. operational activities), unless they relate to the internal financial reporting systems, controls or financial statements. The Statutory Auditor must not perform such activities or reviews himself as it may impair his independence.

The level of understanding expected from the Statutory Auditor regarding the company's ICRM Systems is necessarily less than that expected of the management in general of the company. In particular, the Statutory Auditor's role does not involve extensive testing of how well the ICRM Systems operate.

The objective of the Statutory Auditor is to assess the risks of material misstatements in the financial statements thereby providing a basis for designing and implementing his statutory audit procedures.<sup>35</sup>

To this end, the Statutory Auditor performs risk assessment procedures to understand the company and its environment. This includes the company's internal control, as far as relevant to the statutory audit: e.g. internal controls relating to data that the Statutory Auditor uses in applying external audit procedures. The Statutory Auditor can proceed to inquiries within the company, analytical procedures, observation and inspection.

Such assessments will allow the Statutory Auditor to obtain an understanding of the company's risk assessment process relevant to the preparation of the financial statements and, where applicable, the results of this assessment process.

As part of the assessment of the risks of material misstatement in the financial statements, the Statutory Auditor determines which of the risks identified are "significant risks"<sup>36</sup> and therefore require special consideration. For significant risks, the Statutory Auditor evaluates the design of the company's related controls and determines whether they have been implemented to address those risks, by performing procedures in addition to inquiry of the entity's personnel.

---

<sup>34</sup> See 4<sup>th</sup> and 7<sup>th</sup> Directives.

<sup>35</sup> The Statutory Auditor designs and performs audit procedures whose nature, timing and extent are based on and are responsive to the assessed risks of material misstatements.

<sup>36</sup> According to external auditing standards.

### **5.7.2 *Communicating elements considered to be material weaknesses***

If management has not appropriately responded to significant risks by implementing controls and if, as a result, the Statutory Auditor judges that there is a material weakness in the internal control in relation to the financial reporting process, the Statutory Auditor communicates this matter to the Audit Committee.<sup>37</sup>

Before considering communicating alleged weaknesses, especially to those in charge of governance, the Statutory Auditor should, as far as possible, liaise with Senior Management and/or the internal audit department, if any. Timely liaison may enable the Statutory Auditor to obtain sufficient appropriate evidence about other controls that compensate the potential material weaknesses identified. But if such liaison is not possible, the Statutory Auditor should state that his communication does not take into consideration possible controls that may have been carried out and could compensate the reported weaknesses.

### **5.7.3 *Liaising with the internal audit department***

Under conditions determined by the Senior Management, the internal audit department, if any, liaises with the Statutory Auditor, where possible. This may enable the Statutory Auditor to use the internal audit department's work and obtain a better understanding of the company's internal control relevant to the statutory audit and of its response to his findings.

### **5.7.4 *Issuing the required opinion on consistency***

The overall understanding of the company's ICRM Systems in relation to financial reporting enables the Statutory Auditor to issue an opinion on the consistency of the company's description of those systems with the annual accounts, as required by the 4<sup>th</sup> Directive<sup>38</sup>.

---

---

<sup>37</sup> As required by the 8<sup>th</sup> Directive.

<sup>38</sup> See Article 46 paragraph 2 and Article 51, paragraph 1, second subparagraph of the 4<sup>th</sup> Directive 78/660.

APPENDICES

APPENDIX I: ICRM SYSTEMS – SUMMARY OF TASKS - DEVELOPED MODEL

AREAS	BOARD	AUDIT COMMITTEE	SENIOR MANAGEMENT	MANAGEMENT	INTERNAL AUDIT DEPARTMENT	STATUTORY AUDITOR
<b>Organisation of ICRM Systems</b>	No	No	Yes, steering including setting of overall and specific directions	Yes, execution	No	No
- Design	No	No	Yes	Yes	No direct involvement (recommendations are possible)	No
- Implementation of the systems	No	No	Yes	Yes	No	No
- Improvements	No	No	Yes	Yes	Possible recommendations	No
<b>Day-to-day management of ICRM systems</b>	No	No	No	Yes	No	No
<b>Internal control activities<sup>39</sup></b>	No	No	Yes	Yes	Yes	No
<b>Ongoing monitoring</b>	No	No	Yes, in considering the analysis of the main weaknesses identified and ensuring necessary corrective actions are taken	Yes, in support of Senior Management	Yes, in conducting regular reviews of selected internal control areas (“assessments”) and providing management with recommendations	No
<b>Overall monitoring for internal oversight purposes</b>	Yes	Yes	No	No	Yes, through information to the Board or Audit Committee	No
<b>Internal communication</b>	No	Yes, information to the Board	Yes	Yes, in the framework of the day-to-day running of controls	Yes	N/A

