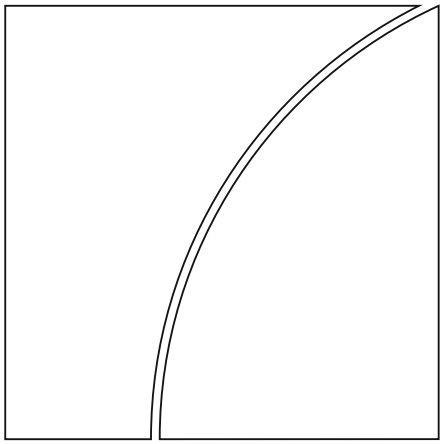
Financial Stability Institute



Occasional Paper
No 11

The "four lines of defence model" for financial institutions

Taking the three-lines-of-defence model further to reflect specific governance features of regulated financial institutions

Isabella Arndorfer
Bank for International Settlements

Andrea Minto
Utrecht University

December 2015

BANK FOR INTERNATIONAL SETTLEMENTS

The views expressed in this paper are those of the authors and not necessarily the views of the Financial Stability Institute, the Basel Committee on Banking Supervision or the Bank for International Settlements.

This publication is available on the BIS website (www.bis.org).

ISSN 1020-9999 (online)

Contents

Executive summary[1]

Since the Global Financial Crisis of 2007–09, the design and implementation of internal control systems has attracted serious academic and professional attention. Much research on the effectiveness and characteristics of internal audit functions has been conducted under the sponsorship of the Institute of Internal Auditors Research Foundation (IIARF) and published in academic and professional journals. Despite these efforts, there has been little systematic analysis of how the design of an internal control system affects the efficiency and effectiveness of corporate governance processes, especially at financial institutions such as banks and insurance companies. The "three lines of defence model" has been used traditionally to model the interaction between corporate governance and internal control systems. We consider the existing three-lines-of-defence model could be substantially enhanced by giving it a specific focus on the regulation of banks and insurance companies. We address this deficiency and attempt to ascertain the extent to which these financial institutions – due to their idiosyncratic features and specific regulatory requirements – need a more effective internal control model. Although our study relates to financial institutions in general, our detailed analysis focuses on banking institutions.

In order to account for the specific governance features of banks and insurance companies, we outline a "four lines of defence" model that endows supervisors and external auditors, who are formally outside the organisation, with a specific role in the organisational structure of the internal control system.

Building upon the concept of a "triangular" relationship between internal auditors, supervisors and external auditors, we examine closely the interactions between them. By establishing a four-lines-of-defence model, we believe that new responsibilities and relationships between internal auditors, supervisors and external auditors will enhance control systems. That said however, we also highlight the risk that new problems could be caused by inadequate information flows among those actors.

[1] The authors would like to thank the reviewers for the valuable comments and suggestions they received which helped improve the accuracy and validity of the investigation: Prof Robert Melville from CASS Business School, Prof Wilco Oostwounder from the University of Utrecht; and Juan Carlos Crisanto, Stefan Hohl and Raihan Zamil from the Financial Stability Institute of the Bank for International Settlements.

1. Introduction: the Global Financial Crisis, corporate governance and the three-lines-of-defence model

There is a wide consensus that substantial failures in corporate governance have been a contributing factor to the Global Financial Crisis (GFC).[2]

Although some commentators have argued that corporate governance reforms have fallen so far short of what many had expected,[3] further corporate governance reforms are seen as essential in reducing the risk of a repetition of a major financial crisis. In particular, the GFC has prompted renewed discussions of the importance of board-level procedural safeguards, including the introduction of legally binding rules to promote board-level risk management committees and the requirement that a chief risk officer (CRO) be appointed to improve board expertise regarding risk management issues.[4]

At the international level, there has been much debate regarding how the corporate governance procedures of financial institutions could be used to improve risk management. This could be done, for instance, by creating a board-level risk management committee; altering board member incentives through varying remuneration schemes; improving oversight; and imposing other substantive rules on compensation with the ultimate goal of promoting financial stability.

The guidelines issued by the Basel Committee on Banking Supervision (BCBS) in 2015 on corporate governance principles for banks emphasise the importance of proper risk management procedures, including, in particular, "an effective independent risk management function, under the direction of a chief risk officer (CRO), with sufficient stature, independence, resources and access to the board."[5] Furthermore, "the sophistication of the bank's risk management and internal control infrastructure should keep pace with changes to the bank's risk profile, to the external risk landscape and in industry practice" so as to identify, monitor and control risks on an ongoing bank-wide and individual-entity basis.[6]

The OECD reaches similar conclusions in that such procedures, especially the position of the CRO, are necessary to better manage the particular risks that banks pose to the larger economy, combining a micro- and a macroprudential approach to supervision. Likewise, the recent Green Paper of the European Commission (EC) on corporate governance at financial institutions and remuneration policies outlines the perceived inadequacies of board-level risk management. Such inadequacies include, in particular, "a lack of understanding of risks", "a lack of authority […] to be able to curb activities of risk takers", "a lack of expertise […] in risk management" and "a lack of real-time information on risks".[7] Consequently, the Green Paper envisages the following recommendations with regard to risk management:

- delineating board-level responsibilities;
- creating a board-level risk supervision committee;

[2] According to the De Larosière Group Report, *Report on the future of financial supervision in the EU*, 25 February 2009, Brussels, corporate governance was one of the most important elements underlying the financial crisis; in the literature, see, for example, HOPT, "Corporate governance of banks and other financial institutions after the financial crisis", in *Journal of Corporate Law Studies*, 2013, 222; CITLAU AND MÜLBERT, "The uncertain role of banks' corporate governance in systemic risk regulation", in *ECGI Law Working Paper*, 2011, no 179.

[3] See HOWSON, "When 'good' corporate governance makes 'bad' financial firms: the global crisis and the limits of private law, *Michigan Law Review*, 2009, pp 44–50.

[4] MÜLBERT, "Corporate governance of banks after the financial crisis – theory, evidence, reforms", *ECGI Law Working Paper*, 2009, no 130; HILB, "Redesigning corporate governance: lessons learnt from the global financial crisis", *Journal of Management and Governance*, 2011, pp 533–538.

[5] Basel Committee on Banking Supervision, *Principles for Enhancing Corporate Governance*, Principle 6. See also OECD Steering Committee on Corporate Governance, *Corporate governance and the financial crisis*, 15.

[6] Basel Committee on Banking Supervision, *Principles for Enhancing Corporate Governance*, Principle 7.

[7] European Commission, *Corporate governance in financial institutions and remuneration policies*, Green Paper, Section 3.4, 2010.

- creating a position of chief risk management officer having familiarity with the "organisational complexity" of the relevant firm; and
- increasing cooperation, not only between relevant supervisory authorities and boards of directors, but also between the risk supervision committee and other parts of the firm.

It follows from the above that internal control system reforms should accompany corporate governance reforms to ensure that banks enhance the quality of their risk-taking, either through curbing misaligned incentives or otherwise reducing the riskiness of business strategies. From this vantage point, the GFC showed that the weakness or ineffectiveness of such procedural safeguards was indeed significant.

Scholars have argued that the primary, if not the sole, justification for regulating internal control systems is to maximise the efficiency and effectiveness with which exposure to risk is managed.[8] Efficiency is thus a central goal of international standard setters and it appears to have been transposed to the agenda of policymakers and regulators worldwide. As far as internal control systems are concerned, efficiency includes, in our view, the way in which work is performed (in terms of qualifications, professionalism and resources), the model/structure underlying the parties involved in the process and the interaction between those parties. This observation holds particularly true for banks.

Recent significant risk incidents and corporate scandals caused by misconduct in financial market operations indicate that banks need to further enhance corporate governance measures.[9] But, most importantly, such incidents have led to a further prioritisation of governmental and supervisory agendas relating to the potential systemic implications of weak internal control systems.[10] This calls for a greater prominence of microprudential policies relating to misconduct at banks. It also calls for closer cooperation between regulators, and external and internal auditors, so as to win back public trust in financial institutions.

Ineffective internal control systems in financial institutions were also significant factors in several recent incidents of fraud; for example, at Société Générale in 2008 and at UBS in 2011; and at a number of global financial institutions with respect to the more recently exposed Libor rate-rigging and foreign exchange rate-fixing.[11] Those events served to remind us that the interconnectedness of financial market participants could amplify shocks, and potentially lead to a collapse of the financial system.[12] A lack of public confidence triggered by behavioural

[8] TIMME, "Corporate control and bank efficiency", *Journal of Bank and Finance*, 1993, 17; JENSEN, "Value maximization, stakeholder theory, and the corporate objective function", *Harvard Business School Working Paper*, 2000, no 58; CHAMI AND FULLENKAMP, "Trust as a means of improving corporate governance and efficiency", *IMF Working Paper*, 2002; LEVINE, "The corporate governance of banks: a concise discussion of concepts and evidence", *World Bank Policy Research Working Paper*, no 3404, 2004; KIRKPATRICK, "The corporate governance lessons from the financial crisis", *Financial Market Trends*, 2009, 3(1); DE JONGHE, DISLI AND SCHOORS, "Corporate governance, opaque bank activities, and risk/return efficiency, *Journal of Financial Services Research*, vol 41, no 1–2, 2012.

[9] Regaining public trust is one of the most topical subjects related to the regulation and supervision of financial undertakings. Regaining such trust regarding behaviours, conduct and culture at banks should win back public confidence: see, for example, Group of Thirty, *Banking conduct and culture: a call for sustained and comprehensive reform*, July 2015; FSB, *Guidance on supervisory interaction with financial institutions on risk culture*, April 2014.

[10] European Systemic Risk Board, *Report on misconduct risk in the banking sector*, June 2015.

[11] For a collection and comment of recent financial scandals, see ERHARD, JENSEN, Putting integrity into finance: a purely positive approach, *ECGI Finance Working Paper*, 2014, 417, Appendix 1.

