QUANTITATIVE METHODS IN ECONOMICS
Volume XVII, No. 4, 2016, pp. 101 – 113

THE THREE LINES OF DEFENCE MODEL AND BANKS IN ALBANIA

Artur Ribaj
Faculty of Economy, University of Tirana, Albania
e-mail: artur.ribaj@yahoo.com
Merita Bejtja
Faculty of Economy, University of Tirana, Albania

Abstract: The three lines of defense model (3LODM) is a valuable framework that outlines internal audit's role in assuring the effective management of risk, and the importance for delivering this of its position and function in the corporate governance structure of Albanian banks. Each line of defense has unique positioning in the organization and unique responsibilities and not combined or coordinated in a manner that compromises their effectiveness. The responsibility for internal control does not transfer from one line of defence to the next line. Independence and objectivity are essential elements to consider Setting up of an internal control system and supporting arrangements by 3LODM is relatively simple. In Albania, the real challenge is ensuring that the perceptions, contribution and expectations of bank's executive management, audit committee and bank's board of directors are aligned, and that risk-related information is symmetric, effectively and consistently obtained, analyzed and used by players of internal control system. Misunderstandings between players/bodies of internal control system lead in luck of optimization achievements for reaching bank objectives. Internal auditing is designed to add value and improve an organization's operations; help an organization accomplish its objectives by bringing in a systematic, disciplined approach; evaluate and improve the effectiveness of risk management, control, and governance processes.

Keywords: three lines of defense, 3LODM model, Albanian banks, risks mamagement

INTRODUCTION

The expectations on internal audit functions are increasing in both sides internally and externally. On the one hand chairmen, boards of directors, audit committees and executive managements all have increased expectations of the depth, quality, objectivity, and independence of the work which needs to be performed by their internal audit function, while on the other hand supervisory authorities are seeking to be able to place more reliance on internal audit functions.

In Albania, the new regulation no. 67, dated on 02.09.2015 "On Internal Control System" [SCBA 2015] took in consideration the Basel Committee document on principles[1], and has given the minimum requirements for setting up an effective internal control system and supporting arrangements by the three lines of defence model established to help the bank develop a sound and reliable internal control system and ensure that business operations are effectively functioning to contain the risks in accordance with risk strategy and governance providing a vital assurance to bank's board of directors[2], audit committee, executive management[3], and supervisory authorities.

Banks management aspiration in Albania is to effectively manage the risk and to create sustainable value to its stakeholders through business objectives such as growth, increased dividend and satisfactory customer service. Banks do not operate in a risk-free environment, but they operate in environments filled with uncertainty, requiring proactive action to address risks in order to survive and prosper. For these reasons, in the Albanian banks, there are many different functions and teams involved in managing and controlling risks. The new regulation no. 67 [SCBA 2015] as per the Basel Committee document on principles, has given the minimum requirements for setting up an effective internal control system and supporting arrangements by 3LOD Model.

Short presentation for each line of defence

The first/front line of defence provided by front line staff and operational management. The systems, internal controls, the control environment and culture developed[4] and implemented by these front line units is crucial in anticipating and managing operational risks.

The second line of defence provided by the risk management, compliance (etc. as exp. legal, HR, financial control, technology and operational) functions provide

---

[1] [BCBS 2012] The internal audit function in banks, Basel Committee on Banking Supervision.

[2] It will have the same meaning with the board of directors in a one tier structure and the supervisory board in a two tier structure or steering committee.

[3] It will have the same meaning with bank's directorate or bank's senior management or executive committee in a one tier structure or the management board in a two tier structure

[4] IRM defines risk culture as "the values, beliefs, knowledge and understanding about risk shared by a groupof people with a common purpose."

the oversight and the tools, systems and advice necessary to support the first/front line in identifying, managing and monitoring risks.

