



Contents lists available at SCOPUS

## ACRN Journal of Finance and Risk Perspectives

journal homepage: <http://www.acrn-journals.eu/>



# Beyond the three lines of defense: The five lines of defense model for financial institutions

Georgios L. Vousinas\*

National Technical University of Athens, School of Mechanical Engineering, Sector of Industrial Management & Operational Research, Greece

### ARTICLE INFO

#### Article history:

Received 25 May 2020

Revised 22 November 2020 and 13 May 2021

Accepted 02 June 2021

Published 07 June 2021

#### Keywords:

Three lines of defense

Five lines of defense

Internal audit

External audit

Regulator

### ABSTRACT

The purpose of this study is to provide an updated version of the widely accepted three lines of defense model (3LoD) to better apply for regulated financial institutions. The author proposes the five lines of defense model (5LoD) which consists of the existing three lines along with external audit and regulators (comprising the fourth and fifth line of defense respectively). In spite of the fact that the bodies forming the two additional lines of defense constitute the external lines of defense, there should be active in supervising and monitoring control issues within the organization, in strong cooperation with the internal lines. This calls for closer interaction among the internal auditors, external auditors and regulators in the design and implementation of an efficient and effective internal control system, aiming to strengthen the existing framework regarding the governance of modern financial institutions, which operate in a highly demanding regulated environment.

## Introduction

The Three Lines of Defense model (3LoD) came into surface around two decades ago and has since become the reference point for delegating control and risk management responsibilities to companies' operations, especially in the financial industry, where it originated. The Institute of Internal Auditors (IIA) formally adopted it in a Position Paper "The Three Lines of Defense in Effective Risk Management and Control" published in 2013 and has since promoted it as a valuable tool for those charged with governance (IIA, 2013). The 3LoD is graphically depicted in the following Figure 1:

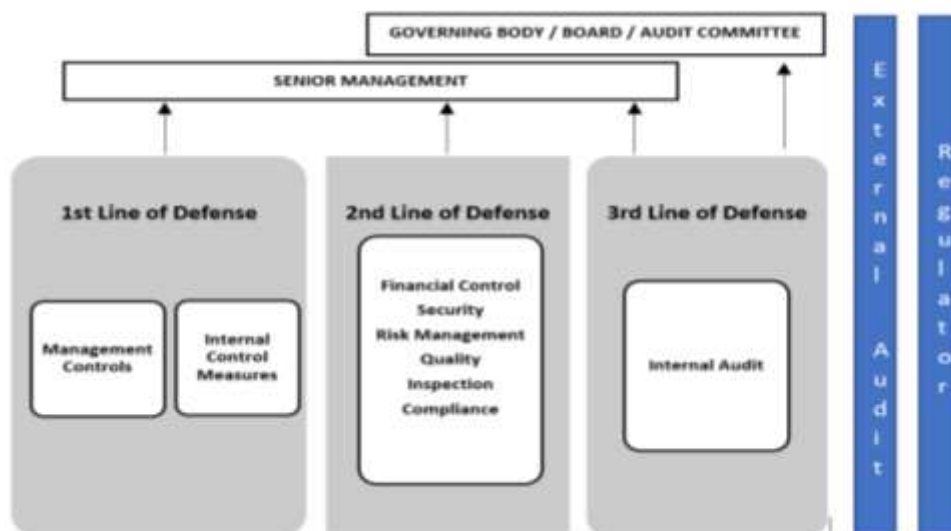
\* Corresponding author.

E-Mail address: [yousinas@yahoo.com](mailto:yousinas@yahoo.com)

ORCID: 0000-0002-0491-8594

<https://doi.org/10.35944/jofrp.2021.10.1.006>

ISSN 2305-7394



**Figure 1.** The Three Lines of Defense Model (adapted from IIA)

The Three Lines of Defense model distinguishes among three lines involved in effective risk management:

- Functions that own and manage risks.
- Functions that oversee risks.
- Functions that provide independent assurance.

The main characteristics of the three lines (with emphasis on the financial sector) can be summarized to the following (IIA, 2013).

*First Line: Management Line*

Those in charge of managing an organization’s risks as well as the risk owners constitute the first line of defense, also referred to as management line. More particularly, the managers in the first line are mainly responsible for running the business i.e. dealing with everyday operational risks and control processes. This includes not only the design of effective control mechanisms but also their operation and proper implementation so as to ensure that business activity is uninterrupted and according to the business plan.

These internal control procedures have been highly automated nowadays, making it easier to identify operational weaknesses and capture all the necessary data as soon as possible to timely implement all the required measures and the competent staff to be notified. It is of major importance to highlight the dual responsibility of the units involved in the first line as they are in charge of both generating revenues while remaining aware of the related risks and controls.

Overall, the main objective of the first line of defense is to improve the possibility that the company’s business goals are fulfilled via the effective implementation of the required risk management procedures and controls mechanisms by the corresponding staff (managers - risk owners). Regarding the examined banking industry, these units include the provision of financial services such as trading, asset management, cross-sales and customer relationship management systems (CRMs). This calls for effective managerial and supervisory controls in place in order to ensure compliance and to highlight possible control breakdown, inadequate processes as well as unexpected events.

