Mechanisms to identify synergies between compliance and operational risk functions

W Mazula
25866982

Mini-dissertation submitted in partial fulfillment of the requirements for the degree Magister Commercii in Banking and Financial Risk Management at the Vaal Triangle Campus of the North-West University

Supervisor: Prof H Zaaiman
Technical advisor: Mr H Cockeran

22 APRIL 2016
PREFACE

This mini-dissertation is the final deliverable in the Centre for Applied Risk Management (UARM)’s taught master’s degree programme. The mini-dissertation was written in article format and consists of three sections: Research project overview, Article and Reflection.

This mini-dissertation is the student’s work. The student was responsible for the final concept, set-up, execution of the research project and writing of the mini-dissertation. The members of the supervisory team contributed in an advisory and technical support capacity to study conception and design, analysis and interpretation of data and critical revision of the manuscript by the student. The mini-dissertation was language edited before submission.

The main study supervisor gave the student permission to submit this mini-dissertation for examination.
ABSTRACT

Academic literature is limited on how to coordinate the compliance and operational risk functions in organisations. The functional overlap between these two functions in financial institutions, such as banks, may result in oversight gaps or unintentional duplication. This paper describes a study on the overlap between these two functions in the second line of risk and control defence. A number of documents were analysed including relevant Basel Committee documents; South African banking legislation and regulations; integrated annual results, risk and capital reports of the four largest South African (the Big Four) banks; as well as internal operational risk and compliance documents of one of the Big Four banks. Based on this study, regulatory and practice based guidelines are proposed, which may be used to improve the efficiency of the compliance and operational risk functions in banks.

Key words: Operational risk, Operational risk function, Compliance risk, Compliance, Compliance function,
ACKNOWLEDGEMENTS

I would like to thank my family, friends, colleagues, fellow students, supervisor and technical supervisor. I need to specifically thank my wife, Vela, my girls Simthandile, Amahle and Zintle. Without their understanding, support and encouragement this research would not have been possible.
# TABLE OF CONTENTS

PREFACE ........................................................................................................................................ II

ABSTRACT ....................................................................................................................................... III

RESEARCH PROJECT OVERVIEW ................................................................................................. 7

ARTICLE........................................................................................................................................... 8

1 Abstract......................................................................................................................................... 8

2 Introduction .................................................................................................................................. 8

3 Background ................................................................................................................................... 10

4 Method.......................................................................................................................................... 15

5 Results and Discussion .................................................................................................................. 17

6 Conclusion .................................................................................................................................... 26

7 References .................................................................................................................................... 27

REFLECTION .................................................................................................................................. 29

APPENDICES .................................................................................................................................. 31
LIST OF TABLES

1. Table 1: Summary of operational risk and compliance risk components
2. Table 2: Big Four banks’ operational risk sub-component types
3. Table 3: Big Four banks’ definitions of compliance risk in their 2014/2015 annual reports
4. Table 4: Different governance and oversight compliance risk reporting structures of the Big Four banks
5. Table 5: Compliance and operational risk measurement tools

LIST OF FIGURES

1. Figure 1: Interaction between compliance and operational risk management functions including measurement tools recommended by the BCBS
2. Figure 2: Three lines of defence communication and information flow
RESEARCH PROJECT OVERVIEW

The Bank Supervision Department of the South African Reserve Bank (SARB) grants licences to banks to take deposits from the general public. Banks could run into financial difficulties and be unable to repay depositors. Banks are supervised by SARB to protect the public at large. SARB established laws and regulations which require that ongoing management of a bank’s risk should include management of compliance risk and operational risk.

The board of directors of a bank is responsible for ensuring the success of policies and procedures to manage compliance and operational risk, while the senior management team is responsible for the management of compliance and operational risk. This is not a simple task and banks have to address the question of how to ensure coordination between the operational risk function and the compliance function within banks on compliance matters.

As a result of a change in role from an operational risk officer to a compliance officer in a banking environment, it became clear to me that close a relationship exist between compliance risk and certain aspects of operational risk. This study looks at the close relationship between compliance risk and operational risk, and provides regulatory and practice based guidelines which may be used to improve the efficiency of the compliance function and operational risk function in banks.

