



# Guidance on the 8<sup>th</sup> EU Company Law Directive

article 41

## Part 2





“Monitoring the effectiveness of internal control, internal audit and risk management systems”

Part

2

## Implementing the 8th EU Company Law Directive

Article 41 – 2b for Senior  
Management

## Questions and Answers for Executive Committees

*8th European Company Law Directive on Statutory Audit  
DIRECTIVE 2006/43/EC – Art. 41-2b*

*14 December 2011*

**Jorge LUZZI, President of the Federation of European Risk Management Associations (FERMA)**

---



Implementing the 8th EU Company Law Directive needs a strong drive from boards and audit committees. This was the goal of our organisations, FERMA and ECIIA, in producing Part 1 of this Guidance. But board members need good support from senior executives to implement processes through the whole organisation, assess risks and manage mitigation plans. They also have to rely on good internal control, embedded in operational processes, to ensure day to day risk control, and assurance by a focused internal audit, targeting major risks and critical processes. By producing this Part 2 of the Guidance, ECIIA and FERMA aim to provide senior executives with practical guidance to be adapted to the culture, activities and organisation of their companies. Good governance depends on managers conscious that good control reinforces management systems.

**Carolyn Dittmeier, President of the European Confederation of Institutes of Internal Auditing (ECIIA)**

---



One of the key objectives of ECIIA is to promote excellent corporate governance across the EU, and to that end we have worked closely with our colleagues in FERMA to produce guidance for both boards and senior management on how best to use the resources of internal audit and risk management to deliver the common goal of effective and well run organisations in both the public and private sectors. It is important in this day and age to ensure that organisations give thought to their internal assurance processes before being subject to complementary external regulation. The 8th EU Company Law Directive coupled with our papers gives organisations the necessary guidance to enable them to move forward with a governance framework that provides a risk aware culture to maximise the opportunities of success.

Carolyn Dittmeier  
President of ECIIA

Jorge Luzzi  
President of FERMA

## CONTENT

Foreword	6
Introduction	7
General executive committee issues	8
Risk management	11
Internal control	14
Internal audit	16
Glossary	18
FERMA and ECIIA	19
Contributors to this publication	19

## FOREWORD

This document complements the Guidance on the 8th EU Company Law Directive (Art. 41), published by FERMA and ECIIA on 21 September 2010, with recommendations for implementing operationally the statement of the Directive: “Monitoring the effectiveness of the internal control, internal audit and risk management systems”.

While general concepts are detailed in the Part 1, senior executives and executive committees will find in this Part 2 answers to questions for improving the governance of their companies. The purpose of FERMA and ECIIA is not to deliver the definitive answer, but to suggest some best practices from among their members to help senior executives adapt those practices to their company.

In particular, the goals and missions of enterprise risk management (ERM), internal control and internal audit are explained in these documents, but our purpose is not to promote any particular organisation model. These functions must be implemented, whether dedicated departments are created for each one or not, depending on the size, the organisation and the culture of the company

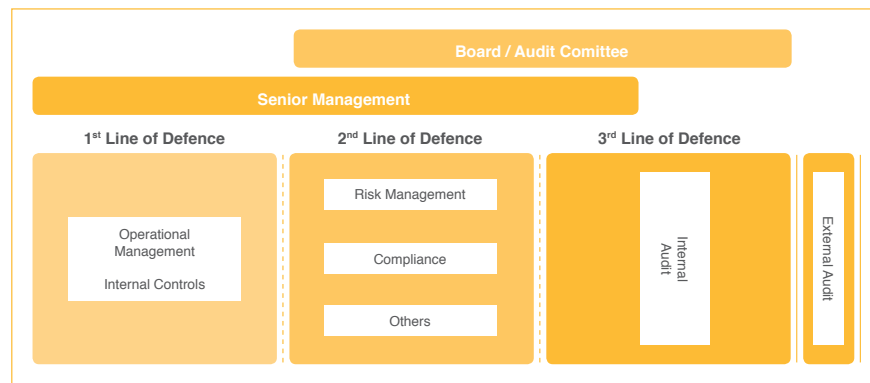
# INTRODUCTION

The objective of this paper is to assist senior management in the implementation of the risk management and internal audit issues associated with the 8th Directive. The paper is set out as a series of questions that senior management may consider regarding the role of risk management, internal control and internal audit.