### *Second Line: Risk Management & Compliance*

If the first line of defense proves incapable of addressing the encountered risks, then the role of the second is automatically upgraded. Management establishes various risk management and compliance functions in the second line to assist the first line controls. The typical functions in this second line of defense (which also apply in financial institutions) include the following:

- A risk management function that enables and monitors the implementation of effective risk management practices in order to help risk owners in identifying, assessing, monitoring, and mitigating the risk inherent in an organization's operations. In financial institutions, it is common practice that the risk management framework is overseen by a dedicated Risk Management Committee, that its key role is to ensure that all business units take all the required steps to manage all kinds of risks. Even more, a Risk Control Self-Assessment (RCSA) procedure is conducted annually, which is a structured methodology that aims to identify and assess risks that may affect the operations and processes of the bank units, thus allowing their proactive management.
- A compliance function responsible for detecting and mitigating risk arising from failure to comply with the provisions of the legislative and regulatory framework. In the banking industry, the compliance department reports directly, via the Audit Committee, to the Board of Directors, has a straight reporting line to the Chief Executive Officer (CEO) and is independent from units with executive duties. Among the main responsibilities of the compliance units in banks are the continuous monitoring and knowledge of the compliance requirements of central banks and other regulatory Authorities and submission of proposals for the amendment of the policy and procedures, in line with regulatory requirements and any identified weaknesses.
- A controllership function, the aim of which (in financial institutions) is to safeguard the trustworthy reporting of the organization's financial results in such a way that is in compliance with the existing legislative and regulatory framework. The senior level executive in charge of managing risks, pushing growth, and supporting the existing management team and the CEO in the financial sector is the Chief Financial Officer (CFO).

Conclusively, the second line of defense comprises of both compliance and risk management control mechanisms, and its key role is to verify the proper function of the existing controls of the first line in addressing the confronting risks a company faces. That is the reason why, in order to operate effectively, the second line must be independent of the first one as well as to be based on clear risk assessment principles.

### *Third Line: Internal Audit*

The third and final line of defense is Internal Audit (IA), which is an independent assurance function that reports directly to Senior Management and the BoD on how the operation of both the first and second line is in line with the expectations of the company's governing body. It also provides assurance that the internal controls and risk mitigation

practices implemented by all the units are sufficient and appropriate for the type and complexity of risk-taking activities. The fact that distinguishes the IA function from the other two lines of defense lies in its high level of organizational independence and objectivity. In financial institutions, a direct reporting line to the CEO and the BoD via the Audit Committee further strengthens the independence of IA.

The IA function performs audits based on an efficient and effective risk assessment methodology. In the case of financial institution, IA performs regularly (at least on annual basis) an overall risk assessment of the company, examining and identifying policies and procedures and even business units that demonstrate a high level of residual risk (i.e. the risk remaining after taking into consideration the existing internal control framework). As such, the IA can only ensure a periodic risk-based assessment compared with the ongoing monitoring that is typical in the other two lines of defense.

The aim of this paper is to enhance the effectiveness of the 3LoD model by proposing a new model that focuses on the special features of the modern regulated financial sector. For this purpose, the five lines of defense model (5LoD) is introduced, adding the external lines i.e. regulators and external auditing, which must be considered as an integral part of the company's internal control system. The paper is organized as follows: The introduction provided a short analysis of the main characteristics of the 3LoD model, while the next section is dedicated to a critical valuation of its main deficiencies, followed by a literature review; in the next section, the new model is developed and analyzed, while the last section presents the concluding remarks and the research proposals.

### **Three Lines of Defense: A critical assessment of the existing weaknesses**

Although the original idea behind the 3LoD was to develop a model of general applicability for all kind of organizations, however, it did not recognize the particularities of specific sectors, such as financial institutions and, more particularly, banks. Banking organizations are complex financial institutions operating in a highly regulated as well as constantly changing business environment, dealing with high levels of risk (Vousinas, 2016). Essentially, the Achilles heel of the 3LoD model lies in the lack of a broad overview of the entire organizational structure resulting in ineffective control measures at multiple layers of the company.

The model also gained a lot of criticism in the time period following the burst of the global financial crisis of 2008 (and the collapse of major banking institutions), mainly due to the high level of complexity of the financial industry (e.g. Mülbart, 2009; Davies, H., & Zhivitskaya, M., 2018). Another reason behind the failure of the 3LoD lies in the fact that, under crisis conditions, it proved insufficient in explaining how the the three lines of defense are incorporated in the corporate governance framework of the companies and how they affect it. Even more, the insufficiencies in the understanding of risk-taking policies and their impact both in and out of the individual financial institution are frequently argued as the origins of the recent banking scandals.

More specifically, the various scandals in the financial industry brought into surface the following problems (analyzed per line of defense):

*First Line of Defense: Conflict of interest among control duties and generating revenues responsibilities.*

It is common in the first line to exist a confusion between the primary goal of achieving the profit targets and the risk management – internal control objectives. And the previous experience has shown that often companies put greater emphasis on the achievement of financial objectives instead of control-oriented. Thus, weakening the first line of defense, allowing the various risks to enter the organization and pass through existing safeguards.

