Guidance on the **8**th EU Company Law Directive

article 41

ECIIA

ferma

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

Guidance for
boards and audit committees

Peter den Dekker, President of FERMA

Running a business has always been a matter of risk taking. The recent crisis has reinforced the necessity of managing risk, and has enhanced public expectations for economic actors to be more proactive in risk control.

What's new with the 8th EU Company Law Directive is that there is a clear responsibility given to boards of directors and to their audit committees. Senior management is expected to be involved in risk management and risk taking. Directors have to give direction depending on the risk appetite of shareholders.

A good risk management system is like management systems on a racing car - they help it to go faster, further and more safely.

Claude Cargou, President of ECIIA

The duty assigned to the board and its audit committee by Art 41 of the 8th Directive to "monitor the effectiveness of risk management and control systems" simply translates the expectations from participants in capital markets to receive transparent and reliable information on significant current and evolving risks for the organisation and on the way these risks are managed.

This fiduciary obligation for boards and audit committees is no longer limited to financial reporting risks, as it was too often the case in the past.

Today, they must also oversee the effective management of the company's strategic, operational and compliance risks.

This is where boards and audit committees can look to internal auditing for objective and independent assurance on the effectiveness of organisation-wide risk and control systems.

As such, internal auditing becomes one of the cornerstones of good organisational governance, supporting boards and audit committees to effectively assume their fiduciary responsibilities towards the company's stakeholders and the public at large.

This 8th EU Company Law Directive gives organisations confidence to take advantage of business opportunities.

Peter den Dekker   Claude Cargou
President of FERMA   President of ECIIA

CONTENT

OBJECTIVE
of this GUIDANCE

The objective of this FERMA/ECIIA Guidance is to assist board members, particularly members of the audit committee, with the implementation of art. 41 of the 8th European Company Law Directive.

In section 2b, the Directive states that:

"[…] the audit committee shall, inter alia: monitor the effectiveness of the company's internal control, internal audit where applicable, and risk management systems […]."

While this seems to be a rather simple statement, "what to monitor" and "how to monitor" are considerably more complex. In order to shed light on "what" and "how" to monitor, this guidance:

1. Provides an overview of the role and responsibilities regarding effective risk management and control assurance for:
    • The board / audit committee[1];
    • The chief executive officer (CEO) and senior management[1];
    • Operational management;
    • Monitoring and assurance functions.
2. Clarifies the recommended interaction between internal control, risk management and internal audit.
3. Suggests good practices for board and audit committee oversight regarding:
    • The risk management process;
    • The internal control system;
    • The internal auditing function.

Notes: • While the 8th Directive assigns this oversight duty to the organisation's audit committee, it remains ultimately the collegial responsibility of the entire board, and this guidance should be read accordingly.
    • The transposition of the 8th Directive into national codes may necessitate further action beyond what is proposed in this guidance.

[1] for the purpose of this paper:
    • board is the board of directors in a one tier structure and the supervisory board in a two tier structure.
    • senior management is the executive committee in a one tier structure and the management board in a two tier structure.

ROLES AND RESPONSIBILITIES
with regard to EFFECTIVE RISK MANAGEMENT AND CONTROLS

Roles and responsibilities

Board

The board provides oversight and direction to senior management by:

- Setting (in cooperation with senior management) the organisation's risk appetite (= amount of risk an organisation is willing to accept in pursuit of value);
- Being apprised of the most significant risks for the organisation and whether senior management is responding appropriately (i.e. in relation to the agreed upon risk appetite).

Chief executive officer and senior management

The CEO, with his/her senior management team, has ultimate ownership responsibility for the organisation's risk management and control framework. He/she:

- Ensures the presence of a positive internal environment and risk culture within the organisation ("tone at the top");
- Provides leadership and direction to operational management and monitors the organisation's overall risk activities in relation to its risk appetite;
- Where evolving circumstances and emerging risks indicate potential misalignment with the risk appetite, the CEO and senior management take the necessary measures to reestablish alignment.

