UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

GORDON INSTITUTE
OF BUSINESS SCIENCE
University of Pretoria

Critical evaluation of operational risk tools used in regulatory capital calculations

Pulane Modiha

26412528

A research project submitted to the Gordon Institute of Business Science, University of Pretoria, in partial fulfillment of the requirements for the degree of:

Master of Business Administration

9 November 2011

ABSTRACT

Bank failures during recent years continue to cause stakeholders to question how board and senior management are overseeing and managing Operational Risk. This research evaluated the use of Operational Risk tools by South African banks who have adopted Advanced Measurement Approach (AMA) for management and calculation of Operational Risk capital, based on the Basel II requirements (Bank for International Settlements, 2006).

The research was conducted under the assumption that when Operational Risk tools are adopted and used as prescribed by the Basel II Framework, it will lead to enhanced risk management practices and allow banks to identify emerging risks where controls can be designed to mitigate risks from materialising.

This study was conducted using a quantitative method – the survey was sent to Operational Risk managers in the main segments of 3 South African AMA banks (ABSA, FIRSTRAND and NEDBANK), and senior managers in the group Operational Risk departments. The study found that Operational Risk tools are used and have been implemented as per Basel II requirements even though there are minor gaps. These tools have also been integrated in day-to-day processes; however there are some improvements required when it comes to a full integration and the use of the tools in the decision making processes.

KEYWORDS

- Basel II Framework
- Internal and External loss data
- Key Risk Indicators
- Risk and Control Self Assessments
- Risk Scenarios
- Internal Audit Findings

DECLARATION

I declare that this research project is my own work. It is submitted in partial fulfilment of the requirements for the degree of Master of Business Administration at the Gordon Institute of Business Science, University of Pretoria. It has not been submitted before for any degree or examination in any other University. I further declare that I have obtained the necessary authorisation and consent to carry out this research.

9 November 2011

Signed: Pulane Modiha

Date

ACKNOWLEDMENTS

In ending my MBA journey, I would like to express my sincere appreciation and gratitude to the following people who have ensured that I complete the tough but exciting and rewarding GIBS MBA.

- The Almighty God, for providing me with wisdom, health, courage and perseverance.
- My husband and my pillar of strength, Eugene Modiha. Thank you so much for your support, love, understanding and most of all for taking care of the household and baby Bonolo.
- My princes, my angel and my beautiful daughter Bonolo. Thank you for loving me regardless of the little time I spent with you.
- My family (the Modihas & Molois) and my helper (mmeAletta). Thank you for your prayers, support and understanding. I love you all.
- A special thank you to my research supervisor, Mr Solomon Moyo for your guidance, positivity and for believing in me.
- My risk experts: Vikesh Mistri, Dr Hennie van Greuning, Hans Bouckaert, Flippie Snyman, Henning Jacques and Vasie Naicker - for your insight and guidance.
- To all my friends and fellow GIBS CMD's who constantly reminded me that "I need to be strong". Thank you for being CMD's in arms and making the journey bearable.
- To my sister, life coach and dear friend, Diana Tshivhase. Thank you for walking this journey with me.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

GLOSSARY

Definition of Terms and Acronyms

- **AMA** Advanced Measurement Approach
- **BCBS** Basel Committee on Banking Supervision
- **BIS** Bank for International Settlements
- **EL** Expected Loss
- **KRI** Key Risk Indicator
- **ORM** Operational Risk Management
- **RCSA** Risk and Control Self Assessment
- **SA** South Africa
- **SARB** South African Reserve Bank
- **TSA** The Standardised Approach
- **UL** Unexpected Loss

CHAPTER 1: INTRODUCTION TO THE RESEARCH PROBLEM

1.1 INTRODUCTION

The recent European debt market and the world economy turning into a deeper recession, has resulted in an increase in banks supervision and monitoring. The continued losses incurred by businesses due to inefficient controls has emphasised once again the need for continual review of regulatory requirements which are set for the financial sector with specific focus on Operational Risk Management (ORM).

There are a number of events that have taken place in the financial sector that emphasise the need for robust Operational risk management. Some of these events are summarised in Table 1.1 below. This table shows fraudulent activities that have taken place in the financial sector since 1995 due to Operational Risk failures or inadequate Operational controls. These are but a few examples of the costly Operational Risk losses in recent years.

Table 1.1: Example of losses experiences due to Operational Risk failures

Trader Name	Year	Financial Loss	Affected Institution
Nick Leeson	1995	£827 million	Barings Bank
John Rusnak	2002	$691 million	Allied Irish Banks
Gianni Gray, David Bullen, Vince Ficarra, Luke Duffy	2003 Oct – 2004 Jan	AU$360 million	National Australia Bank
Jérôme Kerviel	2006 – 2008	€4.9 billion	Société Générale
Kweku Adoboli	2011	$2.3 billion	UBS

Some of the cases not shown in the table above include Lehman Brothers, Bears Stearns and American Insurance Group (AIG) which have gone bankrupt in the recent years due to significant losses experienced resulting from failure in Operational Risk Management (Khan, Guharay, Franklin, Fischtrom, Scanlon, & Shimpi, 2010). As such, the importance of closely monitoring Operational Risk has been emphasised since Operational Risk remains a key risk which could have major repercussion if not managed properly and has not been given appropriate attention (Dutta & Perry, 2007).

The fraud event by Nicholas Leeson which resulted in the collapse of Barings bank is a case which is mostly referred to in Operational Risk Management failures and is regarded to have been the turning point in Operational Risk Management (Power, 2005).

More recently UBS incurred a loss of $2.3 billion which stemmed from what was termed unauthorised speculative trading in various S&P 500, DAX, and EuroStoxx index futures. The true magnitude of the risk exposure was distorted because the trader allegedly falsified his positions with fictitious, forward-settling, cash ETF (exchange traded fund) positions. These fictitious trades concealed the fact that the index futures trades violated UBS's risk limits. This recent event shows that there is need to constantly manage and monitor Operational Risk and continually assess if all current controls are still relevant or if there is a need for better and more effective controls.

