Position Paper

FERMA's comments on the proposed Global Internal Audit Standards by the Institute of Internal Auditors

31/05/2023

Executive Summary:

FERMA provides its comments and suggestions on the proposed Global Internal Audit standards [available here] on behalf of the European risk management profession for consideration by the Institute of Internal Auditors.

1. It is important to be clear on the *independence* of the Internal Audit function and that this independence should be maintained.
2. Cooperation should really be at the heart of the standards since it is vital that Internal Audit cooperate closely with other key functions.
3. Around the language used on risk in the glossary, FERMA recommends some changes to the wording.
4. While recognizing the standards are global, FERMA believes there is room to acknowledge more the EU legislative developments and their knock-on impacts on the Internal Audit profession.
5. The Three Lines Model should also receive more of an explicit reference throughout the standards.

Introduction

The Global Internal Audit Standards provide guidelines for professional internal auditing worldwide. They establish requirements and recommendations for internal audit services and serve as a basis for evaluating their performance. The Standards consist of principles, which are broad descriptions summarizing groups of requirements and recommendations for internal auditing practice. FERMA's comments focus on the importance of the independence and cooperative spirit of the Internal Audit Function, as well as the clarity of the language employed in the document. FERMA looks forward to further engagement with the Internal Audit profession as these standards are developed and formalised.

Comments on the Glossary terms

The following part is structured as follows: for each bullet point, the upper part (in italics) is dedicated to the definition proposed by the IIA. The lower part, on the other hand, gives space for FERMA's comments.

- **Assurance services**: *Services through which internal auditors perform objective assessments to provide statements about conditions compared to established criteria. Such statements are intended to give stakeholders confidence about an organization's governance, risk management, and control processes. Examples of assurance services include financial, performance, compliance, and technology engagements.*

  FERMA suggests that Assurance services are related to "processes", being the risk management and internal control processes (and/or systems) under the responsibility of the 2nd line.

- **Quality assurance and improvement program**: *A program established by the chief audit executive to evaluate and ensure the internal audit function conforms with the Global Internal Audit Standards, achieves performance objectives, and pursues continuous improvement. The program includes internal and external assessments.*

  FERMA believes that these improvement programs must not be confused with the Quality assurance and improvement programs established by the responsibility of the quality manager (ISO 9001)

- **Residual risk**: *The portion of inherent risk that remains after management executes its controls (also called "net risk").*

  Managing risks is an enterprise-wide responsibility, bottom-up and top-down. It is not only about management executing. Further, it may be better rephrased as the portion of inherent risks that remains after the enterprise has implemented treatment measures. It is important to consider that the concept of treatment is wider than the concept of controls since you can also treat risk by transferring it. Therefore, treatment is more accurate than control.

- **Risk:** *The possibility that events will occur and affect the achievement of strategy and business objectives.*

  The definition used is the one of COSO. Adding ISO 3100 of the risk is the effect of uncertainty on objectives may also be useful since uncertainties are the core of risks. Maybe overall the definition could be an uncertain event that might occur and affect the achievement of strategy and business objectives in view of sustainable value creation.

- **Risk appetite**: *The types and amount of risk that an organization is willing to accept in the pursuit of its strategies and business objectives. Risk appetite takes into consideration the amount of risk that the organization consciously accepts after balancing the cost and benefits of implementing controls.*

  FERMA suggests "the pursuit of value" instead of "pursuit of business objectives".

- **Risk assessment**: *The identification and analysis of risks relevant to the achievement of an organization's objectives. The significance of risks is typically assessed in terms of impact and likelihood.*

FERMA suggests adding "evaluation" to identification and analysis; also risk assessment is part of an overall enterprise-wide risk management process starting with the establishment of the context and followed by treatment and monitoring.

Risk management: *A process to assess, manage, and control potential events or situations to provide reasonable assurance regarding the achievement of the organization's objectives.*

FERMA suggests not using "assurance" when referring to risk management since it belongs to a second line responsibility and might seem an overlap with the third line function.

Comments on section 3: "Governing the Internal Audit Function".

Principle n.6: "Authorized by the Board"

The board establishes, approves, and supports the authority, role, and responsibilities of the internal audit function.

While FERMA has no concerns with the standards under Principle 6, we would raise the point that a powerful message to send would be for the Board to emphasize, or possibly even mandate enhanced cooperation between IA and other functions, all the while maintaining the IA function's independence. It is our view that in a constantly evolving landscape, for governance models, such as the Three Lines model to succeed there must be good cooperation across functions. Moreover, we would add that in general the proposed standards miss an opportunity to make explicit reference to the Three Lines model in some key areas.

Principle n.7: "Positioned independently"

The board establishes and protects the internal audit function's independence.

The chief audit executive is sometimes asked to take non-audit roles. We must avoid the misunderstanding that internal audit (3rd line) can simply take over risk management (2nd) roles. It is important that the responsibility and priority of the 3rd line remains to the internal audit.