The board is responsible for the oversight of the company’s risk management and control framework. Everyone in the company plays a role in effectively managing risks, but the primary responsibility for risk management and control is delegated to the appropriate management level within the company. The CEO and the CFO have the final responsibility to the board for the risk management and control framework.

To fulfill these duties effectively, they seek assurance from various sources within the organisation. FERMA and ECIIA support the “three lines of defence” model as a benchmark for future regulatory guidance. See below for details of the model.

## Three Lines of Defence Model



While internal control is embedded in processes in a way of complementing management systems controls, we believe that risk management and internal audit must communicate clearly to understand and agree their respective roles. This document is in four chapters to facilitate this approach: one dedicated to general questions concerning the three functions, followed by a chapter for each of the functions.

## GENERAL EXECUTIVE COMMITTEE ISSUES

### ■ ■ ■ **G1.** Is sufficient time available on the executive committee agenda to present the results of risk management, internal control and internal audit reviews?

As the responsibility for control and the risk management framework is delegated by the board to the executive committee, it is very important to make sufficient time available on the executive committee agenda for the presentation of the results of risk management and internal control reviews. ERM provides a framework for risk management, and the risk management process has to be monitored and reviewed so that decisions on risks to be taken can be made. As internal audit also has oversight of the activities in internal control and risk management, and advises management and the board of directors regarding how to better execute their responsibilities, their reports should also be reviewed thoroughly by the executive committee.

The Executive committee should review major risks at least once a year and examine thoroughly the more important ones regarding strategic development and reputation. Internal control and internal audit programmes should be validated at least once a year. Critical processes and audit statements must be received and reviewed each quarter. Any serious weaknesses or sudden deterioration in the risk environment should be reported to the board without delay.

### ■ ■ ■ **G2.** Are the risk management and control processes in line with the company's objectives and in accord with policies in place?

Risk management aims at creating a disciplined, structured and controlled environment within which risks to the organisation can be anticipated and maintained within predetermined, acceptable limits. Risk assessment is a continuous process requiring regular review as internal and external changes influence the company's strategies and objectives. Circumstances demanding close attention include substantive changes to the operating environment, new personnel, new or revamped information systems, rapid growth, new technology, new products or activities, corporate restructuring, acquisitions and disposals, and foreign operations. It is important to be aware of the processes in place and how flexible they are in light of changes such as those above.

When strategy is approved by the board of directors, taking into account stakeholders' risk acceptance, risk management should align risk limits and risk appetite with the main goals in order to cap expected losses, and to maximise the likelihood of achieving expected returns. Internal processes should identify new critical processes, new areas of significance and new material costs to put under control.

Since profits are in essence the reward for successful risk-taking by a company, the purpose of an internal control system is to help manage and control risk appropriately rather than to eliminate it. Control mechanisms should be incorporated into the business plan and embedded in the day-to-day activities.

■ ■ ■ **G3.** Is the independence of risk management, internal control and internal audit guaranteed so that the executive committee is informed of major risks and control activities?

The risk management, internal control and internal audit departments have to be given the authority by the audit committee or the CEO in such a way that they can operate as independent bodies and in accordance with the three lines of defence model.

Promoting risk awareness and creating transparency, for instance by building a horizontal matrix organisation, can foster the process of getting information on major risks and control activities swiftly to the executive committee. Openness and easy contact for all managers with the members of executive committee and CEO are important to achieve 'early warning' in case of major risks. The executive committee must ask: What is the greatest risk, the most worrying process and the worst internal audit report issues?

Concerning the internal control activities, it is important that the executive committee receives a report on the status of controls and can follow up on the corrective actions that management proposes to take.

■ ■ ■ **G4.** Are audit recommendations settled and implemented with transparent information and communication processes?