[12] For a comprehensive analysis of systemic risk in the financial sector, see BORIO, "Rediscovering the macroeconomics roots of financial stability policy: journey, challenges and a way forward", *BIS Working Papers*, 2011, no 354; NIER et al, "Network models and financial stability", in *Journal of Economic Dynamics and Control*, 2007, 31; AIKMAN et al, "Funding liquidity risk in a quantitative model of systemic stability, in *Financial Stability, Monetary Policy, and Central Banking*, edited by Alfaro, Central Bank of Chile, 2011, pp 371–410; ADRIAN and BRUNNERMEIER, "CoVaR", in *Federal Reserve Bank of New York Staff Report*, 2008, no 348; ACHARYA et al, *Regulating Wall Street*, New York, 2011; KASHYAP et al, "The macroprudential toolkit", *IMF Economic Review*, 2011, 59(2); KORINEK, "Systemic risk-taking: amplification effects, externalities, and regulatory responses", *ECB Working Paper Series*, 2011, no 1345; GOODHART et al, "An integrated framework for analyzing multiple financial regulators", *International Journal of Central Banking*, 2013, 9(1); SCHWARCZ, "Systemic risk", *Georgetown Law Journal*, 2008, 97; SCOTT, "The reduction of systemic risk in the

scandals could eventually deter the public from using the financial system, thus undermining the stability and integrity of the economy at large.[13] Behaviour and culture at banks have never been so high a priority of the agenda of regulatory agencies worldwide, including the introduction of the "Volcker Rule" in the United States[14], the move to a Banking Union in the European Union (EU)[15] and initiatives aimed at establishing an Asia-Pacific financial market.[16]

To avoid a fraudulent scenario from playing out and, once again, addressing public concerns related to the integrity of financial markets, regulators are approaching internal governance shortcomings with a sharper focus on systemic implications. That said, this subject revolves around the efficiency of internal control systems as an essential component of corporate governance and, in our eyes, boils down to a model stipulating the role played by the various parties involved in the internal control system model.

In the financial industry, a de facto regulated sector, internal auditors, supervisors and external auditors are asked to carry out their duties in similar and closely related areas, although each of them has a slightly different focus (eg internal auditors focus on effectiveness and efficiency of operations, supervisors on supervisory issues, etc.).

Recognising the overlapping areas of activities and the need for coordination among these three parties, we conclude that it is necessary to reshape the internal control structure of financial institutions by means of an additional fourth line of defence for external control bodies.

2. Outline of the three-lines-of-defence model

Following extensive discussions within the industry, a three-lines-of-defence model was finally developed by the Institute of Internal Auditors in 2013.[17] It has become the most common benchmark for assigning control and risk management responsibilities to business functions in an organisation. The original idea was to develop a model of general applicability for organisations. However, it did not recognise the peculiarities of certain sectors (such as those of regulated financial institutions).

United States financial system, *Harvard Journal of Law & Public Policy*, 2010, 33; CITLAU AND MÜLBERT, "The uncertain role of banks' corporate governance in systemic risk regulation", in *ECGI Law Working Paper*, 2011, no 179.

[13] According to statistics, banking has gone from being one of the public's most trusted sectors to the least trusted: EDELMAN TRUST BAROMETER, New York, 2014; G30, *Banking conduct and culture. A call for sustained and comprehensive reform*, July 2015; European Commission, Consumer Scoreboard, available at ec.europa.eu/consumers/consumer_evidence/consumer_scoreboards/10edition/docs/consumer_market_brochure_141027_en.pdf

[14] *Dodd-Frank Wall Street Reform and Consumer Protection Act*, § 619. Noteworthy are Mr Volcker's comments on the proposed Volcker rule regulations: "The need to restrict proprietary trading is not only, or perhaps most importantly, a matter of the immediate market risks involved. It is the seemingly inevitable implication for the culture of the commercial banking institutions involved, manifested in the huge incentives to take risk inherent in the compensation practices for the traders. Can one group of employees be so richly rewarded, the traders, for essentially speculative, impersonal, short-term trading activities while professional commercial bankers providing essential commercial banking services to customers, and properly imbued with fiduciary values, be confined to a much more modest structure of compensation?" (Volcker, *Commentary on the Restrictions on Proprietary Trading by Insured Depositary Institutions*, attached to Letter from Paul A Volcker to financial regulatory agencies, 13 February 2012).

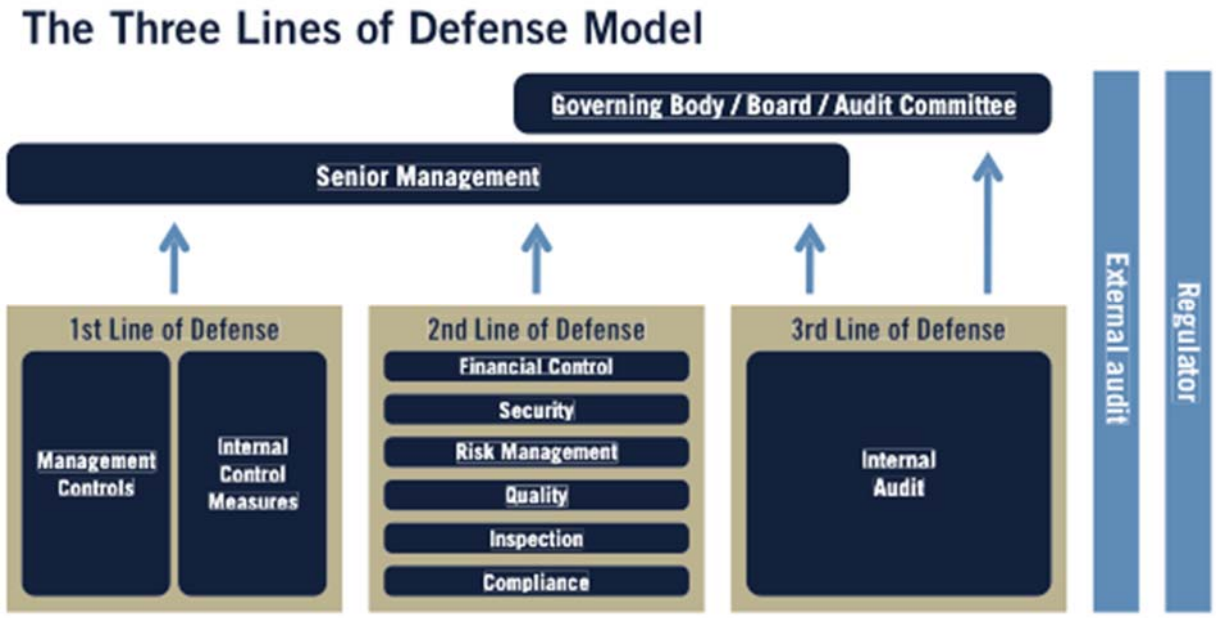
[15] See the speech by DANIÈLE NOUY, Chair of the Supervisory Board of the Single Supervisory Mechanism, *The European banking landscape – initial conclusions after four months of joint banking supervision and the main challenges ahead*, Frankfurt am Main, 17 March 2015, available at www.bankingsupervision.europa.eu/press/speeches/date/2015/html/se150317.en.html. The process of approximation of laws underpinning the Single Rulebook and the Banking Union in Europe is inspired by the main goal of restoring public confidence. In that respect, for instance, "making banking resolution credible" has been rightly, and pointedly, identified as the core challenge for legislators and regulators when drafting the Bank Recovery and Resolution Directive, 2014/59/EU (BRRD). See BRRD, preamble, recital 5, and, among scholars, eg ARMOUR, "Making bank resolution credible", in Ferran, Moloney and Payne (eds), *Oxford Handbook of Financial Regulation*, Oxford University Press, 2014; and BINDER, "Resolution: concepts, requirements and tools", paper presented at a symposium on *Bank Recovery and Resolution in Europe – The EU Crisis Management Directive in Context*, organised jointly by the author and Dalvinder Singh, University of Warwick, at the University of Tübingen, Germany, on 18–19 October 2014

[16] JAMES SHIPTON, Executive Director of Intermediaries Securities and Futures Commission, Hong Kong, *Supervision of intermediaries: key initiatives and focus in 2014*, 4 June 2014.

[17] IIA (Institute of Internal Auditors), Position Paper, *The three lines of defense in effective risk management and contro*l, January 2013.

The main value added of this model is to allow for a coordination of control responsibilities in an effective and efficient manner. To reach this objective, roles and responsibilities need to be clearly communicated to risk and control functions so that each group of professionals understands the scope of its activities and how that scope relates to the activities of other groups.

The model is summarised graphically below:



Graph 1: The Three Lines of Defense Model (IIA (2013))

The characteristics of the model are described in the following sections.

The first line

The revenue-generating business units form the basis of the model and are referred to as the first line of defence. Depending on the type of industry in question, these units may include the production of physical goods or the provision of financial services such as trading, asset management, sales and client relationships. The intention of the model is to assign the basic control and risk management responsibilities to this first line of defence (ie staff and managers working in those revenue generating units). The model assumes that controls in this first line are very granular and based on individual transactions as staff are involved in processes on a daily basis and are familiar with the workflow and possible control weaknesses. Therefore, it is easier for them to implement controls that target more granular processes and detect weaknesses early on. This allows them to provide immediate notification to the appropriate management levels and ensures a timely implementation of necessary measures. With the introduction of automated controls, it has become possible to make control activities comprehensive (ie to capture all relevant data) as well as detailed, given that only exceptional situations are highlighted by a system requiring immediate management review. The control duties in the first line also underline the dual responsibility of units which is to generate business for the organisation while remaining cognisant of the associated risks and controls. This approach has been encouraged by the lessons learned from the GFC, during which risk-taking units did not demonstrate a sufficient awareness of risk and control procedures.

The second line

If the control systems outlined in the first line of defence become ineffective, or are absent, the second line of defence becomes important. It comprises various risk management and compliance functions (ie support functions) such as finance, compliance, risk control, model

validation and back office, whose key duties are to monitor and report risk-related practices and information, and to oversee all types of compliance and financial controlling issues. Over the last twenty years, the second line of defence has evolved considerably in organisations pertaining to the regulated financial industry. With the introduction of a middle office, compliance duties (the introduction of effective market, credit and operational risk management functions, the implementation of an independent price verification function and an independent model validation role) appear to have expanded exponentially.

In response to tighter regulatory requirements and more complex products and processes, organisations have added additional staff and functions in the second line. Without thorough organisation and coordination of responsibilities, financial entities sometimes exhibit considerable control gaps that may call into question their financial soundness. Examples of insufficient second line of defence functions are the rogue trading scandal at Société Générale in 2008 and financial losses at UBS in 2007 which arose from the US mortgage crisis and almost led to the collapse of the latter bank.[18, 19]

As such, the second line of defence defines preventive and detective control requirements, and ensures that such requirements are embedded in the policies and procedures of the first line. The second line must be independent of the first line and apply controls either on an ongoing (eg daily) or periodical basis. It must also be based on clear risk assessment criteria (eg detailed review of transactions of specific business units that exhibit a higher than usual staff turnover or unusually large number of errors or corrections).

