FERMA's Response to the IIA Global Consultation

Three Lines of Defense Review & Survey

Section A1: The case for refreshing and updating the Three Lines of Defense

What is your opinion of the familiar graphic that has been used to illustrate the Three Lines of Defense since 2013? [select one]

- Strongly disapprove
- Mostly disapprove
- Neither approve nor disapprove
- Mostly approve
- **Strongly approve**

What recommendations do you have for improving the Three Lines of Defense graphic?

The Three Lines of Defense graphic is well-known and well-established. It offers simplicity and clarity as regards the attribution of roles within an organization. It avoids confusion and duplication. Risk Management and Internal Audit jointly adopted this model in 2010, and we believe it is well understood and implemented in Europe. We, therefore, recommend only minor graphic changes to keep a simple diagram that is easily remembered and understood by all stakeholders.

These minor changes should highlight the interaction between the three lines of defense in order to illustrate the collaboration between the various lines/functions and show that these lines of defense are not operating in silos.

Many organizations have incorporated the Three Lines of Defense into their corporate governance and already adapted it according to their needs. Making significant changes could, therefore, lead to a proliferation of models in use and lack of clarity for stakeholders.

FERMA and the European Confederation of Institutes of Internal Auditing (ECIIA) used the Three Lines of Defense as the basis for our joint guidance on cyber risk governance first published in 2017 and updated in 2018. We believe this shows the model is robust enough to respond to emerging risks.

Section A2: Assessment of the Three Lines model

What is your opinion of the assessment made of the Three Lines of Defense model described in this section? [select one]

- Strongly disapprove
- **Mostly disapprove**
- Neither approve nor disapprove
- Mostly approve
- Strongly approve

What further comments do you wish to add to the assessment of the Three Lines of Defense model?

We do not support the following development for Internal Audit: *"To expand this description to embrace the role of Internal Audit as a strategic partner and trusted advisor."*

Adaptability and flexibility are the main proposals of the Exposure Document, which remains at the same time very careful to preserve Internal Audit independence.

In our understanding, such adaptability and flexibility can allow Internal Audit to deal with different topics/contexts/processes and create value for the business. It means that Internal Audit can provide recommendations and advice to support more effective assurance within its current responsibilities.

Indeed, to move the Three Lines of Defense from a defensive to a proactive model, the Internal Audit function should work with operational functions to improve their methods of operating and processes and so enhance their performance.

Furthermore, this section should emphasize the role of the Risk Management function in support of the strategy of an organization, which is currently missing in the Exposure Document. Risk managers help determine the success of that strategy in the face of uncertainty by coordinating internal as well as external risk aspects of functions across the organization.

Section B1: Why organizations exist

The exposure document proposes to strengthen the Three Lines of Defense by repositioning it in the context of governance, organizational success, and value creation. To what extent do you approve of this approach? [select one]

- Strongly disapprove
- Mostly disapprove
- **Neither approve nor disapprove**
- Mostly approve
- Strongly approve

What challenges do you see in applying the model to this broader governance context?

The Three Lines of Defense model currently serves two principal goals:

- To increase the performance of an organization through effective management and control of risk.
- To increase the confidence among regulators and external stakeholders.

Regulatory pressure is currently the main driver for adoption of the Three Lines of Defense. Listed companies incorporate it through corporate governance codes, and financial services use it in response to pressure from supervisors. Auditing firms and consultants have also heavily promoted the model.

It is important to understand why other organizations have been less likely to adopt the Three Lines of Defense. In our experience, there is sometimes a misunderstanding by the top management of the roles of the 2nd and 3rd lines of defense. They often perceive these as an extra cost and a further element of complexity, rather than an opportunity to improve the business operating model.

We agree, therefore, that the Three Lines of Defense model should be repositioned as a method of increasing performance and value creation. This is how we will convince more companies to adopt it. However, we believe that the Exposure Document does not yet demonstrate well enough how the model can go beyond a regulatory response and add value to the business.

An effective governance framework must combine the internal objectives of an organization of optimizing performance and creating value with its external drivers, including meeting legal, regulatory, and societal expectations.

