ECIIA

POSITION PAPER

AUDIT PLANNING APPROACH

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

To manage risks effectively is an essential part of good corporate governance. An important role of each organisation is to identify all business risks and uncertainties which the organisation faces, quickly implementing risk mitigating measures and enhancing the system of internal controls. The internal audit function, as an essential part of the corporate governance framework, provides independent assurance that those risks have been properly managed. As the global business environment and its financial and regulatory requirements have become more complex, users of the audited processes have been calling for more pertinent information for their decision making. The rapidly evolving environment (e.g. digitalisation of services, sustainability, information technology) and a shortening life cycle of products requires organisations to embrace change. Agility and a short response time are critical to survival. This leads to new/enhanced risks which the organisation has to deal with and a new risk appetite. To be able to provide an assurance to senior management in a short time period, it is necessary to focus the audit plan on current and future risks and provide a risk-based approach for audit planning.

Background

The planning requirements within an internal audit function are described in IIA-Standard 2010 'Planning': The Chief Audit Executive must establish a risk-based plan to determine the priorities of the internal audit activity, consistent with the organisation's goals.

A risk-based approach focuses on establishing a shorter audit plan as risk-related information becomes available continuously and changes the need for performing an audit engagement in a certain area. Risk-related information includes, but is not limited to, changes in the organisation's business, operations, programmes, systems, risks and controls as well as changes in the organisation's strategies, key business objectives and associated risks as perceived by the senior management and macro-economic factors (e.g. low-interest environment). In today's rapidly changing environment, organisations need to react promptly to constantly shifting customer demand, environmental factors, market rules, internal business processes and regulatory requirements. Organisations have to manage the risk of different local regulatory requirements, which themselves change as the external environmental factors transform (e.g. recent developments in financial technology, such as blockchain and bitcoins).

The risk-based approach facilitates continuous enhancement of the audit plan with regard to changes of the risks the organisations deal/have to deal with. Therefore, a continuous risk-based approach should be prioritised over the traditional multi-year planning approach since the traditional approach does not ensure that risks are being managed in an effective and timely way. The internal audit function cannot provide any timely assurance that new/enhanced/changed risks are being managed in a proper manner using exclusively the multi-year (long-term) audit planning approach. Furthermore, the traditional approach does not ensure that the activities in managing risks and the changes in the system of internal controls are addressed by the internal audit function at an early stage.

[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.

4

The Basel Committee on Banking Supervision (BCBS) guidance "The internal audit function in banks" (BCBS 223) covers audit planning in principles 6 and 7[2]. Regulatory requirements of local regulators usually include provisions for the time span in which all areas of an organisation should be covered or refer to a multi-year plan (e.g. German MaRisk BT 2.3[3] or US SR 13-1 p10[4]).

A multi-year plan is useful to visualise the coverage of the audit universe over a desired time frame. The approach is easy to manage and progress can be monitored against an annual plan. However, aspects that are subject to change over the projected period cannot be sufficiently anticipated. Most multi-year-plans are based on projecting the need for the next audit engagement by using the date of the last audit engagement as a starting point and adding an audit-cycle of a pre-defined number of years depending on the internal audit risk assessment or specific regulatory requirements. This static audit planning approach can result in missing consideration of significant changes in the business the organisation operates, and consequently timely reaction by the internal audit function is not able to provide objective assurance and consulting activity designed to add value and improve an organisation's operations on a timely basis.[5]

The risk-based approach as a dynamic method facilitates focus on the urgent significant risks the organisation faces and allows the internal audit function to react to changes to business strategy, structure, processes and risks on a timely basis. The approach is based on risks and results in holistic assessment of the organisation as a whole and not on processes, which results in thinking in silos. It enables timely implementation of the results of external supervisory/regulatory audits. Furthermore, there is a need for senior management to involve the internal audit function in the early stages of new product approval/ change processes. The risk-based approach leads to changes in organisational culture concentrating its main focus on the risk environment. The audit engagements align with business goals and the data analysis continuously monitoring risks.

The validity of the static projected audit plan for several years is, due to the continuously developing environment including changing regulatory requirements which cannot be anticipated, questionable and not reliable for a medium-term (or longer) prognosis.

---

[2] Principle 6: Every activity (including outsourced activities) and every entity of the bank should fall within the overall scope of the internal audit function.

[...] 31. The head of internal audit is responsible for establishing an annual internal audit plan that can be part of a multi-year plan. The plan should be based on a robust risk assessment (including input from senior management and the board) and should be updated at least annually (or more frequently to enable an ongoing real-time assessment of where significant risks lie). The board's approval of the audit plan implies that an appropriate budget will be available to support the internal audit function's activities. The budget should be sufficiently flexible to adapt to variations in the internal audit plan in response to changes in the bank's risk profile.

Principle 7: The scope of the internal audit function's activities should ensure adequate coverage of matters of regulatory interest within the audit plan.

[3] German MaRisk BT 2.3: The institution's activities and processes, including those outsourced, shall be audited at appropriate intervals, as a general rule within three years. An annual audit shall be conducted where particular risks exist. The three-year audit cycle may be waived in the case of activities and processes which are immaterial in terms of risk.