I selected the South African Journal of Business Management for my article. This journal was selected because it accepts business-related articles that combine theory, practice and application. This article describes the findings of an exploratory qualitative study into a real problem in the researcher’s working environment. The study was based on banking laws, regulations, academic journals, and practical experience, and provides guideline-based recommendations to enable optimum coordination between compliance and operational risk functions.
ARTICLE

1 Abstract

Academic literature is limited on how to coordinate the compliance and operational risk functions in organisations. The functional overlap between these two functions in financial institutions, such as banks, may result in oversight gaps or unintentional duplications. This paper describes a study on the overlap between these two functions in the second line of risk and control defence. A number of documents were analysed including relevant Basel Committee documents; South African banking legislation and regulations; integrated annual results, risk and capital reports of the four largest South African (the Big Four) banks; as well as internal operational risk and compliance documents of one of the Big Four banks. Based on this study, regulatory and practice based guidelines are proposed, which may be used to improve the efficiency of the compliance and operational risk functions in banks.

2 Introduction

In banks, the operational risk and compliance functions should play an important role in ensuring that regulatory fines and penalties are avoided. The roles and responsibilities of both functions often overlap, leading to unintentional duplications and possible gaps in the risk and internal control assessment process. According to Zoet et al. (2009) one of the results of the relationship between internal controls and risk management activities is based on two types of risks, namely, operational risk and compliance risk. In this study the question of how to coordinate the operational risk and compliance functions to achieve optimal coordination within the South African banking sector was investigated. Optimal coordination should assist banks to meet their business objectives.

Laws, regulations and supervisory requirements impose obligations on banks to manage compliance and operational risks. For example, the Basel Committee of Banking Supervision (BCBS) requires each bank to organise its compliance functions and compliance risk management in a way that is consistent with its own risk management strategy and structures. This could allow for the compliance function to reside within the operational risk function, as there is a close relationship between compliance risk and certain aspects of operational risk. Separate compliance and operational risk functions, with suitable mechanisms to ensure close cooperation between the two functions on compliance matters, are also allowed under the BCBS paper (BCBS, 2005). Similarly the South African Reserve Bank (SARB) regulations require that ongoing management of a bank’s risks should include management of compliance risk and operational risk (SARB, 2012). The board of directors of a bank is responsible for
ensuring the success of policies and procedures to manage compliance and operational risk, while the senior management team is responsible for the management of compliance and operational risk. This is not a simple task and banks have to address the question of how to ensure coordination on compliance matters between the operational risk function and the compliance function within banks.

Banks should operationalise compliance requirements as required by the regulations. To satisfy this requirement, banks must institute policies and implement procedures, processes and systems. Employees must be trained to ensure compliance with compliance related laws, regulations and supervisory requirements. Such compliance implies that the processes work well enough to meet regulatory requirements and, as far as possible, avoid the event of a compliance failure. Should the processes be ineffective, operational failures may occur, leading to an operational risk event as a result of failure due to people, processes, systems or external events. Such operational failures could result in fines and penalties imposed because of failure to comply with laws and regulations. The failure of operational controls that have been implemented to manage compliance risk can therefore cause compliance failure leading to operational risk events.

This study focuses on optimal coordination between the compliance and operational risk functions in the second line of defence in banks. The main role of the operational risk and compliance functions in the second line of defence includes designing the operational and compliance risk management tools used by first line of defence to identify and manage risks; applying independent challenges to the use and output of the risk management tools by the first line of defence; developing and maintaining policies, standards and guidelines; and lastly, reviewing and contributing to the monitoring and reporting of risk profiles (BCBS, 2014). This means that both compliance and operational risk functions are expected to perform risk and control assessments in the same bank.

In practice, this situation leads to potential and actual overlap between tasks executed by the two functions. As envisaged by the BCBS, these two functions should cooperate to ensure that duplication of effort is minimised and also to ensure that risks do not fall through the cracks due to a lack of coordination between the two functions. This means that the second line of defence functions should establish an operational framework that allows both functions to optimally assist the first line of defence to make the relevant decisions when it comes to risk identification, management and ownership and, ultimately, achieving the business objectives.

Based on the above, the research question is framed as follows: How could banks assign specific risk and controls tasks to the second line of defence to achieve optimal coordination
between the compliance and operational risk functions? The objective of this study was to propose regulatory and practice based guidelines based on a qualitative, exploratory study into a real problem in the researcher's working environment.