Shareholders and stakeholders should be able to see the advantages of the Three Lines of Defense model in reconciling these objectives, such as:

- No risk of overlap
- More cost efficiency
- Clear roles and responsibilities
- A communication tool
- Contribution to risk culture

Section B2: How governance fosters organizational success and value creation

The exposure document identifies four main complementary and overlapping groups of roles and activities that typically support governance, organizational success, and value creation. They are leadership and oversight; strategy execution; support, guidance, and control; and objective assurance and advice.

These four groups form the basis of the main functions that comprise the model. To what extent do you think this analysis helps advance understanding of the model and improving its application? [select one]

- Strongly disagree
- Mostly disagree
- Neither agree nor disagree
- Mostly agree
- **Strongly agree**

What further comments do you wish to make on this approach?

n/a

Section C1: Building on the model

This section describes the typical roles and responsibilities of each of the main functions that comprise the model as well as key external bodies that contribute to governance, organizational success, and value creation. What is your assessment of this section of the Exposure Document? [select one]

- **Strongly disapprove**
- Mostly disapprove
- Neither approve nor disapprove
- Mostly approve
- Strongly approve

What further comments do you wish to add on this section?

➢ **Clarification of the role of the Risk Management function**

The description of Risk Management in C.1.3 along with the functions of the 2nd line of defense (Compliance, Financial Control and Quality) is incomplete and incorrect:

- The role of the Risk Management function is not to "develop and test policies approved by the governing body" as mentioned in C.1.3.
- There is no explanation of the specific role played by the Risk Management function.

A dedicated Risk Management function is crucial for the organization. Its role should be clarified in order to **avoid confusion with other functions with responsibilities for risk but a different focus**. Risk, Quality, Control and Compliance have their own goals and operational approach.

Risk Management is neither a control function nor a quality function. The role of the Risk Management function is **to help senior management achieve its objectives while highlighting the key risks to success so they can be managed with the organization's risk appetite.**

Risk managers support the senior management and/or the board in the definition of the risk appetite, tolerance and limits of the organization. They contribute to the development and implementation of a risk culture across the organization.

Risk Management is an interconnected function. Collaboration with the first and third lines of defense is a key aspect of the risk manager's role. He or she integrates information from other risk-related functions and acts as a risk conductor to give top management a clear and comprehensive view of the company's risk universe.

In addition, risk managers are responsible for technical activities, such as training internal stakeholders, helping build a risk culture and managing risk transfer. They report to senior management and the board about risk developments and major issues.

➢ **Enhancing the added-value of Internal Audit work**

The management perception of the "assurance" role needs to evolve from that of a "controller" to an "advisor". This evolution will generate the flexibility and adaptability mentioned in the Exposure Document and create a trusted relationship with the first line of defense.

We support the view that adaptability and flexibility can be key success factors for Internal Audit if that means moving from a controller-type role to an advisor-type role without affecting the crucial independence of the function. In our opinion, this independence is mainly ensured by:

- nomination of Internal Audit by the board, with a direct reporting line;
- no involvement of Internal Audit in business activities that can be subject to audit;
- clear roles and responsibilities avoiding overlap or gaps in essential activities.

To ensure a proactive approach and create value, the role of Internal Audit as 3rd line of defense 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 of Defense model should put forward a collaborative approach between Internal Audit and the 1st Line of defense to increase the effectiveness of processes so that they can to meet changing stakeholders' needs.

Section C2: A coordinated approach

The Exposure Document describes the importance of coordination, integration, and alignment across roles as well as the opportunity for Internal Audit to play a lead role in facilitating this. Do you agree that this is an appropriate role for Internal Audit? [select one]

- **Strongly disagree**
- Mostly disagree
- Neither agree nor disagree
- Mostly agree
- Strongly agree

What further comments do you wish to add on this section?

Facilitating the coordination, integration, and alignment across roles cannot be the responsibility of one single function like Internal Audit.

