POSITION PAPER

INTERNAL AUDIT'S ROLE IN GOOD GOVERNANCE

ENHANCING GOVERNANCE THROUGH INTERNAL AUDIT

2

ABOUT ECIIA

The European Confederation of Institutes of Internal Auditing (ECIIA) is the professional representative body of 35 national institutes of internal audit in the wider geographic area of Europe and the Mediterranean basin. The mission of ECIIA is to be the consolidated voice for the profession of internal auditing in Europe by dealing with the European Union, its Parliament and Commission and any other appropriate institutions of influence.

The primary objective is to further the development of corporate governance and internal audit through knowledge sharing, key relationships and regulatory environment oversight.

CONTENTS

ECIIA Head Office:

c/o IIA Belgium
Koningsstraat 109-111
Bus 5, BE–1000
Brussels, Belgium

Phone: +32 2 217 33 20
Fax: +32 2 217 33 20
TR: 849170014736-52

www.eciia.eu

3

INTRODUCTION

ECIIA set up a Banking Committee in 2015 with Chief Audit Executives of European Central Bank Supervised Banks[1]. See the European Central Bank website for a full list of supervised entities.

The mission of the ECIIA Banking Committee is:

"To be the consolidated voice for the profession of internal auditing in the Banking Sector in Europe by dealing with the European Regulators and any other appropriate institutions of influence and to represent and develop the Internal Audit profession and good Corporate Governance in the Banking Sector in Europe"

The paper describes best practice from the practitioners, but it is important to note that, depending on the culture, size, business and local requirements, other options are possible.

Thesis

Internal control is an important cornerstone for banks' long-term sound governance. It should be tailored to the business model, risks and organisational structure.

As risks are more and more complex, there are several functions involved in the implementation and the evaluation of an internal control system. However, it is important to stress the distinctive contribution of internal audit functions. Indeed, as the third line of defence, reporting to senior management and the board, internal audit gives an overall assurance on internal control effectiveness including an independent review of risk and control functions as well as insights on efficiency.

Background

A bank's internal control system is, with its risk governance, one of the two components[2] of its governance framework. There are several functions involved in risk mitigation, reporting and communicating to senior management and the board. Clear accountability of each function must be established with reference to the three lines of defence model:

- Under the first line of defence, operational management has ownership, responsibility and accountability for assessing, controlling and mitigating risks as well as executing corrective actions.
- The second line of defence consists of several functions (compliance, risk management, controllership and other functional departments) that monitor and facilitate the implementation of effective risk mitigation by operational management. These functions support ongoing controls including the industrialisation of automated controls.
- As the third line of defence, an independent internal audit function provides, through a risk-based approach, assurance to the organisation's board and senior management on the quality, consistency and effectiveness of a bank's internal control, risk management and governance systems including the adequacy of the first and second lines of defence.

The design and the implementation of internal control within this organisational structure are under the scrutiny of the board and senior management. For these oversight responsibilities, they can rely on internal audit, whose strategic role is recognised in regulatory and professional requirements. Among other things, internal audit is the best placed to enhance transparent accountability.

[1] Chief Audit Executives from DZ Bank AG, Crédit Agricole SA, ABN AMRO, Grupo Santander, UniCredit S.p.A., KBL European Private Bankers, Nordea, National Bank of Greece.

[2] The other component being the remuneration framework as stated in GL44 from EBA.

4

FUNDAMENTALS

To achieve their mission regarding the efficiency and effectiveness of internal control and for greater added value, internal auditors need clear specification and recognition of:

Internal audit's strategic and distinctive role

To avoid any confusion, it should be explicitly stated that within the 'risk and control functions', internal audit has a unique input:

- It provides an independent and objective assurance to the highest level of the institution. It gives to board and senior management insights about the overall internal control system at the entity, activity and transaction levels. Through its comprehensive approach, internal audit challenges the risk-taking environment, the resource and competence in place with respect to the institution's vision, and even the integrity of the methods and techniques.
- Unlike other lines of defence, internal audit is not involved in designing, selecting, establishing and implementing specific internal control policies, mechanism and procedures and risk limits.
- More than just attesting the execution of a specific rule or procedure, internal auditors assess the design adequacy, operating effectiveness, compliance, efficiency, accuracy and transparent reporting of internal controls as regarding the bank's risk profile and strategies.

Therefore, the internal audit function should be particularly well positioned to have a clear understanding of the organisation mission, vision, strategy and long-term goals (cf. Basel Committee principles regarding internal audit). Internal audit should not be combined nor merged with any other function.

