Making the most of the Internal Audit Function:
Recommendations for Directors and Board Committees

ECIIA

ecoDa a.s.b.l.

CONTENT

This document is a practical tool for directors and board committees*

It was produced by the following working group:
- Roland De Meulder, Member of ECIIA Public Affair Committee (chair)
- Dr Roger Barker, Head of Corporate Governance, Institute of Directors (Vice Chair)
- Louis Vaurs, Advisor to the President of IFACI
- Pierre-François Wéry, Partner, PWC Luxembourg, Governance Risk and controls leader.
- Laurent Berliner, Partner, Deloitte, Luxembourg
- Christian Van Nedervelde, Corporate Senior Vice President Internal Audit, SES
- Béatrice Richez-Baum, Secretary General ecoDa
- Pascale Vandenbussche, Secretary General ECIIA
- Carolyn Dittmeier, Past President ECIIA

The publication was overviewed by both the ECIIA and ecoDa (management) board and by ECIIA 's members.

ABOUT THE ECIIA

The European Confederation of Institute of Internal Auditing, ECIIA is a non profit association based in Brussels. The ECIIA is a confederation of national associations of internal auditing located in 37 countries, including all those of the EU, representing almost 40,000 internal audit professionals. As such, the ECIIA is an Associated Organization of the global Institute of Internal Auditors (the IIA), a professional organization 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. ECIIA's mission is to Furthering the development of Corporate Governance and Internal Audit at European level through knowledge sharing, key relationships and the regulatory environment.

More information on www. eccia.eu

ABOUT ECODA

The European Confederation of Directors' Associations. ecoDa is a not-for-profit association based in Brussels, acting since March 2005 as the «European voice of directors». Through its national institutes of directors (the main national institutes existing in Europe), ecoDa represents around fifty-five thousand board directors from across the EU member states.
ecoDa's mission is to promote good corporate governance and improve the effectiveness of boards of directors and/or supervisory boards, particularly by means of appropriate director training, professional development and boardroom best practice
ecoDa's members: IoD, GUBERNA, IFA, ILA, IC-A, Hallitusammattilaiset ry, the Slovenian association of supervisory board members, the Croatian Association of certified supervisory board members, the Polski Instytut Dyrektorow, the Norwegian institute of directors (Styreinstitutt), the Norwegian StyreAkademiet, the Baltic institute of directors, the Swedish StyrelseAkademien and the Macedonian FYR Institute of Directors.

More information on www.ecoDa.org

** it has been developped by the European Confederation of Institutes of Internal Auditing (ECIIA), in close cooperation with the European Confederation of Directors'associations (ecoDa)*

INTRODUCTION/BACKGROUND

This paper seeks to provide useful guidance to boards, governing bodies and individual directors that wish to make effective use of the internal audit function, particularly in respect of gaining assurance concerning the adequacy of an organisation's risk management and internal control systems.

Internal audit is a key component of modern corporate governance. However, board structures and corporate governance systems exhibit significant variation across Europe. In some countries (e.g. the UK, France), the board consists of both senior members of management and non-executive directors. In other countries (e.g. Germany, Netherlands, or the Nordic countries), the board or supervisory board may be entirely composed of non-executive board members. In such circumstances, senior management may sit on a separate executive board or be excluded from the board altogether.

In this guidance, the term "Board of Directors" is used as a generic term to refer to an organisation's main governing body – however constituted – which assumes primary responsibility for corporate oversight on behalf of relevant stakeholders. The purpose of this guidance is to assist the members of this governing body in making the most of the internal audit function in pursuit of their governance objectives.

The term "board" is also used to encompass the committees of the board – such as the audit or risk committees – which commonly play a particular role in terms of the board's relationship with internal audit. Board committees – consisting of sub-groups of directors – are typically mandated by corporate governance codes or best practice in order to support the functioning of the main board in areas of more specialised boardroom activity.

However, it should also be recognised that there may exist significant variation in the role and functioning of such committees across differing European countries. For example, in the Nordic countries, a key role is played in governance by the nomination committee, which is a committee of the shareholders rather than the board. Local variation in governance practices should therefore be taken into account by directors when applying the recommendations of this guidance.

Notwithstanding the variation in corporate governance systems across Europe, there are some basic characteristics of governance frameworks that are typical in most countries:

- The board provides direction to senior management by setting the organisation's risk appetite. It also seeks to identify the most significant risks facing the organisation. Thereafter, the board assures itself on an ongoing basis that senior management is responding appropriately to these risks.