Operational Risk is defined as “the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk, but excludes strategic and reputational risk” (Bank for International Settlements, 2006, p. 158). The day to day running of a business involves a number of activities which can be grouped into internal business processes, people, systems and external events. All these activities are of significant importance in running a business, as such, it is critical that they are managed in a robust manner. In the event that Operational Risk is not managed effectively this will result in losses to the institution as shown above and more negative impact. The importance of managing Operational Risk has grown over the years due to significant losses that have been experienced in the financial sector because of inadequate management of this risk.

The above cases show the financial impact of not managing Operational Risk adequately, however Gillet, Hubner and Plunus (2009) indicated that severe Operational Risk losses do not only have a financial impact but also affect market performance of the organisations negatively. Financial institutions (companies listed in major European and US stock exchange) from 154 Operational Risk events published between 1990 and 2004 were studied and showed that the announcement of major Operational Risk losses has immediate reputational impact on these listed companies and leads to a decline in their market price.

The above failures resulted in a more firm and formalisation of the implementation and assessment of Operational Risk Management by regulators. The Operational Risk capital charge was not included in the original Basel Accord and Operational Risk is considered immature when compared to the credit risk and market risk (Helbok & Wagner, 2006). This formalised and increased focus on Operational Risk Management resulted in banking regulators requiring banks to hold capital reserves against their Operational Risk exposures in order to absorb exceptional and severe losses should they occur (Cope, Mignola, Antonini, & Ugoccioni, 2009). In order to calculate and manage the Operational Risk, the Basel II Accord was drafted and published by the bank for international settlement specifying all the requirements (BIS, 2006).

The accord provides a framework in which Operational Risk capital should be calculated and set-out principles which banks need to attain in meeting supervisory requirements. The Operational Risk tools that banks need to implement in determining their regulatory capital are also prescribed by the Basel II Accord. Some chief Operational Risk officers view the formalisation of the Operational Risk discipline by regulators as a good step towards best risk management practices, however some view requirements as overly onerous and not providing flexibility towards risk management as initially intended due to the fact that time and money is now spent towards meeting regulatory requirements as opposed to concentrating on day to day risk management (Beans, 2007).

Cummins, Lewis & Wei (2006) highlighted that significant (>$10m) Operational Risk losses affect companies seeking growth negatively. The study also found that the impact is more severe on insurance companies as compared to banks. Strict banks regulations and the introduction of Basel are cited as some of the reasons for this minimal impact on banks. This implies that the market and regulators relies on the banks proper implementation and execution of Basel II principles in their risk management practices.

Given the continued losses experienced by banks recently as a result of Operational Risk failures and the increased focus on proper Operational Risk Management, this study aimed to establish whether the Operational Risk tools

that Basel II prescribes are used by the Advanced Measurement Approach (AMA) banks as intended and whether they reflect the Operational Risk exposure that these banks face in order to manage risk effectively and minimise losses.

Basel II framework provides 3 ways or approaches for calculating Operational Risk capital. These approaches range from the most basic approach to the advanced approaches (BIS, 2006). The AMA requirements are complex to the extent that some regulators encourage banks under their supervision to use a standardised approach or alternative standardised approach as a test case before migrating to advance approaches (Tozer-Pennington, 2010).

The advantage with the use of AMA for internationally active banks is the fact that AMA provides flexibility in the way the risk is managed (Embrechts, 2003). AMA requires the implementation of various internal risk management processes, sub projects and measurement components. This promotes good and accurate risk measurement and reporting to a range of stakeholders. Many of these concepts are new and require a fundamental change in the way that banks manage Operational Risk. The Basel II Accord encourages banks with major Operational Risk exposures and internationally active bank to adopt the AMA approach since it is deemed appropriate in reflecting their risk profile (BIS, 2006, p.158)

Operational Risk tools that feed into Operational Risk capital calculations are broken into five components, namely:

- Internal and external loss data
- Key risk indicators (KRIs)
- Risk and Control Self Assessment (RCSA)
- Audit Findings
- Risk Scenarios

Herring (2002) argued that it is important that the amount of Operational capital reserves held with the regulators truely reflects bank's risk exposure, if not, then banks should not hold Operational Risk capital that is based on inaccurate calculations. If tools used in the Operational Risk calculation do not provide accurate data, the information submitted to the regulatorys will be incorrect and the banks' risk profile will not reflect the risk exposure it faces.

In a case where the incorrect calculation result in a bank holding more regulatory capital, the bank will suffer an opportunity loss. Whereas, in a case where the incorrect calculation results in less capital being held, it may lead to serious reputational issues with the regulators.

Operational Risk is subjective and its scale is broad when compared to market risk and credit risk. Sabatini (2006) state that the role played by business Operational Risk officers is vital in ensuring that the nature of Operational Risks faced by their organisations are understood.

1.2 RESEARCH MOTIVATION

The purpose of the research was important to current risk management practices. McKinsey & Co (2009) conducted a study on the future of Operational Risk and reported that Operational Risk has significant “impact” on financial institutions’ profits and should remain a focal point in financial institutions’ risk management. They also highlight the fact that most senior management were optimistic towards embedding best practices related to Operational Risk Management.

Organisations in different industries approach Operational Risk Management differently. However, for the banking industry Basel II prescribes the minimum requirements banks need to comply with. Some of banks continue to struggle with implementation of Operational Risk tools/ requirements, as prescribed by Basel II and are therefore not measuring Operational Risk accurately.

Jorion (2009) stated that Operational Risk losses can be experienced even if flawless management systems exist and that Operational Risk losses occur as a result of bad management decisions. The failure of Enron provides one example of bad management decisions, where management of Enron actively used their complicated structure to hide transactions leading to financial misstatement of approximately US $ 24billion.