Responsibilities of the parties involved in the system of internal control

Internal audit role must be sustained by:

- A documentation of the respective responsibilities of relevant board committees (Audit Committee and Risk Committee) regarding the system of internal control, their coordination and the interaction with the Chief Audit Executive.
- Clear accountability of each line of defence regarding the control environment (cf. EBA guidance on internal governance). Some organisations choose to formalise these roles in a charter and/or an assurance map.
- Interactions between the second and third line of defence allowing optimal scope coverage. For example:
  - Coordination between the second line of defence functions could be organised within a committee chaired by an executive senior manager who takes decisions for the improvement of internal controls. In participating in this committee, the Chief Audit Executive can give some advice but doesn't take part in decisions to avoid being judge and jury.
  - Internal audit reliance on other risk and control functions. After an independent assessment of their effectiveness, the Chief Audit Executive can decide to rely on some works from the second line of defence functions to reduce internal audit routine and permanent engagements and to enhance its risk-based approach.
  - Leveraging first and second lines of defence remote and continuous controls, as well as mass data analysis, provided that the reliability of the process and of data is confirmed. Even so, internal auditors are not expected to use these tools on a day-to-day basis.
  - Additional work to enhance the level of reliance. When the Chief Audit Executive judges that he cannot rely on other parties' work due to insufficient objectivity (conflict of interest, inadequate reporting relationship), competencies, methodology (from the planning stage) or reliable and relevant evidence, he is entitled to plan additional works.
- Cooperation and mutual information sharing between internal audit and external audit, for example about the relevance of accounting methods as regarding safety and prudence objectives, for instance IFRS 9 and hedge accounting. Nevertheless, the outsourcing from external audit to internal audit is forbidden.

Scope and scale of internal audit evaluation

Internal audit assessment of internal control is not limited to administrative and accounting procedures but covers a broad scope (principles, policy, structure, reporting and control framework including the first and second lines of defence). In assessing organisational culture, structure, resources, tools, method and reporting, internal audit reviews several aspects such as:

- the adequacy of the institution's governance framework in achieving its strategic objectives;
- the design of policies and procedures in compliance with mandatory requirements, relevant internal decisions and risk appetite;
- the quality and efficiency of internal controls implemented by the first and the second lines of defence as well as their risk mitigation escalation process as regarding the bank's strategy including its risk appetite.

In doing so, internal audit provides reliable assurance and insight about the achievement of the bank's operational, reporting and compliance objectives at the entity, activity and transaction levels.

Internal audit risk-based approach

To determine the priorities of the internal audit function regarding the internal control system, the Chief Audit Executive develops a risk-based plan. He considers inputs from senior management and the board and obtains an understanding from the organisation's strategies, key business objectives, trends and emerging issues that could impact the organisation. As part of this planning, internal audit needs to have a continuous and unfettered access to relevant committees and resources to cover a broad scope (risk and compliance functions, key issues linked to the business model including outsourced services, IT (cybersecurity, big data, mobile devices)). At the engagement level, internal auditors use adequate evaluation criteria such as internal policies and procedures, external legal and regulatory requirements, and leading industry-specific or professional practices.

Independence of internal audit, to evaluate risk and control functions effectiveness

This assessment includes organisational structure, resources, tools, method and reporting aspects as well as the proper coordination with other lines of defence functions to allow an effective coverage of the institution's risks. Through its comprehensive approach, internal audit can challenge the risk-taking environment, the resource and competence in place with respect to the institution's vision and even the integrity of the methods and techniques used (such as the risk modelling and accounting measurement, the assumptions and sources of information and the dividend discount mod). Therefore, the internal audit function should be particularly well positioned and not be combined or merged with any other function.

Reliance on other risk and control functions

After an independent assessment of their effectiveness, internal audit can decide to rely on some of their results to reduce routine and permanent engagement and enhance its risk-based approach. Internal audit can also leverage remote and continuous controls, as well as mass data analysis, provided that the reliability of the process and of data is confirmed. Even so, internal auditors are not expected to use these tools on a day-to-day basis.

Internal audit conclusions and opinions

Internal audit results regarding internal control effectiveness and efficiency could be achieved at a micro or a macro level:

- As internal control is a fundamental area of internal audit evaluation, each engagement is an opportunity to assess risk mitigation and the second line of defence regarding the area under review. Internal audit usually gives its conclusions on the effectiveness (related to the organisation's strategies objectives and risks) at each engagement level. These conclusions enhance management's monitoring of the internal control system.