3  Background

Figure 1 shows the typical interaction between the compliance and operational risk functions and the measurement tools used to provide a compliance risk and operational risk profile. The tools are recommended by the BCBS and are typically applied by banks. Problems arise when the risk and control assessment processes are unintentionally duplicated or overlap due to inadequate coordination between the second line risk and control functions.

**Figure 1: Interaction between compliance and operational risk management functions including measurement tools recommended by the BCBS**

Risk and compliance related banking legislation

The Bank Supervision Department (BSD) of the SARB is responsible for regulating banks in South Africa. The legal framework for regulating and supervising the banking sector in South Africa involves three tiers, namely: tier 1, the Banks Act, 1990 (Act No. 94 of 1990); tier 2, the regulations relating to banks; and tier 3, the Banks Act directives, circulars and guidance
notes. South African banking legislation is informed by the South African Reserve Bank Act (Act No. 90 of 1989), the Financial Intelligence Centre Act (Act No. 38 of 2001), and the Companies Act (Act No. 71 of 2008). These acts require and underscore the need for optimal coordination between the operational risk and compliance functions within banks.

For example, the Financial Intelligence Centre Act No. 38 of 2001 (FIC Act) mandates the BSD to supervise and enforce banks’ compliance with the FIC Act. This mandate is expected to ensure that the necessary anti-money laundering and financing terrorism controls are in place within banks. For example, in 2014, the BSD imposed administrative penalties to the four largest banks in South Africa (the Big Four) to the value of R125 million for non-compliance with the FIC Act (SARB, 2015). This example illustrates one of the reasons why banks should address the tasks and activities related to risks and control processes assigned and coordinated between the compliance and operational risk functions. Another reason is to allow the board of directors and senior management to understand critical differences in the roles and responsibilities of the compliance and operational risk functions and how they should be optimally assigned for the bank to achieve its objectives (Anderson and Eubanks, 2015).

The three lines of risk and control defence

The three lines of defence model included in the Committee of Sponsoring Organizations of the Treadway Commission (COSO) internal control framework is a well-known risk and control governance structure. This model addresses how specific duties related to risk and control can be assigned and coordinated within an organisation. Activities linked to the first line of defence are execution, management, ownership of risks and design of controls to respond to risks. The independent operational risk management and compliance functions monitor, assess and report on the risks and controls in the first line of defence, while internal and external audit play the role of independent assurance providers in the third line of defence.

Both the operational risk function and the compliance function place responsibility on the first line of defence to establish and manage controls to mitigate operational risk and compliance risk. The elements of such controls are typically categorised as people, processes and systems. Figure 2 illustrates the three lines of defence model and the intricate flow of risk and control assessment information between the three lines. This study focused on the interaction between the first and second lines of defence and did not extend to the potential coordination between the third line of defence and the second line of defence, or between the third line of defence and the first line of defence.
The first line of defence designs and executes business processes in order to realise the business objectives or goals. According to Haynes (2005) many institutions are exposed to risks associated with the integration of business and operational processes, including compliance risk, resulting in parallel compliance processes and systems in the organisation. This results in duplication as well as compliance requirements not being operationalised as required by the regulations. Zoet et al. (2009) designed a framework for integrating operational risk and compliance risk into their appropriate stage of application in a business process development life-cycle by linking five categories of risk management and compliance (task sequencing, actor inclusion/interaction, effect sequencing, data/information registration and detection control). Operational risk function is involved with new products by ensuring that controls in the form of people, process and systems are considered. The involvement of the compliance function within the new product approval process may be valuable in preventing non-compliance with regulations, which would economically damage a company with fines and penalties (Tanzi et al., 2013).

Operational risk, compliance risk and compliance

Two papers provide international best practice standards for a definition of operational risk, compliance risk and compliance. The first is the International Convergence of Capital Measurement and Capital Standards: A Revised Framework (BCBS, 2004), commonly referred to as the 'Basel Accord', which specifies risk-sensitive capital requirements in respect of operational risk. Another BCBS paper “Compliance and compliance function within banks”
For this study, operational risk is defined according to the BCBS definition: “failed internal processes, people and systems or from external events, including exposure to fines, penalties, or punitive damages resulting from supervisory actions, as well as private settlements” (BCBS, 2004). The BCBS definition of operational risk specifies seven event type classifications, namely: internal fraud; external fraud; damage to physical assets; employment practice and work safety; clients, products and business practices; business disruption and system failures; and, lastly, execution delivery and process management.