The management of Operational Risk is a key component of financial and risk management disciplines that drives net income results, capital management, and customer satisfaction. This make Operational Risk practices relevant to the stability and robustness of any financial system.

Given the above, this research evaluated the use of Operational Risk tools by AMA banks as prescribed by the Basel II Accord/ Framework in regulatory capital calculations.

1.3 RESEARCH PROBLEM

There are many challenges faced by banks globally due to the introduction of Operational Risk capital charge. These challenges centre around the way that Operational Risk tools are implemented and used in managing Operational Risk. The challenges are however more excruciating to banks who have obtained an approval from their regulators to apply the advanced measurement approaches (AMA) to their business line, as AMA requirements are mandatory for these banks. The AMA approach places high reliance on banks' ability to produce credible data and robust processes in the Operational Risk capital calculation as those banks use their own internal models in calculating the regulatory capital charge.

A study by Flamholtz (2009) further highlighted the fact that there are problems associated with banks getting the Operational Risk capital measurements right

and on time for their risk decision making processes and capital calculation purposes. Evans and Womersley (2008) stated that the quantification of Operational Risks would have been easy if banks collated credible and complete data, and they were able to measure Operational losses reliably.

The current debate concerns how financial institutions implement Operational Risk tools in managing Operational Risk; the output the tools provide; and how banks embed Operational Risk in the day to day management of the business (Di Renzo et al. 2007).

1.3.1 Research Problems

Operational Risk tools used by the AMA banks may not be implemented as per the supervisory soundness standards as set out in the Basel II Accord, and may not reflect banks Operational Risk exposure and profile. This is mainly due to the fact that there are challenges associated with the implementation of these tools. Many researchers have identified these challenges, and some are listed in section 2.8 of chapter 2.

The following research problems were identified:

- Banks internal Operational Risk measurement tools are not integrated into the day-to-day risk management processes of the bank (BIS, 2006, p. 150).

- Banks use and implementation of Operational Risk tool do not effectively capture key business environment and internal control factors which reflect the Operational Risk profile (BIS, 2006, p. 151).

1.4 RESEARCH OBJECTIVES

- To evaluate whether the Operational Risk tools are being used effectively by the AMA banks in meeting the supervisory soundness standards as set out in the Basel II AMA requirements and truly reflects the banks Operational Risk exposure and profile.
- To determine whether the Operational Risk Management tools are integrated into banks day-to-day management processes and are inputs into management decision making processes.

CHAPTER 2: THEORY AND LITERATURE REVIEW

2.1 RISK AND RISK MANAGEMENT

Clearly, Valleret, and Fenyes (2007, p. 728), defined risk as “measurable certainty and true uncertainty which cannot be measured”, by this definition they highlight the fact that it is important to know which risks can be measured and which risks cannot be measured.

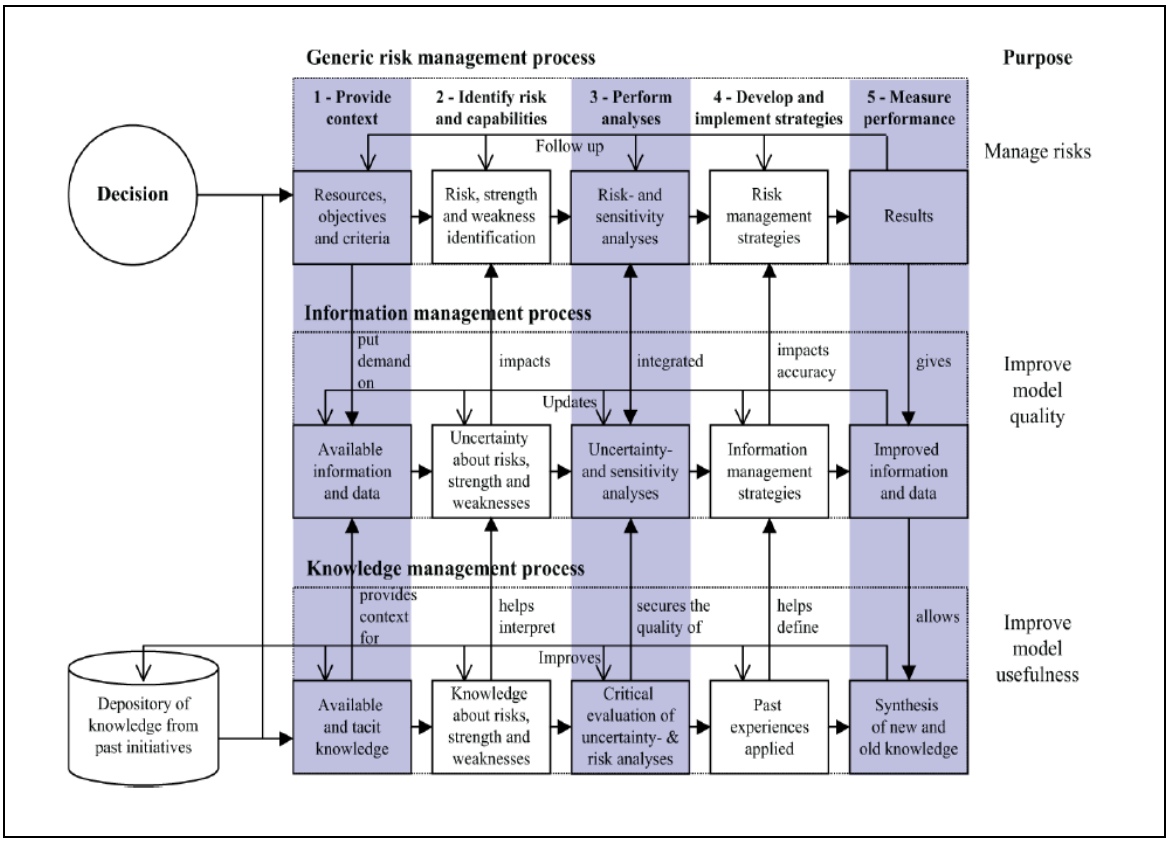
Risk management entails processes and methods where risks are identified, the exposure to such risks is measured, analysed or assessed, capital planning, monitoring and designing of control programmes, and reporting on the risk profile and capital levels to senior management, governance committee and board (Bank for International Settlement, 2010).

