ECIIA
EUROPEAN CONFEDERATION OF INSTITUTES OF INTERNAL AUDITING

Corporate Governance Insights

Reinforcing audit committee oversight
through global assurance

Our goal is to promote excellent corporate governance across the EU. The entire management board of ECIIA and its Public Affairs Committee combined forces and set out key principles that are expressed in this document. This is intended to help governing bodies and authorities to understand better the power of corporate governance if well structured, including the internal audit function. These principles are valid for both the public and private sectors.

I believe that priority must also be placed on providing knowledge and guidance that will in turn lead to valuable information for the boards and other governing bodies, as well as efficient dialogue between all bodies interested in risk and control.

For all these reasons, "internal governance before external regulation" and "not one size but fit for all" are the recurring themes that I back.

Carolyn Dittmeier
ECIIA President

The ECIIA is a confederation of national associations of internal auditing located in 36 countries, including all those of the EU, representing almost 40,000 internal audit professionals. As such, the ECIIA is an Associated Organisation of the global Institute of Internal Auditors (the IIA), a professional organisation of more than 170,000 members in some 165 countries. Throughout the world, the IIA is recognized as the internal audit profession's leader in certification, education and research, maintains the International Professional Practices Framework (IPPF), available in 29 languages, and other guidance. (http://www.theiia.org/guidance)

ECIIA Head Office in Brussels: Koningstraat
109-111, bus 5 - B-1000 Brussels, Belgium

Phone: +32 2 217 33 20 Fax: +32 2 217 33 20
Email: office@eciia.org Web: www.eciia.eu

Management Board

Carolyn Dittmeier (President)
Marie-Hélène Laimay (Vice President)
Kristina Bernotaite
Hans Joachim Busselberg
Philip Ratcliffe
Juan Ignazio Ruiz Zorrilla
Thijs Smit
Martin Stevens

Secretary General

Pascale Vandenbussche

Public Affairs Committee

Ruxandra Bilius
Alessandro Busetti
Roland De Meulder
Richard Nelson
Leen Paape
Ian Peters
Louis Vaurs
Norbert Wagner

Introduction

The ECIIA intends to provide useful guidance to help reinforce the audit committee's oversight capabilities, especially around global assurance[1], which is essential for governing bodies and stakeholders, and internal audit's role in for this purpose.[2]

This guidance integrates the work recently completed or in course with European Associations interested in corporate governance, including FERMA[3] and EcoDa[4], in relation to the implementation of Art. 41 of the 8th European Company Law Directive.[5]

Audit committee oversight must rely on an overarching, comprehensive structure that incorporates all elements of corporate governance, risk and control. Without an efficient structure, oversight itself is potentially a risk. That is why many organisations today struggle with duplicate control functions and inconsistent ways of communicating risk.

1 A comprehensive view of global risk management and internal control

Ensuring the effectiveness of an organisation's internal control and risk management systems is not a simple question of checking how good its compliance systems are. It is also crucial that the entity can also answer broader questions that are critical to the interests of the board, such as:

- How do organisational objectives support and align with the organisation's mission?
- Are significant risks identified and assessed in all areas of the organisation?
- Are risk responses appropriate, proportionate and aligned with the organisation's risk appetite?
- Are the controls responding to risks adequate and effective?
- Are responsibilities and the organisational structures clear enough to make risk mitigation effective?
- Is relevant risk information captured and communicated in a timely manner across the organisation, enabling staff, management, and the board to carry out their responsibilities?

Oversight and assurance is best placed to answer such questions when they are based on solid foundations. That entails every organisation adopting a single well-defined framework for their risk management and internal control systems.

All those involved in the assurance process should evaluate the risk management and internal control system in a comprehensive manner. A complete and cross-functional approach to evaluating risks constitutes a key element of the governance process and must:

- Ensure full coverage of all significant risks
- Identify risks on a global basis
- Ensure that these risks are clearly correlated to the entity's objectives
- Promote a proper and proportionate allocation of resources to the control functions dedicated to monitoring the risks based on their assessed importance.