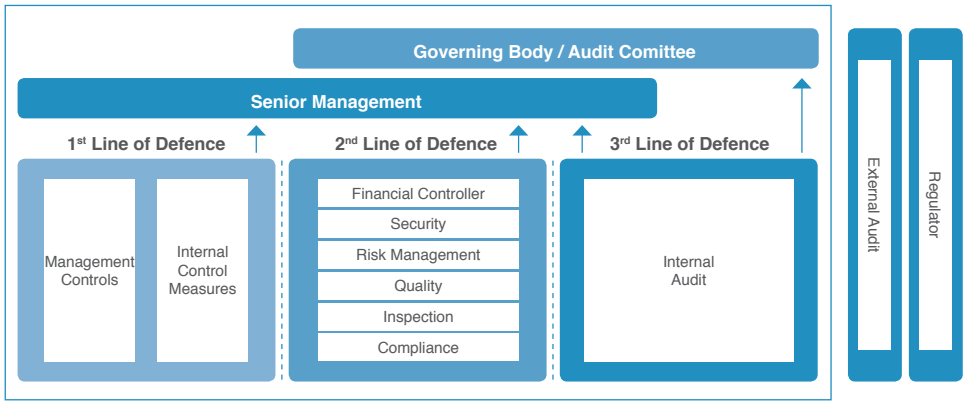
- The CEO and senior management are delegated primary ownership responsibility for the operational functioning of an organisation's risk management and control framework. It is management's job to provide leadership and direction to the employees in respect of risk management, and to control the organisation's overall risk-taking activities in relation to the agreed level of risk appetite.

To ensure the effectiveness of an organization's risk management framework, the board and senior management need to be able to rely on adequate line functions - including monitoring and assurance functions - within the organisation. In order to conceptualise these line functions, ecoDa and the ECIIA endorse the use of the

"Three lines of Defence" model which is already widely adopted within the financial industry, but which can also be productively utilised in a wide range of sectors.

The "Three lines of Defence" structure is a conceptual delineation of an organisation's internal control levels: first line controls, second level monitoring controls and third-line independent assurance. It also provides a framework with which the board can understand the role of internal audit in the overall risk management and internal control process of an organisation.

The Three Lines of Defence



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

The second line of defence consists of activities covered by several components of internal governance (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.

Internal audit forms the organisation's third line of defence. An independent internal audit function will, through a risk-based approach to its work, provide assurance to the organization's board of directors and senior management. This assurance will cover how effectively the organization 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 institution's risk management framework (from risk identification, risk assessment and response, to communication of risk-related information) and all categories of organisational objectives: strategic, operational, reporting and compliance.

The internal audit function is uniquely positioned within the organisation to provide global assurance to the board and senior management on the effectiveness of internal governance and risk processes. It is also well-place to fulfil an advisory role in respect of effective ways of improving existing processes and assisting management in implementing recommended improvements.

In such a framework, internal auditing is a key cornerstone of an organisation's corporate governance.

However, before considering the detailed recommendations of this guidance, it is important to stress that there are three fundamental issues that should be considered by boards in order to ensure that internal audit maximises its contribution to good governance:

- Internal audit should have a reporting line within the organisation which ensures that it is able to function with sufficient independence;
- Internal audit should utilise a risk based approach in developing and executing the internal audit plan;
- A consistently high level of professionalism and quality must be sustained in the internal audit staff's work.

These three conditions are key issues for directors to consider when monitoring the effectiveness of the organisation's internal audit function.

It should be emphasized that the following recommendations for directors are consistent with the globally recognised International Standards for the Professional Practice of Internal Auditing (https://global.theiia.org/standards-guidance/Pages/Standards-and-Guidance-IPPF.aspx)

TOP 10 RECOMMENDED BOARD AND COMMITTEE PRACTICES IN RESPECT OF INTERNAL AUDIT OVERSIGHT

1. Evaluating the need for establishing an internal audit function when such a function does not yet exist.

The introduction to this paper underlined the added value of an independent, professional internal audit function. Not surprisingly, some 90%* of EU- member states require or strongly recommend the presence of an internal audit function within listed companies. In addition, internal audit is generally compulsory for most companies within the financial sector.

For public interest organisations that do not currently have an internal audit function, the Board is in charge to review the need for establishing one. As part of its management oversight role, and based on the underlying rational submitted by senior management, the board should either endorse or challenge this "go/no go" decision.

** Based on ECIIA publication «Corporate Governance Codes on Internal Audit - Current status in the EU», November 2012.*

The probability and (financial) impact of organisational risks and the complexity of the organisation, rather than simply the size of the organisation, should be the decisive factors in the decision to establish an internal audit capability.

For SME's, senior management and the board may decide to opt for some form of outsourcing as a means of obtaining an internal audit capability. It is important to note, however, that in the case of full outsourcing, ultimate accountability for the function's work cannot be delegated away from the company. Ultimate responsibility for internal audit should be formally assigned to an in-house member of staff, preferably a member of senior management.

Listed organisations that have not yet established an in-house or outsourced internal audit function should publicly disclose (e.g. in the corporate governance statement, on the basis of 'comply or explain') why it is not in place and how governance, risk and compliance assurance are being adequately obtained in its absence.

"As we are a SME, we had no internal audit function so far. Now that we are growing fast, our Board has decided to appoint an external provider that will be managed by our CEO"

Recommended practices for boards:

- *In organisations that have no internal audit function, the board should periodically review the need for establishing such a function. Based on the underlying rationale submitted by senior management, the board should then endorse or challenge this "go/no go" decision.*
- *In cases where an organisation's management opts to fully outsource its internal audit function, the board should oversee the entire outsourcing process, including ensuring that an in-house liaison has been formally made accountable for the appropriateness and quality of the outsourced work.*
- *In cases where a public interest organisation has not established an in-house internal audit function, the board should ensure that this decision is publicly disclosed (e.g. in the corporate governance statement). This disclosure should include a meaningful explanation of why this decision has been taken and how global assurance is to be obtained by the board and senior management in its absence.*

2. Assessing and approving the internal audit charter.

The internal audit charter is a formal document that defines the internal audit activity's purpose, authority, and responsibility. The internal audit charter establishes internal audit's position within the organisation, including the nature of the Chief Audit Executive's (CAE) functional reporting relationship with the board and senior management. It also authorises the internal audit department's access to records, personnel, and physical locations relevant to the performance of engagements.