Compliance risk is defined as “the risk of legal or regulatory sanctions, financial loss, or loss to reputation a bank may suffer as a result of its failure to comply with all applicable laws, regulations, code of conduct, and standards of good practice” (BCBS, 2005). Compliance risk refers to events that exclude ‘pure’ operational risk events, such as external fraud, damage to physical assets and other external events, and immaterial or day-to-day operations losses (Birindelli and Ferretti, 2013). Table 1 summarises the main components of the operational and compliance risk definitions in the two BCBS documents.

Compliance refers to laws, rules and standards and covers issues such as market conduct and treating customers fairly, and includes areas such as anti-money laundering and combatting terrorist financing (BCBS, 2005). For example, when a bank deliberately treats customers unfairly it exposes itself to compliance risk.
Table 1: Summary of operational risk and compliance risk components

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>What causes the risk to</td>
<td>Failed internal processes, people and systems or from external events</td>
<td>Failure to comply with laws, regulations, rules, related self-regulatory</td>
</tr>
<tr>
<td>materialise</td>
<td></td>
<td>organisation standards, and codes of conduct applicable to its banking</td>
</tr>
<tr>
<td></td>
<td></td>
<td>activities.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Material financial loss, or loss to reputation.</td>
</tr>
<tr>
<td>What is the impact of the</td>
<td>Loss including exposure to fines, penalties, or punitive damages resulting from supervisory</td>
<td>The risk of legal or regulatory sanctions and reputational risks.</td>
</tr>
<tr>
<td>impact of the risk</td>
<td>actions, as well as private settlements</td>
<td></td>
</tr>
<tr>
<td>Which other risks are</td>
<td>Legal risk</td>
<td></td>
</tr>
<tr>
<td>included?</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Which other risks are</td>
<td>Strategic and reputational risk</td>
<td></td>
</tr>
<tr>
<td>excluded?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Implementation of compliance and operational risk management in banks

The Basel Accord states that banks should have clear roles and responsibilities for an operational risk management function in the second line of defence. These roles and responsibilities include the following actions:

- Develop strategies to identify, assess, monitor and control/mitigate operational risk;
- Track relevant operational risk data and material losses;
- Report operational risk exposures including material operational risk losses at business unit management, senior management and board levels; and
- Establish a well-documented operational risk management system which will ensure compliance with internal policies, controls and procedures including policies for treatment of non-compliance issues. (BCBS, 2004)

The key responsibilities of the compliance function are:

- Advising senior management on compliance laws, rules and standards;
- Providing guidance and educating staff;
- Identifying, measuring and assessing compliance risk;
• Developing new products and new business practices;
• Monitoring and testing compliance;
• Reporting on a regular basis to senior management on compliance matters; and
• Establishing a compliance programme. (BCBS, 2008)

The overlaps in common risks event types, roles and responsibilities between the compliance function and operational risk function require mechanisms for cooperation and effective collaboration (Birindelli and Ferretti, 2008). Solutions to avoid overlaps have been proposed by other authors:

- Birindelli and Ferretti (2008) suggested that the operational risk management system should be used to collect the loss data and to carry out risk self-assessment. A second potential area for collaboration is where the operational risk function supports the compliance function in the mapping of processes and in the reporting of data and risk exposure.
- Scandizzo (2010) recommended that the compliance function should employ the experience of the operational risk function when setting control procedures. Scandizzo also stated that both functions will benefit if there is only one repository for documented risk and controls.
- A synergies model proposed by Birindelli and Ferretti (2013) was based on the areas of responsibility between compliance and operational risk functions, involving the systems for risk identification and measurements that require structured information flows between the two functions.

4 Method

This was an exploratory qualitative study based on information available in documents including relevant Basel Committee documents; South African banking legislation and regulations; integrated annual results, risk and capital reports of the Big Four; as well as operational risk and compliance internal documents of one of the Big Four banks. The intention was to establish regulatory and practice guidelines for specific risk and control tasks in the second line of defence to achieve optimal coordination between the compliance and operational risk functions. The methods used for analysing the four types of documents are now discussed.
Basel Committee

The BCBS issues international best practice guidelines, standards and frameworks, with the understanding that local regulators will adopt the most relevant frameworks such as the Basel III framework. A review of the relevant Basel documents was performed to establish the guidelines or mechanisms proposed to ensure optimum coordination between compliance function and operational risk functions. The Basel documents also provided information on the expected roles and responsibilities for the operational risk function and the compliance risk function in banks.