The abovementioned confusion is clearly seen in the 2008 fraud at Societe Generale that involved a sequence of unapproved, undetected speculative positions for over a year period. The critical weakness of the company's internal control system (as identified by a relevant report by PwC) was proved to be the lack of appropriate awareness of the fraud<sup>1</sup>. More specifically, the main concern of the company was to ensure the proper execution of the transactions only from the operational perspective, neglecting the overall risk environment. This caused a confusion among the performance of controls for validation of the accuracy of the given explanations and corrections in place and the resolution of discrepancies.

Another typical example of this kind of failure in the first line is that of the 2011 Swiss bank UBS rogue trader scandal that caused a loss of over \$2 billion US dollars and was attributed to insufficient controls and an inadequate financial reporting system<sup>2</sup>. In this case, two major control deficiencies came into surface, the controls for relations among different trading desks to safeguard that internal transactions are valid and properly recorded in official books and records, and the control requiring confirmation with counterparties of trades within the bank's equities business.

In order to avoid such unpleasant situations, banks should clarify the role of the first line with respect to risk ownership as well as the responsibility for risk assessment. This calls for enhancing internal control procedures, e.g. by developing dedicated divisional control units to replace the scattered divisional operational risk, compliance, and control resources that typically exist nowadays. In this direction, modern financial institutions engage in various methods such as the usage of balanced scorecards and the creation and monitoring of key risk indicators (KRIs).

*Second Line of Defense: Inadequate monitoring, lack of resources and properly skilled staff*

The aim of the second line is to monitor and address the deficiencies of the first line-of-defense controls by operating compliance and risk management functions. But in order to tackle these shortcomings, it should be properly customized to suit the specific needs of every business sector, especially complex ones like financial institutions. Nevertheless, in the business practice, these functions are distributed all through an organization and the monitoring tasks are usually limited to just a single or specific area thus, creating gaps and deficiencies.

Even more, the resources (human and non-human, i.e. IT) involved in risk management and compliance functions in the second line are often insufficient to support the internal control system and bring down the various risks in an acceptable level. And these resource and budget constraints do not allow supervisors and other stakeholders to conduct reviews themselves and help in addressing existing deficiencies (e.g. the analysis and resolution of suspense

---

<sup>1</sup> Société Générale, Summary of PwC diagnostic review and analysis of the action plan, 23 May 2008

<sup>2</sup> UBS Annual Report 2011

items or unreconciled transactions). There is also a need (especially in the financial sector) for more specialist resources dedicated to risk, compliance and control activities.

Additionally, there might be a lack of the required skills to evaluate in an effective manner procedures and internal controls in the first line, such as the assessment of complex models such as internal ratings or loan loss provisioning (LLP) models in banks. The solution lies in attracting highly skilled working staff, with considerable experience, in the second line functions, rather than in the first line.

The aforementioned fraud case of Societe Generale displayed several weaknesses in the second line as listed below:

- i. Controls were split among different units within the same function or sometimes between several different functions, and due to insufficiently explicit procedures, it was made difficult to obtain an overview of the situation. The problem was deteriorated even more due to the lack of a systematic process for centralizing and escalating red flags to the sufficient management level.
- ii. There was a mismatch among the front office activities and the allocated resources to support and control functions.
- iii. The IT systems failed to keep pace with the growing complexity of the general trading environment and process effectively the performed transactions.

As mentioned before, the key functions of the second line of defense are the compliance and risk management functions, which are in charge of assessing the overall risks related to the operation of an organization. Particularly in the banking sector, owing to the tighter regulatory framework and the even more complicated bank products and procedures, financial institutions have added extra, more specialized staff as well as additional functions in the second line (in close collaboration with the regulating authorities), making the latter an indispensable part of their internal control system. This is attributed to the fact that regulators in banks nowadays play an increasingly substantial role, having to deal with every aspect of operation and strategy concerning the safeguard of financial institutions' soundness.

### *Third Line of Defense: Ineffectiveness of the Internal Audit function*

In order an Internal Audit function to be considered effective in enhancing and safeguarding business value must be properly positioned, sufficiently resourced and has to provide (among others) a risk-based assurance aligns with the strategies, risks and objectives of an organization (IIA, 2017). In the modern banking environment, financial institutions have established an Internal Auditing Committee, which is a part of the Management Committee, gives a higher profile to the IA functions and facilitates effective conduct of risk-based internal audits. In their organizational chart, there is also a distinct IA Department/Division, i.e. an internal auditing unit that operates independently of other departments. The main goal of this department is to design, evaluate and implement a well-established risk-based audit plan (on at least annual basis) performed by experienced auditors that have a deep understanding of the risk profile of the organization. And the primary target of an audit plan is to identify areas of high risk or procedures that require more frequent and scholastic audits.

But when there is a failure in detecting the right high-risk areas, then the effectiveness of the third line of defense is severely weakened, and the focus is placed on areas of low risk profile. The cases of Societe Generale and UBS identified this kind of failures. In the first case, procedures did not reflect the requirement to analyze consistency of risks results and positions, while in terms of supervision, the internal control system was slow in reacting and instantly addressing the most sensitive issues. In the second case (UBS), the IA function proved inadequate for two main reasons: on one hand, it performed only a partial review of the bank's procedures (critical trading desk for US mortgage-backed derivatives), and on the other, despite identified control weaknesses, the audit reports were not finalized in time, causing serious delays that weakened the quality of the reports and eventually allowed fraud to take place.