In order to reach the optimum result from internal audit, it is important that, together with the audited management, a follow up action plan is agreed and implemented within acceptable time limits.

The executive committee must be provided with a summary of non-implemented actions.

On-going contact between internal audit and the audited management can foster transparent information and improve the quality of the communication process.

■ ■ ■ **G5.** Is the executive committee informed of the major risks of the organisation at each level?

The risks review must include major risks across the organisation. Each level must manage major risks without thinking of the level where they arise. If all the major risks arise only at the highest level, the executive committee must question whether all major risks have been identified.

This situation will be reached when an open communication culture operates across the organisation and where all managers can reach the CEO in case of urgency ('open door' policy). This bottom-up communication flexibility should be part of the 'risk aware' culture.

## ■ ■ ■ **G6.** Does the audit planning take major risks and critical control processes into account?

In order to optimise the three lines of defence, it is important to have good and frequent contact between the various parties in these processes, so that the internal audit plan can focus on the critical processes and the major inherent risks.

Risk assessments should provide information on the major risks to assist in preparing the audit plan. Control reviews of critical processes must produce statements about weaknesses. The next year's audit plan must be partially based on this information. The executive committee must be clear on which audits are based on this information.

## ■ ■ ■ **G7.** Do risk management, internal control and audit share information on a regular basis, and take it into account to identify major risks and key critical processes and to mitigate major risks?

The CEO ensures the presence of a positive internal control environment and risk culture within the organisation ('tone at the top'), provides leadership and direction to senior managers, and monitors the overall risk activities in relation to the risk appetite of the organisation.

Each of these functions and processes focuses on different aspects and different areas (financial accounting, strategy, supply chain, credit, human resources and many others). To ensure an effective governance of the organisation, regular sharing of information between risk management, internal control and internal audit is vital. It is especially necessary when action plans are being agreed and reports are presented that there are full transparency and exchange of information.

Risk assessment must take audit findings into account on a regular basis to complete risk knowledge and awareness of events that have occurred, update the risk evaluation and improve risk mitigation plans.

The internal control scope must be improved in the light of audit findings to prevent the recurrence of similar events.

## ■ ■ ■ **G8.** What should be disclosed in annual reports?

National laws and market soft laws define what information stakeholders should receive concerning risks associated with the activities of the company, how they are assessed and mitigated, the internal controls in place and the contents of the chairman's report including internal control and audit.

We recommend contact with the national internal audit institutes and risk management associations for further information. Links to these associations are available on ECIIA and FERMA websites.

## RISK MANAGEMENT

### ■ ■ ■ R1. Does the company have an official risk management system?

A risk management system is a combination of four elements:

- The chairman (or president of the audit committee) and the CEO should set the authority for the chief risk officer to report on major risks;
- The organisation should delegate to managers the authority for taking and limiting risks, and to risk officers for assessing risks;
- Resources must be made available for mitigating risks;
- Competences for risk management must be assessed and training programmes devised and delivered for senior executives, risk managers and risk officers.

### ■ ■ ■ R2. Does the company have a risk strategy? Who is in charge of that strategy? Has the company defined its risk tolerance\*, risk appetite\* and risk profile\*? Is there a clear communication and understanding of this risk strategy and risk procedures?

The risk strategy is part of the company strategy, but should be clearly and meaningfully designed to support it. For instance, development in risky countries, market prices exposure, focus on a lone business or diversification, suppliers' transfer policy, etc, are exposures that need a specific risk policy. The risk strategy should be approved by the board of directors as part of the general strategy and should clarify risks inherent in achieving the business objectives.

Communication of the risk strategy and risk procedures must be assessed through a maturity matrix, internal control processes and the internal audit of the risk management process.

*\*See Glossary*

■ ■ ■ **R3.** Does the organisation have clear, meaningful and measurable objectives, linked with the risk profile? Are these objectives known throughout the organisation?