The third line

The third line of defence, which represents the next level of control, comprises the internal audit function. In the last years, the practice has developed such that it provides independent assurance to senior management and the board on a broad range of objectives, including efficiency and effectiveness of operations, safeguarding of assets, reliability and integrity of reporting processes and compliance with laws and regulations.

For the function to be effective, it needs to be based on the highest level of independence and objectivity. This can best be achieved by implementing structures proposed by the IIA Attribute Standards 1100, which include organisational independence, implementation of a direct reporting line for the chief audit executive and unrestricted access to senior management and the board.[20] Measures taken to ensure this high level of independence include the ability of the internal audit function to meet with the board in the absence of senior management. The board is primarily responsible for an independent audit function and has to be cognisant of potential impairments to objectivity.[21]

Controls performed by the third line of defence are based on an effective risk assessment methodology. In practice, the audit function has to conduct at least annually a risk assessment of the organisation and identify business units or processes that exhibit a high level of residual risk (ie risk remaining after consideration of the internal control environment). As such, the third line can only ensure a periodic risk-based assessment rather than a granular and ongoing monitoring that is typical of the first line of defence.

External controls

Finally, there are additional external levels of controls that complement the three existing internal layers of controls. External auditors are among the most common bodies in this category as they are required by law for most organisations. Particular to the regulated financial sector are the requirements to be subject to review by industry-specific regulatory bodies (eg insurance or bank supervisory authorities) that reside outside the organisation. Even though they are external to

[18] Société Générale, General Inspection Department, *Summary Report*, May 2008.
[19] UBS, *Shareholders Report on UBS's Write-downs*, April 2008.
[20] IIA (Institute of Internal Auditors), *Attribute Standards 1100*, Independence and Objectivity.
[21] OECD, *Principles of Corporate Governance*, September 2015.

the organisation, external auditors are important for the organisation's overall governance and control structure as they set the relevant standards and rules to be implemented and are ultimately responsible for assessing whether these rules are adequately complied with. This might lead to situations where regulatory issues take centre stage in an organisation and determine governance structures and processes.

The discussion below first summarises the features of the most common model in use (the three-lines-of-defence model), sets out the background and reasons for tailoring the existing model to the needs of financial institutions, and finally analyses each bilateral relationship between these three control functions by evaluating the benefits and drawbacks of increased cooperation and communication.

3. Weaknesses and past failures of three-lines-of-defence model

Despite the enthusiastic embrace of the three-lines-of-defence model at major financial institutions over the past few years, the series of banking scandals that have occurred, and in which failures of internal control systems have played a role, have led to substantial financial losses and near-bankruptcies. Taking into account this evidence, we analyse the root causes of these problems and the weaknesses of the three-lines-of-defence model in practice:

1. Misaligned incentives for risk-takers in first line of defence

Many experts agree that the most important control is the first line of defence.[22] However, this responsibility conflicts with the objective of most risk-takers in the first line, which is to generate sufficient revenue and profits for the institution. In the past, management put greater emphasis on and set compensation based on the achievement of financial objectives rather than control-oriented objectives. One of the reasons for the financial difficulties faced by UBS during the US subprime crisis was insufficient controls and financial reporting systems in the context of expanding derivatives trading positions on US residential mortgage-backed securities at the investment bank.[23] While the bank accumulated such positions, this information did not reach the top layers of management and was watered down in general reports, thus concealing the true exposure to the US mortgage market. The question remains of how a bank remunerates traders that meet the control objective but fail to generate revenue for the institution. A way forward could be to introduce a compensation system comprising a low proportion of a flexible bonus element, coupled with the achievement of a mandatory control objective before any bonus is paid out. Moreover, at a higher level of the organisation, the problem could be framed as an issue of improper communication (sometimes compounded by the lack of a properly comprehensive perspective by those who should be primarily concerned).[24]

2. Lack of organisational independence of functions in second line of defence

A common criticism of the effectiveness of controls performed by the second line is the lack of organisational independence of the control functions.[25] Most risk management functions report formally to the board. However, the de facto day-to-day reporting lines and communication channels are more likely to go to senior management than to the board. Critical control functions might lose their independence by being embedded in the organisation through engagement and exchange of information with other functions of the first and second line of defence and – over

[22] LYONS, *Corporate oversight and stakeholder lines of defense*, The Conference Board Executive Action Report, no 365, October 2011; CAPRIGLIONE AND CASALINO, "Improving corporate governance and managerial skills in banking organizations", *International Journal of Advanced Corporate Learning*, 2014, vol 7, issue 3; SPIRA AND PAGE, "Risk management: the reinvention of internal control and the changing role of internal audit, *Accounting, Auditing and Accountability Journal*, 2003, vol 16, no 4, pp 640–661; Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Effective enterprise risk oversight: the role of the board of directors*, September 2009.

[23] UBS, *Shareholders Report on UBS's Write-downs*, April 2008.

[24] *International Professional Practices Framework* (IPPF), Altamonte Springs, FL: The Institute of Internal Auditors, 2013.

[25] ANDERSON AND EUBANKS, *Leveraging COSO across the three lines of defence*, July 2015.

time – might adopt views typically put forward by risk-taking units rather than control units. Remuneration of the second line of defence also plays a crucial role. Banks are struggling to set objectives for control units that compensate sufficiently for risk and control awareness while still allowing the organisation to generate steady profits.

3. Lack of skills and expertise in second line functions

Even if functions in the second line of defence are organisationally independent, they may lack sufficient skills and expertise to challenge effectively practices and controls in the first line such as the validation of complex models (eg models based on internal ratings or interest rate risk in the banking book) or to provide independent valuations of illiquid or hard-to-value instruments. Remuneration and experience in first line functions are still considerably higher and more senior than in second line functions despite the tighter regulation of variable compensation practices. The question remains of how banks can entice highly qualified staff to work in second line functions rather than in first line or risk-taking functions. Jérôme Kerviel of Société Générale maintained unauthorised speculative positions for more than a year without them being detected.[26] Back office and risk control departments at Société Générale launched multiple inquiries relating to irregularities and inconsistencies arising from these speculative trades but did not detect any wrongdoing because Kerviel was able to give untruthful replies that none of the second line control functions challenged sufficiently forcefully.

4. Inadequate and subjective risk assessment performed by internal audit

The effectiveness of the work of internal auditors largely depends on a well-established audit plan based on an annual risk assessment that is comprehensive, objective and which is performed by individuals that have a good grasp of the risk profile of the organisation. Whether internal auditors possess the knowledge, skills and experience required to make these judgments depends largely on the auditors' own experience and exposure to risk-taking and management functions. The purpose of these risk assessments is to identify high-risk areas or processes in an organisation that will be subject to more frequent and rigorous audits. Failure in detecting high-risk areas will lead to audits focusing on the wrong risk areas and undermine the effectiveness of the third line of defence. As in the case of UBS,[27] internal audit performed a review of the critical trading desk for US mortgage-backed derivatives and detected control weaknesses, but failed to finalise the audit report in sufficient time. The delay in validating and finalising the audit report (which took various months) proved critical and weakened the otherwise good quality of the report.

Embedding the external auditors' role in the structure of the defence system could mitigate the shortcomings of the traditional three-lines-of-defence model and increase the soundness and reliability of the risk management framework (which draws on enhanced information and expertise provided by the external auditor). In the next section, we elaborate further on this idea by introducing the rationale behind the four-lines-of-defence model.

4. The concept of the "four lines of defence" model in financial institutions

Since the outbreak of the GFC, the design and implementation of internal control systems have attracted serious academic and professional attention. At the same time, research that investigates the characteristics and effectiveness of internal audit functions has been sponsored by the IIARF at regular intervals and has been published in academic and professional journals.

[26] Société Générale, General Inspection Department, *Summary Report*, May 2008.
[27] UBS, *Shareholders Report on UBS's Write-downs*, April 2008.

We approach the design and implementation of control systems to ascertain the extent to which financial institutions require a specific internal control model.

Whether a four-lines-of-defence model in financial institutions should be theoretically introduced, properly regulated and practically implemented is the starting point of our analysis. It can be seen as a subset of the question of whether it is *appropriate* to address the interactions between internal audit, financial supervisors and external auditors. In approaching the question, one should be aware that we limit the scope of our review of the three-lines-of-defence model to the financial industry.

In the aftermath of the GFC, proposals and reforms relating to the corporate governance of financial institutions and, particularly, to internal control systems, used the three-lines-of-defence model as the basic unit of analysis. That said, there was a risk that this model could not help ensure effective corporate governance and might indeed have exacerbated basic corporate governance weaknesses, especially in regulated sectors such as banking.

More precisely, the three-lines-of-defence model might prove to be unsuitable in dealing accurately with an organisation's operational peculiarities which stem not only from the nature of the business itself[28] but also from the specific institutional framework of the banking and insurance business (regulation and supervision).[29] That framework aims at protecting the different stakeholders of banks and insurance companies against the particular risks inherent to such entities, including vulnerability to a systemic collapse.[30, 31]

Regulations have become increasingly detailed over the past decade. Financial supervisors have, in parallel, been called increasingly upon to deal with every aspect of organisation and strategy regarding the protection of financial institutions' soundness whenever market integrity was at stake.

The motivation for this paper is to investigate and examine why financial institutions are different from other sectors, and to improve the effectiveness of the three-lines-of-defence model. We also propose a new model that focuses on the specificities of the financial sector rather than one that overlooks it. In addition, the three-lines-of-defence model could be strengthened by making supervisors and external auditors an inherent part of the internal control and risk monitoring systems. Depending on the size, nature and complexity of an entity, though, there may be other parties involved in the management of risk. Such parties need to be considered an integral part of the model: a fourth line of defence may exist by way of external auditors and/or regulators,[32] particularly so for financial institutions.

[28] Banks run a unique business in that they are intermediaries between savers and users of capital. Banking is considered to be a specific kind of activity resulting in high complexity, the involvement of many stakeholders and the existence of a high level of interlinkages amongst market participants. See, for example, DE HAAN AND VLAHU, "Corporate governance of banks: a survey", *DNB Working Paper*, 2013, 386, 2; MEHRAN, MORRISON AND SHAPIRO, *Corporate governance and banks: what have we learned from the financial crisis*, Federal Reserve Bank of New York, 2001, 502, 3.

[29] This is also traditionally known as "structural law" in Anglo-Saxon financial history: COATES, "The Volcker rule as a structural law: implications for cost-benefit analysis and administrative law, *ECGI Law Working Paper*, 2015, no 299.