The third line of defence provided by the internal audit, provides a level of independent assurance that the risk management and internal control framework is working as designed. Internal auditing has to consider as an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes

Benefits of approaching the three lines of defence model

It improves communication by clarifying roles and responsibilities; it improves the effectiveness of risk management because it positions risk as an enterprise-wide concern and provides independent assurance; front/first line staff (sometimes, called risk/business owners[5]) have greater confidence in the quality of their assessment of uncertainty in their areas of responsibility; oversight (second line staff) that support the monitoring process functions such as compliance and risk management and assurance providers (auditors third line) are able to plan their efforts and resources based on the risk-based bank's requirements; it helps banks' executive management to delegate and coordinate risk management duties across the bank; the bank's board of directors and audit committee has a governance process in place that provides protection for future business performance; it helps supervisory authorities to rely on their reports for performing some supervision over internal control system, the adequacy and effectiveness of ICS.

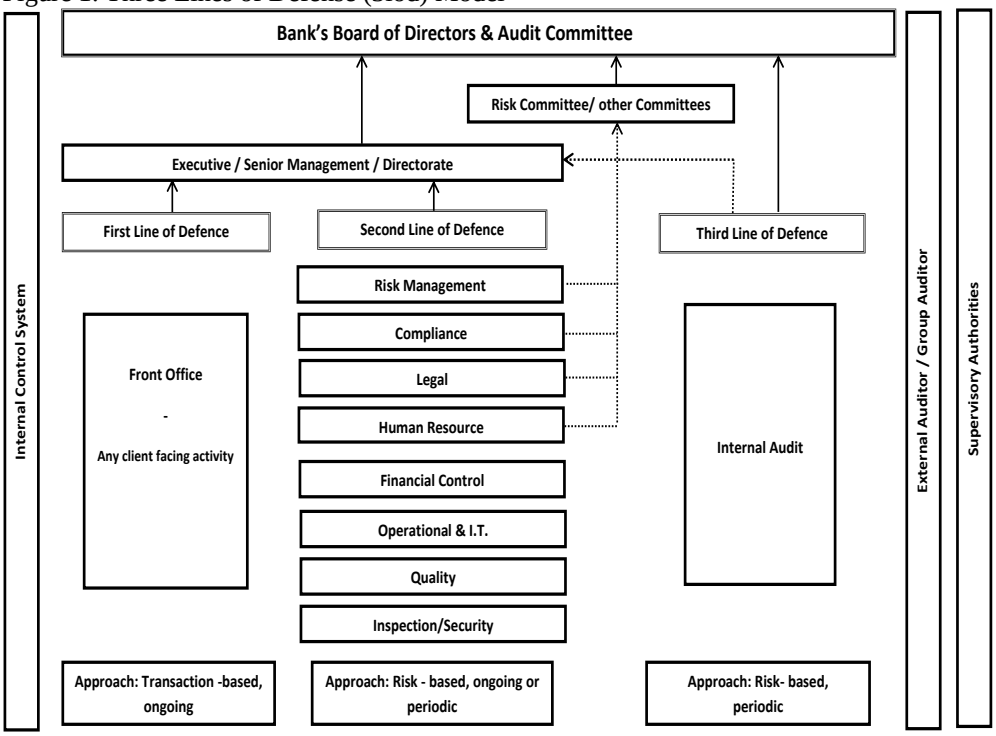
THREE LINES OF DEFENCE (3LOD) MODEL (FIGURE 1)

The new regulation no. 67 "On the Internal Control System" [SCBA 2015] is confessing a strong internal control system using the three lines of defense model, including an independent and effective internal audit functions, as part of sound corporate governance. This model will provide a framework for good governance, a valuable framework that outlines internal audit's role in assuring the effective management of risk, it will bring transparency and fosters collaboration. Every employee in the bank who has a delegation, deploys resources or makes decisions is responsible and accountable for managing the associated risks. This ensures that all areas involved in risk communicate in a meaningful way to better manage risk controls within the bank.