The models applied in identifying risks must be exhaustive and not be conditioned by any excessive focus on specific regulatory or other specialized issues. In recent years, organisations have focused much attention on single risk areas, such as legal or financial issues high-lighted by the credit crunch, because regulation has been intense in those areas. But if organisations pursue this strategy, they can place disproportionate attention and allocation of resources on such risks.

The process for assessing risk must reside at entity level, and single organisational functions that are dedicated to the assessment of specialized risks must be placed within a single, enterprise risk process. This process must prioritise risks on the basis of their

[1] By global assurance, it is intended the means for obtaining independent and objective verification as to the adequacy of the global design and functioning of the risk management and internal control system.

[2] It should be noted that around 90% of corporate governance codes of the EU member states recognise Internal audit is an essential part of the corporate governance framework; this paper is intended to, among other things, ensure the effectiveness of Internal audit through the audit committee oversight process.

[3] ECIIA and FERMA (European Federation of Risk Manager Associations) issued joint Guidance on the 8th EU Directive regarding "Monitoring the effectiveness of internal control, internal audit and risk management systems", in two parts: "Guidance for Boards and Audit Committees", published on the 21st of September 2010 and "Implementing the 8th EU Company Law Directive Article 41 – 2b for Senior Management - Questions and Answers for Executive Committees" issued on the 14th of December 2011 , See: http://www.eciia.eu/about-us/news/press-conference-brussels-announcing-new-guidance-8th-eu-company-law-directive

[4] European Confederation of Directors' Associations.

[5] Art. 41 of the 8th European Company Law Directive (Directive 2006/43/EC states: "…the audit committee shall, inter alia: monitor the effectiveness of the company's internal control, internal audit where applicable, and risk management systems…".

correlation to the entity's objectives. In addition, it must consider the extent to which the combination of different risks potentially impact each objective, or on multiple objectives considered together.

The adoption of global systematic risk management processes, such as the Enterprise Risk Management (ERM)[6] framework, is intended to guarantee a structured approach for the identification and measurement of effective levels of risk in all areas of the organisation: from strategic risk, to those emerging in operational, financial and legal areas. ERM creates integrated and efficient internal governance. This framework is valid both in private and public sectors.[7] While ISO guidelines are also relevant and useful for implementing risk management processes, the ERM framework provides an unrivalled, comprehensive view of global risk management and internal controls.

The framework should be implemented so that it becomes embedded in management and control processes at all levels. This is achieved by establishing effective communication processes, and by integrating ERM into the planning and management reporting process via defined risk indicators and appropriate incentive systems.

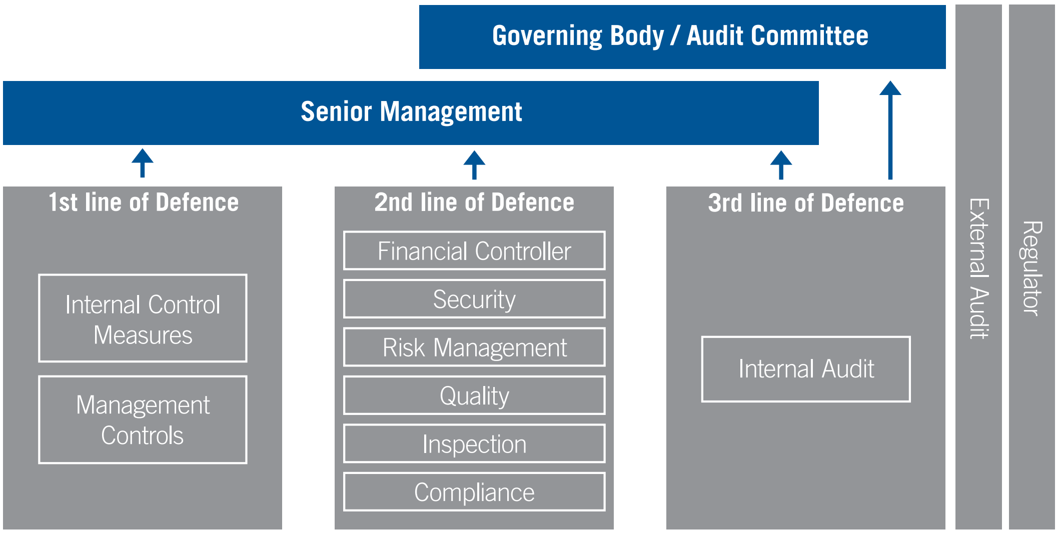
2 The Three lines of Defence model for global assurance

The ECIIA endorses the "Three lines of Defence" model by boards, or other governing bodies. In fact, the ECIIA considers this model to be essential for establishing clearly-structured corporate governance systems. The model is already widely adopted within the financial industry, but should be extended beyond that sector.