Emblemsvåg (2010) suggested that there are many approaches to risk management with common objectives but different processes. Emblemsvåg (2010) argued that many risk management processes overlook the importance of:

- Organisational capabilities – based on strengths and weaknesses,
- Information quality management, and
- Knowledge management

Emblemsvåg (2010) furthermore suggested that the risk management processes should always include the 3 key processes, as illustrated in Figure 2.1.

Figure 2.1: Risk Management Process



Source: Emblemsvag (2010), Management Consulting

The argument is that risk is all about uncertainty and it is important that the level of uncertainty is reduced to minimal through the inclusion of the above elements in risk management processes. These elements are regarded as vital in providing perspective and wisdom in ensuring an efficient risk management.

Understanding organisational capabilities allows the risk controls / mitigations to be designed and implemented with ease. This process enables risk management to be aligned with the strategy of the organisation. The management of information quality assists in mitigating the uncertainty presented by the risk. Knowledge management allows learning capabilities as risk management is all about understanding the business environment in order to identify the risk (Emblemsvåg, 2010).

2.2 BANKS RISK EXPOSURES

There are numerous types of risks in banking, mainly as a result of the banking industry's transformation in recent years. Transformational developments such as de-regulation of banks have increased competition globally and resulted in increased sophistication in banking products, instruments and services (Basel Committee on Banking Supervision, 2001). Changes in the banking industry have resulted in a shift from the banking system's focus on domestic policies to attention being given to the cross border banking as well (Tripe, McIntyre, and Wood, 2009). As such Van Greuning (2009) identified 3 categories of banking risks, namely:

- Financial
- Operational, and

- environmental risks

Van Greuning (2009) further identified sub categories of the above identified banking risks as follows:

Table 2.1: Categories and sub categories of bank risks

Financial Risks	Operational Risks	Environmental Risks
Balance Sheet structure	Internal fraud	Country and political risks
Earnings and income statement structure	External fraud	Macroeconomic policy
Capital Adequacy	Employment practices and workplace safety	Financial infrastructure
Credit	Clients, products, and business services	Legal infrastructure
Liquidity	Damage to physical assets	Banking crisis and contagion
Market	Business disruption and system failures (technology risks)	
Interest rate	Execution, delivery, and process management	
Currency		

Source: Analysing Banking Risk (2009)

Kuritzkes and Schuermann (2007) grouped the above risks into known, unknown and the unknowable variables. A known variable is when the risks are known and can be identified and quantified. The unknown risks can be identified however cannot be quantified (for example, some Operational Risk), and unknowable risks cannot be predicted nor quantified (for example, September 11 event). Kuritzkes and Schuermann (2007) highlighted the importance of understanding the nature of different risks and their impact on earnings in order to be able to manage the known and unknown.

Banks are then expected to put certain amount of money aside in order to guard against possible failures resulting from these risk exposures. This amount of money is called regulatory “capital”. There is an international framework / accord which determine the calculation of the minimum capital that banks need to hold as a cushion against bankruptcy. It is perceived that a well-capitalised bank will reduce the chances of insolvency (Federal Deposit Insurance Corporation, 2007).

2.3 CAPITAL

The need and use of capital differs per individual, businesses and industry. Some businesses use capital for funding purposes, whilst some require capital to ensure that they are able to operate their businesses and take advantage of

business opportunities to support their growth strategies. Capital use for financial institutions is somewhat different (from the non-financial institutions) due to the nature of the banking activities (for example, lending and trading). These activities require the bank to put capital aside to cover the risk exposure. As a result, banks need to, in addition to the funding requirements put aside capital for their risk exposures (Rowe, David; Jovic, Dean; Reeves, Richard, & 2004).

The need to hold capital resulted in banks being regulated and supervised in order to ensure that that they hold sufficient capital reserves in order to ensure stability in the banking system. It is crucial that banks are adequately regulated and supervised as banks play a significant role in ensuring economic growth and their failures have knock-on effects or can result in systematic risk (Valova, 2007). Therefore the amount of capital banks need to hold with their regulators is called “regulatory capital”. Regulatory capital is held with the objective that it will help banks survive the possible losses resulting from their risk exposures. It is not held or intended to fund banks assets, but specifically to absorb financial risk (Elizalde & Repullo, 2006).

Valova (2007) further noted banking regulations goals as:

- Safeguard of the banking industry;
- Ensuring healthy competition amongst banks and providing universal standards for all banks; and

- Encouraging meaningful decision-making exercises

The framework which provides guidance on how regulatory capital is to be calculated is called the “Basel Accord”.

2.4 EVOLUTION OF THE BASEL ACCORD

Eight banks went bankrupt in the United State during the period 1965 to 1981. There was a continued failure of banks during 1980s due to their comprehensive lending without sufficient security. This increased the possibility of banks failures and raised a concern with different bank regulators (Zaher, 2007).

The central bank governors of the group of 10 counties (G 10) formed the Basel Committee on Banking Supervision in 1974. The G 10 countries constituted of Belgium, Canada, France, Germany, Italy, Japan, Netherlands, Sweden, Switzerland, United Kingdom and United States. This committee initiated a capital measurement system for credit risk exposures called the Basel I accord in 1988.