Members of senior management have responsibility for managing risks within their spheres of responsibility related to their units' objectives by:

- Converting strategy into operational objectives;
- Identifying and assessing risks adversely impacting the achievement of these objectives;
- Effecting risk responses consistent with risk tolerances.

Operational management

Senior management assigns responsibilities, including for risk management procedures, to managers in specific processes, functions or departments (the "risk owners"). Accordingly, these managers play a more hands-on-role in executing particular, day-to-day, risk procedures. For instance, they identify, assess risks and determine risk responses through the development of effective internal controls. (e.g. developing protocols for new product development).

Note: While internal control policies and procedures are an integral part of an organisation-wide risk management framework (i.e. they are established to help ensure risk responses are effectively carried out), some organisations - particularly in the financial sector - have established a centralised internal control function for facilitating and coordinating the consistent and adequate design and effective operation of internal controls established by operational management. However, this monitoring activity does not take away any of the duties of operational management for managing risks in its sphere of responsibility.

Risk monitoring and assurance functions

Centralised risk management function (risk monitoring)

While the basis of sound risk management is that every part of an organisation is responsible for managing risks in its own area of activity, this should be operated in an integrated, holistic approach to ensure alignment with the organisation-wide objectives and strategy.

FERMA/ECIIA, therefore, supports the establishment of a centralised risk management function for coordinating and helping effect risk management across the organisation. While best practice is to nominate a chief risk officer, smaller organisations may assign this responsibility to another senior executive.

FERMA/ECIIA is further of the opinion that this individual should report through the CEO to the board. He/she is responsible for monitoring risk management progress and for assisting operational managers in reporting relevant risk information up, and across the organisation.

Specific responsibilities of a chief risk officer (or similar function) include:

- Establishing risk management policies, defining roles and responsibilities, and setting goals for implementation;

- Providing a framework for risk management in specific processes, functions or departments of the organisation;

- Promoting risk management competence throughout the organisation;

- Establishing a common risk management language (e.g. regarding risk categories and measures related to likelihood and impact);

- Facilitating managers' development of risk reporting, and monitoring the reporting process;

- Reporting to the CEO and the board on progress and recommending action as needed.

Internal audit function (risk assurance)

The internal audit function

- Provides objective assurance to the board and senior management that risks are understood and managed appropriately, and

- Serves as an in-house consultant proposing solutions for improving the organisation's governance, risk management and control structure.

As such, internal audit actively contributes to effective corporate governance providing however that certain conditions – fostering its independence and professionalism – are met.

FERMA/ECIIA therefore recommends that best practice is to establish and maintain an independent, adequately and competently staffed internal auditing function, which

- Acts in accordance with the International Professional Practices Framework – IPPF, set by the global Institute of Internal Auditors[1]

- Reports to a sufficiently high level in the organisation to be able to perform its duties and that it should have an active and effective reporting line to the board (or its audit committee).

[1] www.theiia.org/guidance/standards-and-guidance/interactive-ippf

Establishing a professional internal audit function should be the rule, not only for large and medium size institutions but also for smaller entities. This is the more so because the latter may not be able to deploy a full organisational structure to ensure the effectiveness of its governance and risk management processes. In any case, for small organisations that have not established an "in-house" internal audit function, it should be a requirement to disclose to their stakeholders on an annual basis that they have considered how the necessary assurance on the effectiveness of the organisation's governance, risk management and control structure is to be obtained (i.e. through internal audit).

Interaction between the various actors in risk management and internal control

As mentioned before, the board and the CEO are respectively responsible for providing oversight and monitoring risk management strategies and processes. To effectively assume these duties, they seek assurance from various sources within the organisation.