[5] Functions that own and manage risks, the international risk management standard, AS/NZS ISO 31000, introduced the term "risk owner" (the person or entity with the accountability and authority to manage a risk).

Three lines of defence model (3LODM) needed to support the effective internal control system. The model of "lines of defence" has its origin in military planning, football sports and health protection, while the origin of the 3LOD Model appeared years ago following its adoption by the former United Kingdom FSA[6]. This model provides a straightforward and effective way to enhance communications on risk management and control by clarifying essential roles and duties. This model rapidly gained universal recognition providing assurance from various sources within the bank to the bank's management to effectively get done its duties.

Figure 1. Three Lines of Defense (3lod) Model



Source: own proposal

The model differentiates between functions that own and manage risks (front/first line), functions overseeing, monitoring risks (second line) and functions providing independent assurance (third line). Different parts and levels of a bank play different roles in risk management, and the interaction between them determines how effective the entire-bank is in dealing with risk. Regular and ongoing dialogue by internal audit with the first/front and second lines of defence is needed so that the

[6] Three lines of defence model is implied as part of the functional segregations and reporting structures that the FSA looks for when undertaking its risk assessment (ARROW) visits.

function has a more timely perspective of business direction and business issues. Internal audit can therefore play a valuable advisory role to help the executive management improve the first and second line of defence processes with advice, facilitation and training. Internal audit can also identify where there are gaps in the first two lines of defence and advice on how they can be under control. Internal audit can also play a valuable role in helping the board ensure that governance structures are effective in identifying and managing internal risks.

Changes to the regulation no. 67, dated on 02.09.2015 "On the Internal Control System" [SCBA 2015] promote internal audit's role as a core part of the third line of defence and avoid undermining its unique position in monitoring and providing assurance on the management of risk. If the role and duties of internal audit are combined with roles and duties from the first two lines of defence, boards have to be aware of potential conflicts of interest and then the struggles for safeguarding the objectivity and independence of internal audit assurance. The independence and objectivity of internal audit are vital in its support of the board and audit committee. Both "independence" and "objectivity" have a specific meaning in an internal audit environment. The Glossary of The Institute of Internal Auditors [see IPPF 2011] refers to independence as the freedom from conditions that threaten the ability of the internal audit activity to carry out internal audit responsibilities in an unbiased manner. Objectivity is referred to in the Glossary as an unbiased mental attitude that allows internal auditors to perform engagements in such a manner that they believe in their work product and that no quality compromises are made. Objectivity requires that internal auditors do not subordinate their judgement on audit matters to others.

The expectations on internal audit functions are increasing in both sides internally and externally. On the one hand chairmen, boards of directors, audit committees and executive managements all have increased expectations of the depth, quality, objectivity, and independence of the work which needs to be performed by their internal audit function, while on the other hand supervisory authorities are seeking to be able to place more reliance on internal audit functions.

Bank's board of directors[7], it has to decide the bank's risk appetite which is the amount of risk a bank is willing to accept in recreation of value. This decision has to pass after getting analyses and advices of audit committee of the most significant risks for the bank and if bank's chief executive officer and bank's executive management are responding appropriately (i.e. in relation to the agreed upon risk appetite). Bank's audit committee reports to the board of directors on the effectiveness of internal control and risk management systems based on information it acquires directly or with the assistance of the audit functions. The chief executive officer and bank's executive management members have ultimate ownership

[7] For responsibilities of bank's board of directors, audit committee and executive management related to internal control system, refer to [Ribaj 2015].

responsibility for the bank's risk management and control framework. They should: ensure the presence of a positive internal environment and risk culture within the bank ("tone at the top"); provide leadership and direction to first and second line of defence and monitors the overall risk activities in relation to its risk appetite; take the necessary measures to reestablish alignment where evolving circumstances and emerging risks which indicate potential misalignment with the bank's risk appetite; convert the strategies into operational objectives; identify and assess risks adversely impacting the achievement of these objectives; implement risk responses consistent with risk tolerances. Each executive management member has responsibility for managing risks within his/her sphere of responsibility, while chief executive officer is fully responsible to the board of directors for managing risks of the entire bank activities.