As FERMA has stated elsewhere, it is our opinion that the independence of Internal Audit is mainly ensured by:

- The nomination of Internal Audit by the board, with a direct reporting line; Based on practices in place in many SMEs, the "direct reporting line" could be both hierarchical or functional.
- No involvement of Internal Audit in business activities (where the IA became the 1st line) that can be subject to audit.
- Clear roles and responsibilities avoiding overlap/gaps/mislead with other roles or functions is essential activities. FERMA believes that the independence of Internal Audit is vital to ensure credibility in its assurance responsibilities. Furthermore, and in the context of independence, or within Principle 7 more broadly, it might be wise to refer to the principle of proportionality in terms of scope of responsibility of auditors. Put another way, there should be some formal

recognition of the difference in bandwidth between IA in large organizations and smaller enterprises.

Comments on section 4

Principle n.9: "Plans strategically"

The chief audit executive plans strategically to ensure the internal audit function fulfills its mandate and is positioned for long-term success.

Principle n.9.1: "Understanding Governance, Risk Management, and Control Processes"

While FERMA has no fundamental concerns with the majority of what is written in this standard concerning the requirements, we do however suggest a slight reframing of understanding risk management and control processes.

Risk Management is 1) responsible for identifying, analysing and managing risks in cooperation with risk owners; and 2) guiding senior management in achieving its objectives by highlighting the key risks and opportunities so they can be managed with the organization's risk appetite. It provides an independent view on the risk profile and strategy of the organization by assessing, explaining, and proposing solutions to manage risks in consultation with risk owners. When an Enterprise Risk Management (ERM) model is implemented, it focuses on risks whose nature is such that they can affect the business performances and the realization of the strategic and operational objectives. The perspective is, therefore, wider than an operational process. Action following a risk analysis can be a joint review with the management of the risk mitigation strategy, leading to the development of new and more advanced controls and/or transfer of the risk.

Principle n.9.6: "Coordinate and Reliance"

FERMA starts with a question in this section, to whom are IIA referring to when they write "other providers of assurance and advisory services that includes a basis for relying upon their work"?

It is FERMA's view that to ensure a proactive approach and create value, the role of Internal Audit as 3rd line should not rely solely on evaluating compliance with procedures and processes. Its work should also be specific to the context of the audited location, culture, business line, and so on.

The Three Lines model puts forward a collaborative approach between Internal Audit and the 1st Line of to increase the effectiveness of processes so that they can meet changing stakeholders' needs.

- Internal Audit should not shoulder risk managers' responsibilities. Moreover, the Internal Audit should not autonomously launch initiatives that would undermine its independence as provider of assurance.
- The proximity between the Internal Audit and the first lines could be seen as an opportunity.

Internal Audit should work in concert with others, e.g., 1st/2nd line, but also by relying on external sources that the internal processes are aligned to the best practices of national and internal standards; it positively affects the performance of the company.

Principle n.11: "Communicates Effectively"

The chief audit executive ensures the internal audit function communicates effectively with its stakeholders.

In Standard 11.3 "Communicating Results", it should be formalised that Internal Audit results and conclusions must be an input for Risk Management, for example.

The need for close cooperation between Internal Audit and Risk Management could be reemphasised within these principles.

Both Risk Management and the Internal Audit are involved in the oversight of risks but from different perspectives. They complement each other. This is why they must share and exchange information, knowledge, data, and analysis to inform the executive management.

To create effective collaboration between Risk Management and Internal Audit, the two functions should interact regularly and share the results of their activities:

- ERM results and risk analysis must be an input for Internal Audit: The results of the ERM analysis can be integrated into the audit plan and used for the evaluation of Risk Management practices. If the audit shows a less than expected level of effectiveness, Risk Management should re-evaluate the final exposure as well as the related internal controls.
- Internal Audit results and conclusions must be an input for Risk Management: The findings from audit activities can trigger new risk analysis in the ERM process. Risk Management can evaluate the need for a wider risk assessment based on a specific operational finding by Internal Audit.

Other comments

- Not at once easy to analyse the documents with its combination of sections, principles, domains, and standards.
- We would also like to emphasise a wider point that while we recognise the important stride forward this document makes, it is also short of some explicit reference to EU-legislative developments that will directly impact the Internal Audit profession in the EU. For instance, with reference to the Corporate Sustainability Reporting Directive (CSRD) and the Corporate Sustainability Due Diligence Directive (CSDDD), companies will be obligated to report on and implement the principle of Double Materiality. Perhaps even at a conceptual level, the IA standards could reflect this development.

Contact person: Charles Low, Head of EU Affairs, Charles.low@ferma.eu

FERMA - The Federation of European Risk Management Associations brings together 22 national risk management associations in 21 European countries. FERMA represents the interests of more than 5000 risk and insurance managers in Europe active in a wide range of business sectors from major industrial and commercial companies to financial institutions and local government bodies. More information can be found at www.ferma.eu