South African banking legislation and regulations

The objectives of analysing the South African Banks Act and the regulations relating to banks were to:

- Establish the recommended governance and oversight structures for compliance and operational risk functions; and
- Identify gaps between international best practice standards set by Basel Committee and South African legislation and regulations with respect to compliance and operational risk.

2014 integrated annual reports and risk and capital reports of the Big Four banks

The aim of the review of the 2014 integrated annual reports, as well as the risk and capital annual reports, of the Big Four banks was to do a comparative analysis of qualitative publicly available information on compliance and operational risk functions. This analysis looked at the consistency and overlaps of governance and oversight structures, and definitions of compliance and operational risk.

Internal documents

Internal documents relating to the operational risk and compliance functions of one of the Big Four banks were studied to identify areas of duplication, overlaps and reporting structures between the two functions. In studying the documents, the Basel Committee risk measurement tools used for risk identification and control assessment and the tasks and responsibilities of the compliance and operational risk functions in banks were considered as the benchmark for identifying the practical guidelines.
5 Results and Discussion

The findings from the four types of documents are now discussed and combined into proposed guidelines for coordinating the compliance and operational risk functions in the second line of defence in a bank.

Basel Committee

The Basel Committee documents described mechanisms of coordination which could be established between the compliance and operational risk functions. These are as follows.

a) Communication and sharing of information within the second line of defence

The operational risk function and the compliance function in the second line of defence should share external market information about events and conditions that are relevant for decision making by the first line of defence. This information should be reliable, timely and accessible (BCBS, 1998). Typical challenges experienced by this study's researcher in practice are:

- International external market information or events shared by the second line of defence are not adapted to the specific business environment of the first line of defence. This results in the information not necessarily assisting the first line of defence to make informed decisions.
- The compliance function and operational risk function at times report the same compliance related external events to the first line of defence due to lack of communication between the two functions.

b) Clear roles, responsibilities and reporting between the compliance and operational risk functions

The international banks that participated in the Basel Committee 2008 Implementation of Compliance Principles survey indicated that the seven different compliance tasks cited in the Background section can also be performed by staff from other non-compliance departments in addition to the compliance function (BCBS, 2008). This may result in duplication of tasks when there is inadequate coordination of responsibilities.
c) Governance structures as the third mechanism of coordination

The Basel Committee review of principles of sound management of operational risk survey indicated the involvement of several control groups in the second line of defence’s review of risk and control assessments (BCBS, 2014). Inadequate coordination within the second line of defence could lead to duplications when performing risk and control assessments. The same Basel Committee paper mentioned that a number of banks reported that their second line of defence responsibilities were not yet fully implemented, or were inadequately structured and coordinated (BCBS, 2014).

South African banking legislation and regulations

The results of the researcher’s review of the South African legislation for supervising banks in comparison to international best practice are now discussed.

a) Governance and oversight of compliance and operational risk functions.

The 2014 Ernst and Young (EY) international risk management culture survey indicated that banks are streamlining and integrating current management committees to break down silos, close risk oversight and control gaps, and clarify roles and responsibilities to strengthen their three lines of defence (EY, 2014). Accordingly, the SARB recommends that board and senior management teams must have oversight over operational risk, and the risk and capital management board sub-committees must have oversight on reported operational risk. The audit, director’s affairs, and risk and capital management board of director’s sub-committees should have oversight on compliance risk reported by the compliance function (SARB, 2012). Compliance and operational risk is reported to the risk and capital management board sub-committee, which should have an integrated view of compliance and operational risks.

b) Roles and responsibilities

The compliance and operational risk functions have clear roles and responsibilities according to the regulations relating to banks. The Banks Act indicates that compliance risk should be managed as part of the risk management framework (SARB, 2012). This raises the question as to whether compliance risk should be managed like other risks in the bank as part of the risk management process where, for example, credit risk and market risk report to the head of risk. The EY 2014 international risk management culture survey report indicated that the role of the risk function continues to expand, with some banks now ensuring that the risk function is involved with compliance risks (EY, 2014).
It is therefore imperative that the risk and compliance functions cooperate when the risk function is involved in compliance risk.

c) Definitions

The South African regulations relating to banks do not provide a definition of compliance risk, but they define regulatory and supervisory risk. This may result in a non-standard way of identifying and managing compliance risk within the Big Four banks.