This model, which is rapidly gaining universal recognition, can be illustrated as follows:

Three Lines of Defence Model
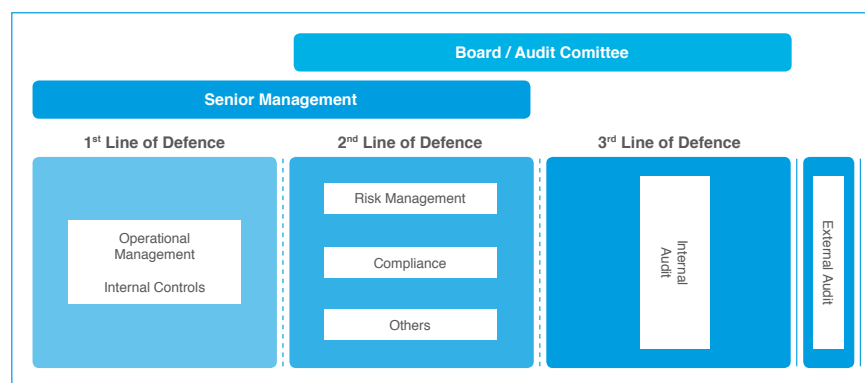
As a first line of defence

Operational management has ownership, responsibility and accountability for assessing, controlling and mitigating risks together with maintaining effective internal controls.

As a second line of defence

The risk management function facilitates and monitors the implementation of effective risk management practices by operational management and assists the risk owners in defining the target risk exposure and reporting adequate risk related information through the organisation.

In addition to the centralised risk management function, and as part of this second line of defence, some organisations have established a separate compliance function to monitor compliance risks, i.e. risks of non-conformity with applicable laws and regulations as well as internal regulations (including fraud). In this capacity, the compliance function reports directly to senior management.

Other specific monitoring functions may include health & safety, supply chain, environmental and quality functions.

As a third line of defence

The internal audit function will, through a risk based approach, provide assurance to the organsation's board and senior management, on how effectively the organisation assesses and manages its risks, including the manner in which the first and second lines of defence operate. This assurance task covers all elements of an organisation's risk management framework, i.e. risk identification, risk assessment and response to communication of risk related information (throughout the organisation and to senior management and the board).

General remark

External auditing can be considered as a fourth line of defence, providing assurance to the organisation's shareholders, board and senior management regarding the true and fair view of the organisation's financial statements. However, given the specific scope and objectives of their mission, the risk information gathered by external auditors is limited to financial reporting risks only and does not include the way senior management and the board are managing/monitoring (strategic/ operational/ compliance) enterprise-wide risks, and for which the risk management and internal audit functions respectively provide monitoring and assurance.

AGENDA
for the AUDIT COMMITTEE

Effectiveness of risk management

Best practices

FERMA/ECIIA considers that risk management, internal control and audit functions provide reliable information channels for the board of directors to monitor the effectiveness of risk management and internal control systems.

With regard to *risk management*, the board and/or the audit committee needs to receive, at least yearly, a review of the organisation's major risks. It needs to know how the business model is impacted by major risks, and how value generation could be enhanced by opportunities or reduced by vulnerabilities. If necessary, it needs also to have appropriate information about specific risks according to evolution of strategy, external environment or particular risks inherent to the activity of the company.

While the above information is generally reviewed by the full board, the audit committee needs to receive information on risk governance (steering committees, definition of acceptable and accepted limits, benchmarks, controls and audit) to assess the effectiveness of the risk management systems. If there is a "risk committee" included in the board sub-committees, then some aspects of risk monitoring, control or mitigation will be delegated to this committee. Last, internal audit reports to the audit committee on the maturity, dissemination and effectiveness of the risk management systems.

- The company has defined its risk strategy and appetite. The CEO has designated a chief risk officer or equivalent. Risk owners have been designated for each major risk;

- Risk owners have fixed meaningful and measurable objectives and controls, recognised throughout the organisation; risk ownership is part of the delegation of authority and the remuneration mechanisms (bonus system) should include appraisal of risk taking;

- A centralised risk management function is in charge of the implementation of the risk strategy. It provides the company with a formal risk management framework, and dedicated training programmes to improve the risk management culture and promote a common language throughout the organisation;

- Senior management periodically receives reports on major risks' evolution and on the implementation of mitigation plans. Management also communicates a risk dashboard, with key risk indicators, at least once a year to the audit committee;

- Critical risks and emergent risks are escalated to the appropriate management level as soon as they are identified.

Effectiveness of internal control

Best practices

In respect of *internal control*, the board and the audit committee need to receive assurance that adequate and effective controls exist to monitor and manage the critical risks, and that a process exists to report adequately on this monitoring. Senior management, together with the independent functions of internal and external audit, provides this assurance to the audit committee regarding the effectiveness and efficiency of internal control.