[4] US SR 13-1 p10: Internal audit should develop and periodically revise its comprehensive audit plan and ensure that audit coverage for all identified, auditable entities within the audit universe is appropriate for the size and complexity of the institution's activities. This should be accomplished either through a multi-year plan approach, with the plan revised annually, or through an approach that utilizes a framework to evaluate risks annually focusing on the most significant risks. In the latter approach, there should be a mechanism in place to identify when a significant risk will not be audited in the specified timeframe and a requirement to notify the audit committee and seek its approval of any exception to the framework. Generally, common practice for institutions with defined audit cycles is to follow either a three- or four-year audit cycle; high-risk areas should be audited at least every twelve to eighteen months.

[5] According to the IPPF definition the internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes.
IPPF 2050 "The Chief Audit Executive should share information, coordinate activities, and consider relying upon the work of other internal and external assurance providers to ensure coverage and minimize duplication of efforts".

5

FUNDAMENTALS

As a first step, the basis and dimensions of the risk-based approach need to be established. In most institutions an approach for evaluating risks (including method or system) is already available and can therefore be leveraged by the internal audit function taking into account independence considerations (e.g. an existing approach by risk management, which can be leveraged for the risk-based approach of the internal audit function). In the risk-based approach, the audit plan is driven from the organisation's risk register[6] and facilitates the improvement of the risk management framework. Therefore, the internal audit function can concentrate on improving the organisation's risk maturity and is able to provide an assurance on risk management processes as well as management and reporting of key risks. The chosen approach to evaluate the risks should be consistently reflected in the audit universe structure, e.g. a process for risk evaluation would also require a process-oriented structure in the audit universe.

Both aspects, risk orientation and audit universe structure, should also consider the inter-linkage with the existing internal controls system. In particular, defined key controls can provide structure and feedback on design and effectiveness of existing controls.

Define criteria used in risk-based approach

The risk-based approach should not contradict requirements for audit frequency demanded by local regulators (e.g. an annual audit of a certain area). Therefore, provisions have to be taken in order to correctly reflect these requirements (e.g. by means of an override of the risk assessment).

The criteria used in the risk-based planning approach need to be defined and formalised. The results of first and second level controls, key risk indicators monitored by second level of defence, material organisational changes addressed in new product approval/change processes, ongoing incidents and macro-economic factors as well as regulatory changes should be considered in the audit plan on a timely basis. Due to the fact the risks each organisation meets depend on the business, location, organisational structure, products, clients and service providers, the internal audit function needs flexibility to react to the changing internal and external factors on a timely basis. In order to establish a clear and sound risk-based internal audit planning approach and benefit from its advantages, binding guidelines on its implementation and form are necessary. These guidelines must then be introduced to local/home supervisors promoting its acceptance to further initiate changing local regulations. In doing so, the risks identified by supervisors can be considered.

Define role of the internal audit function as third line of defence in anticipating new emerging risks

The internal audit planning process is critical to establish audit engagements that the internal audit function can perform to identify significant risks on a timely basis and provide benefit to the organisation. While there are often a number of compulsory audit engagements due to regulatory requirements, the internal audit function has the opportunity to deliver increased risk coverage, cost savings, enhanced customer protection, sustainability of delivered products and measurable value to the organisation by identifying and performing audit engagement across the organisation's value chain. Emerging risks can arise from many sources: economic or demographic shifts, changes in the competitor and customer landscape or technology. Internal audit acts towards assuring the organisation is aware of, and responding to, those emerging risks.

There are multiple drivers behind the growing importance of executing a robust and comprehensive risk-based audit planning approach. The Chief Audit Executive is challenged by the Audit Committee and senior management to provide the assurance that all significant risks have been identified and properly managed.

[6] IPPF 2050 "The Chief Audit Executive should share information, coordinate activities, and consider relying upon the work of other internal and external assurance providers to ensure coverage and minimize duplication of efforts".

Furthermore, there is an increased risk due to expanding operations in emerging markets and developing countries, and increased regulatory demands as well as focus on cost savings across all functions. The internal audit function can improve the organisation processes through value-based audits and recommendations thinking widely about future risks from a macro-economic viewpoint. It can delve into the organisation's strategy in view of the macro-economic changes and trends and link these trends back to management frameworks.

Review and report the audit plan on a timely basis

The overall structure of internal audit's audit universe and risk assessment should be adequately communicated within the organisation.

On a regular basis the annual audit plan will be reviewed, updated and reported accordingly, taking into account any significant changes in the overall risk profile including events/incidents or other risk information of a short-term nature which were not available at the time of the original planning. Any significant deviations to the initial plan should be highlighted and reported to the board of managing directors and the supervisory board/Audit Committee on a regular basis.

Further, a proof of sufficient coverage of the audit universe in view of the external requirements as well as the internal risk assessment has to be documented and available at any time. The timely coverage in the audit plan can be achieved by making respective provisions in the risk-based approach.

Some examples of how to include this aspect (not an exhaustive list):

- a risk factor can be added which increases over time, thereby giving audit objects which have not been audited for some time higher preference
- knock-out criteria which force taking an audit object into the audit plan when it reaches the audit interval or
- audit objects are reviewed in the planning processes based on when they were last audited (oldest first).

Based on the approach, all audit objects of the audit universe are considered in the planning. The audit plan for the next period (full year) is drawn up consisting of the audit objects with the risk defined as part of the planning process.

An overall process should be developed and documented which incorporates entity specifics to the above-mentioned aspects and then translates to an individual risk-based approach specific to the company. It should also cover a comprehensive documentation, minimum requirements for regular reviews and rationale for changes of the risk assessments.

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