Due to these "internal" failures, the role of external auditors is becoming more and more important in the structure of financial institutions' internal control system, assisting in addressing the inadequacies of the classic 3LoD model and in preventing fraud. More specifically, beside the traditional validation of financial reports, external auditing enhances the reliability of the risk management framework by conducting periodic risk assessments and analyzing the overall risk tolerance of the institution. Additionally, it reviews the security measures that an organization has in place for addressing corporate fraud and, by developing efficient crisis management plans for use in fraud incidents or corruption allegations, can assist in ensuring adequate corporate governance practices.

### **A literature review on the three lines of defense**

The 3LoD model has been widely accepted as a benchmark for designing and implementing an effective total governance management system for the control of business risks. But as analyzed in the previous section, the model has proven to be limited and restrictive, and it is not equipped to reflect the current challenges of modern organizations. In this section, a literature review is performed in order to highlight the existing research on the addressing of the model's weaknesses and the proposals on how it can be strengthened and improved. It should be pointed out that the relevant research is fragmented and vague, and the critical issue of the update of the 3LoD was put on the epicenter only after the burst of the global financial crisis of 2008 and the collapse of major financial institutions.

According to the findings of Lyons (2011, 2015), the global financial crisis has highlighted the necessity of improving the existing enterprise risk management (ERM) practices, especially at the board and general management level. In order to address this, the author proposes two additional internal lines of corporate defense, a fourth line – board committees and sub-committees and a fifth line – the BoD itself, with the application of which companies can enhance their ERM methods. Even more, organizations can use these extra lines as a mechanism for making individuals or groups to account for the performance of their operational duties.

A couple of relatively recent reports point out that as companies grow in size and regulatory as well as risk environments become even more complicated, the three lines become more blurred (Ashby et al., 2012; Power et al., 2013). In particular:

Ashby et al. (2012) tried to shed light on risk culture by conducting detailed interviews with senior risk executives of nine major UK financial institutions. According to their empirical findings, the most critical issues regarding risk

culture happened between the first and second line of defense, suggesting that this (usually taken for granted) distinction may not be helpful in advancing the related debate. In a similar research report, Power et al. (2013) aimed to discover and analyze how the risk culture agenda was taking shape inside different organizations, studying several banks and insurers in the United Kingdom. The findings raised concerns about the closeness of the second line risk function with first line business operations, identifying tensions and skepticism about the very possibility of measuring and reporting on risk culture, justifying that the demarcation of roles among the first and the second line is, indeed, fuzzy.

On the other hand, Protiviti (2013) follows a different, integrated approach through which an organization responds to risk. More specifically, it characterizes the first line of defense as the “tone of the organization” and places the business-line leaders and process owners as the ultimate owners of risk, holding them accountable for the results. In the second line, it positions independent the compliance and risk management functions with the required escalation authority to serve as a viable defense line instead of serving as mere facilitating or reporting mechanisms. And positions the IA function (third line) to extend its value proposition to risk management. Finally, this approach provides direction to the BoD and senior management as to how an organization should approach risk management and compliance and highlights the fact that when significant issues are escalated to the management’s attention, it is totally up to them to hold the appropriate balance among the protection and creation of business value.

In order to significantly improve all three lines of defense in operational risk management, Luburić (2017) proposes the application of the principles of both quality and risk management and concludes that the successful functioning of all the lines mainly requires good communication channels among them as the strengthening itself increases the number of connections and topics for communication.

Boughey (2017) provides criticism on the 3LoD model, stating that it has caused many difficulties to financial institutions despite been developed to be straightforward enough so as to be generally applicable. Indeed, the model was originally designed for the purpose of enhancing banks’ operational risk management practices, as well as assisting regulators to better understand the risk owner of every business function (BCBS, 2011). But the model in its simplest form proved insufficient to increase personal accountability as well as to provide distinction among the first and second line.

Mabwe et al. (2017) investigate operational risk governance and internal control frameworks in UK financial institutions since the 2000s in order to examine the effectiveness of the traditional three lines of defense model. The empirical results showcase that financial institutions do not clearly understand the three lines, a fact that leads to replication of roles and coverage gaps. The findings also highlight the different ways of the model’s practical implementation by banks, attributed to the special requirements of the sector as well as the diverse business plans. Finally, on the critical issue of managing operational risk, the authors suggest that the best practice will come from those institutions who understand how their lines of defense work in practice and manage them, respectively.

And the most recent contribution aiming to address the weaknesses and towards the update of the 3LoD model is the exposure document released by the IIA (IIA: The Three Lines of Defense Exposure Document, 2019) that provides an analysis of the model and makes proposals on how it can be strengthened and further improved.



According to this document, the model is considered limited, and the following key opportunities for development are highlighted:

- The significance of coordination as well as collaboration associated to organizational priorities and operational needs.
- To promote a proactive as well as a reactive role in achieving business goals.
- To shed light on the “blurring of the lines” and provide adequate solutions.
- To be properly adapted so as to be able to be easily adopted by any kind of business, regardless of the size and/or sector.
- To update the existing graphical representation to address modern issues.
- To broaden the existing analysis to enhance the role of the internal auditor as both a strategic partner and a trusted advisor.

