Comments from ECIIA on European Banking Authority

Consultation Paper EBA/CP/2015/03

Draft Guidelines

on sound remuneration policies under Article 74(3) and 75(2) of Directive 2013/36/EU and disclosures under Article 450 of Regulation (EU) No 575/2013

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

Web: www.eciia.eu
TR : 849170014736-52

The ECIIA (the European Confederation of Institutes of Internal Auditing) would like to thank you for offering the opportunity to comment on the

Consultation Paper on the

Guidelines on sound remuneration policies', built on the 'Article 74(3) and 75(2) of Directive 2013/36/EU and disclosures under Article 450 of Regulation (EU) No 575/2013'.

The European Confederation of Institutes of Internal Auditing (ECIIA) is a confederation of national associations of internal auditors speaking for the profession in the wider geographic area of Europe and the Mediterranean basin. It represents a membership base of over 40,000 internal audit professionals. The ECIIA is an associated organisation of the global Institute of Internal Auditors (The IIA), a professional body with more than 181,000 members in some 190 countries. Throughout the world, The IIA is recognised as the internal audit profession's leader in certification, education and research regarding internal auditing. The IIA also maintains the International Professional Practices Framework (IPPF) which includes the *International Standards for the Professional Practice of Internal Auditing,* the definition of internal auditing, the code of ethics, practice advisories and other guidance. (http://www.theiia.org/guidance/standards-and-guidance/interactive-ippf/.)

The ECIIA welcomes the strengthening of guidance on the role of the board of directors, the board's collective competencies and obligations, and the specific tasks of management, control functions, and internal audit and the other assurance functions. However, as the EBA's document will represent an important point of reference for the banking sector in Europe, it is essential to have a common view and understanding of how risk management should work. Under the Three Lines of Defence model, outlined below, internal audit operates as the third line of defence and its role differs significantly from the control functions of the second line.

In the footnote to paragraph 26, and in paragraph 99, the Paper describes the Independent control functions as comprising risk management, compliance and internal audit functions. The task of the internal audit function is NOT to control, but (working alongside others) to AUDIT the control functions, giving assurance to the Board and Supervisory Bodies. Therefore, it is vitally important to distinguish clearly between the second and the third line of defence and their different roles and dependencies.

Unfortunately, the consultative document reflects an important inconsistency in the EBA Guidelines on Internal Governance, EBA GL 44, which needs to be corrected. Paragraph 35 of the executive summary of EBA GL 44 includes internal audit as one of the control functions, as do the guidelines themselves. For example paragraph D.24.4 confuses the internal control framework, which includes internal audit, with internal control functions, which do not. Paragraph 14.9 gets it right "An audit committee (or equivalent) should, inter alia, monitor the effectiveness of the company's internal control, internal audit, and risk management systems". So too does paragraph 29.3, which defines the role of the Internal Audit function (IAF) as follows: "The IAF should evaluate the compliance of all activities and units of an institution (including the RCF and Compliance function) with its policies and procedures.

Therefore, the IAF should not be combined with any other function." This definition is in line with the Three Lines of Defence model.

The Three Lines of Defence model is an internationally recognised and valuable tool in understanding the different roles played in the governance and management of risk. It can be illustrated as follows:

- As a first line of defence, the organisation's operational management has ownership, responsibility and accountability for assessing, controlling and mitigating risks.
- As a second line of defence, the risk management function (and also other supporting functions like compliance, quality management, controlling) facilitates and monitors 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.
- As a third line of defence, the internal auditing function will, through a risk based approach, provide assurance to the organisation's board and senior management, on how effective 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. from risk identification, risk assessment and response, to communication of risk related information.

It is essential to reflect that internal audit is the only function for the Board, independent of management, that can oversee all other functions (first and second lines). This is not always the case in the current draft as the control functions (risk and compliance) in some paragraphs are presented at the same level as internal audit. The ECIIA would therefore request that the draft be amended throughout to reflect this concern.

The ECIIA would also request that the EBA, in its review of governance next year, takes account of the issues raised under this consultation and amends those areas of EBA GL 44 where the role of internal audit is misrepresented.

Once again, the ECIIA would like to thank you for offering the opportunity to participate in this debate. We are always interested and willing to take part in future consultations and would like to discuss about these comments during a meeting.

