EUROPEAN CONFEDERATION OF INSTITUTES OF INTERNAL AUDITING (IVZW)

Phil Tarling
PRESIDENT

Carolyn Dittmeier
VICE PRESIDENT

Head Office: c/o IIA Belgium – 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

Re: CP44

Brussels, 13 January 2011

Dear Sirs,

The ECIIA (the European Confederation of Institutes of internal Auditing) would like to thank the European Banking Authority (the EBA) for offering the opportunity to comment on its Consultation Paper No. 44 "The Guidebook on Internal Governance". We are pleased to participate in the consultation of this important guidance, aimed at enhancing and consolidating supervisory expectations in order to improve the sound implementation of internal governance arrangements in financial institutions.

.

The ECIIA is a confederation of national associations of internal auditing located in 35 countries, including all those of the EU, representing over 35000 internal audit professionals. As such, the ECIIA is an Associated Organisation of the global Institute of Internal Auditing (the IIA), a professional organisation of more than 170000 members in some 165 countries. Throughout the world, the Global IIA is recognised as the internal audit profession's leader in certification, education and research regarding internal auditing. The Global IIA also maintains the International Professional Practices Framework (IPPF), which includes the *International Standards for the Professional Practice of Internal Auditing* (available in 29 languages), the definition of internal auditing, the code of ethics, practice advisories and other guidance. (http://www.theiia.org/guidance/standards-and-guidance/interactive-ippf/).

This worldwide organisational structure and globally recognised guidance framework for our profession allows the ECIIA to provide you with some comments on

- internal auditing's contribution to effective internal governance;
- internal auditing's interaction with other controlling functions**,** such as the risk management function and the compliance function, as referred to in the Guidebook.

The ECIIA understands that the goal of this consultation paper is to consolidate and update all the existing EBA/CEBS guidelines on internal governance in the present Guidebook whose principles are directly aimed at a sound implementation of internal governance. As such, the ECIIA welcomes the initiative of the EBA and would like to constructively comment on some specific paragraphs and principles of the Guidebook.

Paragraph 19

The ECIIA believes that the statement “the management body should rely on the work of control functions” may assume that the control functions carry some responsibility in that regard. The ECIIA would recommend rephrasing the sentence like “the management body should be able to rely ...”

Principle 7 – Composition, appointment and succession

The ECIIA believes it is a best practice for an organisation to periodically assess its management for each position in order to provide continuity in the conduct of business (the so called ‘management replacement matrix’).

Principle 10 – Organisational functioning

The ECIIA believes that each member of the management body should receive timely clear and sufficient documentation relevant to issues to be discussed in the meeting, in order to guarantee full information and awareness of problems to be discussed.

The ECIIA believes it would be beneficial to refer in § 75-77 to the full scope of activities of the audit committee, as referred to in Art. 41 of Directive 2006/43/EC, as this scope relates directly to the three key areas within the internal governance area: internal control, risk management and internal audit.

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

Principle 11 – Corporate values and code of conduct

The management body should receive on a regular basis information on the effective implementation and respect of the code of conduct within the organisation.

Principle 12 – Conflicts of interest at institution level

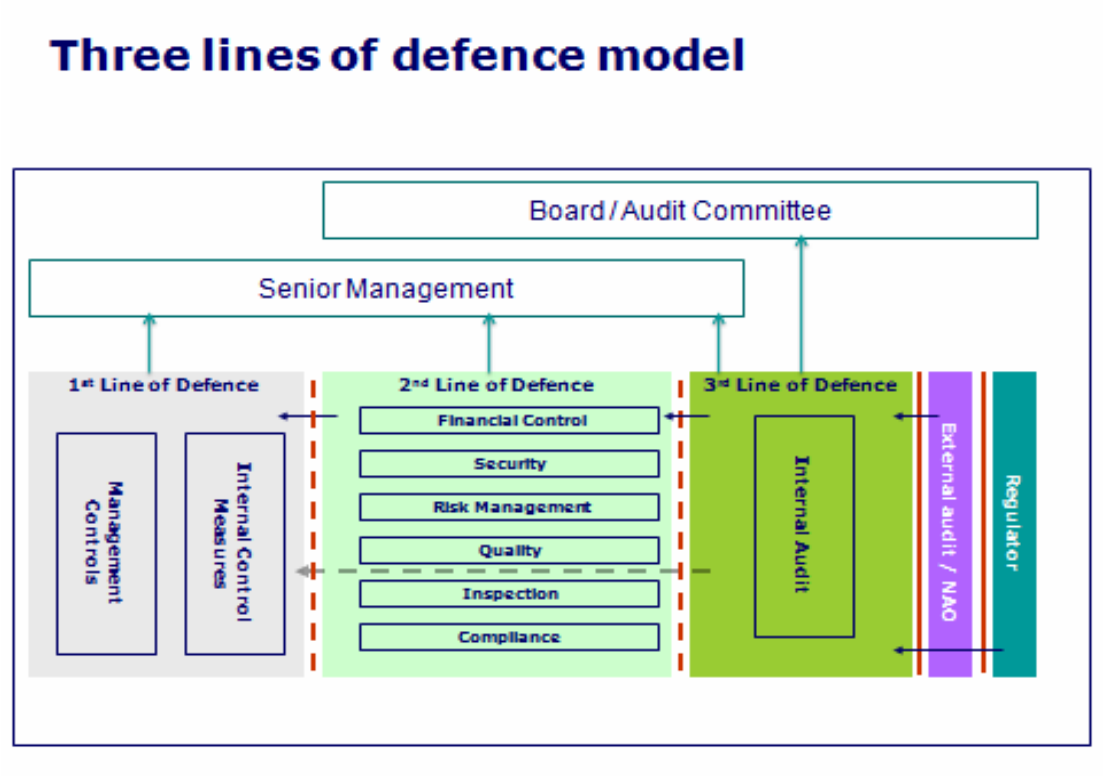
The ECIIA believes that significant suppliers/partners and government officials should be considered in the list of relationships within a code of conduct as defined in § 81.