### **Beyond the 3LoD model: The five lines of defense model for financial institutions**

After the analysis of the weaknesses of the 3LoD model and the relevant literature review, it is justified that the model needs to be substantially updated in order to address the challenges of modern regulated financial institutions, given both their significance and the complexity of their activities. Taking into consideration the aforementioned proposals of IIA and those stemming from the literature as well as the series of banking scandals, the five line of defense model (5LoD) for financial institutions is proposed to share as a theoretical framework and towards a more efficient internal control system, as a substantial part of modern corporate governance practices. Essentially the 5LoD is the 3LoD model with the addition of two extra lines - regulator and external audit (external lines of defense). It must be pointed out that the developed model may apply to financial institutions in general, but the thorough analysis and the focus is placed on regulated banking institutions.

In the initial paper of IIA regarding the 3LoD model (IIA, 2013) it is emphasized the fact that these two external bodies (although outside the organizations' structure) can have an important role in the organization's overall governance and control structure, especially in regulated industries, such as financial institutions. Even more, regulators periodically perform an independent and objective function to assess the whole or part of the first, second, or third line of defense. Finally, it is clearly stated that when external auditors and regulators are coordinated in an effective way, they can be considered as additional lines of defense, providing assurance to an institution's shareholders, including senior management and the BoD. More analytically, the two new lines are analyzed below.

#### *Fourth line: Regulator*

The traditional duties of regulators are the application and monitoring of rules designed to increase transparency and accountability in various areas, such as capital requirements, financial reporting etc., but the focus is placed on large financial institutions due to their critical role in the economy as a whole. Typically, financial regulation sets the expectations for organizations to follow that are enforced via a continuous process of inspection, review, reporting, and applicable penalties.

Nevertheless, the role of the regulators in the fragile banking environment has gradually become crucial due to the ever-growing risk cases, corporate scandals as well as in response to crisis events that highlighted the weaknesses of the existing internal control systems. And all these risk incidents have led to putting these deficiencies in the top of supervisory and governmental agendas. Thus, regulating the internal control systems of modern financial institutions has proven a necessity for mitigating risks and maximizing both their efficiency and effectiveness.

This requires, as mentioned before, to build a strong relationship among the third line of defense (IA) and regulators. As underlined in the Basel Committee on Banking Supervision (BCBS) paper on the internal audit function in banks (BCBS, 2012), this relationship is achieved by establishing a direct communication channel among IA and regulators. More specifically, supervisors must communicate with the internal auditors of the supervised banks in a regular basis in order to evaluate the effectiveness of the internal control system. This includes the measures for addressing the existing deficiencies and risk exposures, the main findings, and recommendations, as well as the corrective actions taken in response to the latter.

So, the fruitful cooperation among the third line of defense - IA and the proposed fourth - Regulators is proved vital for banking institutions in order to develop and maintain an efficient as well as effective internal control system. By adding the fourth line of defense in the design of a reliable internal control framework, financial institutions enjoy a series of advantages as follows:

- The deeper involvement of the supervisors creates a more holistic approach to the risk control framework.
- Establishing a two-way information channel develops win-win relationship among regulators. This is achieved as supervisors share more relevant information with the IA function and vice versa thus, enhancing the overall effectiveness of the internal audit /function.
- As supervisors become a substantial part of the financial institution's internal structure, they are actively involved in the effectiveness of the risk management and control procedures as any other business unit.
- Beside the interconnection with IA, a closer cooperation with the compliance departments of the financial institutions is developed, contributing to better implementing the regulatory framework. This collaboration can also have positive effects in motivating both parts to propose improvements towards a more proactive, improved and harmonized regulatory environment.

#### *Fifth line: External Audit*

As mentioned before, the recent global crisis brought into surface the urge to improve the role of the external audit function of banks, following the several identified vulnerabilities in the risk management procedures, internal control mechanisms and corporate governance procedures of banking institutions (BCBS, 2014). External audit offers an extra level of independent assurance for all stakeholders regarding the precision of a firm's financial reporting as well as the systems that support it. And as financial institutions are moving towards more and more extended types of external reporting that reflect both financial and non-financial capitals, opportunities arise for even greater value for stakeholders, as well as additional needs for assurance, both for internal and external auditors.

The main role of the external audit is the review of financial statements in order to verify that they are a valid as well as a reasonable account of both past financial performance and current financial position and that are consistent

with a suitable financial reporting framework. At this point, it must be highlighted that the external auditor's opinion is highly relevant in establishing the credibility of financial statements and strengthening the financial soundness of the institution. Nevertheless, the main duties of the external auditors vary from that of the internal auditors as the former are primarily involved with the financial statements, whereas the latter have a broader range of activities. The external auditor confirms that financial statements provide a fair reflection of the financial position and performance of the company in all material respects (OECD, 2015) thus, playing a vital role in maintaining market confidence in audited financial statements. But in the banking sector, this public role is strongly related to financial stability, owing to banks' financial mediation role within the economy as a whole. And just like internal auditors, external auditors are independent assurance providers to senior management, board of directors and shareholders.

From the above, the critical role of external audit in the design and implementation of a proper internal control system in modern banks is proven, but at this point, it is important to shed light on the terms and scope of the relationship among external audit with the other lines, i.e. IA and regulator, that justify its role as the fifth line of defense.

Regarding the relationship with the regulator, external auditors play a critical role, from the regulatory perspective, by ensuring that supervisory policies and procedures (which require confidence in audited financial information) are effective, based on accurate data and suitable. To achieve this, a strong, beneficial for both parties and productive relationship among external auditors and supervisors must be established towards an effective contribution to the internal control system of banks.