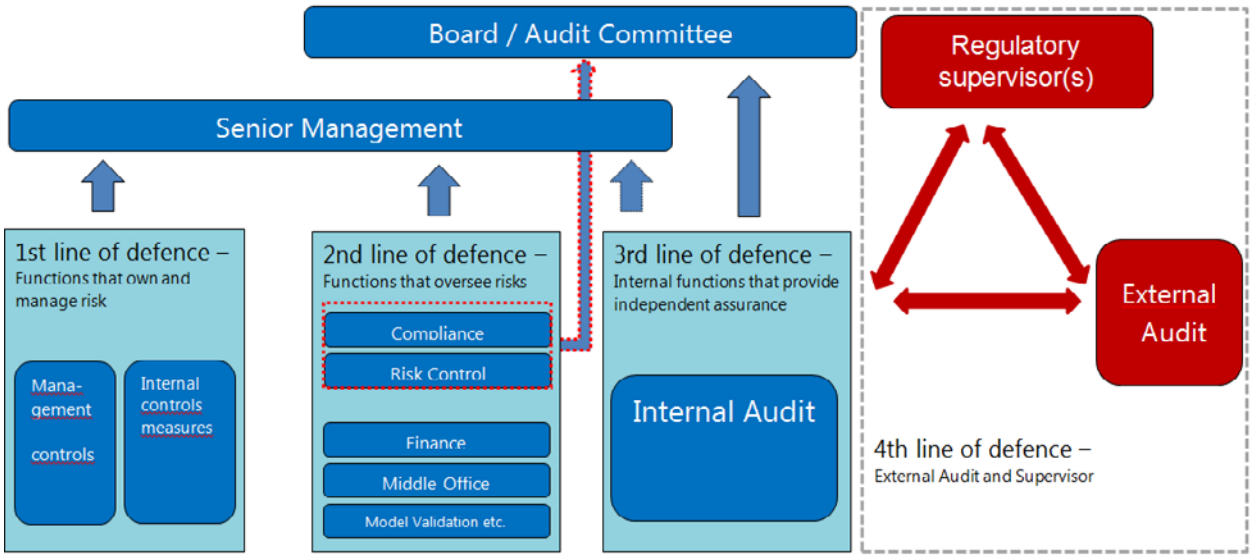
[30] HOPT, "Corporate governance of banks and other financial institutions after the financial crisis", *Journal of Corporate Law Studies*, 2013, 243; VAN DER ELST, "Corporate governance and banks: how justified is the match", *ECGI Law Working Paper*, 2015, 284, 24.

[31] MÜLBERT, "Corporate governance of banks", *European Business Organization Law Review*, 2009, 422. The regulator represents the interests of those parties, like the public interest, that are unable to protect themselves through private mechanisms due to the absence of appropriate rights or incentives (see eg ALEXANDER, "Corporate governance and banking regulation", *Cambridge Working Paper*, 2004, 17, 3).

[32] HOPKIN, *Risk management*, Kogan Page Publishers, 2013, 193.

For a long time, international standard setters did not require a close relationship between supervisors, and internal organs and functions.[33] More recently, they have called for a stronger interaction, particularly with respect to enhancing dialogue with the board and senior management on the governance of risk, including the development of an institution's risk appetite framework and an assessment of its risk culture. In that respect, the Federal Reserve has recently addressed the issue and, building upon the 2003 *Policy statement on the internal audit function*, issued a new section entitled *Enhanced internal audit practices*. That section encourages examiners to "rely on the work performed by internal auditors" and to "supplement their examination procedures through continuous monitoring and an assessment of key elements of internal audit".[34] The BCBS paper on the internal audit function in banks reaches similar conclusions when describing the relationship between internal audit and supervisors.[35] It not only provides an overview of supervisory expectations relevant to the internal audit function (including quality assessment) but also explicitly underlines the benefits of enhanced communication between supervisors and internal audit functions.

The four-lines-of-defence model is meant to precisely address this "deficiency" by assigning a specific role to external parties (namely, external auditors and banking supervisors) in relation to the design of the internal control system, acknowledging that, although they remain outside the organisation's boundaries, they constitute a vital element of assurance and governance systems.



Graph 2: Four-lines-of-defence model for financial institutions

As the four-lines-of-defence model intends to enhance coordination between external parties and internal auditors, greater communication is at the basis of its success. Communication works by reducing, if not eliminating, asymmetric information among the parties involved, provided, of course, that the *treatment* of information is such as to make risk control systems more effective.

[33] More recently, Financial Stability Board, *Supervisory intensity and effectiveness. Progress report on enhanced supervision*, 7 April 2014.
[34] Board of Governors of the Federal Reserve System, *Supplementary policy statement on the internal audit function and its outsourcing*, 2013.
[35] Basel Committee on Banking Supervision, *The internal audit function in banks*, June 2012.

In some cases, imposing additional disclosure requirements may prove counterproductive if it causes the parties involved in the fourth layer to change their behaviour in an adverse way. This would aggravate the problem of moral hazard to the detriment of the effectiveness of the internal control systems.[36] Increasing the amount of information is not good in and by itself, and may even result in less effective and efficient control systems.[37]

In that respect, the four-lines-of-defence model would entail a new setup of processes and rules, especially in terms of information that internal auditors, external auditors and supervisors are respectively required to share (or not allowed to share). These rules set forth the categories of information made available to whom, the procedures for obtaining documents and records, and the rules for limiting the release of exempt and confidential supervisory information and for protecting confidential information.

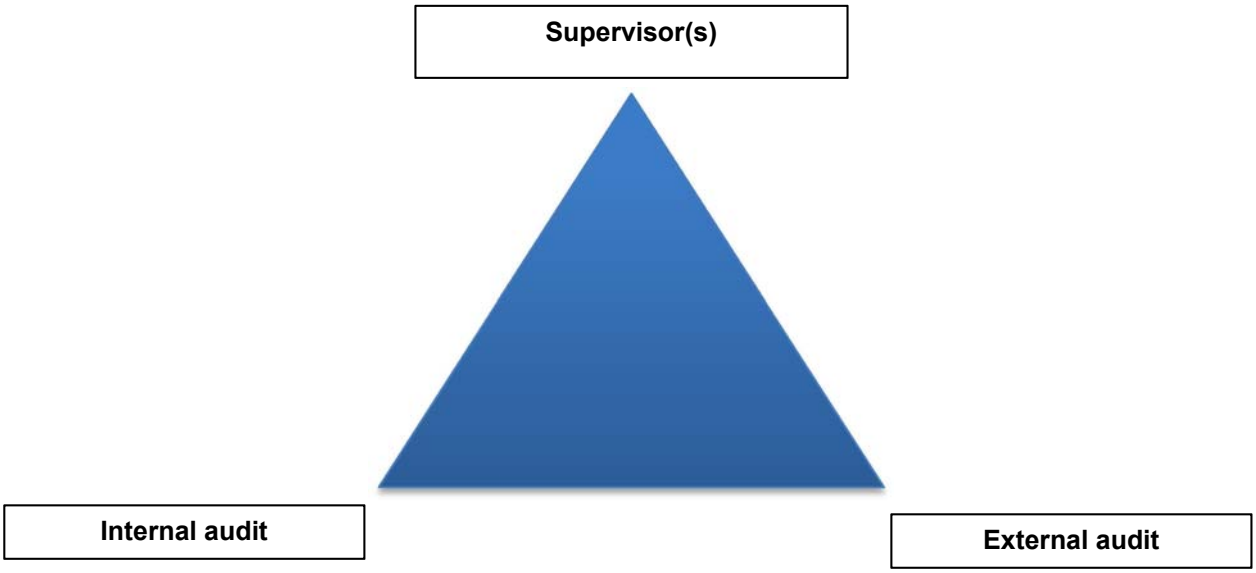
As the business of banking has grown in complexity over time, the tasks of banking supervisors and external auditors are actually becoming increasingly demanding. This holds true particularly in regulatory regimes where competencies are shared between a centralised supervisory authority and national supervisory authorities, as in the EU.[38] The growing complexity of transactions and markets is making supervisory agencies less able to reduce information asymmetries. As a consequence, supplementary approaches should be sought to reduce such asymmetries. The additional line of the defence might help in that respect. In fact, internal auditors, banking supervisors and external auditors face similar challenges and their role should be seen increasingly as complementary.

Not only do bank supervisors benefit from the result of the internal auditing work but they also turn to external auditors for certain additional tasks or for the collection of supplementary information when this contributes to their supervisory work. At the same time, moreover, external auditors could also benefit from a relationship with supervisors. In carrying out their duties, they could obtain access to information that would help them in discharging their responsibilities more effectively. This would lead to a triangular relationship between internal auditors, banking supervisors and external auditors.

[36] In the absence of disclosure agreements about the treatment of information, the internal audit of one bank might reveal confidential information regarding the situation of another bank.

[37] The same problem arises, for instance, when government should optimally disclose information about banks' assets during a financial crisis: see FARIA-E-CASTRO, MARTINEZ AND PHILIPPON, "Runs versus lemons: information disclosure, fiscal capacity and financial stability", *National Bureau of Economic Research*, 2015.

[38] On the distribution of tasks between the ECB and NCAs, see ECB, *Guide to banking supervision*, November 2014. In the literature, see FERRARINI AND CHIARELLA, "Common banking supervision in the eurozone: strengths and weaknesses", *ECGI Law Working Paper*, 2013, 223; EILIS, "European Banking Union and the EU single financial market: more differentiated integration, or Disintegration?", *University of Cambridge Faculty of Law Research Paper*, 2014, no 29; FERRARINI, "Single supervision and the governance of banking markets", *ECGI Law Working Paper*, 2015, 294.



Graph 3: The “regulatory triangle”

According to the four-lines-of-defence model, the external auditors might provide an autonomous assessment of the first three lines where this is relevant to the audit of the organisation’s financial reporting and to compliance with regulatory requirements. In this sense, by providing additional assurance to shareholders and senior management, external auditors, regulators and other external bodies have an important role to play in an organisation’s overall governance and control structure.

Moreover, the interaction between control functions (ie the internal audit function) and supervisors might result in an improvement to the tools and methods that could be used by supervisors in order to intensify their oversight of financial institutions, aiming at delivering pre-emptive, rather than reactive and outcome-based supervision. In other words, by virtue of improved communication channels with internal audit, supervisors might be provided with useful and reliable information to support their judgments and enable them to be more forward-looking in their assessments of risk. Better informed supervisors, armed with accurate information, help in ensuring that market stability is being maintained.

Especially in times when, more than ever, financial institutions must regain and command the confidence of the public and of those with whom they do business, a closer relationship between internal auditors, supervisors and external auditors would lend credibility and confidence to the financial sector. Greater mutual understanding of the respective roles and responsibilities of these three actors would improve the effectiveness of each area, as they have complementary concerns regarding the same matters even though the focus of their concerns is different.