Sincerely,

Henrik Stein
Board member

Thijs Smit
President

Below, we have prepared a first draft of the detailed comments

Page	Text of consultation paper	Suggested version (plus rationale given)
27	26. The supervisory function should take into account the input provided by all competent corporate functions and bodies (e.g. committees, control functions [10], human resources, legal, strategic planning, etc.) and business units about the design, implementation and within the oversight of the institution's remuneration policies. 10 Independent control function comprises organisational units, independent of the business and corporate functions that are responsible for controlling and monitoring the operations and risks arising from those operations, ensuring compliance with all applicable laws, rules and regulations and advising the management functions on the matters within their area of expertise. Independent control functions typically comprise risk management, compliance and internal audit functions. Further details on control functions, can be found in the EBA Guidelines on Internal Governance (GL44), points 27 to 29.	26. The supervisory function should take into account the input provided by all competent corporate functions and bodies (e.g. committees, control and assurance functions [10], human resources, legal, strategic planning, etc.) and business units about the design, implementation and within the oversight of the institution's remuneration policies. 10 Control function comprises organisational units that are responsible for controlling and monitoring the operations and risks arising from those operations, ensuring compliance with all applicable laws, rules and regulations and advising the management functions on the matters within their area of expertise. Control functions typically comprise risk management and compliance functions. Independent assurance functions are independent of the business and corporate functions and typically include internal and external audit. **Rationale:** Instead of referring to the inconsistency in GL44 it is essential to reflect that internal audit is the only function for the Board that can oversee all other functions and as such no control, but an assurance function.
34	58. The internal control functions should be independent and have sufficient resources, knowledge and experience to perform their tasks with regard to the institutions' remuneration policy. The independent control functions should cooperate actively and regularly with each other and other relevant functions and committees with regard to the remuneration policy and risks which may arise from remuneration policies.	58. The functions within the internal control framework should ~~be independent and~~ have sufficient resources, knowledge and experience to perform their tasks with regard to the institutions' remuneration policy. They ~~independent~~should cooperate actively and regularly with each other and other relevant functions and committees with regard to the remuneration policy and risks which may arise from remuneration policies. **Rationale:** The required degree of independence varies between the typical control functions risk

		management, compliance on the one hand and internal audit on the other hand. For internal audit functions these are outlined in the international standards (IIA) and the code of ethics.
35	99. The internal control functions (i.e., internal audit, independent risk management and independent compliance functions), the business support functions (e.g. legal, human resources) and the relevant committees of the management body (i.e., risk, nomination and audit committees) should be properly involved in the identification process, also on an ongoing basis. In particular where a risk committee is established, it should be involved in the identification process without prejudice to the tasks of the remuneration committee. Institutions should ensure a proper exchange of information among all internal bodies and functions involved in the identification process.	99. The internal control functions (~~i.e., internal audit, independent~~ risk management and ~~independent~~ compliance functions), the business support functions (e.g. legal, human resources) and the relevant committees of the management body (i.e., risk, nomination and audit committees) should be properly involved in the identification process, also on an ongoing basis. In particular where a risk committee is established, it should be involved in the identification process without prejudice to the tasks of the remuneration committee. The internal audit function should not have an active role in the identification process, in order to minimise potential conflicts of interest in performing the central independent review. Institutions should ensure a proper exchange of information among all internal bodies and functions involved in the identification process. **Rationale:** Having an active role in the identification process exposes the internal audit function to potential conflicts of interest in the central independent review of the policy and practices.
44	205. Where control functions' staff receive variable remuneration, it should be appraised and the variable part of remuneration determined separately from the business units they control, including the performance which results from business decisions (e.g. new product approval) where the control function is involved. 206. The criteria used for assessing the performance and risks should be exclusively based on the internal control functions'	205. Where staff of functions in the control framework receive variable remuneration, it should be appraised and the variable part of remuneration determined separately from the business units they control, including the performance which results from business decisions (e.g. new product approval) where the control function is involved. 206. The criteria used for assessing the performance and risks should be exclusively based on the control framework functions' respective objectives. Variable remuneration

	objectives. Variable remuneration for control functions should exclusively follow from control objectives, e.g. the Tier 1 ratio, the non-performing loan ratio, the non-performing loan recovery rate, or audit findings. Their variable remuneration should not be based on market-oriented business objectives, e.g. earnings, return on equity, loan or balance sheet growth. The institution should consider to set a significant lower ratio between the variable and the fixed components of remuneration for control functions compared to the business units they control.	for control framework functions should exclusively follow from their objectives. ~~e.g. the Tier 1 ratio, the non-performing loan ratio, the non-performing loan recovery rate, or audit findings~~ Their variable remuneration should not be based on market-oriented business objectives~~, e.g. earnings, return on equity, loan or balance sheet growth~~. The institution should consider to set a significant lower ratio between the variable and the fixed components of remuneration for those functions compared to the business units they control. **Rationale** It is very important to disconnect variable remuneration of control framework functions from front office performance. The criteria used for assessing the performance and risks should be exclusively based on the functions' objectives. However, the mentioned examples of objectives would potentially create conflicts of interest for the respective functions. The criteria have to be closely linked to the actual performance (quality and quantity) of the function. For the internal audit function, they should not be linked to the audit results and qualification of staff.
63	229. Institutions should make qualitative ex-ante risk adjustments when determining the bonus pool and staffs' remuneration through e.g. the use of balanced scorecards that explicitly include risk and control considerations such as compliance breaches, risk limit breaches and internal control indicators (e.g. based on **internal audit results**) or other similar methods.	229. Institutions should make qualitative ex-ante risk adjustments when determining the bonus pool and staffs' remuneration through e.g. the use of balanced scorecards that explicitly include risk and control considerations such as compliance breaches, risk limit breaches and internal control indicators (e.g. based on **internal ~~audit~~ control results**) or other similar methods. **Rationale** The risk and control considerations should include the results of all internal control functions.