Regulators are interested in the results of the internal control framework review performed by the external audit as they are often unable to conduct reviews themselves due to lack of resources and budget constraints while missing knowledge of critical internal information. But if the supervisor gained access to such valuable data, it would substantially enhance its effectiveness, and it could prove vital to external auditors who, due to their external role, normally do not have access to such crucial and detailed information. On the other hand, when such detailed information is provided by the regulators to the external auditors, the latter are enabled to form a much more spherical and clear opinion on the soundness of financial statements, establishing a valuable interconnection between both parties.

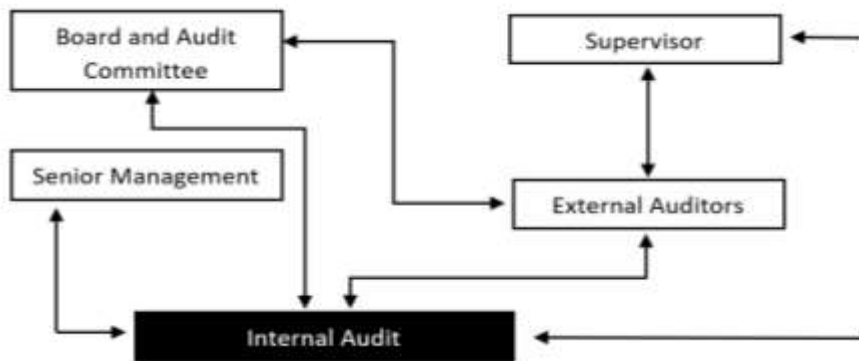
As for the usual relationship among internal and external auditors, a common aspect of the responsibilities of both parties is to offer an independent assessment and act as assurance providers. But, as analyzed before, the external audit function focuses on the reliability and integrity of financial statements, the scope of activities of the internal audit is much broader and includes, among others, an assessment of the efficiency and effectiveness of the risk management processed and of compliance with the legislative and regulatory framework. So since both internal and external auditors share a number of common goals, an effective coordination and cooperation among them can be nothing but beneficial for both parties and, therefore, for financial institutions' overall internal control efficiency.

In particular, the coordination of the third and the fifth line becomes of major importance for both parties as external auditors on one side have the opportunity to increase the effectiveness of financial statements auditing, while from the other side, that of internal auditors, the additional amount of essential information helps in improving the IA work. Even more, internal auditors can benefit from external auditors' specialized knowledge about financial

institutioning, while the external auditors can benefit from internal auditors' deep internal knowledge about the banks' risk environment and internal control system. Finally, their collaboration also helps in maintaining the effectiveness of banks' entire corporate governance, as both internal and external auditors are meaningful parties that provide assurance to the institution's shareholders, senior management and the BoD.

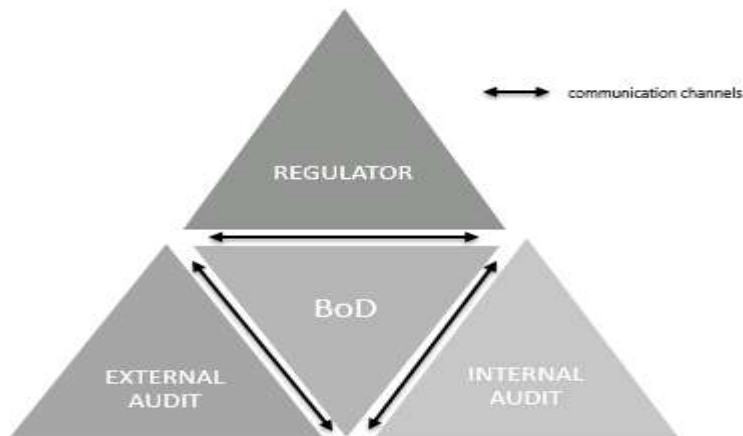
*The communication channels among IA, external lines of defense and BoD*

The previous analysis highlighted the need for stronger cooperation among the regulators and external auditors from one side and the internal auditors on the other side via the establishment of the right communication channels. These channels, on one hand between the internal line of defense (IA) and the external ones (External Auditors and Supervisory authorities) and on the other between the latter and the governing bodies i.e. BoD and senior management, are clearly depicted in the next Figure:



**Figure 2.** Internal Audit Function's communication channels with Supervisor & External Auditors (adapted from BCBS)

And due to the fact that internal auditors, regulators and external auditors are all independent assurance providers to the financial institution's governing bodies, their close cooperation can result in more efficient internal control systems. In order to highlight this type of "triangular" relationship amongst internal auditors, regulators and external auditors, the independent assurance pyramid for effective internal control systems in financial institutions is introduced, as depicted in the next figure:



**Figure 3.** The independent assurance pyramid for effective internal control systems in financial institutions

As shown above, in the “heart” of the pyramid is the BoD, where all the assurance providers report to and which is the supreme governing body of the financial institution. This pyramid essentially shows the value of the 5LoD model as the external lines of defense collaborate with the internal assurance provider - IA in providing additional assurance to shareholders and the BoD while assisting the latter in the implementation of an overall effective and efficient internal control system.