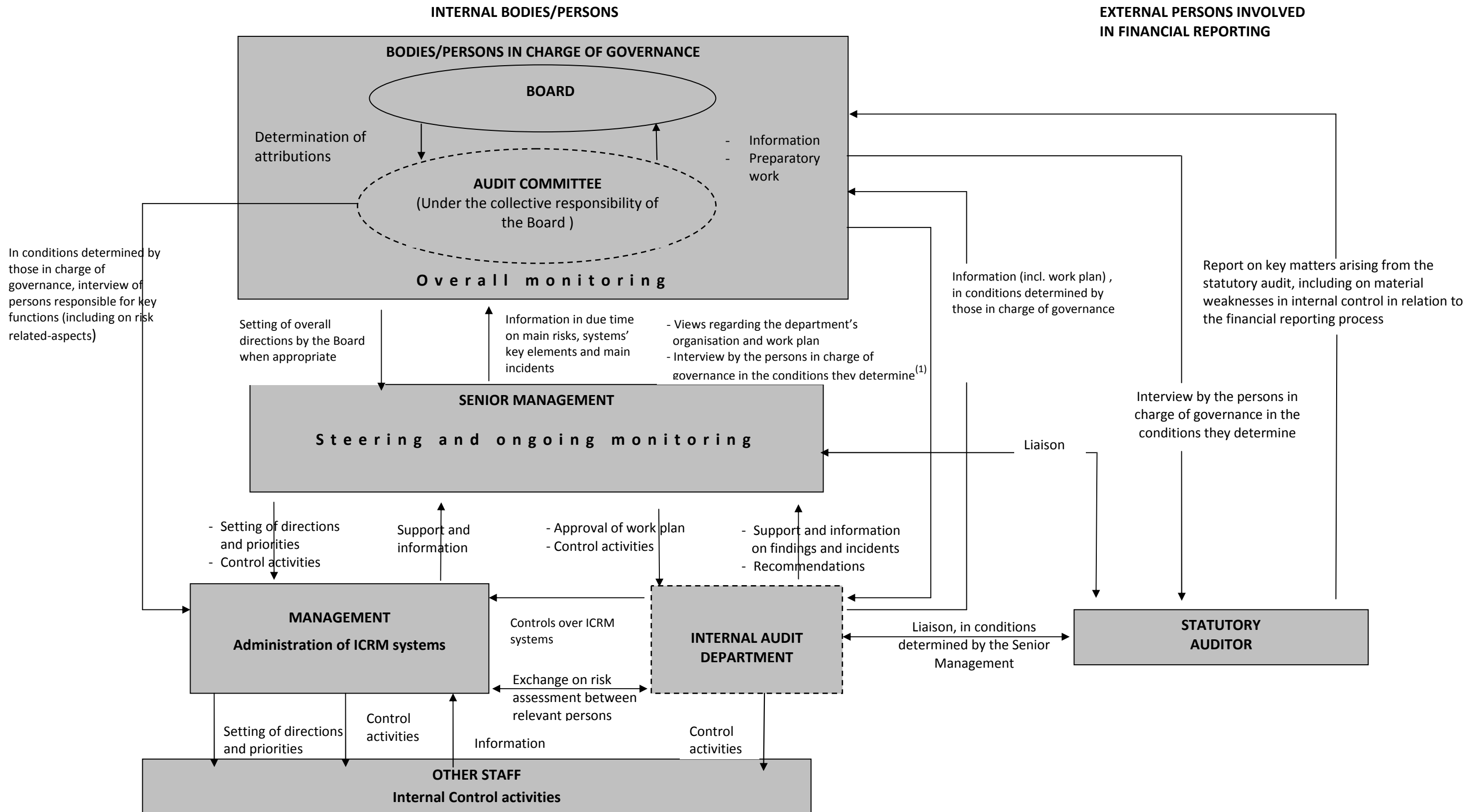
<sup>39</sup> Other staff is also involved in internal control activities

**APPENDIX II: ICRM SYSTEMS - SUMMARY OF TASKS – SIMPLIFIED MODEL**

AREAS	BOARD	SENIOR MANAGEMENT	MANAGEMENT	STATUTORY AUDITOR
<b>Organisation of ICRM systems</b>	No	Yes, steering, including setting of overall and specific directions	Yes, execution	No
- Design	No	Yes	Yes	No
- Implementation of the systems	No	Yes	Yes	No
- Improvements	No	Yes	Yes	No
<b>Day-to-day running / Administration of ICRM systems</b>	No	No	Yes	No
<b>Internal control activities<sup>40</sup></b>	No	Yes	Yes	No
<b>Ongoing monitoring</b>	No	Yes (in considering the analysis of the main weaknesses identified and ensuring that necessary corrective actions are taken)	Yes	No
<b>Overall monitoring for oversight purposes</b>	Yes	No	No	No
<b>Internal communication</b>	N/A	Yes	Yes	N/A