The internal audit charter also defines the scope of the internal audit activities. In order to optimise the contribution of internal audit to an effective governance structure, its scope of activity should preferably cover the full portfolio of

organisational risks (strategic, operational, reporting, compliance) and include both assurance and advisory activities.

"In recent years we have been asked to provide consultancy services on a wider range of risks and business areas as the executive team has realised the value of our work. However, through the internal audit charter, our audit committee confirmed that our primary role is to serve the business as assurance providers; any consultancy work that internal audit carries out is secondary to its core focus. We have three criteria that need to be satisfied if we are going to carry out consultancy work. Firstly, the work we are being asked to do needs to materially impact the business. Secondly, we must have the skills within the team to be able to carry out the work. And thirdly, we must be able to have the time to do the work without jeopardising our activities in the core assurance programme".

Although providing assurance that risks are understood and managed appropriately is internal audit's core activity, internal auditing staff may also be permitted by the charter to serve as in-house consultants to management on issues of risk management and internal control. However, while fulfilling such an advisory role, internal audit should also ensure that its independence and objectivity are not compromised.

Final approval of the internal audit charter should always reside with the board.

A sample internal audit charter is included in the annexe to this paper.

Recommended practices for boards:

- *The board should review the internal audit charter to ensure that it allows the internal audit function to fully assume its responsibilities as a key assurance provider in respect of organisation-wide risk management and control.*
- *The board should approve the internal audit charter.*

3. Ensuring effective communication lines between the Chief Audit Executive (CAE) and the board.

"As the Senior Vice President and Director of Internal Audit, I report directly to the Chairman of the Board, thus ensuring Group Internal Audit's independence within the organisation. All activities and processes can be audited. I meet with the Chairman of the Board on a monthly basis and work closely with the Chairman of the Audit Committee, having informal meetings approximately six times per year. I am regularly invited to attend Audit Committee meetings and discuss our activities. During these meetings, the audit committee members review the risk management and internal control system, approve the Internal Audit Plan, review a selection of high risk audit reports, and monitor the timely implementation of audit recommendations. In addition with my reporting relationship

In order to ensure the independence of the internal audit function and the objectivity of its assessments, it is important that the internal audit function is not placed hierarchically under parts of the organisation that are themselves subject to internal audit scrutiny.

The CAE should have an open communication line with the board and/or relevant board committees. This is particularly important when the CAE has reason to believe that senior management has exposed the organisation to a level of residual risk that may be unacceptable to the organization on the basis of its agreed risk appetite. In such a case the CAE must be able to report the matter to the board for evaluation.

Recommended practices for boards:

- *The board should ensure that the CAE is accountable to a dedicated board member or, when applicable, the chair of the board audit committee (or other relevant board or governance committee).*
- *The CAE should enjoy direct and unrestricted communications with the board or, when applicable, with the chair of the relevant board committee.*

with the board and the audit committee, I also have a direct line of communication with the Group CEO and CFO with whom I have monthly meetings.".

- *The board should conduct direct discussions with the CAE at least once a year without the presence of the CEO or other senior managers.*
- *The board should be informed of any significant differences of opinion that arise between senior management and the CAE on significant risk and control issues.*

4. Evaluating the internal audit plan.

The CAE is responsible for developing a risk-based plan on an annual basis to determine the priorities of internal audit activities, consistent with the organisation's goals.

In this regard, the CAE should take into account the organisation's risk management framework, including using the risk tolerance levels set by senior management and the board for the different activities or parts of the organisation. If such a framework does not exist, the CAE should define its own risk-based assessment criteria as the basis for the internal audit plan in consultation with senior management and the board.

The final internal audit plan should be submitted to the board for approval.

The audit plan should be "dynamic", i.e. insight gained during the business year and/or evolutions in the organisation's risk profile could result in an updating of the plan at relatively short notice. Such changes and the underlying rationale for those changes should be clearly communicated and coordinated with senior management and the board.

Recommended practices for boards:

- *The board and the CEO should provide input to the CAE in his/her drafting of a risk-based internal audit plan.*

"We continuously re-assesses our audit plan through a process known as "dynamic risk assessment". This allows us adjust the annual audit plan to take account of emerging risks and to reprioritise assurance activities as required. We have a quarterly refresh to make sure that we are actually auditing the areas we need to, and whether there are areas where we should pull back from, or if we can rely on the work provided by other assurance providers. We simply need this flexibility built into our audit plan: we have already made dramatic changes to it within just the first quarter of the year and have switched our focus with regards to areas for review. "

- *The board and the CEO should discuss with the CAE the content of the audit plan. Particular attention should be paid to*
  - *the process used by the CAE to assess areas of significant risk to the organisation, which may affect the targeting of internal audit activities;*
  - *the extent of the internal audit universe, which will affect the potential breadth of internal audit's activities within an organisation;*
  - *the extent to which both design and performance of internal control systems will be considered in the course of internal audit activity;*
- *After having reviewed and discussed the plan, and proposed changes as necessary, the board should formally approve the internal audit plan.*
- *The board and the CEO should discuss and approve any significant changes to the plan during the year proposed by the CAE.*

5. Assessing the staffing of the internal audit function.

In order to be effective, the internal audit function must possess sufficient resources, both in terms of numbers of staff and staff proficiency.