A dashboard report should be devised and updated by businesses. These reports should include follow up of mitigation plans and key risk indicators (KRI). KRI must be defined according to risks and business, such as:

- Financial risks: market price, foreign exchange, counterparties
- Regulation risks: financial impact, political sensitivity;
- Country risks: revenue, asset values, employees and other factors relative to the country risk level;
- Health and safety: frequency rate, severity rate.

■ ■ ■ **R4.** How are major risks or control failures escalated within the company and who are they reported to? Does the company identify and record new and emerging risks?

Major risks must be escalated through the bottom-up risk review process (see G5). The risk review must be reported to the executive and audit committees.

The significant internal and external operational, financial, compliance and other risks identified must be assessed on a continuous basis, with a periodic review depending on the activity cycle.

The company should have a survey of events that have occurred in its organisation, its business and in similar businesses. This benchmark should be used to improve the scope of the risk catalogue and the risk evaluation.

■ ■ ■ **R5.** What are the qualifications/competences of the risk manager? Does the CEO/Chairman set the tone at the top about a positive risk culture? Is the principle of risk ownership embedded in the delegation of authority? Is it integrated in the compensation mechanisms (bonus system)?

Risk managers should have received a minimum basic training which should include how to improve the company risk culture. Companies must include risk management in their managers' training programme.

The CEO must talk about risk appetite when speaking about the company strategy.

Senior executives' annual targets must be linked to the risk appetite and risk profile. Incentive policies should include criteria linked to risk management.

## ■ ■ ■ R6. Does a proper risk management function exist in the company?

In the past ERM was linked with insurance management, finance or legal divisions. A proper risk management function must be created and sponsored by the CEO. It could be incorporated into a 'corporate governance division', with ethics and compliance, internal control and internal audit (see R8).

## ■ ■ ■ R7. What resources are available to build and maintain the risk management system?

Different resources are required at different levels:

- The executive committee must be supportive of a risk management culture;
- A corporate team (which may be focused solely on risk management, depending on the size of the company) must provide the process, methods and information technology tools;
- Risk officers must be designated at the different levels of the organisation (not exclusively focused on risk management);
- All managers must be risk managers and trained to a risk culture.

## ■ ■ ■ R8. How should ERM be linked with internal control and internal audit

ERM, internal audit and internal control must keep their independence but have to work in a close relationship:

- Mitigation plans should include internal control activities related to operational risks, and actions arising from internal audit reports;
- Major risks must be monitored by internal control as critical processes;
- Major risks should be audited and be part of the internal audit plan.

## INTERNAL CONTROL

### ■ ■ ■ C1. Who is in charge of internal control and who does he/she report to?

Internal control is the set of processes and procedures put in place to help managers organise and control the day-to-day operations of the organisation. As such, internal control is the responsibility of everyone in the organisation. However, some organisations have an internal control function because of the nature of the industry or legislation, such as Sarbanes-Oxley in the USA.

### ■ ■ ■ C2. Have the critical internal control areas been identified? Has the executive committee identified critical processes on which to be kept informed?

The critical internal control areas should be identified by risk management and internal audit working closely together and sharing the results of their work. They are the ones that the executive committee may wish to track and internal audit may include in their annual plan.

### ■ ■ ■ C3. Do the company's culture, code of conduct, human resource policies and performance reward systems support the business objectives? Are there established channels of communication for individuals to report suspected breaches of law or regulations or other improprieties?

The key question is how the business objectives of the organisation are set and communicated through the various levels. Each objective should have its associated risks identified and mitigating actions to manage those risks detailed, in place and operating effectively. Similarly the organisation needs to ensure it has appropriate channels to report control failures and potential breaches of laws and regulations. Also necessary is a clear scheme of delegation so that managers at all levels are aware of the limits of their authority to commit the organisation.

■ ■ ■ **C4.** Who monitors the adequacy of the internal control system? Are there processes to review the adequacy of financial and other key controls for all new systems, projects and activities?

A key part of any effective internal control system is a mechanism to provide feedback on how the systems/processes are working so that shortfalls and areas for improvement can be identified and changes implemented. In the first instance if there is an internal control department, it will help managers implement sound internal controls. The operation of key controls will then be subject to review by internal and external audit along with other review agencies, both internal and external to the organisation. If no internal control department exists, guidance may be sought from risk management or internal audit.