Key points related to internal control

- The CEO and senior management are in charge of internal control. Through delegation of authority all operational managers "inherit" a portion of that responsibility. It is important for the audit committee to know whether this principle of responsibility has been openly communicated throughout the organisation, and whether operational management has been given the proper tools (budget, resources) to assume this responsibility and accountability.

- The organisation's culture, code of conduct, human resources policies and performance reward systems are critical components of the internal control system. It is important for the audit committee to assess whether these components are supportive of the organisation's strategic objectives.

- The culture of the organisation should encourage individuals to report suspected breaches of law or regulations or other improprieties. Critical for this system to work is the protection of the people who "blow the whistle". The audit committee should be aware of how the whistleblowing mechanism works and what the organisation is doing with the complaints.

• Any internal control system can only be adequate if properly monitored. The audit committee should monitor the processes that are in place to review the adequacy of financial and other key controls, including management reviews. The audit committee should also be informed about serious control deficiencies. Through delegation of authority, control becomes everyone's responsibility within the organisation. Some organisations have implemented a process of periodic control self-assessments, whereby operational entities within the organisation reflect on the risks inherent to their processes and on the quality of the controls that are in place. The aggregated results of these workshops can also assist the audit committee in monitoring the organisation's internal control system.

Effectiveness of internal audit

Best practices

In line with international standards, *internal auditors* document relevant information to support the conclusions and management response to their audits. The audit committee should assure that its agenda includes periodic review of the following:

- The internal audit charter and independence of the internal audit function;
- Internal audit plans and allocated resources, including audit risk assessment criteria;
- Professional competence of the internal audit function: providing advice to the CEO regarding performance evaluation, compensation changes, hiring, dismissal of the head of internal audit;
- Quality assessment reviews in accordance with the International Standards for the Professional Practice of Internal Auditing including periodic outside assessments.

In line with its standards, the internal audit function reports to the audit committee and to the CEO on the effectiveness of the risk management and control systems, providing advice for continuous improvement by management. Internal audit will identify potential conflicts of interests at the various levels of operations based on a global oversight and insight as to the consistency between strategic objectives and operations, with diagnostics as to any misalignments.

Key points related to internal audit

- The independence of internal audit should be formalised in the internal audit charter, signed by the CEO and the chairman of the audit committee. But, even more important for the audit committee is to check whether this independence also exists in practice. Does internal audit have true direct and unlimited access to the audit committee and the board? Does internal audit report independently on business issues, without interference from senior management? Does objective reporting influence future career opportunities of internal auditors?
- Internal audit has limited resources. It is therefore essential to allocate these resources to the most critical areas. Does the audit committee challenge the internal audit plan and budget when presented? How does internal audit assess the organisation's risks, the risk management process implementation and risk management maturity?

Is there a link to the organisation's own risk mapping? Is internal audit focusing on what is easy to audit rather than what needs to be audited? When approving the audit plan, does the audit committee know what is **not** going to be audited?

- It is important to monitor whether the organisation is really doing something with the assessments made by internal audit. The speed with which management implements internal audit's recommendations is an indication of the value which it places on internal audit. More controls are not always the best option; better controls are. When management does not act properly or promptly on audit findings, the audit committee can invite managers to its meeting to understand why not. The organisation defence mechanism includes three lines of defence. It is therefore critical that the first and second lines of defence are properly assessed by internal audit, without duplicating the work of these other lines.

- In some organisations senior management or the board is expected to issue and publish an annual statement on internal control or an assurance declaration. It is important for the audit committee to know whether internal audit has had an independent review of this management reporting process or has been part of it.

Audit committee

Best practices

Risk management and internal control feature on the agenda of the audit committee.

The audit committee reports to the board of directors on the effectiveness of internal control and risk management systems based on information it acquires directly or with the assistance of the audit functions.

Good audit committee practices include a review of all lines of defence in an organisation, including their interaction.