The first line of defence – front line management

The first/front line of defence (business operations - risk and control in the business) is the front-line employees who must understand their roles, duties and responsibilities with regard to processing transactions and who must follow a day-to-day and ongoing identification, assessment, control and risk management of risks associated with those transactions. Employees of business units undertake risk within assigned limits of risk exposure and are accountable for that. The head of front line or business unit is empowered with the responsibility and accountability to effectively plan, build, run and monitor its unit's day-to-day risk environment. Every front line unit head in cooperation with his/her supervisor provides direction regarding risk treatment for those risks that are outside of his/her business unit's risk tolerance. The clear understanding of the concept of front line staff and its management as the first/front line of defence is the key to success of 3LODM.

The first/front line of defence is formed by managers and staff who are responsible for identifying and managing risk as part of their accountability for achieving objectives. Collectively, they should have the necessary knowledge, skills, information, and authority to operate the relevant policies and procedures for risk mitigation and compliance with process should ensure an adequate control environment. There should be adequate managerial and supervisory controls in place to ensure compliance and to highlight control breakdown, inadequacy of process, unexpected events and reporting on progress to bank's management. This requires an understanding of the bank objectives, the environment in which it operates, and the risks it faces. The quality of the people, systems and the organization culture of the bank is the main determinant of success. They are responsible for defining and set up internal control in their business area, through clear roles and responsibility, segregation of duties and daily controlling tools.

The second line – mainly the risk management & compliance

The second line of defence has the support functions/units (Risk Management, Compliance, Financial Control, Legal, Human Resources, Operations and

Technology, etc.) which provide independent oversight over the risk management activities and processes of the first/front line of defence units and assists them with advisory, monitoring and reporting adequate risk-related information mainly by the compliance unit and the risk management unit. These two units may have direct reporting lines either to the bank's executive management or to the respective committees (exp. Risk Management Committee, Corporate Governance Committee, etc.) which report to bank's board of directors. These committees should be involved in monitoring the second line of defence units' activities.

- Compliance function/unit supports the first/front line units in managing risks arising from non-compliance with applicable laws and regulations and advises them on all areas of regulatory principles, rules and guidance, including leading on any changes, and undertakes monitoring activity on key areas of regulatory risk;
- Risk management function[8]/unit is an integral part of all bank processes. It defines and prescribes the financial and operational risk assessment processes for the business, maintains the risk registers and undertakes regular reviews of these risks in conjunction with line management, facilitates and monitors the implementation of risk management practices, assists the first/front line units, and consolidates the communication of risk-related information within the bank;
- Other second line of defence functions/units have responsibility for providing independent oversight over the first/front line units within their spheres of responsibilities related to their respective units objectives.

To be effective the second line of defence units (the support functions) need to work with and support the first/front line of defence units, and in cooperation with bank's management to provide to them:

- Oversee for ensuring that risks in the first/front line of defence units have been appropriately identified and managed;
- The policies, frameworks, tools and techniques that are practical, adaptable and effective for allowing the front line to manage for success;
- Define strategies for implementing bank policies and procedures;
- A bank-wide view of risks (a risk map and limitations) based on the collected information, participating in the business unit's risk meetings, reviewing risk reports and validating compliance to the risk management framework requirements;
- A monitoring report, overseeing the consistency of definitions and measurement of risk with the objective of ensuring that risks are actively, effectively and appropriately managed.

The second line of defence in a cooperative view, might be seen as playing a multirole, anticipating what might go wrong up front and being ready to react,

[8] ISO 31000 espouses eleven key principles that underpin effective risk management.

while at other times acting as another set of eyes for the front line and shouting advice and encouragement when needed. Sometimes the second line steps up to the front if reinforcements are necessary and other times it drops back in cover defence.