The **required capacity** of the internal audit function should be primarily based on the risk-based audit plan. The CAE should report the impact of any resource limitations implied by the plan to the CEO.

The relevant board committee should carefully monitor any decision by the CEO to adjust the internal audit function's capacity (as defined within the budgetary framework of the organisation). It should formally approve any list of high risk areas which will not be covered by the internal audit process due to budgetary constraints.

The internal audit function should **collectively** possess, or have access to, the **knowledge, skills, and other competencies needed to execute the plan**.

This will include a balanced set of **technical skills** which allow it to understand the types of risk faced by the organisation and to evaluate the effectiveness of associated risk responses.

In addition to these technical skills, internal auditors should also demonstrate good interpersonal and communicating skills (both oral and written).

The board should ensure that an external assessment of the internal audit function is conducted at least once every five years - or more frequently if warranted - by a qualified, independent reviewer or review team from outside the organisation (see point 6 "Assuring the quality of the internal audit function's work" for more details).

The board should devote significant thought and effort to the process of appointing the **Chief Audit Executive**. As the main contact point for the board and the audit committee (or other relevant governance committee), this position must be staffed appropriately and with great care. Although the CEO may assume direct control over the CAE hiring process, the board must ensure that it is appropriately consulted during this process regarding the functional profile and selection of the CAE. Furthermore, in view of the need to ensure the CAE's independence and objectivity, the board should also oversee his/her dismissal process.

Finally, the board should also be consulted on the CAE's remuneration package in order to evaluate whether:

- the level of his/her remuneration package ensures a status within the organisation that allows him/her to carry out the assigned responsibilities.

- the variable performance part of his/her remuneration package is based on personal performance rather than being linked to the financial results of the organisation (avoiding any real or perceived impairment of his/her independence and objectivity).

Recommended practices for boards:

- *the board and the CEO should obtain from the CAE advice on the impact of resource limitations on the internal audit plan.*
- *the board should decide to adjust the internal audit function's capacity and formally approve any decision to omit high risk areas from internal audit scrutiny due to resource constraints.*
- *the board should periodically obtain assurance from the CAE that the internal audit function collectively possesses - or has access to - the required communication and technical skills to execute the internal audit plan effectively and to report engagement conclusions and recommendations adequately.*

"Our internal audit team is small (5 people). Therefore we use specialists in different areas to assist us for specified audit missions. These specialists are part of the company most of the time. For IT, we use external resources"

- *the board should be appropriately consulted by the CEO regarding the functional profile of the CAE, and decisions in respect of his/her intended appointment/ dismissal and remuneration package. The board should challenge the CEO's decision on these issues in cases where the CAE's independence or objectivity could be impaired.*

6. Gaining assurance regarding the quality of the internal audit function's work.

Monitoring the quality of the internal audit function is - in the first instance – the responsibility of the CAE. In order to fulfil this responsibility, the CAE should develop and maintain a quality assurance and improvement program that covers all aspects of the internal audit function, in accordance with The IIA's International Standards for the Professional Practice of Internal Auditing (the Standards). Such a program will assess the efficiency and effectiveness of the internal audit function and identify opportunities for improvement.

The quality assurance and improvement program should include both internal and external assessments.

Internal assessments should include ongoing performance monitoring of internal audit by means of direct supervision as well as periodic self-assessments.

External assessments should be conducted at least once every five years - or more frequently if warranted - by an independent reviewer from outside the organisation qualified according to IIA Standards.

Recommended practices for boards:

- *the board and the CEO should review the quality of the internal audit function on an annual basis.*

- *the board should periodically review the required frequency for external assessments of the internal audit function. Whilst every five years should be the minimum frequency.*
- *the board should review the qualifications and independence of the external reviewer or review team, including any potential conflicts of interest.*
- *the board should ensure that it is informed in a timely manner of the results and related actions for improvement of the internal audit assessment process and determine the required frequency for the internal assessments.*
- *the board should effectively monitor the adequate and timely implementation of the corrective actions following the external quality assessment.*
- *independent of, and in addition to the external quality review, the board should assess the performance of the internal audit function based on:*

  - the degree to which the audit planning has been implemented;

  - the clarity and conciseness of internal audit reports;

  - the added value of audits for re-enforcing existing governance, risk and control processes;

  - the acceptance by senior management of significant internal audit recommendations (i.e. those meant to remedy material risk management and control deficiencies);

  - customer satisfaction on the part of the recipients of internal audit services. In this respect, and in line with good internal audit practice, the CAE could send out customer satisfaction surveys to the owners of the processes under audit after each assignment, as well as an annual quality survey to senior management and the board.