■ ■ ■ **C5.** Are authority, responsibility and accountability defined clearly so that decisions are made and actions taken by the appropriate people?

Every organisation needs a clear scheme of delegation which delineates the responsibilities and accountabilities of everyone in the organisation.

■ ■ ■ **C6.** Are arrangements in place to assess periodically the effectiveness of the organisation's control framework?

A key requirement of many of the internal control requirements encompassed in legislation throughout the EU and the rest of the world is an annual attestation as to the adequacy and effectiveness of the internal control system. Such attestation should be clearly evidenced. The review of the control framework will be the responsibility of the audit committee who will receive information and assurances from internal audit, risk management and the external auditors.

■ ■ ■ **C7.** What is the training programme dedicated to internal control and who must follow this programme?

In all organisations every employee should receive appropriate training and advice as to their responsibilities with regard to and the meaning of internal control. Assurance about these matters will be sought by the audit committee as part of its work on assessing the state of internal control across the organisation.

## INTERNAL AUDIT

### ■ ■ ■ A1. Does the organisation have an independent internal audit function and who does it report to?

The role of internal audit in an organisation is twofold:

First, to provide assurance to the board/audit committee that the internal control and risk management systems are in place and working as expected;

Second, to help senior management identify ways to manage their key risks in the most effective manner by working with risk management to identify and effect mitigating actions to reduce risks to the desired level.

To ensure internal audit is able to discharge these functions, internal audit reports directly to the CEO/CFO and the audit committee and takes no part in the day-to-day operations of the departments it reviews.

### ■ ■ ■ A2. Who appoints the head of internal audit?

The head of internal audit is appointed/approved by the audit committee. This is to ensure that the candidate has the necessary independence to report without fear or favour to the audit committee on the state of risk management and internal controls throughout the organisation. For a similar reason when the head of internal audit leaves, the audit committee will wish to satisfy itself about the reasons.

### ■ ■ ■ A3. Who assesses internal audit?

The audit committee assesses the performance of the internal audit function by receiving performance information from the function itself and consulting appropriate directors and the external auditors. In addition, the function should be independently reviewed by an external agency such as the Institute of Internal Auditors (IIA), as specified in the International Professional Practices Framework, issued by the IIA.

### ■ ■ ■ A4. Is there appropriate communication to the executive committee and is direct access to it assured for the head of the internal audit?

To ensure independence of the function and to preserve the independence of the reports produced, the chief audit executive should have regular meetings with the executive committee to review the findings of the audit reports and to discuss any new or emerging risks. In addition the chief audit executive should be able to take a matter directly to executive committee or the audit committee if he/she feels the matter is of sufficient importance.

- ■ ■ **A5.** How are the proposed audit activities prioritised? Is the determination linked to the organisations' risk management plan and internal audit's own risk assessment? Are the internal audit plan and budget challenged when presented?

The work of internal audit should be set out in a risk-based plan challenged and approved annually by the audit committee. This plan should be informed by the work of other review agencies such as external audit and risk management and should contain sufficient work for the head of internal audit to be able to form an overall view as to the adequacy of the risk management process operated by the organisation. If there is no formal risk management process or if the process is flawed, then internal audit will need to rely on some other method of assessing the key activities and controls for its review. This could be based on its own risk assessment.

- ■ ■ **A6.** Are there effective follow-up procedures to ensure that appropriate change or action occurs in response to changes in risk and control assessments?

Any major changes or actions should be reported to the audit committee along with the timescale and key responsibilities for action. Although the key responsibility for implementation lies with line management, progress on these changes should be verified by internal audit who should keep the audit committee up to date on progress.

- ■ ■ **A7.** Does internal audit assess the first and second lines of defence\*?

As set out in the glossary, the first line of defence is operational management and internal control. The second line is the major control functions within the organisation, such as risk management compliance, health and safety, and quality, safety and environmental processes. Review of these functions will be included in the internal audit plan.