The third line – internal audit

The third line of defence (functions that provide independent assurance) is that of internal auditors[9] who report independently to the bank's board of directors/audit committee charged with the role of representing the bank's stakeholders relative to risk issues. Sitting outside the risk management processes of the first two lines of defence, its main roles are to assess independently the effectiveness of processes created in the first and second lines of defense and to ensure that they are operating effectively and to advise them how could be improved. Tasked by, and reporting to the board of directors/audit committee, it provides an evaluation, through a risk-based approach, on the effectiveness of governance, risk management, and internal control to the bank's bord of directors. It can also give assurance to supervisory authorities that appropriate internal controls and processes are in place and are operating effectively.

Internal audit undertakes a program/platform of risk-based audits covering all aspects of both first and second lines of defence. Internal audit may take some assurance from the work of the second line functions and reduce or tailor its checking of the first/front line. The level of assurance taken will depend on the effectiveness of the second line, including the oversight committees (corporate governance committee, risk management committee, etc.), and internal audit will need to coordinate its work with compliance and risk management as well as assessing the work of these functions. The findings of these independent reviews from these audits need to be effectively communicated and reported to bank's management (board of directors, audit committee and executive management) aiming that appropriate actions need to be taken to maintain and enhance the internal control system of the bank.

Major roles and responsibilities of an internal audit can be summarized as per following: evaluates and provides responsible assurance risk management; reports risk management issues and internal controls deficiency identified directly to the audit committee and provides recommendations for improving the organization's operations, in terms of both efficient and effective performance; evaluates information security and associated risk exposures; evaluates regulatory compliance program with consultation from legal counsel; maintains open communication with

[9] IIA's financial services code: "internal audit is tasked to include in its scope three different aspects of corporate culture, namely: the risk and control culture of the organisation; the customer-facing culture with regard to the organisation acting with integrity towards its dealings with customers and markets; and the design and operating effectiveness of policies and processes to ensure that they in line with the objectives, risk appetite and values of the organisation."

management and audit committee; engages in continuous education and staff development ; provides support to the company's anti-fraud programs, red flags, etc.

The Institute of Internal Auditors (IIA), which is the internal professional organization that oversees internal audit guidance, certification, education, and research, defines internal auditing as: "An independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization to accomplish its objectives by bringing a systematic, disciplined, approach to evaluate and improve the effectiveness of risk management, control and governance process"[10]. This feature has evolved over the last years becoming clearly distinct from the external audit and covers all activities in a bank not just its financial situation.

Considering internal audit as the third line of defence, banks have to be clear that internal audit should never be relied upon as a primary control measure. Internal audit's role is largely detective and corrective, to detect control weaknesses or breakdowns and to suggest the need for improvements or corrective actions. It is a dangerous view and against the regulation no. 67, dated on 02.09.2015 "On the Internal Control System (ICS)" [SCBA 2015] if bank's executive management nominates the internal audit unit as the only responsible controller of bank's risks. Internal audit should never be relied upon or expected to detect every control breakdown, error or deficiency, because it does not review every single transaction. The third line of defence has a key role to play but if the first and second line is relying on it to pick up every mistake through each transaction or if the bank management continually relies on its internal audit unit to guaranty the function of the ICS, the bank is going to lose[11].

Other responsible lines

A well-coordinated interaction between the involved actors, including a clear segregation of duties, is a key element of sound governance structures. The external auditors and supervisory authorities are the useful bodies for checking over bank's internal control system for the different roles and responsibilities regarding effective risk management and control, to ensure that there are neither gaps in controls nor unnecessary duplications, and respective roles and responsibilities must be clearly defined.