My team conducts an annual self-assessment, which comprises around 300 questions around internal audit positioning, resourcing, planning, methodology, reporting and quality. The team also produces a questionnaire – incorporating input from the audit committee – which is sent out annually by the chief executive (to preserve independence) via the intranet to the senior management group. Responses are not anonymised, so internal audit can follow up any comments with the individuals involved to improve the quality of its work. In addition, we try to get structured feedback from key auditees after every audit review on internal audit's performance during the planning, fieldwork and reporting phases. The feedback considers – among other issues – auditor competence, communication and business understanding.Together with the audit committee, we have also set a list of KPIs that are contained in the audit charter. These include for instance KPIs on planned report delivery, our focus on key risk for the business, the number of recommended actions closed by management, etc…".

7. Overseeing the relationship between the internal audit function and the organisation's centralised risk monitoring function.

Whilst the management of each part of an organisation should be responsible for managing risks in its own area of activity, this should take place within in an integrated, holistic framework aimed at aligning organisation-wide objectives and strategy.

Many organisations have established a centralised risk management function for coordinating and developing risk management activities across the organisation. Whilst best typical practice for larger organisations is to nominate a chief risk officer (CRO), smaller organisations may assign this responsibility to another senior executive.

The CRO (or similar function) is responsible for monitoring overall risk management capabilities and resources, and for assisting operational managers in reporting relevant risk information up and across the organisation.

Specific responsibilities of a CRO (or similar function) include:

- Establishing risk management policies, defining roles and responsibilities, and setting goals for implementation;
- Providing a framework for risk management in specific processes, functions or departments of the organisation;
- Promoting risk management competence throughout the organisation;
- Establishing a common risk management language (e.g. regarding risk categories and measures related to likelihood and impact);
- Facilitating managers' development of risk reporting, and monitoring the reporting process;
- Reporting to the CEO and the board on progress and recommending action as needed.

In this role, the CRO (or similar function) typically act as a "second line of defence" risk monitoring function (see the Introduction for a description of how this fits into the three lines of defence model).

To avoid overlaps and/or gaps in organisational risk monitoring, it is important that the internal audit function coordinates appropriately with the CRO (or similar function).

"We closely coordinate our activities with centralised, second line, monitoring functions such as Compliance, Quality and Health-Safety-Environment (HSE). Among other things, we obtain their engagement programs to build our own audit plan and then share it with these functions. Joined or complementary audits can then be organised to be more effective and to avoid duplication of work. Furthermore, as part of our scope of work (formalised in the internal audit charter), we are also requested to assess the maturity level of those centralized risk monitoring functions (scope exhaustiveness, risk measurement methods, organisation and staffing, work methodology, ….)"

As a "third line" assurance function, internal audit should not only evaluate the effective design and proper functioning of risk and control systems implemented by (first line) operational management, but also the way in which second line of defence monitoring functions - such as centralised risk management - operate.

Recommended practices for boards:

- *The board and the CEO should ensure that there is appropriate task allocation and coordination between the internal audit function and second line of defence functions, such as risk management, financial controls and compliance.*
- *The board and the CEO should ensure that the internal audit function evaluates both first and second line of defence risk management activities as part of its internal audit plan and provides assurance on how both lines of defence operate.*

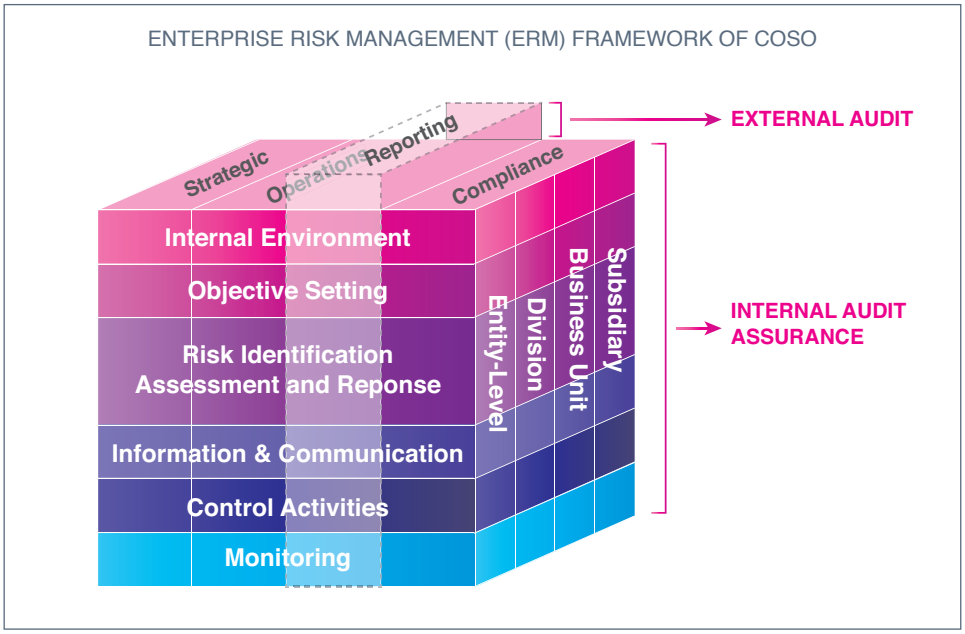
8. Coordinating the internal audit function with the work of external audit.