2014 integrated annual reports and risk and capital reports of the Big Four banks

The integrated annual risk and capital reports of the Big Four banks were studied, with the aim of comparing public information relevant to compliance and operational risk functions.

In general, the operational risk definition for the Big Four banks is aligned to the international best practices issued by the Basel Committee and South African regulations. The operational risk events recommended by the Basel Committee are included as sub-types of operational risk in the definitions, but the Big Four banks also include additional sub-types of operational risk as per Table 2 (see p.22). Three of the Big Four banks include compliance risk as a subset of operational risk. Therefore, compliance risk is seen as part of operational risk in these banks, and mechanisms that allow coordination between the compliance and operational risk functions should be considered.

The definitions of compliance risk differ among the Big Four banks. Standard Bank and Nedbank define compliance risk according the Basel Committee definition. Barclays Africa does not define compliance risk and FirstRand Bank defines regulatory risk instead of compliance risk according to South African regulations relating to banks. As shown in Table 3, these difference in definition could be due to compliance risk not being explicitly defined by the Banks Act and the regulations relating to banks in South Africa.
Table 3: Big Four banks’ definitions of compliance risk in their 2014/2015 annual reports

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliance risk is the risk of legal or regulatory sanction, financial loss or damage to reputation that the group may suffer as a result of its failure to comply with laws, regulations, and codes of conduct and standards of good practice applicable to its financial services activities.</td>
<td>Compliance risk is not defined.</td>
<td>Regulatory risk is the risk of statutory or regulatory sanction and material financial loss or reputational damage as a result of failure to comply with any applicable laws, regulations or supervisory requirements.</td>
<td>The risk of legal or regulatory sanctions, material financial loss, or loss to reputation the group may suffer as a result of its failure to comply with laws, regulations, rules, related self-regulatory organisation standards, and codes of conduct applicable to its banking and other activities.</td>
</tr>
</tbody>
</table>

In the publically available reports, governance and oversight processes for reporting operational risk were similar to those recommended by regulations relating to banks as described in South African legislation and regulation. However, the governance structures for reporting compliance risk varied between the Big Four banks as demonstrated in Table 4.
Table 4: Different governance and oversight compliance risk reporting structures of the Big Four banks

<table>
<thead>
<tr>
<th>Compliance function governance structure</th>
<th>Standard Bank</th>
<th>Barclays Africa</th>
<th>FirstRand Bank</th>
<th>Nedbank</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliance committee</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audit committee</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Risk capital and management committee</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Reputational and conduct risk committee</td>
<td></td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Social and ethics committee</td>
<td></td>
<td></td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Regulatory risk management committee</td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Directors affairs committee</td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
</tbody>
</table>
Table 2: Big Four banks’ operational risk sub-component types

<table>
<thead>
<tr>
<th>Aspects of Operational risk</th>
<th>Standard Bank</th>
<th>Barclays Africa</th>
<th>FirstRand Bank</th>
<th>Nedbank</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>What causes this risk to materialise?</strong></td>
<td>Inadequacy of, or a failure in, internal processes, people and/or systems or from external events.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>What is impact of this risk?</strong></td>
<td>Loss</td>
<td>Direct or indirect loss</td>
<td>Loss</td>
<td>losses</td>
</tr>
<tr>
<td><strong>Which other risk is included in operational risk?</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Legal risk</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Compliance risk</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Technology risk</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Internal and External fraud - Financial crime risk</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Tax risk</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>HR/people risk</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Model risk</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transaction/Process risk</td>
<td></td>
<td>Yes</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Accounting/Financial reporting risk</td>
<td></td>
<td>Yes</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Information risk</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>External supplier risk</td>
<td></td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Payment process risk</td>
<td></td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Project risk</td>
<td></td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Environmental and social risk</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business continuity</td>
<td></td>
<td></td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Premises and security risk</td>
<td></td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cyber risk</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical commodities</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Which other risks are specifically excluded in operational risk?</strong></td>
<td>Regulatory risk, Financial Crime and Product Design Risk</td>
<td>Strategic, business and reputational risks</td>
<td>Strategic and reputational risks</td>
<td></td>
</tr>
</tbody>
</table>

Page 22 of 31
Internal documents

Compliance and operational risk-related internal documents of one of the Big Four banks' were reviewed. The aim of the review was to establish whether the bank's compliance and operational risk and control measurement tools are aligned to international best practice standards issued by the Basel Committee and legislation.