External auditing can be considered as a fourth line of defence, providing assurance to the organisation's shareholders, board and senior management regarding the true and fair view of the organisation's financial statements. However, given the specific scope and objectives of their mission, the risk information gathered by external auditors is limited to financial reporting risks only and does not include

[10] [IIA 2015) http://www.iia.org.au/aboutIIA/whatisinternalaudit.aspx

[11] ACE publication, 2011 "This third line role compares internal audit to that of a goalkeeper in a football match. When the ball is lost in midfield (first/front line) and the defence (second line) fails to pick up the opposition's attack, it is left to the goalkeeper (third line) to save the day.

the way senior management and the board are managing/monitoring strategic/operational/compliance) enterprise-wide risks, and for which the risk management and internal audit functions respectively provide monitoring and assurance. External audit not only provides the shareholders with assurance but also delivers valuable information to the board of directors, the audit committee, executive management and supervisory authorities. External auditor contributes as an outside body, providing assurance regarding the true and fair view of an organisation's financial statements. It can also be seen as an outside check on internal governance functions, including possible observations on the effective implementation of the three lines of defence model.

The supervisory authorities through on-site and off-site examinations supervise periodically the business frontlines, the oversight functions and internal auditors to ensure that they are carrying out their tasks to the required level of competency and operating effectively and according to best practices. They receive annually the report of external auditor and the audit report for internal control system, and may ask to get other detailed reports for oversight and the front line (business), and may act on any items of concern from any party. Also, the supervisory authorities review the activity of internal control system structures from the front/first line units to the bank's board of directors for being compliant with legal and regulatory framework, their internal regulatory acts, action plans, activity reports, corrective actions, and their roles' responsibilities for being completely and accurately.

Supervisory authority in Albania has under supervision 16 banks, which include on-site and off-site examinations through monthly or quarterly financial data monitoring, to reaffirm their safety and soundness, and have regular (two-way) communication[12] with the structures of internal control system. They discuss the risk areas identified by both parties and measures received or to be received.

CONCLUSIONS

Setting up of an internal control system and supporting arrangements by 3LOD Model is relatively simple. The real challenge is ensuring that the perceptions, contribution and expectations of bank's executive management, audit committee and bank's board of directors are aligned, and that risk-related information is symmetric, effectively and consistently obtained, analyzed and used by players of internal control system. Misunderstandings between players/bodies of internal control system lead in luck of optimization achievements for reaching bank objectives.

The three lines of defence is a well-known model in developed countries, and as the other models, either it is a tool to simplify complex functions and relationships in a way that makes them easier to explain and understand, or it is only as strong as

[12] Refer to the paper "Some Principles for Banks' Internal Control System in Albania"

the people that work within it and it has to be tailored to the specific context in which the bank operates.

In the 3LOD model, the management of risks is strongest when there are three separate and clearly identified lines of defense. Each line of defense has unique positioning in the organization and unique responsibilities and not combined or coordinated in a manner that compromises their effectiveness. The responsibility for internal control does not transfer from one line of defence to the next line. Independence and objectivity are essential elements to consider.

The third line of defence (internal audit) provides independently assessed risk information to the bank's board of directors /audit committee for the same risk issues reported by the bank's executive management. This independently assessed risk information might be different with what is reported by first or second line of defence. The assessment of third line does not always align with the risk reality as perceived by the first/front line, the second line of defence and bank's executive management. This difference is what adds value to the internal control system framework.

Internal auditing is designed to add value and improve an organisation's operations; help an organisation accomplish its objectives by bringing in a systematic, disciplined approach; evaluate and improve the effectiveness of risk management, control, and governance processes.

Neither the board of directors nor the audit committee is considered part of one of the three lines of defence. These bodies play key roles within the bank's risk management and control structures by assuming their oversight and monitoring duties.