External auditors provide assurance to the organisation's shareholders, board and senior management that the organisation's financial statements provide a 'true and fair' view of the organisation's financial performance and current financial position.

Given the specific scope and objectives of their mission, the risk information gathered by external auditors is typically limited to financial reporting risks, and does not include the way senior management and the board/audit committee are managing/monitoring the organisation's strategic, business and compliance risks.

However, these are areas in which the internal audit function can provide assurance to senior management and the board and audit committee (or other relevant governance committee).

This distinction between external and internal audit assurance can be graphically illustrated as follows:



Whilst the objectives of external and internal audit activities are different, there may be some potential areas of overlap, particularly in the area of financial reporting. In particular, external audit may provide "management letter comments" in relation to internal control weaknesses noted in the course of their audit engagement.

Internal audit should consider these points in its audit planning process and may activate separate follow up activity to ascertain the effectiveness of management's corrective actions. Similarly, external audit should consider internal audit findings as an input into their own work.

"We use, among other things, the results of the risk assessment performed by the external auditors in relation to their evaluation of financial reporting controls for building our own

The board and the audit or other relevant committee have an oversight role to play in ensuring an adequate and effective coordination between internal and external audit activities, avoiding duplication and optimising the use of each other's work.

internal audit plan.
We also meet with them on a regular basis to share audit plans and the results of our work. This way we mutually update our risk assessment information and aim at avoiding duplication of work. We also jointly participate in every audit committee meeting."

Recommended practices for boards:

- *The board and CEO should ensure that there is an open communication between internal and external auditors, they should oversee the manner in which the activities of the internal audit function and those of external audit optimise the use of each other's work and avoid any risk of duplication.*

9. Assessing internal audit reporting.

The board should take an active role in clearly formalising their internal audit reporting and communication needs, including the required frequency of reporting.

As a minimum requirement, internal audit reporting to the board should include significant risk exposures and control issues arising from internal audit activity, a progress report on the fulfilment of the internal audit plan and any issues of concern regarding the staffing and resources made available to the internal audit function.

"Every month we have an activity report that goes to the executive directors, the executive heads and the audit committee members.
We go through what we have completed, and what we are about to start, and explain whether we are behind schedule or if we need further resources.
We also provide the audit committee with a list of recommendations and actions that have been completed, and I am upfront about highlighting which recommendations have not been implemented by management. Keeping the audit committee informed about our progress is key to building trust and earning respect."

Recommended practices for boards:

- *Based on a comprehensive overview, the board should periodically consider and evaluate:*
  - *The most significant findings of internal audit during the latest audit period;*
  - *The progress and adequacy of implementation of internal audit recommendations by management;*
  - *Progress in executing the audit plan;*
  - *Issues of concern regarding the staffing and resources made available for the internal audit function.*

10. Monitoring management follow-up of internal audit recommendations.

The CAE should establish a follow-up process to ensure that internal audit recommendations have been implemented effectively. Alternatively, it should confirm that senior management has fully understood and accepted responsibility for the risks of not taking action.

If by not acting on an internal audit recommendation, the CAE believes that senior management has exposed the organisation to a level of residual risk that may not be acceptable to the board, he/she should discuss the matter in the first instance

with senior management. If the management decision regarding residual risk is not explained to the satisfaction of the CAE, the CAE should report the matter to the board or relevant board committee.

Recommended practices for boards:

"We are very public about saying which recommendations and actions are overdue and we chase this with the management teams that are responsible for them. We keep the audit committee in the loop. Every quarter I take a report to the audit committee that also provides an update of where we are and a performance overview. The audit committee wants to know that we are independent and that we can stand up to management and provide an independent challenge."

- *The board should assess the progress of the implementation of the audit recommendations, placing specific emphasis on major risk and control issues and implementation backlogs.*
- *The board should discuss the causes of significant backlogs and follow-up with management.*
- *The board should discuss with the CAE those cases where, by not acting on an internal audit recommendation, the CAE believes that senior management has exposed the organisation to a level of residual risk that may not be acceptable to the board.*

ANNEXES

Annexe 1: SAMPLE INTERNAL AUDIT CHARTER (source: Institutes of Internal Auditors)

INTRODUCTION:

Internal Auditing is an independent and objective assurance and consulting activity that is guided by a philosophy of adding value to improve the operations of the <organization>. It assists <organization> in accomplishing its objectives by bringing a systematic and disciplined approach to evaluate and improve the effectiveness of the organization's risk management, control, and governance processes.

ROLE:

The internal audit activity is established by the Board of Directors or oversight body (hereafter referred to as the Board). The internal audit activity's responsibilities are defined by the Board as part of their oversight role.

PROFESSIONALISM:

The internal audit activity will govern itself by adherence to The Institute of Internal Auditors' mandatory guidance including the Definition of Internal Auditing, the Code of Ethics, and the International Standards for the Professional Practice of Internal Auditing (Standards). This mandatory guidance constitutes principles of the fundamental requirements for the professional practice of internal auditing and for evaluating the effectiveness of the internal audit activity's performance.

The Institute of Internal Auditors' Practice Advisories, Practice Guides, and Position Papers will also be adhered to as applicable to guide operations. In addition, the internal audit activity will adhere to <organization> relevant policies and procedures and the internal audit activity's standard operating procedures manual.