In this bank, operational risk and compliance functions use the measurement tools recommended by the Basel Committee to assist the first line of defence to identify, manage and accept ownership of compliance and operational risks shown in Table 5.

Table 5: Compliance and operational risk measurement tools

<table>
<thead>
<tr>
<th>Basel Committee tools</th>
<th>Operational Risk Function</th>
<th>Compliance Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit findings</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Internal Loss Data Collection and Analysis (ILD)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>External Loss Data Collection and Analysis (ELD)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Risk Assessment – Risk controls self-assessment (RCSA)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business Process Mapping</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Risk and Performance indicators – Key Risk Indicators (KRI) and Key Performance Indicators (KPA)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Scenario analysis</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Measurement</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Comparative analysis – Comparing results of various assessment tools</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Compliance risk management plan (CRMP)</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Breaches log</td>
<td></td>
<td>Yes</td>
</tr>
</tbody>
</table>
Proposed operational and compliance risk regulatory and practice based guidelines

Guidelines to establish optimal cooperation on compliance risk between the compliance and operational risk functions are now proposed. These guidelines are based on the mechanisms, models and frameworks discussed in the background study; the Basel Committee risk and control measurement tools; the intricate flow of risk and control among the three lines of defence; and findings from the documents analysed as part of this study. The guidelines are further based on the standards recommended by Tarantino (2008).

The guidelines could be used to ensure that the compliance function and operational risk function collaborate to assist the first line of business to make informed decision and achieve the business objectives. Accordingly, the guidelines are discussed, clearly demonstrating first line of defence and second line of defence roles and responsibilities.

First line of defence

a) Business managers in the first line of defence agree to take responsibility for identifying, managing, executing and owning the compliance and operational risks in their business areas.

b) The first line of defence managers should map business processes to the audited regulations, identify compliance risks, and design controls to mitigate these risks. The aim of this process is to avoid redundant compliance risk management activities. It is therefore critical to create a matrix that captures:
   o Relationship among business processes;
   o Risk associated with the processes;
   o Internal controls deployed to mitigate the risks;
   o Assessments used to validate the effectiveness of the controls; and
   o Regulations to which the internal controls apply.

Second line of defence

a) The second line of defence must standardise, rationalise and prioritise the operational and compliance risk scoring system. An agreement on a risk scoring system between the three lines of defence is required for the system to be successful. The expectation is that agreement on the risk scoring system will allow risk and controls with the highest scores to be the first candidates for process and technology improvements by the first line of business.
b) The second line of defence must advocate for increased standardisation and automation of controls designed by the first line of defence to mitigate compliance and operational risks. Automated controls enhance the probability of mitigating risks as there is no manual intervention. Automated controls should also allow for greater effectiveness and efficiency of governance of the compliance and operational risk management processes.

c) The second line of defence should create an internal compliance and operational risk controls grading system in order to advise first line management to improve internal controls. This compliance and operational risk controls system should be regarded as competitive advantage and not simply as a cost of doing business.

Coordination between operational risk and compliance functions

a) Establish or use an existing forum to play the role of a combined assurance committee, which will have oversight for all significant operational risk and compliance requirements or plans. This combined assurance committee must:

- Analyse reports highlighting significant operational and compliance risks exposures and trends;
- Consider the appropriateness of risk mitigation strategies devised to minimise risk exposure;
- Facilitate the coordination of mitigation initiatives;
- Evaluate compliance and operational risk reports and recommend improvements to them;
- Provide oversight of the risk and compliance functions in measuring, monitoring and managing risk;
- Review, monitor and approve risk and compliance initiatives and projects;
- Monitor potentially catastrophic losses; anticipate risk and compliance issues;
- Monitor the respective overall exposure to risk by creating comparable compliance risk and operational risk profiles;
- Consider unsatisfactory reports from audit on compliance and operational risk; and
- Provide oversight of the aggregated risk model.

b) The combined assurance committee needs to provide a channel of communication between the different stakeholders, e.g. sharing the results of the information depicted in Figure 1. For example, in order to avoid duplications, the operational risk function would share the results of the risk control self-assessment, and the compliance function would share the results of the compliance risk management plan before the functions perform the control assessment.
6 Conclusion

The purpose of this study was to propose regulatory and practice guidelines to promote optimal coordination between the operational risk and compliance functions within the second lines of defence. The researcher could not find an international best practice framework, standard or policy that provides a clear explanation on how to ensure coordination between the two functions.