- ■ ■ **A8.** Does internal audit issue an annual opinion on internal control and risk management systems?

As part of the board's annual assessment as to the state of internal control and risk management across the organisation, it is usual for the chief audit executive to be asked to provide an overall control assessment covering these issues. This forms part of the board's annual assurance process that enables it to provide assurance on the internal control system to shareholders, regulators and other interested parties.

*\*See Glossary*

## ■ ■ ■ A9. What is the training programme dedicated to internal audit, and who must follow this programme?

In order to be able for internal audit to fulfill its role as set out above, it is necessary to ensure that the members of the department are suitably trained and qualified. This necessitates that each member receives appropriate training in the auditing of risk management and internal control. Such training needs can be met by utilising the many IIA training courses and encouraging senior staff in the department to qualify as internal auditors. (Certified Internal Auditor in continental Europe and Chartered Member of the Institute of Internal Auditors in the UK and Ireland.)

## GLOSSARY

### Risk appetite

The level of risk that the company is willing to take: high return - high risk; low risk - low return, or a portfolio of different exposures. Risk appetite is strategic and relates primarily to the business model.

### Risk tolerance

The maximum amount of risk that the company can bear despite controls. Risk tolerance is more operational and relates primarily to the company's targets.

### Risk acceptance

Changes in the acceptability to stakeholders of particular risks despite risk control measures taken by the company.

### Risk profile

Description of the risks facing the organisation. Various risk profiles may be considered, such as:

- A few low risks with assured returns;
- A portfolio of a number of higher risks with the potential for high earnings/ losses;
- A mix of high and low risks.

### First line of defence

Operational management and internal control.

### Second line of defence

---

Control functions such as risk management, compliance, health and safety, and quality, safety and environmental processes.

### Third line of defence

---

Internal audit.

## FERMA AND ECIIA

### FERMA: [www.ferma.eu](http://www.ferma.eu)

The Federation of European Risk Management Associations (FERMA) brings together 21 national risk management associations of 19 countries. It represents a wide range of business sectors from manufacturing to financial services, charities and health organisations, as well as local government organisations. FERMA's objectives are to support its members by coordinating, enhancing awareness and effective use of risk management, insurance and risk financing in Europe. FERMA organises a bi-annual forum and a bi-annual benchmarking survey on the status of risk management in Europe presented at a seminar for all its members.

### ECIIA: [www.eciia.eu](http://www.eciia.eu)

The European Confederation of Institutes of Internal Auditing (ECIIA) is the professional representative body of 35 national Institutes of Internal Audit in the wider European area. The ECIIA's objective is to support corporate governance and the internal audit profession in the European Union and in the ECIIA's member countries and to promote the application of the global Institute of Internal Auditors' Standards and Code of Ethics to all internal audit professionals in the public and the private sector. The ECIIA undertakes research on topics related to internal audit, business control, risk management and corporate governance. It publishes position papers, briefings, reports and a newsletter.

## CONTRIBUTORS TO THIS PUBLICATION

**Michel DENNERY:** Vice-President FERMA; Risk Management Director – GDF SUEZ

**Marie Gemma DEQUAE:** Past President FERMA; Risk Manager - Partena Group

**Richard NELSON:** Past President ECIIA and Past President Chartered Institute of Internal Auditors



### **FERMA**

Federation of European Risk Management Associations  
Avenue Louis Gribauumont, 1 /B4, 1150 Brussels, Belgium

Tel: +32 2 761 94 32

Fax: +32 2 771 87 20

Email: [florence.bindelle@ferma.eu](mailto:florence.bindelle@ferma.eu)

Web: [www.ferma.eu](http://www.ferma.eu)

### **ECIIA**

European Confederation of Institutes of Internal Auditing  
Koningsstraat 109 -111 bus 5, 1000 Brussels, Belgium

Tel: +32 2 217 33 20

Fax: +32 2 217 33 20

Email: [office@eciia.org](mailto:office@eciia.org)

Web: [www.eciia.eu](http://www.eciia.eu)