- The Chief Audit Executive can also give a more cross-cutting opinion on critical issues regarding the internal control system to the board and senior management. This opinion is based on the main issues highlighted by internal audit's risk-based assessment and various information such as:
  - board and senior management expectations,
  - guidelines and findings of the supervisors,
  - internal audit results from several previous engagements, open issues and related action plans on different topics (risk and control culture, risk management and compliance processes, proper communication and information between all levels of the bank, IT governance, achievement of operational objectives…),
  - other assurance providers' relevant conclusions such as operation losses stated by the second line of defence and automated controls run under the supervision of these functions.

As this kind of statement can be resource consuming, the frequency, scope and type of opinion (negative or positive) should be discussed to limit any impacts on the internal audit plan. In any case, care should be taken about a transparent communication, the scope of the opinion, the supporting information and the criteria used, which should be discussed with board and senior management.

Internal audit contribution to the improvement of internal and external reporting

Internal audit can be involved in the examination of the quality of risk functions reporting to the board and senior management. Occasionally the internal audit function can evaluate the bank's external reporting regarding internal control. The list of external criteria such as regulatory reporting (internal liquidity adequacy assessment process (ILAAP), internal capital adequacy assessment process (ICAAP), supervisory review and evaluation (SREP),liquidity coverage ratio (LCR) corporate social responsibility (CSR), etc.) must be clearly defined with expected ownership and data quality.

- During his engagements or when monitoring corrective actions, the Chief Audit Executive must discuss with senior management unresolved issues and, if needed, escalate the information to the board. There should be a common understanding of materiality thresholds.
- Internal auditors must follow integrity and confidentiality rules. In this context, they closely interact with supervisors by sharing information. To support the legitimacy of internal audit within the bank, the practical arrangements and expectations of this two-way communication should be discussed with the board as the highest body within the institution to whom internal audit is accountable.

7

APPENDIX

Main references

- EBA Guidelines on internal governance under Directive 2013/36/EU. September 2017.
- IIA. IPPF_ International Professional Practices Framework (including internal audit Mission, Definition, Code of Ethics, Professional Standards, Implementation Guidance). January 2017.
- Basel Committee. Corporate governance principles for banks. July 2015.
- Arrêté du 3 novembre 2014 relatif au contrôle interne des entreprises du secteur de la banque, des services de paiement et des services d'investissement soumises au contrôle de l'Autorité de contrôle prudentiel et de résolution.
- Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC37.
- Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012.
- IIA UK Financial services code – Effective internal audit in the financial services sector. July 2013.
- Committee of Sponsoring Organizations of the Treadway Commission (COSO) Internal Control – Integrated Framework Executive Summary. May 2013.
- Basel Committee. The internal audit function in banks. June 2012.
- ECIIA. Corporate governance insights. Reinforcing audit committee oversight through global assurance. May 2012.
- EBA guidelines on internal governance of September 2011.

OUR MISSION

To be the consolidated voice for the profession of internal auditing in Europe by dealing with the European Union,its Parliament and Commission and any other appropriate institution of influence and to present and develop the internal audit profession and good corporate governance in Europe.

IIA Armenia	www.iia.am
IIA Austria	www.internerevision.at
IIA Belgium	www.iiabel.be
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.siseaudit.ee
IIA Finland	www.theiia.fi
IIA France	www.ifaci.com
IIA Germany	www.diir.de
IIA Greece	www.hiia.gr
IIA Hungary	www.iia.hu
IIA Iceland	www.fie.is
IIA Israel	www.theiia.org.il
IIA Italy	www.aiiaweb.it
IIA Latvia	www.iai.lv
IIA Lithuania	www.vaa.lt
IIA Luxembourg	www.theiia.org/sites/luxembourg
IIA Montenegro	www.iircg.co.me
IIA Morocco	www.iiamaroc.org
IIA Netherlands	www.iia.nl
IIA Norway	www.iia.no
IIA Poland	www.iia.org.pl
IIA Portugal	www.ipai.pt
IIA Serbia	www.uirs.rs
IIA Slovenia	www.si-revizija.si
IIA Spain	www.auditoresinternos.es
IIA Sweden	www.theiia.se
IIA Switzerland	www.svir.ch
IIA Turkey	www.tide.org.tr
IIA UK & Ireland	www.iia.org.uk
IIA former Yugoslav Republic of Macedonia	www.aiam.org.mk

European Confederation of Institutes of Internal Auditing (ECIIA)

c/o IIA Belgium
Koningsstraat 109-111
Bus 5, BE–1000
Brussels, Belgium

www.eciia.eu

The Institute of Internal Auditors