Key points related to the performance of the audit committee

- Monitoring risk management, internal control and internal audit requires a considerable time commitment from the audit committee. Meetings alone may not be sufficient for comprehensive understanding and assurance. The audit committee needs to know how much effort, resources and budget are needed to perform as expected.

- To fulfil its responsibilities, the audit committee spends time assessing information provided by senior management, reviews major risks and critical processes each year, challenges senior management objectives about these items and benchmarks company practices.

- The work of the audit committee can only be valuable if sufficient time is allotted on the board agenda for the audit committee to present the results of its work. The audit committee should also feel that the board is taking appropriate action on its report.

- Leading audit committees have therefore their own performance and effectiveness assessed on an annual basis.

APPENDICES

Risk management

Introduction to enterprise risk management

Risk taking is inherent in exploiting business opportunities. However, it was often not clearly expressed in decision processes. Enterprise risk management (ERM) in business aims to manage risks to an acceptable level (that has been determined by the board of directors and the senior management). This is linked to developing the company, creating and sustaining value, and targeting its objectives successfully.

It includes the methods and processes used by organisations to manage risks and seize opportunities related to the achievement of their objectives. ERM provides a framework for risk management, which typically involves identifying particular events or circumstances relevant to the organisation's objectives (risks and opportunities), assessing them in terms of likelihood and magnitude of impact, determining a response strategy and monitoring progress. By identifying and proactively addressing risks and opportunities, business enterprises protect and create value for their stakeholders, including owners, employees, customers, regulators and society overall. It includes the external (regulatory, reputation, etc.), strategic (inherent to business model), financial, compliance and operational risks. Due to the globalisation of business, the interdependency between different risks has become an important element to be treated in the risk management process.

Being a key part of the governance structure of an organisation, ERM helps preserve value and augments decision-making by setting acceptable levels of risk appetite as well as embedding risk management in businesses planning and management processes. When embedded, it becomes part of the organisation's culture.

Global risk management standards

Most standards are broad guidelines that are applicable to all kind of organisations, but must be adapted to the organisation's characteristics, activities and culture. Current global standards include ISO 31000, COSO ERM and the FERMA Standard adopted from the UK.

Responsibility for risk management and reporting lines

In most organisations, there are risk management professionals at corporate and business level who are responsible for dissemination of the risk culture, general reporting, process and methodology. This should be regarded as good practice to improve risk management. However managing the business risks remains the duty of management along with its responsibility to meet business plans and targets.

Risk managers report to senior management as a staff function using routine risk management reporting processes. They may be part of a central function or embedded in the divisional structures. The risk management function reports either to a risk committee or to the audit committee.

Internal control

Introduction to internal control

Internal control has existed since ancient times. In Hellenistic Egypt there was a dual administration, with one set of bureaucrats charged with collecting taxes and another with supervising them.

Internal control is defined as a process effected by an organisation's structure, work and authority flows, people and management information systems, designed to help the organisation accomplish specific goals or objectives while minimising the likelihood that unwanted events will occur. It helps direct, monitor and measure the organisation's resources. It plays an important role in preventing and detecting fraud, protecting the organisation's resources and reducing adverse effects of liabilities.

Global internal control models

The COSO Internal Control-Integrated Framework is the most widely used framework. It defines internal control as a process, effected by an organisation's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following three categories: (a) Effectiveness and efficiency of operations; (b) Reliability of financial reporting and (c) Compliance with laws and regulations.

Responsibility for internal control and reporting lines

Ultimately, the responsibility for internal control lies with the board of directors. Through delegation of authority, operational management will be responsible for the development and maintenance of controls in its area of responsibility. For example, internal audit may be required by its organisation to provide an overall "control opinion" which concludes with an assessment/risk grading for the areas reviewed.

Many codes on corporate governance require senior management or the board of directors to report on the internal control system. This report should include details of non-compliance with rules and regulations, material weaknesses in internal control, financial adjustments and their materiality to the income statement of the organisation, and other risks and/or exposures that require changes to internal control.

Internal audit

Introduction to internal audit

The Institute of Internal Auditors (IIA) defines internal audit as "an independent, objective assurance and consulting activity designed to add value and improve an organisation's operations. It helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes".