RECOMMENDATIONS

1. The model of three lines of defense should be functional at every bank in Albania, regardless the size or complexity of the bank.
2. Banks in Albania for each line in the 3LODM should have clearly defined roles and duties that have to be supported by appropriate policies, procedures, and reporting mechanisms for ensuring the effectiveness and efficiency of internal control system.
3. To enable the staff of first/front line of defence units achieving the business objectives and an effective risk management, the bank's management has the responsibility to identify and assess risks and to ensure that the control activities are enforced and monitored and to notify regularly the staff of business units, the information: Critical and highly rated residual risks in a map; planned mitigation actions for each main risk and person to act; the existing risk mitigation actions status; the main risk indicators; incidents and breakages including historical/trend, analysis/statistics, status of mitigation actions and lessons learned;

4. To improve efficiency and avoid duplication of effort while ensuring all significant risks are addressed appropriately, the information should be shared and activities coordinated among each of the lines of defense;
5. The staff of first/front line of defence units has to report to upper management every issue related to the risks of internal control system. This information by the second line of defence has to be collated with other risk reports and assessed and reported, both independently and directly, to the bank's executive management (and to the respective committee, if exists), who has to represent to the bank's board of directors the risk assessment issues on the bank activities;
6. Banks need to provide a solid foundation for the three lines of defence so that they are all aware of what they are defending and from what they are threating and limiting disruptions to the business frontline;
7. Banks' management must ensure that the three lines work together effectively and efficiently, while limiting overlaps and gaps and maintaining their discrete duties so as to not compromise the defence model;
8. The bank has to have defined its risk strategy and appetite. Risk officers to be designated for each major risk, and they should have fixed meaningful and measurable objectives and controls, recognized throughout the bank;
9. First/front line units are part of the delegation of authority and the remuneration mechanisms (bonus system) should include appraisal of risk taking;
10. The employees of the three lines should have dedicated training programmes to improve the risk management culture and promote a common language throughout the bank;
11. Internal Audit future continuously challenge is to identify, implement and improve the Information Technology Systems to give a fully support business need, preventing the bank's risks; push responsible managers through Semi Annual Follow Up-s processes, on faster and better audit finding's implementation;
12. Executive management and chief executive officer periodically should receive reports on major risks' evolution and on the implementation of mitigation plans, and by them the critical risks and emergent risks should be escalated to the appropriate management level as soon as they are identified. Also, the Executive management and chief executive officer should communicate periodically a risk dashboard, with key risk indicators, to the internal audit department, audit committee and board of directors.

REFERENCES

BCBS (2010) Principles for enhancing corporate governance. Basel Committee on Banking Supervision.

BCBS (2012) The internal audit function in banks. Basel Committee on Banking Supervision.

BCBS (2015) Corporate governance principles for banks. Basel Committee on Banking Supervision.

EU (1984**)** Qualifications of persons responsible for carrying out the statutory audits of accounting documents: eighth Directive, Law Directive 84/253/EEC of the EU.

EU (2006) On statutory audits of annual accounts and consolidated accounts, Directive 2006/43/EC, European Commission.

IIA (2015) About IIA & their Profession. [on-line:] http://www.iia.org.au/aboutIIA/what isinternalaudit.aspx

IPPF (2011) International Professional Practice Framework. The Institute of Internal Auditors Global, Edition updated for 2012.

Law (2006) On Banks on the Republic of Albania. Law No. 9662, 18.12.2006, amended.

Ribaj A. (2015) Banks' Internal Control System, the case of Albania. International Journal of Science and Research, [on-line:] https://www.ijsr.net/archive/v4i10/14101501.pdf

Publications of CIA-Certified Internal Auditor, CIIA – Chartered Internal Auditor, CFSA-Certified Financial Services Auditor, CGAP-Certified Government Auditor, CCSA-Certified, Control Self-Assessment, CRMA-Certified Risk Management Auditor and COSO-Committee of Sponsoring Organizations of the Tread way Commission.

Publications on: Policy position paper on risk management and internal audit; and briefing on whistleblowing

SCBA (2015) On the Internal Control System, regulation approved by Supervision Council of Bank of Albania