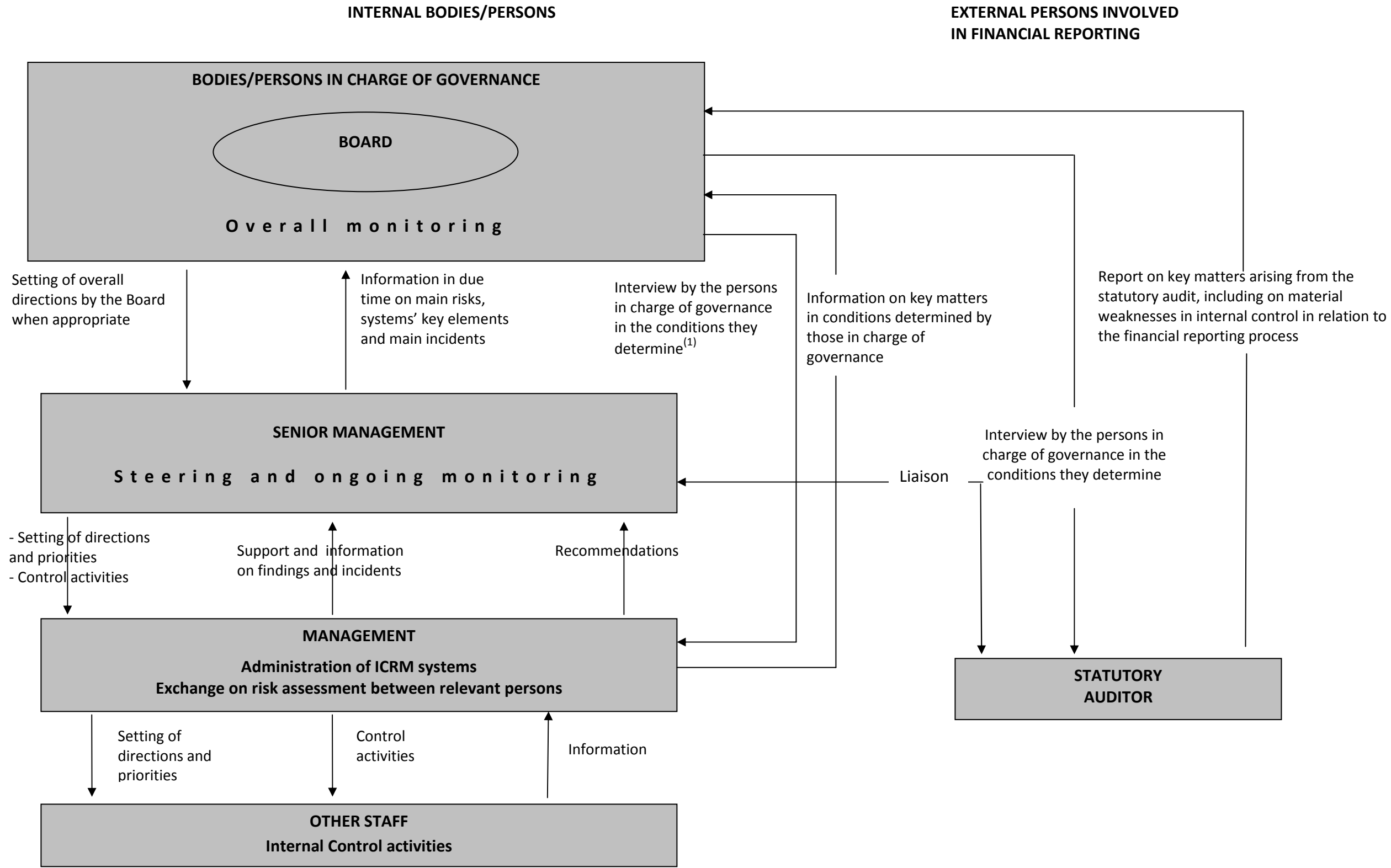
<sup>40</sup> Other staff is also involved in internal control activities

**APPENDIX III: ICRM SYSTEMS - KEY INTERACTIONS - DEVELOPED MODEL**



<sup>(1)</sup> In a two tier system, those conditions may be determined by the Board and/or the Senior Management