The Basel Committee promotes communication and sharing of information within the second line of defence to identify overlaps and unintentional duplications within this line of defence. Furthermore, Basel Committee promotes processes to improve efficiency within the second line of defence, and to ensure collaboration between the operational risk function and the compliance function.

Even though the recommendations were developed within the South African banking context, these guidelines should also be of value for banks in countries that comply with the international best practice set by Basel Committee to promote coordination within the second line of defence. A logical extension of this study would be to extend the research to cover the interaction between all lines of defence and to develop mechanisms to ensure that the recommendations achieve the desired outcome to minimise the penalties and fines imposed by regulators as a result of non-compliance with laws and regulations.
7 References


Note: Journal allow 20 pages and the article is 20 pages
REFLECTION

My research focused on compliance risk and operational risk. These two risks require ongoing management by banks. This research also focused on the relationship between the compliance and operational risk management functions in banks.

Even though the Basel Committee stated that there is a close relationship between compliance risk and certain aspects of operational risk, I found that academic literature on how to coordinate the compliance and operational risk functions in organisations is limited.

The board of directors of a bank is responsible for ensuring the success of policies and procedures to manage compliance and operational risk, while the senior management team is responsible for the management of compliance and operational risk. This is not a simple task and banks have to address the question of how to ensure coordination between the operational risk function and the compliance function within banks on compliance matters.

To understand how to ensure coordination between the two functions, I had to understand the following:

- The three lines of defence model which addresses how specific duties related to risk and control can be assigned and coordinated within an organisation. This model places responsibilities on the:
  - first line of defence to identify, manage and own compliance risk and operational risk;
  - first line of defence to design controls to mitigate compliance risk and operational risk;
  - second line of defence to provide the measurement tools for identifying the compliance risk and operational risk; and
  - second line of defence to advise, monitor and assess the compliance and operational risks identified.

- The definitions of compliance risk and operational risk. If I did not research the definitions of compliance risk and operational risk, I would not have understood that compliance risk is a sub-set of operational risk and that it refers to events that exclude ‘pure’ operational risk events and day-to-day operations losses.

When doing the research on coordination, I came across the proposed solutions by Scandizzo and Birindelli and Ferretti on how to avoid overlap and duplication between the compliance and operational risk functions in terms of compliance risk.
While researching coordination of the compliance and operational risk functions, I was able to review the international best practice issued by Basel Committee. I also reviewed the South African Banks Act and Regulations to establish the governance and oversight structure for compliance risk and operational risk in South African banks. I analysed the annual reports and risk and capital reports of the four largest banks in South Africa by asset size to establish the qualitative information presented on compliance and operational risk available to the public. I used the practical situation of one of the big four banks in South Africa to identify area of duplication, overlaps and reporting structures through the review of internal compliance and operational risk documents.

I used the regulatory requirements and practice to recommend guidelines which may improve the efficiency of the compliance and operational risk function in banks. I learned through the explanatory qualitative study that doing research involves multiple disciplines.

Through this research, I established that when banks have independent compliance and operational risk functions responsible for managing compliance risk and operational risk, respectively, there should be mechanisms to promote optimal coordination and reduce unintentional duplications.

The structure of the MCom in Banking and Financial Risk Management and course work done in the year 2014 and 2015 assisted me with how to write the article. My work experience in operational risk and compliance risk also gave me background information and experience on compliance and operational risk management. Because I had this background, I felt that I had a strong foundation regarding these issues, which allowed further understanding of these subjects.

I realised how difficult it is to work full-time and study part-time. However, I came to the conclusion that I want to consider studying beyond the Masters in Banking and Financial Risk Management, because of the reward of learning, to some degree, about new ideas and about applying these ideas in the work environment. I discovered that, as I continue to learn about the coordination between compliance risk and operational risk, I want to explore the option of applying the recommendations of the guidelines in my work environment.

I have learned that it is not an easy task to coordinate the compliance and operational risk functions, if the roles and responsibilities are not clear between the first line of defence and second line of defence, as well as within the compliance function and operational risk function in the second line of defence.
APPENDICES

1. South African Journal of Business Management Instructions to Authors