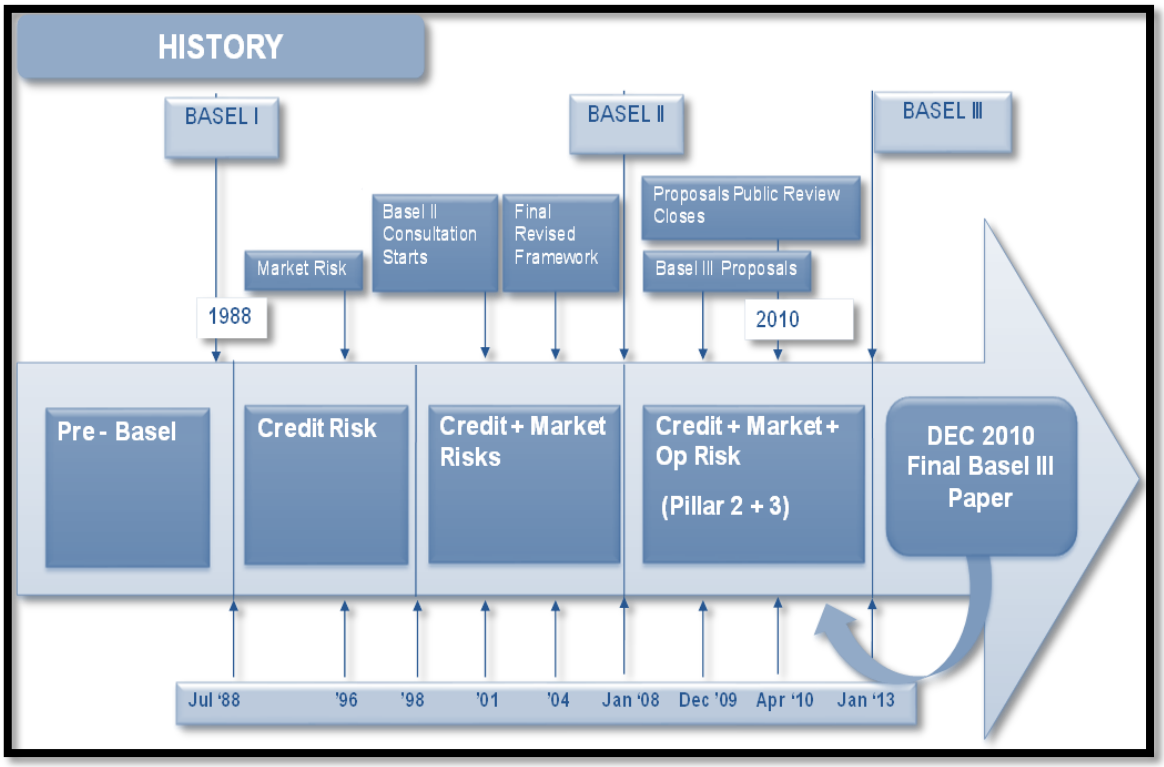
The general purpose of Basel I was to:

1. Strengthen the stability of international banking system, and
2. Set up a fair and consistent international banking system in order to decrease competitive inequality among international banks.

The accord was amended in 1996 to include the market risk exposure. The addition of Operational Risk was finalised in 2004, and the new Basel II accord was published in 2006.

In order to ensure that banks are sufficiently capitalised and remain liquid in the wake of possible large losses. Basel Committee on Banking Supervision reviews and updates the Basel framework on an ongoing basis. The finalisation of Basel III is underway (Triana, 2011). The figure below, illustrates the evolution of the Basel Accord/Framework.

Figure 2.2: Evolution of Basel Framework



Zaher (2007) highlighted some of the shortcomings of Basel I which resulted in the birth of Basel II: The main criticisms of Basel I have been:

- Partial segregation of credit risk – Basel I provided four broad risk weightings (0%, 20%, 50% and 100%) based on 8% minimum capital ratio.
- Stagnant calculation of defaulting risk – Basel I did not take into account the changing nature of default risk, as it was assumed that a minimum of 8 and capital ratio is sufficient to protect banks from failure.
- No appreciation of “term-structure of credit risk” – capital charges set at the same level regardless of the maturity of a credit exposure
- Basic computation of possible upcoming “counterparty risk” – Basel I assumed a common market to all actors, it ignored the different level of risks associated with different currencies and macroeconomic risk.
- No appreciation of “portfolio diversification effects” – summing up all risk provides incorrect judgment of risk.

In January 2007 the European banks officially adopted the requirements of Basel II for the first time, South African banks implemented Basel II in 2008, US regulators have delayed the implementation and the Chinese regulators adopted these requirements in 2010. The requirements for Basel II were primarily meant for the internationally active banks. The registrar of banks in South Africa “Errol Kruger” (2005) highlighted the following financial rewards with the implementation and adoption of the Basel II Accord:

- Cost of capital will reduce, enabling more marginal investment projects to become viable.
- The level of transparency and quality of information will be improved.
- The quality of decision-making will be heightened.
- The country's standing and credibility in the international arena will improve to the benefit of the economy as a whole.
- The adoption of Basel II constitutes a factor that positively impacts on the country and individual bank assessments by rating agencies.

This study pays more attention to the Operational Risk element of the Basel II Accord, as such the discussion to follow analyses Operational Risk in details.

Due to the recent financial crisis, Operational Risk has received more attention from regulators and the banking industry. The results of the study by de Fontnouvelle, de Jesus-Rueff, Jordan and Rosengren (2006) suggested that banks economic capital for Operational Risk exceed that of market risk, and large banks have started putting aside billions of rands towards Operational Risk Management. It was furthermore noted that Operational Risk does not only impact on the banks which experienced losses, but extends to other banks (contagion), customers and tax payers.

Operational Risk is not a new risk; it is the first risk that banks need to assess before transacting; for example, banks need to determine whether they have sufficient human resources that are sufficiently trained even before deals are

concluded or products such as loans are granted. The only change with Operational Risk is that it now has “its own management structure, tools, and processes much like credit or market risk” (Petria and Petria, 2009, p. 97).