AUTHORITY:

The internal audit activity, with strict accountability for confidentiality and safeguarding records and information, is authorized full, free, and unrestricted access to any and all of the organization's records, physical properties, and personnel pertinent to carrying out any engagement. All employees are requested to assist the internal audit activity in fulfilling its roles and responsibilities. The internal audit activity will also have free and unrestricted access to the Board.

ORGANIZATION:

The Chief Audit Executive will report functionally to the Board and administratively to the Chief Executive Officer.

The Board will approve all decisions regarding the performance evaluation,

appointment, or removal of the Chief Audit Executive as well as the Chief Audit Executive's annual compensation and salary adjustment. The Chief Audit Executive will communicate and interact directly with the Board, including in executive sessions and between Board meetings as appropriate.

INDEPENDENCE AND OBJECTIVITY:

The internal audit activity will remain free from interference by any element in the organization, including matters of audit selection, scope, procedures, frequency, timing, or report content to permit maintenance of a necessary independent and objective mental attitude.

Internal auditors will have no direct operational responsibility or authority over any of the activities audited. Accordingly, they will not implement internal controls, develop procedures, install systems, prepare records, or engage in any other activity that may impair internal auditor's judgment.

Internal auditors must exhibit the highest level of professional objectivity in gathering, evaluating, and communicating information about the activity or process being examined. Internal auditors must make a balanced assessment of all the relevant circumstances and not be unduly influenced by their own interests or by others in forming judgments.

The Chief Audit Executive will confirm to the board, at least annually, the organizational independence of the internal audit activity.

RESPONSIBILITY:

The scope of internal auditing encompasses, but is not limited to, the examination and evaluation of the adequacy and effectiveness of the organization's governance, risk management, and internal control processes in relation to the organization's defined goals and objectives. Internal control objectives considered by internal audit include:

- Consistency of operations or programs with established objectives and goals and effective performance
- Effectiveness and efficiency of operations and employment of resources
- Compliance with significant policies, plans, procedures, laws, and regulations
- Reliability and integrity of management and financial information processes, including the means to identify, measure, classify, and report such information.
- Safeguarding of assets

Internal Audit is responsible for evaluating all processes ('audit universe') of the entity including governance processes and risk management processes.

It also assists the Audit Committee in evaluating the quality of performance of external auditors and maintains proper degree of coordination with internal audit.

Internal audit may perform consulting and advisory services related to governance, risk management and control as appropriate for the organization. It may also

evaluate specific operations at the request of the Board or management, as appropriate.

Based on its activity, Internal audit is responsible for reporting significant risk exposures and control issues identified to the Board and to Senior Management, including fraud risks, governance issues, and other matters needed or requested by the Board.

INTERNAL AUDIT PLAN:

At least annually, the Chief Audit Executive will submit to the Board an internal audit plan for review and approval, including risk assessment criteria. The internal audit plan will include timing as well as budget and resource requirements for the next fiscal/calendar year. The Chief Audit Executive will communicate the impact of resource limitations and significant interim changes to senior management and the Board.

The internal audit plan will be developed based on a prioritization of the audit universe using a risk-based methodology, including input of senior management and the board. Prior to submission to the Board for approval, the plan may be discussed with appropriate senior management. Any significant deviation from the approved internal audit plan will be communicated through the periodic activity reporting process.

REPORTING AND MONITORING:

A written report will be prepared and issued by the Chief Audit Executive or designee following the conclusion of each internal audit engagement and will be distributed as appropriate. Internal audit results will also be communicated to the Board.

The internal audit report may include management's response and corrective action taken or to be taken in regard to the specific findings and recommendations. Management's response, whether included within the original audit report or provided thereafter (i.e. within thirty days) by management of the audited area should include a timetable for anticipated completion of action to be taken and an explanation for any corrective action that will not be implemented.

The internal audit activity will be responsible for appropriate follow-up on engagement findings and recommendations. All significant findings will remain in an open issues file until cleared.

PERIODIC ASSESSMENT:

The Chief Audit Executive is responsible also for providing periodically a self assessment on the internal audit activity as regards its consistency with the Audit Charter (purpose, authority, responsibility) and performance relative to its Plan.

In addition, the Chief Audit Executive will communicate to senior management and the Board on the internal audit activity's quality assurance and improvement program, including results of ongoing internal assessments and external assessments conducted at least every five years.

Internal Audit Activity charter

Approved this _____ day of _____, _____.

_____	_____
Chief Audit Executive	Chief Executive Officer
_____	_____
Chairman of the Board of Directors	Chairman of the Audit Committee

Annexe 2: SAMPLE AUDIT COMMITTEE CHARTER (source: Institutes of Internal Auditors)

PURPOSE

To assist the board of directors in fulfilling its oversight responsibilities for the financial reporting process, the system of internal control, the audit process, and the company's process for monitoring compliance with laws and regulations and the code of conduct.

AUTHORITY

The audit committee has authority to conduct or authorize investigations into any matters within its scope of responsibility. It is empowered to:

- Appoint, compensate, and oversee the work of any registered public accounting firm employed by the organization.
- Resolve any disagreements between management and the auditor regarding financial reporting.
- Pre-approve all auditing and non-audit services.
- Retain independent counsel, accountants, or others to advise the committee or assist in the conduct of an investigation.
- Seek any information it requires from employees-all of whom are directed to cooperate with the committee's requests-or external parties.
- Meet with company officers, external auditors, or outside counsel, as necessary.