The "Three lines of Defence" structure is a valid conceptual delineation of control levels: line controls, second-level monitoring controls and third-line independent assurance.[8]

Under the first line of defence, operational management has ownership, responsibility and accountability for assessing, controlling and mitigating risks.

The second line of controls consists of activities covered by several components of internal governance



[6] Enterprise Risk Management (ERM)- Integrated Framework - Committee of Sponsoring Organisations of the Treadway Commission, September 2004.
[7] ERM was adopted by INTOSAI, the standards setting body for the public sector external auditors.
[8] The graph notes information flow on risk and control aspects to senior management and the governing bodies, not to be construed as organisational reporting lines.

Effective Internal Audit:

- Internal auditing should be properly structured and should be required for all organizations where there is a public interest.
- Reporting lines for the chief audit executive should enhance organizational independence.

(compliance, risk management, quality and other control departments). This line of defence monitors and facilitates the implementation of effective risk management practices by operational management and assists the risk owners in reporting adequate risk-related information up and down the organisation.

Efficient and effective interaction between these components is also essential for a truly effective internal control system. That is because it impacts significantly the overall control environment, as well as establishing the essential element of proper and efficient communication and information flow through the organisation.

As the third line of defence, an independent internal audit function will, through a risk-based approach to its work, provide assurance to the organisation's governing body and senior management. This assurance will cover how effectively the organisation assesses and manages its risks and will include assurance on the manner in which the first and second lines of defence operate. This assurance encompasses all elements of an organisation's risk management framework: from risk identification and assessment processes to the internal control system as a response to mitigating risks; this includes communication throughout the organisation and to senior management and the governing body of risk-related information.

Organisations need clear accountability for risk

Organizational management is responsible for designing and operating an effective system of risk management and internal control. The "three lines of defence" model provides valid guidance on clear accountability for risk management and internal control.

While the above-mentioned functions operate within the organisation, the statutory, or external, auditor contributes as an outside body, providing assurance regarding the true and fair view of an organisation's financial statements. It can also be seen as an outside check on internal governance functions, including possible observations on the effective implementation of the three lines of defence model.

3 Internal audit and global assurance

Internal audit evaluates the internal governance mechanisms of the enterprise through a comprehensive and integrated approach. It takes into account the risk factors that allow it to strategically plan an adequate coverage of the entity's processes in relation to diverse control objectives, consistent with the needs of global enterprise-level risk management:

- Strategic
- Operational
- Reporting
- Compliance and fraud.

In the context of the ERM framework, the internal audit function provides independent assurance. This is designed to help the enterprise develop a sound and reliable internal control system and ensure that business operations are effectively functioning to contain the risks in accordance with risk strategy and governance objectives.

Of course, in order to achieve this, internal audit must be independent and have adequate resources available, supporting both efficient and effective audit planning and management. Criteria to enhance independence and ensure the adequacy of the internal audit function are provided in the Annex.

Internal audit activity results in systematic improvements to the internal governance (risk management and internal controls) of the organisation. This can be reviewed by governing bodies by, for example, assessing the:

- Significance of risks mitigated through the implementation of audit recommendations
- Significance of audit recommendations
- Proportion of audit recommendations implemented within an acceptable time frame by management.

This information can be reported to the audit committee or governing bodies in addition to audit risk assessments, plans and reports on overall audit activity, as they are normally provided by internal audit.