Building upon the triangular relationship between internal auditors, supervisors and external auditors, the next sections of this paper clarify the benefits of a four-lines-of-defence model by examining each of the interactions between them. Our review of the current literature indicates that no studies directly address the issues related to such a model. Let us consider each relationship in turn, as each is an important element in developing an effective control system that contributes to the best allocation and management of risk within individual institutions.

5. Relationship between functions of the third and fourth line of defence

5.1 Relationship between external auditors and supervisors

The first relationship under review is the one between external auditors and regulatory authorities. While each of these two functions have their own scopes and approaches, the same areas and topics may be subject to a qualified exchange of information and viewpoints.[39]

We should first analyse the responsibilities of external auditors and supervisors before elaborating on the features of their relationship and the peculiarities of their interaction.

The role of the external auditor is primarily to review financial statements to ensure that they are free from material misstatement and prepared in accordance with an appropriate financial reporting framework.[40] It must be mentioned at the outset that the auditor's opinion is highly relevant in establishing the credibility of financial statements and underpins the financial soundness of the institution. As is the case for internal auditors, external auditors provide an independent assurance to the board, senior management and shareholders. However, the scope of activity of the internal auditor differs from that of the external auditor as the latter is primarily concerned with the financial statements. The external auditor attests that financial statements provide a fair reflection of the financial position and performance of the company in all material respects.[41]

In order to ensure the independence of external auditors, several governance arrangements must be put in place. The audit committee of the board should identify and nominate suitable candidate firms to act as external auditors and approve their appointment. Mandatory tenure limits and rotation are now commonly imposed on external auditors to avoid situations where they gradually lose their objectivity and independence as they become too closely engaged with the organisation over time. Furthermore, certain jurisdictions have introduced a limit on the amount of non-audit services provided by the auditor to prevent external auditors from being involved in auditing their own work. Financial institutions can further enhance auditors' independence by publicly disclosing payments to external auditors for non-audit services and prohibiting auditors from having a stake in the audited organisation.[42]

Some key responsibilities of banking supervisors are to "authorise banks, conduct ongoing supervision, address compliance with laws and undertake timely corrective actions to address safety and soundness concerns especially with potential risks to financial stability".[43] One of the cornerstones of effective supervision is the operational independence of the supervisor together with a sound governance framework within the supervisory authority. Following changes to the regulatory environment and in response to the shortcomings highlighted by the GFC, the scope of supervisory activities has been broadened to include additional responsibilities such as a review of the operational risk management framework, an assessment of internal control frameworks and of the adequacy of internal and external audit.[44]

[39] Appreciation of the work of internal audit has been pointed out by the Committee of European Bank Supervisory in comments related to "Proposed Redrafted International Standard on Auditing 610 – The Auditor's Consideration of the Internal Audit Function", March 2007.
[40] ISA (International Standard on Auditing) 200, *Overall Objectives of the independent auditor and the conduct of an audit in accordance with International standards on Auditing*, paragraph 11.
[41] OECD, *Principles of Corporate Governance*, September 2015.
[42] OECD, *Principles of Corporate Governance*, September 2015.
[43] Basel Committee on Banking Supervision, *Core Principles for Effective Banking Supervision*, Core Principle 27, September 2012.
[44] Ibid.

In practice, the growing complexity and internationalisation of financial institutions has meant that a single institution is rarely subject to a single regulatory authority. Institutions may be subject to more than one regulator for the following specific reasons:

- Cross-border banking and insurance groups. A financial institution may be part of a large, internationally active foreign-owned banking or insurance group. In this case, the regulator located in the country of the branch or subsidiary is referred to as "host regulator" whereas the regulator of the foreign holding company acts as "home regulator". To facilitate the exchange of information between the home regulator and (the various) host regulators, so called "supervisory colleges" have been implemented. Such colleges should be permanent but flexible structures that allow for collaboration, coordination and information-sharing among the regulatory authorities of cross-border financial groups.[45]
- Country- or region-specific structures. Such structures may require financial institutions to be subject to a special arrangement such as a supranational supervisory authority in addition to a local supervisor. An example of such a supranational supervisory body is the "Single Supervisory Mechanism" (SSM) which represents a centralised bank supervisory authority vested in the European Central Bank (ECB). Although it was established in 2014, a precise division of power has yet to be agreed by the participating national supervisors and the SSM.[46, 47]
- Various regulatory bodies in the same jurisdiction. Depending on the assignment of financial oversight responsibilities in a specific jurisdiction, various regulators (eg bank and insurance regulators, and securities and exchange commissions) may be charged with the oversight of a financial institution.

These additional layers of supervisory review may add complexity to the way supervisors interact with external auditors. Supervisors should ensure that each regulator involved complies with the scope of the review it is charged with to avoid possible overlaps.

Having laid out the responsibilities of the external auditor and supervisor, we analyse in greater detail the features of their relationship and how they could benefit from each other. Their mutual interest lies in the fact that the auditor may obtain information regarding risk and operational practices that are otherwise not directly accessible to the supervisors.

Supervisors might be interested in the results of a review of the internal control framework performed by the external auditor as supervisors are often not able to conduct reviews themselves due to resource and budget constraints. If the supervisor were to receive such information, it would improve the effectiveness of supervision. Supervisors also collect information and focus their reviews on an assessment of the organisation's ability to comply with financial regulations pertaining to the jurisdiction in question. This information, in turn, may have an impact on the financial statements and prove interesting to external auditors who – by the nature of their duties – might not have access to detailed information. Information provided by the supervisor may enable the external auditor to form a better opinion of the soundness of financial statements.[48]

[45] Basel Committee on Banking Supervision, *Principles for Effective Supervisory Colleges*, June 2014.
[46] ECB, *2015/839 Decision of 27 April 2015 identifying the credit institutions that are subject to a comprehensive assessment (ECB/2015/21)*.
[47] Global Risk Regulator, "ECB single supervisor's relations with national authorities still in flux", *The Banker*, June 2015.
[48] Basel Committee on Banking Supervision, *External audits of banks*, March 2014.

One needs to take into consideration that there is a hierarchical relationship between the supervisors and the external auditor: supervisors have an obligation to assess the adequacy of the external audits, the power to establish the scope of external audits and may determine the standards to be followed in performing such audits. The supervisor may also require the use of specific approaches in the planning and performing of the external audits.[49]

Furthermore, certain jurisdictions allow bank supervisors to request external audit firms to review areas beyond the statutory requirements of external auditors, if deemed appropriate.[50]

In some jurisdictions, external auditors have a duty to report matters of material significance[51] to the supervisor.[52] One needs to critically assess this obligation as this is only possible in jurisdictions where external auditors are protected from litigation or legal proceedings when disclosing confidential information to third parties (safe harbour).[53] If such safe harbour protection does not exist, external auditors may need to resort to alternative measures. They may, for instance, decide to report confidential issues indirectly to the supervisors through the bank's management. Alternatively, external auditors may also consider obtaining explicit approval from the board and management permitting them to disclose confidential information to supervisors.[54]

However, there are instances where external auditors voluntarily decide to report on issues that are outside the scope of their duties but may nevertheless be of interest to bank supervisors. This might be the case if the external auditor detects significant deficiencies in internal control processes or opaque business structures intended to circumvent financial regulations.[55]

Whatever the scope of cooperation and exchange of information is, the autonomy of the various parties should not be impaired and each party should be in a position to independently perform work within its respective statutory scope and responsibilities. Clear boundaries of responsibilities should exist and all parties should ensure that confidentiality regimes are complied with.

Communication between these parties could take the form of written reports or oral exchanges such as, periodic or ad-hoc, informal or formal meetings. Meetings could be of a bilateral (ie between external auditor and supervisor) or trilateral nature (ie between external auditor, supervisor and the chair of the audit committee). Systemically important banks have been encouraged to implement trilateral meetings.[56]

Supervisors have been encouraged to prepare written reports on important issues and exchange these with management, the board and the external auditors.[57] Written documents could include

[49] Basel Committee on Banking Supervision, *Core Principles for Effective Banking Supervision*, Core Principle 27, September 2012.
[50] Basel Committee on Banking Supervision, *External audits of banks*, March 2014.
[51] The term "material significance" requires interpretation in the context of the specific legislation relevant to the regulated entity. A matter or group of matters is normally of material significance to a regulator's function when, due to either its nature or its potential financial impact, it is likely of itself to require investigation by the regulator. (Material significance is sometimes determined by establishing a single rule method, e.g. 5% of pre-tax income or 0.5 % of total assets)
[52] Basel Committee on Banking Supervision, *External audits of banks*, March 2014.
[53] Directive 2014/65/EU (MIFID II), Article 77; Directive 2013/36/EU (CRD IV), Article 63.
[54] Basel Committee on Banking Supervision, *External audits of banks,* March 2014.
[55] Ibid.
[56] Basel Committee on Banking Supervision, *External audits of banks*, March 2014.
[57] Ibid.

extended reports on the audited financial statements, which are submitted to the supervisor but are not available to the general public.

An interesting survey conducted by the Independent Forum of Independent Audit Regulators (IFIAR)[58] analysed the quality of external auditors. It collected information on inspections of the quality of the external audits of public interest entities and of systemically important financial institutions (SIFIs). The three main areas of finding reported in the 2014 Survey for SIFIs relate to audit of the Valuation of Investment and Securities (27% of inspected audits had findings), Internal Control Testing (27%) and audit of Allowance for Loan Losses and Loan Impairments (17%).

A finding does not necessarily indicate that the financial statements were misstated but implies that the auditor's performance fell below the expected level of diligence that would have satisfied the public interest role of the audit. It also implies that the audit failed to provide the level of assurance about the financial statements that it was supposed to ensure and that was required by professional standards. Confidence in the auditor's execution of this assurance function should not await the ex post result of an inspection of the auditor.

Regulatory capital ratios, as well as other indicators of financial strength, such as liquidity and leverage ratios, are produced alongside banks' standard financial reports but are not audited in the same way. This may create an expectations gap for society: what may be a bank's most looked-at indicator is not audited. External auditors could perform assurance tasks related to such regulatory requirements (including capital ratios and risk-weighted assets, and leverage and liquidity ratios). Requirements for the independent scrutiny of regulatory capital information have evolved piecemeal across the world; some countries mandate publically available assurance reports, some only require financial institutions to inform regulators while others have no reporting requirement whatsoever. Given the size and importance of the banking sector – and the systemic risk posed to global financial markets – credibility and reliability are crucial.