More specifically, regulators benefit from the interaction with internal and external auditors as both provide an independent assessment of the other lines of defense and assurance as well as additional information for specific tasks. So this collaboration can lead to the enhancement of the procedures and methodology utilized by the regulating authorities in performing their duties, contributing to a more proactive rather than reactive supervision.

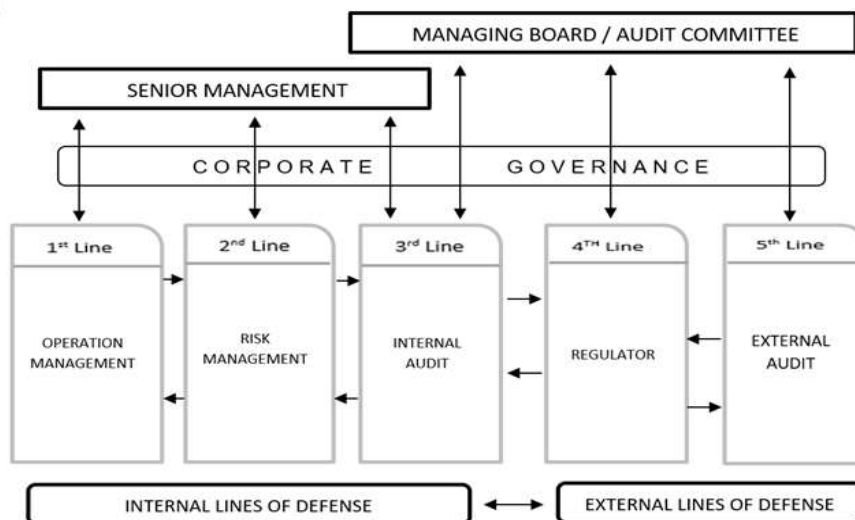
At the same time, a closer relationship with supervisors is beneficial for external auditors as during their duties, they can gain access to valued information that would assist them in fulfilling their responsibilities more effectively.

And regarding the classic interaction with internal auditors, both parties share a common goal in providing an independent assurance and assessment function and their interaction - knowledge sharing can only be beneficial for themselves and the financial institutions. It is this close collaboration that contributes the most in building a strong internal control system, leading to more efficient corporate governance practices.

Finally, as depicted in the above figure, the BoD is put on the epicenter of the financial institution’s corporate governance system as it has the general oversight of the organization and all independent assurance parties (both internal and external) refer to it. As a result, the existence of proper and strong communication channels among them is critical for mitigating overall risks and developing efficient internal control systems.

*The graphic depiction of the 5LoD model*

The proposed 5LoD model that justifies the critical role of regulators and external auditors as additional lines of defense in the design and implementation of an effective and efficient internal control system of modern financial institutions is graphically depicted in the next figure:



**Figure 4.** The Five Lines of Defense Model for financial institutions

As been made clear in the above graph, the model distinguishes among the traditional three lines which form the internal lines of defense (and exist in all kind of companies) and the bodies forming the external lines of defense (external audit and regulating authorities), which are considered critical for financial institutions. Another difference with the 3LoD model is the addition of arrows among all lines showcasing the importance of coordination and collaboration between the five lines of defense (as analyzed before) in the development of an optimal internal control system, aligned to the strategic priorities and special operational needs of financial institutions. Moreover, through the alliance of all lines and the direct report to the senior management and the BoD, it is emphasized that all the five lines of defense contribute to the formation of the required internal control infrastructure and combination of processes and structures toward the enhancement of the efficiency and effectiveness of financial institutions' corporate governance procedures. Overall, the proposed figure evolves the graphical representation of the traditional 3LoD and aims to reflect the evolution and improvement of the model with the new lines of defense, the established collaboration among them and the emphasis on the enhancement of the corporate governance framework.

### **Concluding remarks**

The Three Lines of Defense model has served as a widely accepted, simple and effective risk management and control framework, helping to assure the ongoing success of risk management initiatives; and initially was considered appropriate for any organization, regardless of size or complexity. However, the 3LoD model was heavily criticized for not recognizing the particularities of specific sectors such as those of regulated financial institutions, particularly in the aftermath of the recent global financial crisis of 2008. The several banking scandals that occurred in the post-crisis era and the relevant literature review also highlighted the existing weaknesses, justifying that the current 3LoD model must be updated to better apply for financial institutions.

In order to address these problems, the author proposes the five lines of defense model (5LoD), which consists of the existing three lines along with external audit and regulators (comprising the fourth and fifth line of defense, respectively). The key benefits of using the 5LoD model in financial institutions for designing and implementing efficient and effective internal control systems are listed below:

- Addition of two additional lines of defense, regulator and external audit, for further strengthening financial institutions' internal control systems.
- Highlights the increasing significance of collaboration among all lines of defense (internal and external) for enhancing internal control procedures.
- Emphasizes the crucial role of internal and external auditors and regulators as independent assurance providers to the senior management and the BoD of financial institutions (as shown in the independent assurance pyramid).
- The cooperation of internal and external lines helps in developing a more proactive and reactive approach to the identification, analysis, and preparedness for both opportunities and threats instead of focusing only on defensive actions (as in the 3Lod model).
- Takes into consideration the particularities of the financial industry (which is a de facto regulated sector) thus, enabling an easier adoption and implementation by any financial institution.