4 Ensuring proper distinction between internal audit assurance and statutory and external audit assurance

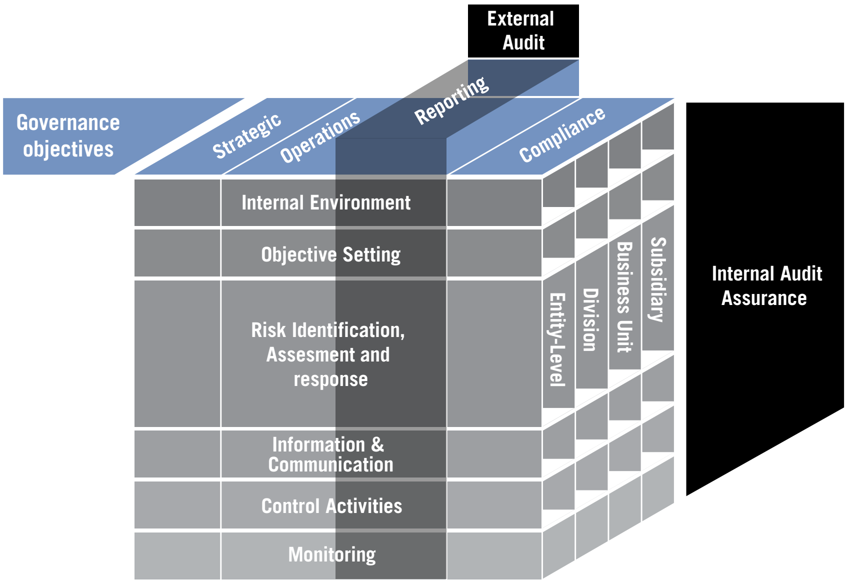
Significant attention has understandably been placed on the reliability of the system of external or statutory audit of listed companies and public entities. This clearly forms a key source of information and assurance for shareholders, lending institutions, potential investors and stakeholders in general. Less specific attention has been placed on the internal reporting processes, both financial and operational, that form the basis for the board and senior management to make proper and timely strategic decisions.

The external or statutory auditor performs limited work to assess to assess the internal control environment and financial reporting processes. These are directed at planning and executing its examination of the financial statements. The internal auditing function's role is much wider. It examines all processes that provide assurance to the audit committee and board that underpin the reliability of internal communication and information. This information is typically pervasive and formulates the basis for the strategic and operational decisions of management at all levels up to and including the board. Assurance can include:

- Budgetary management reporting
- Risk reporting
- Operational performance reporting
- Operational processes underlying accounting and reporting
- IT processes which, in complex environments, must ensure proper integration of diverse databases and systems.

In environments in which financial reporting processes are not highly integrated with operational or management control processes, circumstances can arise in which the financial reports directed to

Enterprise risk management and assurance:



shareholders and investors are successfully audited by the statutory auditor while internal reporting mechanisms are defective or untimely. The need to ensure the strength and reliability of the strategic decision-making process of the board is thus equally important to the financial reporting process.

For this reason, the audit committee should obtain an understanding of the assurance role of internal audit over those information processes that do not pertain strictly to financial reporting. It should also ensure a proper distinction is made between the financial auditing carried out by statutory auditors, and the internal auditing of all other control objectives.

Ample standards and guidelines exist that explain how an external auditor may utilise internal audit work.[9] The assurance provided over the overall internal control/risk management framework by internal audit creates an important foundation for the statutory auditor. This work also allows the external auditor to appreciate the strong points of the organisation and to address the implications of significant weaknesses that could impact financial reporting processes.

Regular dialogue between the statutory auditor, audit committee and internal audit as regards the latter's activity and findings will automatically reinforce the strength of the assurance process.

The internal audit function should not be used to perform specific procedures for the statutory auditor, as it generally detracts from internal audit's ability to ensure the aforementioned scope of assurance over broad governance objectives in the presence of limited resources.

[9] For example, standards and guidance of the International Auditing and Assurance Standards Board (IAASB): International Standard on Auditing (ISA) 610 "Using the Work of Interal Auditors", February 2009.