COMPOSITION

The audit committee will consist of at least three and no more than six members of the board of directors. The board or its nominating committee will appoint committee members and the committee chair.

Each committee member will be both independent and financially literate. At least one member shall be designated as the «financial expert,» as defined by applicable legislation and regulation.

MEETINGS

The committee will meet at least four times a year, with authority to convene additional meetings, as circumstances require. All committee members are expected to attend each meeting, in person or via tele- or video-conference. The committee will invite members of management, auditors or others to attend meetings and provide pertinent information, as necessary. It will hold private meetings with auditors (see below) and executive sessions. Meeting agendas will be prepared and provided in advance to members, along with appropriate briefing materials. Minutes will be prepared.

RESPONSIBILITIES

The committee will carry out the following responsibilities:

Financial Statements

- Review significant accounting and reporting issues, including complex or unusual transactions and highly judgmental areas, and recent professional and regulatory pronouncements, and understand their impact on the financial statements.

- Review with management and the external auditors the results of the audit, including any difficulties encountered.

- Review the annual financial statements, and consider whether they are complete, consistent with information known to committee members, and reflect appropriate accounting principles.

- Review other sections of the annual report and related regulatory filings before release and consider the accuracy and completeness of the information.

- Review with management and the external auditors all matters required to be communicated to the committee under generally accepted auditing Standards.

- Understand how management develops interim financial information, and the nature and extent of internal and external auditor involvement.

- Review interim financial reports with management and the external auditors before filing with regulators, and consider whether they are complete and consistent with the information known to committee members.

Internal Control

- Consider the effectiveness of the company's internal control system, including

information technology security and control.

- Understand the scope of internal and external auditors' review of internal control over financial reporting, and obtain reports on significant findings and recommendations, together with management's responses.

Internal Audit

- Review with management and the chief audit executive the charter, activities, staffing, and organizational structure of the internal audit function.

- Have final authority to review and approve the annual audit plan and all major changes to the plan.

- Ensure there are no unjustified restrictions or limitations, and review and concur in the appointment, replacement, or dismissal of the chief audit executive.

- At least once per year, review the performance of the CAE and concur with the annual compensation and salary adjustment.

- Review the effectiveness of the internal audit function, including compliance with The Institute of Internal Auditors' International Professional Practices Framework for Internal Auditing consisting of the Definition of Internal Auditing, Code of Ethics and the Standards.

- On a regular basis, meet separately with the chief audit executive to discuss any matters that the committee or internal audit believes should be discussed privately.

External Audit

- Review the external auditors' proposed audit scope and approach, including coordination of audit effort with internal audit.

- Review the performance of the external auditors, and exercise final approval on the appointment or discharge of the auditors.

- Review and confirm the independence of the external auditors by obtaining statements from the auditors on relationships between the auditors and the company, including non-audit services, and discussing the relationships with the auditors.

- On a regular basis, meet separately with the external auditors to discuss any matters that the committee or auditors believe should be discussed privately.

Compliance

- Review the effectiveness of the system for monitoring compliance with laws and regulations and the results of management's investigation and follow-up (including disciplinary action) of any instances of noncompliance.

- Review the findings of any examinations by regulatory agencies, and any auditor observations.

- Review the process for communicating the code of conduct to company personnel, and for monitoring compliance therewith.

- Obtain regular updates from management and company legal counsel regarding compliance matters.

Reporting Responsibilities

- Regularly report to the board of directors about committee activities, issues, and related recommendations.

- Provide an open avenue of communication between internal audit, the external auditors, and the board of directors.

- Report annually to the shareholders, describing the committee's composition, responsibilities and how they were discharged, and any other information required by rule, including approval of non-audit services.

- Review any other reports the company issues that relate to committee responsibilities.

Other Responsibilities

- Perform other activities related to this charter as requested by the board of directors.

- Institute and oversee special investigations as needed.

- Review and assess the adequacy of the committee charter annually, requesting board approval for proposed changes, and ensure appropriate disclosure as may be required by law or regulation.

- Confirm annually that all responsibilities outlined in this charter have been carried out.

- Evaluate the committee's and individual members' performance on a regular basis.

Internal Audit Activity charter

Approved this _____ day of _____, _____.

_____ _____

Chairman of the Board of Directors Chairman of the Audit Committee

ECIIA

European Confederation of Institutes of Internal Auditing
Koningsstraat 109 -111 bus 5, 1000 Brussels, Belgium

Tel: +32 2 217 33 20
Fax: +32 2 217 33 20
Email: office@eciia.eu
www.eciia.eu

ECODA- THE EUROPEAN CONFEDERATION OF DIRECTORS' ASSOCIATIONS
THE EUROPEAN VOICE OF DIRECTORS
42, rue de la Loi, 1040 Brussels, Belgium

Tel: +32 2 231 58 11
Fax: +32 2 231 58 31
Email: beatrice.richez-baum@ecoda.org
www.ecoda.org

This publication is sponsored by