Various national institutes of the internal audit profession around the globe cooperate and subscribe to this definition and are following the standards that are commonly developed.

Global internal audit standards

With its International Standards for the Professional Practice of Internal Auditing, the IIA provides for a worldwide, common understanding of the internal audit profession, including essential requirements of how to meet the expectations and responsibilities of the internal audit function and the internal auditors.

The Standards are principles-based, mandatory requirements consisting of statements of basic requirements for the professional practice of internal auditing and for evaluating the effectiveness of performance. These are internationally applicable at organisational and individual levels, and include interpretations that clarify terms or concepts stated in the Standards.

Responsibility for internal audit and reporting lines

The head of internal audit reports periodically to senior management and to the board or the audit committee on the internal audit activity's purpose, authority, responsibility and performance relative to its plan. The main reporting line is to the audit committee. The audit committee approves the annual audit plan, as well as reviewing the assessment of internal control and risk management systems.

External audit

The role of the external audit

The primary role of the external audit is to express an opinion on whether an organisation's financial statements are free of material misstatements. For a thorough assessment of the financial statements, the independence of the external auditors is crucial. Therefore, any relationship between external auditors and the organisation, other than retention for the audit itself, must be disclosed in the external auditor's report.

In order to provide a high level of assurance that the financial statements follow the appropriate basis of accounting, e.g. International Financial Reporting Standards (IFRS) or Generally Accepted Accounting Principles (GAAP), external auditors gather necessary evidence to issue the audit report.

Assessment of risk management and internal control

The external auditor's understanding of the company's risk management and internal control systems provides a basis both to plan the audit and assess control risk. Control risk is defined as the risk that material misstatements will not be prevented or detected by the client's internal control and is thus a key variable for external auditors to determine whether the client's internal control is effective. The external auditor's knowledge should, for example, include the relevant risks and design of controls to manage these risks, how they are defined and whether they have been placed in operation or not.

Cooperation with internal audit

Although external audit and internal audit have some complementary relationships, coordination of their activities is essential. Internal audit's evaluations of the internal control systems provide significant information for the external auditor's assessment of control/risk affecting the financial statements.

The ideal situation is when the external and internal auditors meet periodically to discuss their scope of work, methodology and audit coverage.

FERMA: www.ferma.eu

The Federation of European Risk Management Associations (FERMA) brings together 20 national risk management associations of 18 countries. It represents a wide range of business sectors from manufacturing to financial services, charities, health organisations and local government bodies. 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 biennial forum and a biennial benchmarking survey on the status of risk management in Europe. The results of this survey are presented at a seminar for all members.

ECIIA: www.eciia.eu

The European Confederation of Institutes of Internal Auditing (ECIIA) is the professional representative body of 33 national Institutes of Internal Audit in the wider European area. The ECIIA's objective is to support the position of internal audit professionals 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, briefing reports and a quarterly newsletter.

Contributors to this publication

Michel DENNERY: FERMA Board Member; Risk Management Director - GDF SUEZ

Marie Gemma DEQUAE: FERMA Board Member; Risk Manager - Partena Group; Director of Risk Management Research Platform - Vlerick Leuven Gent Management School

Jean-Pierre GARITTE: Former President ECIIA; former Chairman of the Board of the global Institute of Internal Auditors

Roland De MEULDER: Adviser to the managing board of ECIIA; former Chairman of the Internal Auditing Standards Board

Chantal PIERRE: Former Secretary ECIIA; former Secretary of the Board of the global Institute of Internal Auditors

Michèle F. RÜDISSER: Senior Lecturer in Organisational Control and Governance - University of St. Gallen

T. Flemming RUUD: Professor of Business Administration, in particular internal control / internal audit - University of St. Gallen

Paul TAYLOR: FERMA Board Member; Director of Risk Assurance - Morgan Crucible

FERMA

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

Tel: +32 2 761 94 31
Fax: +32 2 771 87 20
Email: info@ferma.eu

ECIIA

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

Tel: +32 2 217 33 20
Fax: +32 2 217 33 20
Email: office@eciia.org