**APPENDIX IV: ICRM SYSTEMS - KEY INTERACTIONS - SIMPLIFIED MODEL**



<sup>(1)</sup> In a two tier system, those conditions may be determined by the Board and/or the Senior Management

**APPENDIX V: ICRM SYSTEMS - PROVISIONS OF THE EUROPEAN DIRECTIVES**

BOARD	AUDIT COMMITTEE,	SENIOR MANAGEMENT	INTERNAL AUDIT FUNCTION, IF ANY, IF NOT, OTHER PERSONNEL PERFORMING SIMILAR FUNCTIONS	STATUTORY AUDITOR
<ul style="list-style-type: none"> <li>– Member States may permit the functions assigned to the audit committee to be performed by the administrative, or supervisory body as a whole (8<sup>th</sup> Directive Article 41 § 1).</li> </ul>	<ul style="list-style-type: none"> <li>– Member States may permit the functions assigned to the audit committee to be performed by the administrative, or supervisory body as a whole (8<sup>th</sup> Directive Article 41 § 1).</li> <li>– Member States may provide for exemptions:               <ul style="list-style-type: none"> <li>. They may exempt certain public-interest entities from the obligation to have an audit committee (8th Directive Article 41 § 6.);</li> <li>. They may allow or decide that the provisions laid down in paragraphs 1 to 4 shall not apply to any public-interest entity that has a body performing equivalent functions to an audit committee (8<sup>th</sup> Directive Article 41 § 5.).</li> </ul> </li> </ul>			
<ul style="list-style-type: none"> <li>– For companies whose securities are admitted to trading, the corporate governance statement shall contain:               <ul style="list-style-type: none"> <li>. a description of the main features of the company’s internal control and risk management systems in relation to the financial reporting process. (Article 46a 1. (c) of the 4<sup>th</sup> Directive);</li> <li>. a description of the main features of the group’s internal control and risk management systems in relation to the process for preparing</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>– Without prejudice to the responsibility of the members of the administrative, management or supervisory bodies, the audit committee shall monitor the effectiveness of the company’s internal control, internal audit where applicable, and risk management systems (8th Directive Article 41 § 2. b).</li> </ul>		<ul style="list-style-type: none"> <li>– Without prejudice to the responsibility of the members of the administrative, management or supervisory bodies, the audit committee shall monitor the effectiveness of the company’s internal control, internal audit where applicable, and risk management systems (8<sup>th</sup> Directive Article 41 § 2. b).</li> </ul>	<ul style="list-style-type: none"> <li>– The statutory auditors shall express an opinion concerning the consistency or otherwise of the description (of the main features of the IC &amp; RM systems in relation to financial reporting) with the annual accounts for the same financial year (4<sup>th</sup> Directive Article 46a 2. and Article 51(1), second subparagraph).</li> </ul>

BOARD	AUDIT COMMITTEE,	SENIOR MANAGEMENT	INTERNAL AUDIT FUNCTION, IF ANY, IF NOT, OTHER PERSONNEL PERFORMING SIMILAR FUNCTIONS	STATUTORY AUDITOR
<p>consolidated accounts (article 36 (2) (f) of the 7<sup>th</sup> Directive).</p> <p>– Member States may permit the information required to be set out in a separate report published together with the annual report (Article 46a 2. of the 4<sup>th</sup> Directive and Article 36 (2) (f) of the 7<sup>th</sup> Directive).</p>				
<p>– The administrative, management and supervisory bodies have collectively the duty to ensure that, when provided separately, the corporate governance statement is drawn up and published in accordance with the requirements of the Directive. Such bodies shall act within the competences assigned to them by national law (Article 50b of the 4<sup>th</sup> Directive and Article 36a of the 7<sup>th</sup> Directive).</p>	<p>– The statutory auditor or audit firm shall report to the audit committee on key matters arising from the statutory audit, including on material weaknesses in internal control in relation to the financial reporting process (8<sup>th</sup> Directive Article 41 § 4.).</p>	<p>– The administrative, management and supervisory bodies have collectively the duty to ensure that, when provided separately, the corporate governance statement is drawn up and published in accordance with the requirements of the Directive. Such bodies shall act within the competences assigned to them by national law (Article 50b of the 4<sup>th</sup> Directive and Article 36a of the 7<sup>th</sup> Directive).</p>		<p>– The statutory auditor or audit firm shall report to the audit committee on key matters arising from the statutory audit, including on material weaknesses in internal control in relation to the financial reporting process (8<sup>th</sup> Directive Article 41 § 4.).</p>