We have explored developments in a number of countries to illustrate the importance of increased cooperation between bank supervisors and external auditors:

1. United Kingdom:

The Prudential Regulation Authority (PRA) of the United Kingdom recently issued a consultative document[59] laying out the rules for external auditors of the largest UK banks for the provision of written reports to the PRA as part of the statutory audit cycle. The PRA asked external auditors to contribute to its supervision of firms by directly engaging in a pro-active and constructive way to support judgment-based supervision and help promote the safety and soundness of firms supervised by the PRA. The insights gained by auditors when they carry out high-quality audits should help enhance the effectiveness of the relationship between the auditors and the supervisor.

There have been improvements in the last few years such as a closer and more frequent engagement between supervisors and external auditors. The PRA keeps monitoring the quality of auditor-supervisor dialogue. In a survey of external auditors, it was noted that the vast majority of engagements was considered only 'reasonable' and that the PRA's aim was to improve this engagement in the longer term. In particular, in individual cases both supervisors and auditors considered that there was room for improvement in the frankness with which information was shared, how often it was shared and what was covered in bilateral meetings.

[58] IFIAR Report on 2014 Survey of Inspection Findings, 3 March 2015.
[59] Prudential Regulation Authority, *Engagement between external auditors and supervisors and commencing the PRA's disciplinary power over external auditors and actuaries*, consultative paper, February 2015.

2. Switzerland:

For many years, the Swiss Financial Market Supervisory Authority (FINMA) has adopted a dualist approach whereby on-site examinations are outsourced to approved and licensed external auditors. A recent IMF assessment [60] noted significant weaknesses in Swiss supervision. FINMA should provide more guidance to auditors to ensure greater supervisory harmonisation across entities and should complement the auditors' work with its own in-depth-examinations of selected issues. In addition, the payment of auditors by a supervised entity was viewed critically as auditors should not be paid by a supervised entity but rather by a "FINMA-administered bank-financed fund". The IMF also noted that FINMA's on- and off-site supervisory resources had been increased in recent years but still needed to be strengthened.[61] Resources were insufficient to supervise and regulate the entire banking system in a way that met the Core Principles for Banking Supervision, including sufficient in-depth on-site work and oversight of supervisory work done by external auditors, particularly for small- and medium-sized banks.

3. United States:

A recent IMF report [62] examined the relationship between supervisors and external auditors, and noted "that supervisors meet periodically with external audit firms to discuss issues of common interest relating to bank operations". It also noted that there was no "safe haven" protection for external auditors in reporting issues to regulators. However, according to Part 363 of the Federal Deposit Insurance Corporation (FDIC) rules, a bank must inform its supervisor within 15 days of having received written information from the auditors about a violation that was committed. This gap is somehow mitigated by the frequent contact between supervisors and auditors in the course of examinations and planning. Furthermore, although the supervisors cannot set the scope of the external audit, they could encourage the auditors to include new issues. However, the report highlighted weaknesses relating to the fact that supervisors do not have legal powers to add specific issues to the scope of the external audit in order to address issues that are not normally covered by such an audit.

4. Hong Kong:

The Hong Kong Monetary Authority (HKMA) devotes significant efforts to ensuring effective communication channels with external auditors. Furthermore, its powers to commission external auditor reports for supervisory purposes further supports the relationship between the HKMA and the external auditors, and the understanding of the HKMA's supervisory concerns. However, a recent IMF report[63] states that there are two areas in which the HKMA lacks powers and where the legislative framework could be enhanced: the HKMA lacks powers to reject the appointment of an external auditor, when there are concerns over its competence or independence, and it does not have direct power to access the working documents of the external auditor even though the HKMA is able to address issues that arise by indirect means. While the HKMA has been able to work around these restrictions, amendments to the relevant legislation should be made.

[60] IMF Country Report 14/143, Switzerland: Financial Sector Stability Assessment, May 2014.
[61] IMF Country Report 14/264, Switzerland: Detailed assessment of compliance – Basel Core Principles for Effective Banking Supervision.
[62] IMF Country Report 15/170, United States: Financial Sector Assessment Program, July 2015.
[63] IMF Country Report 14/131, People's Republic of China – Hong Kong Special Administrative Region, Report on the Observance of Standards and Codes, May 2014.

5.2 Relationship between internal auditors and supervisors

Governments and international organisations are calling for an increasing role of the internal audit of banks.[64] Officers from national supervisory authorities have been holding hearings on internal control tools and procedures in response to the GFC and its impact on the overall exposure to risk.[65] The Federal Reserve,[66] the European Banking Authority (EBA),[67] and other national supervision agencies worldwide have likewise expressed concern about the lack of effective risk management and internal auditing. In response to such concerns, international standard setters have amplified the tasks performed by the internal audit function, for example, by requesting, with the introduction of Basel III, annual reviews of specific processes in credit, market and liquidity risk calculations.[68]

There is nonetheless an ongoing debate about the role played by internal auditing in the collapse of financial institutions. There remains much work to do in identifying the relevant shortcomings. Scholars have so far limited their analyses to the internal audit function in isolation. While these studies provide useful evidence linking conditions in the banking industry to the effectiveness of internal control systems, they tend to focus essentially on the relationship between the internal audit and other pillars of the internal control structure (ie the first and the second lines).[69]

In general, research on the effect of the interaction between internal auditors, supervisors and external auditors on the efficiency of corporate governance appears sparse, if not absent. In particular, there is little theoretical and practical evidence so far concerning the degree to which the three-lines-of-defence model suits the corporate governance of financial institutions. This gap suggests several fruitful avenues for research on the matter, which we discuss in the following paragraphs.

As the four-lines-of-defence model is meant to improve cooperation between internal auditors and external parties (ie external audit and supervisors), a greater command of their interaction is required, particularly as regards the relationship between the internal audit function and the supervisors.

[64] The role of internal audit from a regulatory perspective was emphasised in the Basel II International Convergence of Capital Measurement and Capital Standards of 2004. In that context, paragraph 165 entrusts internal audit with the responsibility for reviewing the overall risk management process at least annually by specifically focusing on internal processes related to the reporting of regulatory capital requirements. Examples of these internal processes are validation of changes in risk measurement processes, verification of data sources, and accuracy of appropriateness of volatility assumptions.

[65] BERNARD SHERIDAN, Director of Consumer Protection, speech delivered at the IIA Ireland Conference, 16 April 2015; LUIGI MARIANI, Deputy Head, Supervision Department, Bank of Italy, "The internal control systems for money laundering", speech at the 10th Meeting on Compliance, AICOM (Associazione Italiana Compliance), 25 June 2014.

[66] Federal Reserve, *Supplemental policy statement on the internal audit function and its outsourcing*, January 2013.

[67] EBA, Guidelines on Internal Governance, September 2011.

[68] With reference to the regulation policy in Europe, for instance, Article 74 of Directive 2013/36/EU (CRD IV) contains a general provision on internal governance and controls authorising the European Banking Authority (EBA) to issue guidelines in that regard. The EBA Guidelines on Internal Governance provide relevant information for EU Member States on implementing supervisory principles in this area. Paragraph 29 of the EBA Guidelines determines the specific features of an effective and adequate internal audit function in a financial institution. Nevertheless, in the absence of an EU-harmonising detailed rule on the matter, EU Member States are in charge of determining and implementing detailed standards with regard to supervision of the internal audit function.

[69] On the importance of having well established and stringent control measures to enforce good governance practices, see, within the vast literature, SOH AND MARTINOV-BENNIE, "The internal audit function: perceptions of internal audit roles, effectiveness, and evaluation, *Managerial Auditing Journal*, 2011, vol 26, issue 7, pp 605–622; LENZ AND HAHN, "A synthesis of empirical internal audit effectiveness literature pointing to new research opportunities", *Managerial Auditing Journal*, 2015, vol 30, pp 5–33; CHEVERS, DELROY AND MUNROE, "The internal audit process and good governance: toward a research model", *Academy of Business Research*, 2013, vol I, pp 48–58.

In a four-lines-of-defence model, the interaction between internal audit and supervisors gains particular relevance. On one hand, it allows supervisory authorities to promote best practices, and to identify and address risks before they become serious problems. On the other hand, it makes the internal control system more aptly structured on the basis of four layers of controls.

Although in several jurisdictions worldwide the internal audit function of banks is responsible for disclosing material information, insofar as is necessary to guarantee the soundness of the institution, this interaction is *one-way* and, more importantly, is the result of the authority exerted by the financial supervisor over the internal audit function of an institution.[70] In fact, this interaction is related essentially to the supervisory assessment of the internal audit function.

Principle 26 of the BCBS *Core Principles for Effective Banking Supervision*[71] determines that the supervisor should ascertain that banks have adequate internal control frameworks for the establishment and maintenance of a properly functioning operating environment and that take into account their specific risk profiles. This appraisal is intended to guarantee an independent internal audit function as a fundamental component of an adequate overall internal control framework. To this end, the document defines the criteria that should be used by the supervisor to assess whether the institution has an independent, permanent and effective audit function.

However, a sharper focus on a direct communication channel between internal audit and supervisors is one of the main points of the BCBS document. *The internal audit function in banks*. Principle 16 states that: "Supervisors should have regular communication with the bank's internal auditors to (i) discuss the risk areas identified by both parties, (ii) understand the risk mitigation measures taken by the bank, and (iii) understand weaknesses identified and monitor the bank's responses to these weaknesses."[72]

The adoption of a fourth layer in the design of the internal control framework would have practical implications, specifically in the way by which information circulates among internal audit and supervisors. According to such a model, supervisors would receive as much information as if they were part of the organisation's internal structure and were as closely involved in the effectiveness of the risk management control process of the financial institution as any other internal business unit. Moreover, supervisory authorities would share relevant information with the internal audit function as far as this could increase the effectiveness of the internal audit work, making the information channel a two-way one to the benefit of internal audit and supervisors alike.[73]

This has the potential to have a significant impact on the interaction between the internal audit function and the supervisors. It could make internal auditors more inclined to provide information, even on a voluntary basis. In that perspective, there are social psychology theories on disclosure worth mentioning as they offer some ideas that could prove fruitful in designing the mechanism/structure of communication between internal audit and supervisors. Researchers have shown that people are more inclined to disclose information to people they trust and who