2.5 BASEL II – OPERATIONAL RISK

Basel II provides banks with 3 options that they can use to calculate regulatory capital for Operational Risk:

1. Basic Indicator Approach, under this approach the bank holds the income for an average of 3 years, only where the income was positive (negative income excluded from the calculation). The detailed capital calculation guidance is provided under the Basel II Framework (Jobst, 2007).
2. The Standardised Approach (TSA), under which a bank would apply different pre-set percentages to annual gross income for each of the eight business lines (e.g. the least percentage is 12 applied to asset management and retail banking income, and the highest is 18 percent applied to income arising from trading and sales and Corporate finance) when calculating the required capital as an annual average over a three year period;
3. The Advanced Measurement Approach (AMA), under this approach banks calculate the capital requirement for Operational Risk using their own internal models. AMA is the most advanced and complex option

under Basel II for Operational Risk and allows a bank to calculate its regulatory capital charge based on internal risk variables and profiles, and not based on exposure proxies like gross income.

4. Internationally active banks with a high level of sophistication are encouraged to use more advanced approaches and not the basic indicator approach. Once banks get approval to use the advance approaches they can only revert back to less advanced approaches if the regulator deems fit or if they do not comply with the requirements of the approved advanced approach. As a result banks have no power to choose to go back to simpler approaches once they have selected advanced approaches; however they are allowed to select different approaches for different parts of their business, for example, if a bank has operations in South Africa and Internationally, they may select advanced approaches for the South African operations and either basic or standardised approach for the international operations.

2.6 THE ADVANCED MEASUREMENT APPROACH (AMA)

This study focuses only on the banks who have obtained approval from their regulators to use this (AMA) approach for the Operational Risk regulatory capital calculation. Hence more focus is paid on this approach and not the others.

The Basel II Accord provides for qualitative and quantitative requirements that banks need to meet under AMA. This approach requires a much more sophisticated Operational Risk environment when compared to others. A bank need an actuarial model for quantifying the Operational Risk capital, however the Basel framework does not make a mention of the measurement system that banks need to use in producing the Operational Risk regulatory capital. Whichever system is chosen it should capture “potentially severe tail loss events” and the models should be validated independently.

Regulators expect banks to calculate the regulatory capital requirements as “the sum of expected loss (EL) and unexpected loss (UL)”. Banks will be allowed to exclude the expected loss in the calculation only if they are able to demonstrate to the regulator that these losses are being included and built within their business practices.

A simple Modelling of Operational is based on the Loss Distribution. The loss distribution is normally based on the assumptions made around the frequency and severity of Operational Risk loss events (Grody, Harmantzis, Kaple, 2007).

A summary of qualitative requirements is provided below:

- Banks should have Operational Risk Management department which provide an independent oversight.

- Operational Risk Management must be included in day to day running of the business.
- Reporting of Operational Risk losses to senior management
- Documentation of Operational Risk system
- Independent checks and confirmation by internal and external auditors

Sabatini (2005) summarises these qualitative and quantitative requirements into a Framework that Operational Risk officers should implement in their Operational Risk Management practices. He reckons that this framework will provide effective Operational Risk Management within organisations if properly implemented. This framework is in line with the key features of AMA model.

The framework and the Basel II Accord require banks to have governance structures which set the tone from the top and instil the risk management culture within their organizations. Both these frameworks identify key Operational Risk tools such as;

- Risk events reporting (loss data).
- Key Risks Indicators identification,
- Risk self assessment and the integrated reporting.
- Risk Scenarios
- Internal Audit findings

These Operational Risk tools are discussed in details in the next section.

2.7 OPERATIONAL RISK TOOLS

Basel II requires banks to create board approved risk methodologies and identify risk appetites (the amount of risk the banks are willing to take) continuously in their Operational Risk Management practices (Bank for International Settlements, 2006). These methodologies should define how Operational Risk tools are to be implemented and embedded in their business processes (Sandford, 2008). The key Operational Risk Management tools are internal and external data, key risk indicators, risk and control self assessment, audit findings and risk scenarios. Each of the tools is discussed below.

2.7.1 Internal and External loss data

Internal loss and external loss data are important elements of the AMA Operational Risk capital calculation. Basel II requires banks to track their internal loss data in order to tie their risk estimates to their actual loss experience. This data can also be used to validate outputs of other Operational Risk tools, for example, it can be used as the linkage connecting the internal loss occurrences to the risk management and internal control environment controls assessment (Bank for International Settlements, 2006).

It is critical for banks to have collated internal loss data and use external loss data as inputs to scenarios calculation; however the challenge with the use of external data is the fact that all sources of external loss database have

limitations when it comes to eloquent calculation of the loss frequency. The calculation of the robust loss frequency is an important part of an Operational Risk capital calculation (Birade & Mark, 2009).

External loss data enables banks to benchmark themselves against other banks of similar sizes and risks, and allows them to see their performance in relation to their peer (McEachen, 2003). This information helps banks to design controls in cases where their loss patterns are not in line with their peers.

Sabatini (2003), stated that it is important to identify losses when they occur as failure to do so will result in an inability to manage them. However the study by David, Anderson, and Aven (2007) concluded that banks should focus on the probability of whether losses will happen, as opposed to focusing time and effort on the historical data analysis. They further state that this approach prevents banks from implementing pro-active risk management and designing controls and mitigations to prevent these losses from happening.

One of the requirements with regard to Operational Risk loss data is the need to have documented procedures for assessing the on-going relevance of information reported to senior management (Bergmark & Tattam, 2005). Garrity (2007) stated that some of the obvious Operational Risk losses (for example interest claims) maybe be extracted out of General Ledger accounts, however noninterest related losses maybe hidden in any account with different classification. Furthermore Garrity (2007) suggested that whichever approach is

followed by banks in ensuring that the loss data is collected appropriately across the business lines, it is important that management is certain of the loss data integrity before they can make decisions.

Cope (2009) argued that the AMA measurements standards are too high; given the fact that there is no enough data (internal and external) which allows the AMA banks to estimate high percentiles in their modelling, for example, 99.9th percentile as required by some regulators, notably US federal banks.