Annex

Ensuring the adequacy of the internal audit function

The positive value of internal audit depends, of course, on its own quality structure or performance. This justifies the importance the Directive places on the oversight role of the audit committee. Criteria applicable to this oversight process include:

- The effective independence of the internal audit function. The independence of an internal audit function from operational and control functions is essential to guarantee its effectiveness through objectivity and insight.
- The completeness of the mandate of internal audit as approved by the board. Among other things, internal auditing should have full, free and unrestricted access to any function or activity under review. No organisational function or activity should be considered to be outside the scope of review by internal auditing.
- The management of the internal audit function in accordance with IIA Standards; Adoption of The IIA's International Standards for the Professional Practice of Internal Auditing should be mandatory for conducting internal audit work.
- The implementation and results of the quality assurance review process[10] required by the International Standards (IPPF), including the external assessment every five years by assessors qualified under IIA standards. The competency of the chief audit executive ("fit and proper"), requiring strong leadership capability in addition to technical and communication skills.
- The adequacy of resources, both human and technical, including diversity of professional competencies and the certification process of internal auditors conducted by the IIA.[11]

Reporting lines for the chief audit executive should enhance organisational independence In order to ensure the effective independence of the internal audit function:

- The chief audit executive should report to a level within the organisation that allows the internal audit activity to independently fulfil its responsibilities.
- Hiring, remuneration, and dismissal of the chief audit executive should be a decision reserved to the governing body.
- The audit committee or board, or similar governing body, on the recommendation of the chief audit executive or executive committee, should approve the scope and budget of internal auditing.
- Key issues raised by internal auditing should be reported to the audit committee.
- The audit committee should meet at least annually with the chief audit executive without the presence of management.

The above points are illustrative and not necessarily exhaustive, to be fully covered through separate guidance.

[10] Issued by the Institute of Internal Auditors, global body of the profession.

[11] CIA-Certified Internal Auditor, CIIA – Chartered Internal Auditor, CFSA-Certified Financial Services Auditor, CGAP-Certified Government Auditor, CCSA Certified Control Self Assessment and CRMA-Certified Risk Management Auditor.

Our mission

- To be the consolidated voice for the profession of internal auditing in a widely defined Europe by promoting sound corporate governance with the European Union, its Parliament and Commission and other European or global institutions.
- To promote corporate governance and the profession in economically emerging countries, as appropriate, within the wider geographic area of Europe and the Mediterranean basin.
- To promote the mission of the Global IIA.

IIA Austria	www.internerevision.at
IIA Azerbaidjan	www.audit.gov.az
IIA Belgium	www.iiabel.be
IIA Bosnia and Herzegovina	www.interni-revizori.info
IIA Bulgaria	www.iiabg.org
IIA Croatia	www.hiir.hr
IIA Cyprus	www.iiacyprus.org.cy
IIA Czech	www.interniaudit.cz
IIA Denmark	www.iia.dk
IIA Estonia	www.theiia.org/chapters
IIA Finland	www.theiia.fi
IIA France	www.ifaci.com
IIA Germany	www.diir.de
IIA Georgia	www.theiia.org/chapters
IIA Greece	www.theiia.org/chapters
IIA Hungary	www.iia.hu
IIA Iceland	www.fie.is
IIA Italy	www.aiiaweb.it
IIA Latvia	www.iai.lv
IIA Lithuania	www.theiia.org/chapters
IIA Luxembourg	www.theiia.org/chapters
IIA Montenegro	www.iircg.co.me
IIA Morocco	www.theiia.org/chapters
IIA Netherlands	www.iia.nl
IIA Norway	www.nirf.org
IIA Poland	www.iia.org.pl
IIA Portugal	www.ipai.pt
IIA Romania	www.aair.ro
IIA Serbia	www.theiia.org/chapters
IIA Spain	www.iai.es
IIA Sweden	www.internrevisorerna.se
IIA Switzerland	www.svir.ch
IIA Tunisia	www.iiatunisia.org.tn
IIA Turkey	www.tide.org.tr
IIA UK & Ireland	www.iia.org.uk

European Confederation of Institutes of Internal Auditing
Koningsstraat 109-111 Bus 5
BE – 1000 Brussels, Belgium.
www.eciia.eu