[70] See, among others, Deutsche Bundesbank, *Gesetz über das Kreditwesen – KWG*, January 2015; Bank of Italy, *Disposizioni di vigilanza prudenziale per le banche*, circular no 285, 17 December 2013, IV(3); Wet Financieel Toezicht, Section 3:17(2), Netherlands; and Hong Kong Monetary Authority, *Supervisory Policy Manual - Internal Audit*, July 2009. For a comparative analysis, see European Confederation of Institutes of Internal Auditing, *Banking Internal Auditing in Europe*, Berlin, 2009.
[71] Basel Committee on Banking Supervision, *Core Principles for Effective Banking Supervision*, September 2012.
[72] Basel Committee on Banking Supervision, *The internal audit function in banks*, June 2012.
[73] In that respect, see Basel Committee on Banking Supervision, *The internal audit function in banks*, §75, June 2012.

reciprocate with their disclosures.[74] This outcome, however, does not suggest that the traditional and hierarchical relationship between supervised entities and supervisor should be superseded but rather that it should be integrated. As the empirical evidence shows, it is not always in the best interest of bankers to disclose information, at least if there are no incentives to do so, or if any form of "gainful/rewarding" is not present.[75]

Building on the existing literature, and cognisant of the contradictory findings across some of the previous contributions on behavioural economics and self-disclosure, we consider it possible to reconcile and improve communication patterns by virtue of the conceptualisation of a two-fold relationship between internal audit and supervisors. Thanks to a four-lines-of-defence model, we assume that it should be possible to achieve both:

a. *A vertical relationship*. The nature of this relationship is the result of the mandate the bank supervisor is entrusted with. It takes place when the supervisor assesses the quality of the internal audit function. This is essentially a hierarchical relationship; the internal audit being subordinated and subject to the review of the supervisor;

and

b. *A horizontal relationship*. This relationship arises when the supervisor is perceived to be part of the internal control system and engages in a horizontal relationship whereby it approaches the counterparty at the same hierarchical level. The supervisor is supposed to reciprocate by sharing information regarding risk and risk mitigation measures, thus again collaborating at the same level with the internal audit. The supervisor manages this relationship and must overcome internal audit's reluctance to disclose confidential information.

In this context, one of the main issues that arises is the treatment of information. As the model is conceived to reduce asymmetric information among the parties involved, it should be implemented provided that the *treatment* of information is such as to make the risk control system more effective. When deciding on whether and how to disclose public and private supervisory information, supervisors need to deal with challenges relating to the collection of information from financial institutions and to the disclosure of this information. However, the internal auditor's liability related to disclosure of confidential information to third parties should also be addressed. Internal auditors must be protected against litigation when disclosing confidential information in good faith (so-called safe harbour), as there is such legal protection for external auditors.[76] If there is no shield, the hypothesis that a four-lines-of-defence model promotes interaction would be negated as internal audit would be deterred from being collaborative. Such a situation would fail to improve the amount and quality of information at the disposal of supervisors.

Furthermore, endowing the supervisor with a role in the internal control system may jeopardise the supervisor's independence and objectivity. In other words, creating deeper and more extensive communication channels might cause supervisors to step in and influence, to some

[74] SUNSTEIN, "Behavioral economics and paternalism", *Yale Law Journal*, 2012; HORENSTEIN AND DOWNEY, "A cross-cultural investigation of self-disclosure", *North American Journal of Psychology*, 2003, 5(3), pp 373–386; ANTAKI, BARNES AND LEUDAR, "Self-disclosure as a situated interactional practice", *British Journal of Social Psychology*, 2005, 44 (2), 181–99.
[75] OSTBERG, "Disclosure, investment and regulation", *Journal of Financial Intermediation*, 2006, vol 15, pp 285–306; HERTZBERG, LIBERTI AND PARAVISINI, "Information and incentives inside the firm", *Journal of Finance*, 2009; ORLOV, "Optimal design of internal disclosure", *Simon Business School Working Paper*, 2015, no 6.
[76] See ISA 610.

extent, the strategy or business model of an institution. This could create undue interference in the decisions of that institution as a private undertaking.

More generally, according to anecdotal evidence, imposing additional disclosure requirements – without properly setting the rules and the boundaries – may prove counterproductive, causing the parties involved in the fourth layer to alter their behaviour. This would aggravate the problem of moral hazard to the detriment of the effectiveness of the internal control system.[77] Increasing the amount of information is not, in fact, good in itself and may even result in a less effective and efficient control system.[78] This could represent one of the possible negative effects of disclosing supervisory information.

In that respect, the four-lines-of-defence model requires a new setup of processes and rules, especially regarding the extent to which internal auditors, external auditors and supervisors, respectively, are required and allowed to share information.

These rules should set forth the categories of information that may be shared and determine to which parties the information may be disclosed. They should further establish the procedures for obtaining and protecting confidential documents and records, and for distributing them to a limited set of recipients. We acknowledge the need for formalising processes, including the organisation of meetings and their documentation to monitor the topics discussed (ex ante and ex post results). We also deem of great importance the guarantee of a certain degree of flexibility in order to convene *ad-hoc* meetings by both parties if a subject matter requires doing so.

We thus identify a need for establishing standards on how to foster the relationship by balancing the obligation of the supervisor to assess the internal function with his collaborative role in maintaining an open and constructive work relationship for information-sharing purposes.

From an organisational perspective, we would suggest to segregate the "assessor role" (vertical relationship) from the "collaborator role" (horizontal relationship), for instance, by requiring the supervisory authority to assign different teams/individuals to each of the assessor and collaborator roles.

As the role and responsibilities of internal auditors and banking supervisors differ according to jurisdictions, policymakers and regulators should overcome jurisdictional segregation and set out an integrated and coherent list of sound practices aiming at implementing a more holistic approach to the risk control framework, endowing the external auditors with a specific role. From a regulatory perspective, therefore, it is crucial to address the potential risks relating to the lack of detailed harmonised regulation governing the relationship between supervisors and internal auditors. This gap might leave a certain degree of flexibility in establishing and maintaining this relationship, causing eventually disparities in the way financial institutions and supervisors are held responsible for sharing information.

5.3 Relationship between internal auditors and external auditors

As mentioned earlier, a common feature of the responsibilities of both parties is to provide an independent assessment. While the external auditor focuses on the financial statements, and attests that these are free from material misstatements, the scope of activities of the internal auditor is much broader and includes – inter alia – an assessment of the efficiency and

[77] In the absence of disclosure agreements about the treatment of information, the internal audit of one bank might gain confidential information regarding the situation of another bank.

[78] The same problem arises, for instance, when government should optimally disclose information about banks' assets during a financial crisis: see FARIA-E-CASTRO, MARTINEZ AND PHILIPPON, Runs versus lemons: information disclosure, fiscal capacity and financial stability, *National Bureau of Economic Research*, 2015.

effectiveness of operations, of the reliability and integrity of reporting processes, and of compliance with laws and regulations.

In general, one needs to be critical of the use of the work of internal auditors for the purpose of the external audit. A recent Public Company Accounting Oversight Board (PCAOB) inspection report mentioned critically that, in many instances, the external auditor does not have a sufficient basis to rely on outsourced work.[79] Furthermore, a recent study of internal audit departments in North America revealed that more than 50% of respondents anticipated an increase in the number of hours that their internal audit functions would have to provide in direct assistance to external auditors.[80]

Nevertheless, benefits for both parties could be maximised by better aligning audit programmes and templates and making use of coordinated walkthroughs between internal and external auditors to avoid duplication. Furthermore, both parties should communicate early in the audit process about what the external auditor needs in order to use the work of the internal audit's testing of controls.[81]

External auditors may rely on work performed by internal auditors under certain circumstances: First, the external auditors need to clarify if their jurisdictions allow them to obtain direct assistance from internal auditors. There are jurisdictions that specifically prohibit reliance on external auditors for work performed by the internal auditors. When such "outsourcing" regimes are allowed, external auditors should first consider the effectiveness, independence and objectivity of the internal audit function, and its quality and skill sets, before considering charging it with carrying out certain audit tasks. External auditors are encouraged to minimise the amount of work carried out by the internal audit function and to perform more of the work directly to ensure that they are sufficiently involved in the audit process.[82]

Prior to using internal auditors' work, several arrangements need to be in place: the external auditors should consider obtaining written approval from "an authorised representative" of the financial institution under review to ensure that the internal auditors can perform their duties for the external auditors in an unobstructed way. Furthermore, internal auditors should commit in writing to keeping specific matters confidential, as instructed by the external auditors. They should also inform the external auditors of any threat to their objectivity.[83]

During the fieldwork, external auditors need to closely supervise and review the work of internal auditors.[84] External auditors should challenge all of the evidence and findings obtained by the internal auditors. They need to be satisfied that internal auditors provide adequate evidence and findings in support of their conclusions. Throughout the fieldwork, external auditors should remain cognisant of the possibility that the internal auditors' evaluations might not be adequate.

In parallel, the internal auditor may consider regular exchange of views with the external auditor. Even though internal audit tends to have more detailed insights into the organisation, it could

[79] The PCAOB is a non-profit corporation established by Congress to oversee the audits of public companies in order to protect the interests of investors and further the public interest in the preparation of informative, accurate and independent audit reports.
[80] Institute of Internal Auditors, *Intersecting roles – fostering effective working relationships among external audit, internal audit, and the audit committee*, March 2015.
[81] Ibid.
[82] ISA 610 (revised 2013), *Using the work of internal auditors and related conforming amendments*, March.
[83] Ibid.
[84] ISA 200, *Overall objectives of the independent auditor and the conduct of an audit in accordance with International Standards on Auditing*, paragraph 11.

still benefit from the external auditor's assessment of the institution under review, drawing on the external auditor's experience with other organisations in the same industry. It is not common practice for internal audit to outsource work to external auditors. On the contrary, to ensure independence of the outsourced service provider, internal audit is advised to outsource work to other firms than the chosen external auditor.[85]

Practice Advisory 2440-1 of the IIA stipulates that the internal audit charter or organisational policy may determine that results of the audit shall be communicated to "other interested or affected parties" such as external auditors.[86] If the internal auditor detects critically sensitive information and decides to inform the external auditor outside of its normal chain of command, this act is referred to as external whistleblowing. The internal auditor needs to evaluate whether its local jurisdiction protects it against law suits.[87] Generally, an exchange of written communication and standard audit reports are highly recommended. It is common for internal audit to forward all audit reports to the external auditor and, likewise, for the external auditor to provide a copy of its report to internal audit and debrief it on significant issues in a bilateral meeting.

A contentious point in the relationship between internal and external auditors has been the question of assigning responsibilities for conducting the follow-up of external audit recommendations. In general, follow-up processes are required to ensure that management action plans are timely and adequately implemented. Standard 2402 of the Information Systems Audit and Control Association (ISACA) sets out that external auditors may delegate follow-up to the internal audit function. If this is the case, the audit charter or engagement letters should clearly stipulate such responsibilities.