2.7.1.1 Internal loss data

In order to analyse the root cause of Operational Risk losses and group Operational Risk events that are identical, Basel II accord provides 7 events type in which Operational Risk losses should be recorded and classified:

- Employment practices and workplace safety (these are events arising from the acts inconsistent with employment, health or safety laws or agreements, from payment of personal injury claims or from diversity or discrimination events.
- Internal fraud is defined as losses due to acts of type intended to defraud, misappropriate property or circumvent regulations, the law or company policy (excluding diversity/discrimination events) which involves at least one internal party

- External fraud is defined as losses due to acts of a type intended to defraud, misappropriate property or circumvent the law, by a third party
- Clients, products, and business practices are defined as losses arising from unintentional or negligent failure to meet a professional obligation to specific (including fiduciary and suitability requirements), or from the nature or design of a product. Losses in this category include losses due to fiduciary breaches, misuse of confidential customer information, improper trading activities, money laundering, and sale of unauthorised products, etc.
- Damage to physical assets is defined as losses due to loss or damage of physical assets from natural or man-made disasters or other events (e.g. fire, explosion, terrorism, etc.)
- Business disruption and system failures are defined as losses arising from disruption of business or system failures including hardware and software failure, system development, and infrastructure issues
- Execution, delivery and process management is defined as losses from failed transaction processing or process management or from relations with trade counterparties and vendors.

The above loss events are to be mapped or grouped into 8 business lines, namely (Bank for International Settlements, 2006):

1. Corporate finance
2. Trading and Sales

3. Retail banking
4. Commercial banking
5. Payment and Settlement
6. Agency services
7. Assets management, and
8. Retail brokerage

Banks are expected to have IT systems where these losses are recorded.

2.7.1.2 External data

As highlighted above, external data may be obtained from various public and private data sources such as Operational Riskdata eXchange (ORX). ORX collects data from over 50 institutions globally, in over 120 countries. Cope (2010) cautioned banks to carefully choose external data which is relevant to their risk exposures, as the information published on Operational Risk events is varied.

2.7.2 Key Risk Indicators (KRIs)

Osborne (2006) defined key risk indicators as an early warning of potentially serious hazards. Osborne (2006) provided examples of such events which may trigger a KRI as follows:

- Employees turnover in a key positions
- An increase in the number of transactions

- unexpected increase in clients grievances
- Information technology systems alterations

These indicators provide signal to risk management and compliance functions that something needs attention.

The Sounds Practices for the Management and Supervision of Operational Risk consultative paper (2010) stated that KRIs present useful information about risk exposures and should be used to observe the risks associated with them. It further highlighted the fact that it is important that key risk indicator breaches are escalated to relevant bodies in order to ensure that remedial actions are put in place.

Key risk indicators play an important role in Operational Risk Management, however the study by Scandizzo (2005) highlighted that there is little available guidance from different bodies such as regulators, internal audit and external consultants on how best should key risk Indicators be implemented in order to ensure that they are complete, valid and relevant to business. As a result, the practical implementation of key risk indicators may be inconsistent.

McDermott and Davies (2008) further stated that it is important to obtain management buy-in and have a strong governance framework, where Operational Risk tools such as key risk indicators can be identified, monitored, reported and acted upon. However, achieving buy-in for Operational Risk

managers in most organisations remains a challenge, and therefore a need exists to move from risk administration to risk management; which could be a daunting task for risk officers.

Another tool which is critical in managing Operational Risk is call Risk and Control Self Assessment.

2.7.3 Risk and Control Self Assessment (RCSA)

Risk and Control Self Assessment is a process where banks internal processes are assessed against threats and weakness. Subsequently assessment of the impact of the identified threats is conducted to evaluate the inherent risk exposure. Once the inherent risk has been assessed, the controls and control effectiveness is assessed in order to evaluate the residual risk the bank is faced with (Bank for International Settlements, 2010).

Jallow, Majeed, Vergidis, Tiwari, and Roy (2007) highlighted the fact that risk assessments in business processes are critical in order to ensure business continuity. Issues which are viewed as hazard to business can be identified analysed and mitigating controls designed.

Joseph and Engle (2005) agreed that risk control self assessment can be an effective tool used for improving the business; however they are often designed by the business or internal management without the involvement of independent auditors. Joseph and Engle (2005) furthermore argued that auditors can benefit immensely from the use of this tool since among other responsibilities they need to assess the internal control environment.

It is important that the results from the risk and control assessments conducted by banks management are in line with the control environment as assessed by internal or external auditors. The audit findings are normally used to address

the control breakdowns or enhancements as identified by auditors and serve as an important tool in Operational Risk Management.

2.7.4 Audit Findings

Principles for the management of Operational Risk stipulate that the bank should utilise 3 lines of defence, the first being the business line management, second line being the Operational Risk function and the third line is an independent review of the Operational Risk Management, controls and systems (Bank for the International Settlements, 2010). Internal audits act as a third line and should provide an independent review of the effectiveness of the Operational Risk Management and bank frameworks.

Internal and external auditors are expected to conduct audit assessment of the Operational Risk Management practices and measurement structure in line with the AMA requirements (Bank for International Settlements, 2006), hence the Audit findings are considered an important tool in Operational Risk Management.

According to Staciokas and Rupsys (2005) the internal audit function has been used by organisations internally to enhance their business processes and by regulators to obtain assurance on organisation's functions such as liquidity levels and the protection of their assets.

Internal Audit is required to provide an independent assurance of the bank's control environment (Yeh, 2008). Consequently, it is important that institutions act on the control weaknesses or early risk warnings identified by such parties as regulators and Internal Audit. However, institutions often do not fully implement these recommendations; as compliance is normally not seen as contributing significantly towards business profits (Osborne, 2006). Contrary to the above statement, a study by Sarrens and De Beelde (2006) found that there is a greater expectation from senior management on internal audit delivery when it comes to the uncovering of control weaknesses within business units under their review. Internal audit is regarded as providing a supporting role to senior management on business functions. On the flip side, internal audits expect senior managers to be proactive in identifying and putting risk management structure in place and also expect senior management buy-in and support in executing their function.