Both Risk Management and the Internal Audit are involved in the oversight of risks but from <u>different perspectives</u>. <u>They complement each other.</u> This is why they must share and exchange information, knowledge, data, and analysis in order 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:

1) <u>ERM results and risk analysis must be an input for Internal Audit</u>: 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.

2) <u>Internal Audit results and conclusions must be an input for Risk Management</u>: 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.

Section D1: Scalability

The exposure document describes ways in which the model can be adapted to suit the needs of an organization, including a maturity model. To what extent do you approve of this more flexible approach? [select one]

- Strongly disapprove
- Mostly disapprove
- Neither approve nor disapprove
- Mostly approve
- **Strongly approve**

What further comments do you wish to add on this section?

The core concept of Three Lines of Defense is valid for a small or a large organization. The model should be flexible enough for SMEs[1] to apply, since strict implementation can require significant resources.

Flexibility in the context of an SME can be reflected in:

- Dedicated or shared functions and the use of integrated or outsourced solutions. In small companies, the 2nd line functions (Risk Management and Compliance) are usually assigned to managers with other business responsibilities, but Internal Audit must remain independent to ensure credibility in the assurance activity.
- Size of the team for each function. One person vs a structured team
- Organizational position within the group. In small companies, a high-level position, usually reporting to the CEO, helps successful commitment.
- Complexity of the model. In small companies, the Risk Management approach is usually simplified. It focuses on qualitative evaluations and aims to identify and monitor a small number of critical risk situations. In large companies, the Risk Management model can be more sophisticated, based on the nature of the business, and use more resources.

[1] SMEs are used in the context of the European Union definition of an SME: https://ec.europa.eu/growth/smes/business-friendly-environment/sme-definition_en

Section D2: "Blurring of the lines"

The exposure document provides a way of explaining and allowing for the "blurring of the lines," recognizing that the Internal Audit function can provide value in nonassurance roles, as long as there is clear assessment of the potential impact on the effectiveness of governance and safeguards are considered. Ultimate responsibility rests with the governing body to determine the structure and roles most appropriate for the organization. To what extent do you approve of this approach? [select one]

- **Strongly disapprove**
- Mostly disapprove
- Neither approve nor disapprove
- Mostly approve
- Strongly approve

What further comments do you wish to add on this section?

➢ **Risk Management and Internal Audit functions have a different scope/ approach on risks**

Risk Management and Internal Audit are interrelated functions; however they **operate fully independently from each other.** Because of the difference in perspective as well as the different approach to risks, the same function cannot perform both roles.

Risk Management and Internal Audit have different tasks:

- **Internal Audit** has the responsibility to provide independent assurance that the action plans to avoid or mitigate identified risks have been implemented and are being followed. It focuses on operational and process risks, for instance, that arise from an incorrect implementation of a specific procedure in a location. The possible responses to an audit usually concern the reinforcement or improvement of the procedures or processes.
- The **Risk Management** responsibility is to manage the risk and internal control system. 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 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.

Having one function in charge of both Risk Management and Internal Audit would risk a lack of clarity within the organization.

Overall

Please add any further comments you may have about the exposure document and the overall direction it proposes for refreshing the Three Lines of Defense in effective Risk Management and control.

In summary, we believe that no material changes are needed but a shift in emphasis could be valuable. Any revision should have the four following objectives:

- Minor graphic changes to reflect interactions between the lines only. No change to the structure is needed.

- Reposition the Three Lines of Defense model as a tool to increase performance and value creation for an organization. It should show the advantages of an efficient risk governance framework for shareholders and management in achieving the business objectives, internal and external.

- Avoid blurring the lines, which can bring confusion and weaken the Three Lines of Defense model. Further clarification and explanation of the distinct roles and responsibilities of Risk Management and Internal Audit are needed, instead, to show:
    - The specificity of the Risk Management function in support of the strategy of the organization;
    - The added-value of Internal Audit as advisor for the first line of defense;
    - The need for close collaboration between the two functions.

- Describe how the model can be used by an SME

Contact Person: Julien Bedhouche, FERMA EU Affairs Adviser, julien.bedhouche@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 4700 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