- Places the focus on the significant impact of effective risk management and control procedures in organizations' overall performance, justifying their role as added value factors.
- Contributes to the advancement of the graphical representation of the traditional 3LoD model by adding new extra lines of defense, distinguishing among internal and external ones and emphasizing on the strong collaboration among them (via the proper communication channels), leading to the enhancement of the entire corporate governance framework.
- It further emphasizes the critical role of internal auditors as independent assurance providers, advisors of the BoD and trusted insiders, being the critical link among the internal and external lines of defense.

The 5LoD model also points out that beside the fact that the bodies forming the two additional lines of defense constitute the external lines of defense, they should play an active role in supervising and monitoring control issues within the organization, in strong cooperation with the internal lines. This calls for closer interaction among the internal auditors, external auditors and regulators from one side and the governing bodies from the other in designing and forming an effective and efficient internal control system that will help financial institutions to mitigate risks and better operate in a constant changing environment.

In conclusion, in spite of the crisis-driven research interest and the numerous banking scandals as well as the growing importance of the 3LoD model in the modern corporate governance practices, academic contributions and discourse on the subject remain fragmented and vague. This study aims to fill this research gap by introducing the 5LoD model in order to address the weaknesses toward building more efficient internal control systems in financial institutions and hopefully initiating a fruitful academic discourse on this crucial subject.

## References

- Ashby, S., Palermo, T. and Power, M. (2012), Risk culture in financial organizations - An interim report, CARR discussion paper (November), 1-25.
- Basel Committee on Banking Supervision (2011), Principles for the sound management of operational risk. Basel, Switzerland: Bank for International Settlements Communications.
- Basel Committee on Banking Supervision (2012), The internal audit function in banks, June 2012.
- Basel Committee on Banking Supervision (2014), External audit of banks, March 2014.
- Boughey, S. (2017), The Three Lines of Defence: A Sisyphean Labour? Available from: <https://www.risk.net/risk-management/5349766/the-three-lines-of-defence-a-sisyphean-labour>. Accessed 6.1.2020.
- Davies, H., & Zhivitskaya, M. (2018). Three lines of defence: a robust organizing framework, or just lines in the sand? *Global Policy*, 9, 34-42.
- IIA (2013), The Three Lines of Defense in Effective Risk Management and Control. Accessed 21.10.2019. Available from: <https://na.theiia.org/standards-guidance/Public%20Documents/PP%20The%20Three%20Lines%20of%20Defense%20in%20Effective%20Risk%20Management%20and%20Control.pdf>
- IIA (2019), The Three Lines of Defense Exposure Document. Accessed 21.10.2019. Available from: <https://global.theiia.org/about/about-internal-auditing/Pages/Three-Lines-of-Defense-Review-Exposure-Document-and-Survey.aspx>
- Luburić, R. (2017), Strengthening the Three Lines of Defence in Terms of More Efficient Operational Risk Management in Central Banks. *Journal of Central Banking Theory and Practice*, 6(1), 29-53.
- Lyons, S. (2011, October), Corporate oversight and stakeholder lines of defense. In The Conference Board Executive Action Report (No. 365).
- Lyons, S. (2015), Enterprise Risk Management and the Five Lines of Corporate Defense. *The Journal of Enterprise Risk Management*, 1(1).
- Mülbert, P. O. (2009). Corporate governance of banks after the financial crisis-theory, evidence, reforms. ECGI-Law Working Paper, (130).
- OECD, Principles of Corporate Governance, September 2015.
- Power, M., Ashby, S. and Palermo, T. (2013), Risk culture in financial organizations - A research report (November), 1-103.
- Protiviti (2013), Applying the five lines of defense in risk management The Bulletin Vol 5 (4). Available from: [https://www.protiviti.com/sites/default/files/united\\_states/insights/the-bulletin-vol-5-issue-4-applying-5-lines-defense-managing-risk-protiviti.pdf](https://www.protiviti.com/sites/default/files/united_states/insights/the-bulletin-vol-5-issue-4-applying-5-lines-defense-managing-risk-protiviti.pdf). Accessed 6.1.2020.
- Société Générale (2008), Summary of PwC diagnostic review and analysis of the action plan, 23 May 2008. Available from: <https://www.societegenerale.com/sites/default/files/23%20May%202008%20The%20report%20by%20audit%20firm%20PWC.pdf>, Accessed 21.10.2019.
- The Institute of Internal Auditors (2017), The International Professional Practices Framework. Available from: <https://na.theiia.org/standards-guidance/Public%20Documents/IPPF-Standards-2017.pdf>. Accessed: 21.10.2019
- UBS (2011), Annual Report 2011. Available from: <http://www.annualreports.com/Company/ubs-ag>. Accessed 21.10.2019.
- Mabwe, K., Ring, P., & Webb, R. (2017), Operational risk and the three lines of defence in UK financial institutions: is three really the magic number? *Journal of Operational Risk*, *Forthcoming*.
- Vousinas, G. (2016), The critical role of Internal Auditing in addressing bank fraud: A conceptual framework. *Case Studies Journal ISSN (2305-509X)–Volume, 5*.



© 2021 by the authors. Licensee ACRN Publishing, Austria, Editor in Chief Prof. Dr. Othmar M. Lehner. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY SA) license (<https://creativecommons.org/licenses/by-sa/4.0/>)