5.4 Transition from the three lines to the four lines of defence: the quest to design an effective model for financial institutions

This paper challenges the conventional reliance on the three-lines of defence model by arguing that it has proven less effective in "complex" corporate structures such as the ones governing financial institutions. The Achilles heel of the three-lines-of-defence model stems from a lack of comprehensive overview of the organisational structure. This results in a sub-optimal distribution of the relevant information and ineffective control measures at multiple layers of the organisation. On top of that, deficiencies in the understanding of risk-taking policies, and their impact inside and outside the individual financial institution, as well as of the way in which relevant data have been compiled – paired with cultural and behavioural failures - are commonly argued as root causes of the recent corporate scandals in the financial industry. These are lessons that carry important implications for the efficiency of the three-lines-of-defence model and call for alternative models.

It would be possible to further elaborate on the three-lines-of-defence structure in an attempt to suggest an "enlightened" model under which some of the incentives aiming at enhancing independence and professionalism would be in place. Nevertheless, as much as such an approach would help in overcoming existing deficiencies, there would remain the problem of incomplete information: the lack of material information required to ensure that internal risk and

[85] Institute of Internal Auditors, Practice Advisory 2050-3, *Relying on the work of other assurance providers*, October 2010.
[86] Institute of Internal Auditors, Practice Advisory 2440-1, *Disseminating results,* January 2009.
[87] Institute of Internal Auditors, Practice Advisory 2440-2, *Communicating sensitive information within and outside the chain of command*, May 2010.

control systems are capable of assessing, measuring, managing and curbing the risks to which financial institutions are exposed to. If the three-lines-of-defence model were the panacea for poor corporate performance and misleading risk management that theoreticians predict it should be, the call for supervisors to engage in an active dialogue and to play an integrative role would not have reached such a degree of urgency and topicality.[88]

A shift to a fourth line of defence articulation would be accompanied by a closer interaction between internal auditors, external auditors and supervisors. Although internal auditors, external auditors and supervisors have traditionally been expected to engage in close interaction, empirical research has shown that reality has not matched what theory predicted would happen.[89]

In many countries, supervisors have traditionally relied on the work performed by external auditors, for instance, by using them for on-site inspection functions.[90] In most jurisdictions, auditors have a duty to report or alert banking supervisors regarding certain matters. In the EU, Article 12(2) of Regulation (EU) No 537/2014 on specific requirements regarding the statutory audit of public-interest entities,[91] includes the requirement that an "effective dialogue shall be established between the competent authorities supervising credit institutions, on the one hand, and the statutory auditor(s) and the audit firm(s) carrying out the statutory audit of those institutions, on the other hand". However, the absence of a dialogue and relationship between the auditors and prudential supervisors in the pre-crisis period was identified as a significant weakness.[92] A number of cases over the past decade have shown that, even when dialogue had been established, supervisors and external auditors were not incentivised to contribute to each other's tasks. A recent survey conducted by the Bank of England shows that although 70% of supervisors have access to audit information, either directly or through the bank being supervised, only 50% review this information as part of their regular inspection of banks.[93] On top of that, only a few supervisors request a Long Form Audit Report (LFAR) along with an annex to the financial statements. That said, empirical evidence brings to the fore the question of whether the work performed by external auditors should be relied upon. Indeed, recurring deficiencies have been detected in the external audit of SIFIs relating to judgemental elements of balance sheet items or processes.

[88] Bank of England, *Engagement between external auditors and supervisors and commencing the PRA's disciplinary powers over external auditors and actuaries*, Consultation Paper | CP8/15; EBA, *Consultation on Draft Guidelines on communication between competent authorities supervising credit institutions and statutory auditors*, October 2015.

[89] See FREREJACQUE AND LINCOLN, *Financial supervisors & external auditors: partnering for financial stability*, September 2015, Centre for Financial Reporting Reform (CFRR), Austrian National Bank, 28 September 2015, Vienna – also for a detailed picture of the national provisions at stake.

[90] PECCHIOLI, "Prudential supervision in banking", *OECD Working Paper*, 1987.

[91] The most recent definition of public-interest entities (PIEs) in the European Union is included in Article 2(13) of Directive 2014/56/EU and is as follows: "'Public-interest entities' means:

(a) Entities governed by the law of a Member State whose **transferable securities are admitted to trading on a regulated market** of any Member State within the meaning of point 14 of Article 4(1) of Directive 2004/39/EC;

(b) **Credit institutions** as defined in point 1 of Article 43(1) of Directive 2013/36/EU of the European Parliament and of the Council, other than those referred to in Article 2 of that Directive;

(c) **Insurance undertakings** within the meaning of Article 2(1) of Directive 91/674/EEC; or

(d) **Designated by Member States** as public-interest entities, for instance undertakings that are of significant public relevance because of the nature of their business, their size or the number of their employees."

[92] Bank of England, *Engagement between external auditors and supervisors and commencing the PRA's disciplinary powers over external auditors and actuaries*, Consultation Paper | CP8/15; Report of the Parliamentary Commission on Banking Standards, *Changing banking for good*, vol II (www.parliament.uk/documents/banking-commission/Banking-final-report-vol-ii.pdf), where paragraph 1,053 states that: "The Commission recommends that the Court of the Bank of England commission a periodic report on the quality of dialogue between auditors and supervisors."

[93] FREREJACQUE AND LINCOLN, *Financial supervisors & external auditors: partnering for financial stability*, Centre for Financial Reporting Reform (CFRR), Austrian National Bank, 28 September 2015, Vienna.

The cross-cutting issues involving supervisors and external auditors lend this area a high mark of interest from a practical standpoint. In that respect, several initiatives have been undertaken to improve the interaction between supervisors and external auditors.

In particular, the BCBS explored the interaction between supervisors and external auditors. It found a positive correlation between an enhanced relationship, on the one hand, and an improved audit quality of banks' financial statements and effective banking supervision, on the other.[94] Similar conclusions and recommendations were formulated by other standard setters, regulators and supervisory agencies, such as the EBA,[95] the Bank of England and the World Bank.[96]

The external auditor could indeed be a valuable ally for the supervisory authority, particularly in areas where skills and resources are scarce.[97] The recent GFC underscored the importance of closer cooperation between external auditors and banking supervisors – who possess distinct skills and knowledge – in improving the oversight of banks' activities and overcoming weaknesses in the risk management, valuation, control and governance processes of banks as well as in their statutory audit and financial supervision.[98]

The PRA put forward strong arguments supporting the valuable ancillary benefits of auditor‑supervisor dialogue, and, particularly, the discussions that take place around accounting and auditing issues. Such discussions help improve the quality of external audits, especially in situations where auditors are notified of key areas of regulatory interest in advance. Dialogue ahead of an audit engagement provides the auditor with a better understanding of how regulators use financial statements in their decision-making process. This focus on issues of regulatory interest may also allow the auditors to challenge firm management at a greater level of granularity than would otherwise be the case, to the benefit of the overall risk management system.

Supervisors and external auditors are important contributors to an effective control system and are endowed with the power to challenge the system itself. Better communication and closer interaction between internal auditors, supervisors and external auditors can result in a control system capable of capturing deficiencies and weaknesses in the first and second line, by means of information that would not be available otherwise. Besides, such an interaction has the potential to foster the creation of an environment that supports the independence, objectivity and integrity of internal and external audit work. In that respect, the reliability of external auditors' performance and output could be enhanced by the supervisor ensuring that the process for external auditor appointment was fair, objective, transparent and independent of the bank's management, and well documented.

In the roadmap to the adoption of the innovative four-lines-of-defence model, communication between the three parties to the triangular relationship is an important issue to focus on. Specifically, the scope of information, the form of communication and the timing/frequency of communication are important elements in reinforcing the overall consistency of controls. By

[94] Basel Committee on Banking Supervision, *External audits of banks*, March 2014.
[95] EBA, *Consultation on Draft Guidelines on communication between competent authorities supervising credit institutions and statutory auditors*, October 2015.
[96] World Bank: Centre for Financial Reporting Reform (CFRR), *Financial supervisors and external auditors: building a constructive relationship*, forthcoming.
[97] International Monetary Fund, "Towards a framework for financial stability", *World Economic and Financial Surveys*, Washington, 1998, p 36.
[98] EWALD NOWOTNY, Governor of the Austrian National Bank, speech at the conference *Supervisors and Auditors: Building a Constructive Relationship*, Vienna, 28 September 2015; Basel Committee on Banking Supervision, *Letter to the International Auditing and Assurance Standards Board (IAASB)*, April 2013.

establishing and implementing a four-lines-of-defence model, the following features of the relationship should be mandated and effectively implemented:

a) Regularity of information provided:

- definition of the terms and scope of the interaction; and
- exchange of information before and during the audit engagement, allowing flexibility (eg ad hoc meetings whenever necessary).

b) Quality of interactions:

- ex post feedback on quality of interactions and information-sharing; and
- regular assessment of independence and objectivity[99] of each party involved (eg the conditions of an external auditor's appointment).

c) Clear definition of authority and scope:

- Supervisors should have the power to request access to any type of information retained by external/internal audit;
- all three parties should jointly set the audit scope of the subject matter to be reviewed (eg joint discussion of financial statements); and
- all three parties should share their audit methodology and discuss critical action plans.

This model should not be implemented on a "one size fits all" approach[100] but rather on a case by case basis that would depend on the size and scale of operations and the range of activities pursued.

6. Conclusion

Following the line of argumentation set out above, we conclude that regulated financial institutions require a sound four-lines-of-defence model with an emphasis on the relationship between internal audit (third line of defence) and external audit and supervisors (both comprising the fourth line of defence). Despite their external status, the entities forming the fourth line of defence should be active in supervising and monitoring control issues in the organisation. This means that close interaction between the internal audit function, external audit and supervisors is crucially important. We highlighted the advantages and risks that arise from an increased collaboration between these three functions. Further research is required to develop possible solutions to the problems we identified.

Furthermore, it will be worth observing the changes made henceforth in the supervisory and audit practices applying to the financial sector in order to identify and address key issues in institutions at an earlier stage and be closer to the operations of the organisation without compromising the independence of the third- and fourth-lines-of-defence functions.

[99] See Basel Committee on Banking Supervision, *The internal audit function in banks*, April 2012, Principle 12.

[100] In the European banking system, proportionality is a key principle of the application of the so-called Single Rule Book (the harmonised set of rules under which the Banking Union operates). Both the European Commission and the European Parliament have emphasised that the diversity of the EU banking system should be acknowledged. See EBA, *Proportionality workshop: the application of the principle of proportionality in the context of institutional and regulatory reforms*, July 2015.