The ECIIA also recommends to extend the conflict policy to transactions with related parties (see §130).

Principle 21 – Internal control framework

To effectively assume its duties, the management body will seek assurance from various sources both within and outside the institution. Regarding internal sources of assurance, the ECIIA fully supports the “Three Lines of Defence” (3LoD) - model as a benchmark for internal governance guidance. This model, which is rapidly gaining universal recognition, was also presented by one of the panellists at a seminar organised by the European Commissionin October 2009 on *“Corporate Governance in Financial Institutions / Panel 2: Governance issues related to Internal Control and Risk Management”* (http://webstream.ec.europa.eu/scic/markt/091012/day1or-2.wmv)

The 3LoD - model can be illustrated as follows:



- As a **first line** of defence, the institution’s operational management has ownership, responsibility and accountability for assessing, controlling and mitigating risks.

- As a **second line** of defence, the risk management function, compliance function and similar functions facilitate and monitor the implementation of effective risk management practices by operational management and assist the risk owners in reporting adequate risk related information up and down the institution.

- As a **third line** of defence, the internal auditing function will, through a risk based approach, provide assurance to the institution’smanagement body, on how effective the institution 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

institution's risk management framework: i.e. from risk identification, risk assessment and risk response to communication of risk related information.

While the above mentioned functions operate within the organisation, the external auditor contributes as an outside body, providing assurance regarding the true and fair view of an organisation's financial statements.

This three lines of defence model has been increasingly applied to corporate governance, and particularly risk management, over recent years. The ECIIA finds that it is a useful tool to explain and demonstrate the different roles in internal governance and the interplay between them. It also forms the basis of a recent paper, jointly issued by ECIIA and the Federation of European Risk Management Associations (FERMA) on "Guidance for boards and audit committees on the implementation of Art 41. 2 of the 8th Directive" (see separate attachment). As such, the ECIIA proposesto integrate the three lines of defence model in the EBA's Guidebook on internal governance to clarify the various roles and interactions.

Principle 26 – Internal Audit function

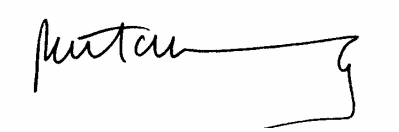
The internal audit function is considered universally as a key player in the internal governance framework. The ECIIA believes that, in order to recognise this key role, principle 26 could be further elaborated in order to emphasise:

- The independence of the internal audit function, having a dual reporting line to both the supervisory and management components of the institution's management body;
- The professionalism of the internal audit function in accordance with universally recognised standards and ethics rules issued by the Institute of Internal Auditors, institute already referred to in this document (http://www.theiia.org/guidance/standards-and-guidance/interactive-ippf/);
- The mandate of the internal audit function to review and assess both the first line of defence (internal control measures implemented and monitored by operational management) and the second line of defence (the risk control/management and compliance functions);
- Internal audit function is a valuable source of information to help management with Principle 16 - Assessment of the internal governance framework;
- The mandate of the internal audit function to includeevaluating the effectiveness of the management of risks related to information systems, communications, business continuity and fraud in their scope;
- The Quality Assurance Review programme that covers all aspects of the internal audit functionand requires an external review every five years.

The ECIIA would be happy to assist the EBA in the further developing of this principle. Given the mandate of internal audit to assess the first and second lines of defence, its value in providing information to help assess the internal governance framework and the scope of its work to include information systems and business continuity, etc, the ECIIA recommends that internal auditing is dealt with in a separate chapter in the Guidebook rather than a principle covered under the Internal Control chapter.

Once again, the ECIIA would like to thank the European Banking Authority for offering us the opportunity to participate in this consultation, and is offering to assist you in developing future recommendations and/or regulatory measures in this respect.

Sincerely,



Phil Tarling

President ECIIA

Attachment: ECIIA/FERMA guidance for boards and audit committees