Osborne (2006) in his governance report highlighted that bank's control environment is changing to be more risk based. Osborne (2006) mentions that audit approaches are now risk based and compliance assessments are changing to take risks into account which in turn add more value and provides alignment between audit and risk management practices. Osborne (2006) further more stated that the challenge with this risk approaches will be that

auditors will be expected to stay on top of emerging risks in providing audit opinions and inputs into Operational Risk tools.

The internal audit assessment or findings are then used as an Input in conducting risk scenario assessments.

2.7.5 Risk Scenarios

A risk scenario is a forward looking business risk which is defined by business experts and has a possibility of realising into a significant monetary loss. Risk scenarios are informed by the business environment and internal control factors (internal losses, KRIs, RCSA), external data, audit findings and other risk information (e.g. business continuity plan assessments). Risk scenarios and internal loss data are the key inputs into the Operational Risk capital modelling process (Bank for International Settlements, 2006).

It is important to ensure that the quality of data that feeds into scenarios identification is of good integrity, given the fact that scenarios are subjective. Vigorous methodologies and frameworks need to be design to ensure consistency in the scenarios information and the information from other Operational Risk tools (Bank for International Settlements, 2010).

In the scenario identification processes, banks need to evaluate low frequency but catastrophic risks which could force them out of business; and hold

Operational Risk capital against those risk types (Lynn, 2006). Risk scenarios should be forward looking. Senior management or risk experts who have intimate knowledge of the business need to be involved in scenario identification, analysis and quantification. A study by Tchernobai (2006), found that there is a risk that data could bias when using in-house or internal loss modelling mechanisms and this results in lower capital charge.

Jimenez-Rodriguez and Feria-Dominguez (2008) suggested that Operational Risk tools such as scenarios will be implemented with accuracy if banks have risk managers and senior management who understand the business and are risk conscious.

Berley (2006) was of the view that many catastrophic Operational Risk failures are as a result of failure in strategy planning and not only the result of Operational (people, system and processes) control breakdowns. Berley (2006) argued that conventionally, processes and financial reporting were done by people who did not understand the strategies of their companies. In identifying scenarios the first important step is the understanding of the business strategy and the risks related to the strategy. Berley (2006) identified some of the internal and external environment factors to be considered in scenario planning as follows:-

Table 2.2: Internal and External environment factors in Scenario planning

Internal Environment	External Environment
Historic and prospective financial forecast and results	Economic conditions (currency risk, interest rates and other variables)
Employee feedback and performance	Regulations
Balance Sheet and Cash Flow Statement review	Customer surveys
Retirement (are key personnel about to retire in the next year?)	Analyst opinion about your company
Risk appetite and more importantly does it correlate to your objectives?	Political sentiments worldwide
Growth prospects	Markets (operating in the growing, declining or maturing markets?)
People – do your employees perform at high quality across the organisation, do you develop people to help you grow or always go outside for talent?	Competition – what are your competitors doing?

Rosengren (2006) highlighted 3 main challenges faced by the regulators and supervisors due to banks use of risk scenarios:

- Ensuring that scenarios models used by banks are valid

- Lack of consistency in capital numbers produced from scenarios model for similar banks or banks with similar risks exposures
- Inability to guarantee that the internal loss data occurrences align with the estimation of the Operational Risk exposure.

Demoulin, Embrechts and Neslehova (2006) warned that not all Operational Risk data can be modeled or can be quantitatively analysed with ease. Demoulin et al. (2006) made reference to loss data relating to legal risk versus loss data relating to damage to physical assets. The loss data relating to legal risk requires a clear cut analysis compared to data relating to damage to physical assets.

Lubbe and Snyman (2009) emphasised the fact that statistical models should be validated by an independent, credible and experienced model expert given the complexity of these models. Lubbe and Snyman (2009) further mentioned that the input into capital calculation consists of internal loss (which is historic) and scenario analysis (prospective). Scenarios are then described and quantified at different probability or frequency levels. The scenarios are modeled individually and the annual frequency is assigned, for example:

- 1 in 2 year single loss event;
- 1 in 5 year single loss event;
- 1 in 7 year single loss event;
- 1 in 25 year single loss event;

- 1 in 40 year single loss event;
- 1 in 100 year single loss event.

2.8 CHALLENGES WITH OPERATIONAL RISK TOOLS

A study by Dutta and Perry (2006) highlighted the fact that Operational Risk quantification is fairly new, and that techniques and tools used are at an infancy stage which could lead to inconsistencies and inaccuracies of data used in the capital calculation.

The study tested the use of loss data as one of the tools used in the Operational Risk capital calculation. Dutta and Perry (2006) findings revealed that there were concerns around inconsistencies on how data is modelled per institution and the inconsistencies resulted in different capital values when different systems are used. The study raised questions as to whether the loss data used in measuring Operational Risk provides a reasonable estimate of the exposure.

Research by Danescu and Muntean (2005) found the historical losses of banks to be a problem since it does not illustrate all the risk exposures faced by the institutions. Basel II recommends that banks use external data (Bank for International Settlements, 2006); however the challenge with external data is its inconsistency, trustworthiness and the fact that the different banks have different control environments.

Basel II requires banks to use risk scenarios in calculating regulatory Operational Risk capital. A study by Point (2005) found that many banks are

not prepared to embrace the risk scenario input into Operational Risk capital calculations as they do not have recognised methodologies and systems even though the risk of rare, extreme loss is not easy to measure using other tools.

The requirement by Basel II to have 5 years' data is viewed as bias, since banks may use data which is not current and does not relate to future risk and controls (Scandizzo, 2005). It is important for banks to use the tools to help mitigate the current risks and future risks, and not necessarily for regulatory risk purposes. Hence the Operational Risk frameworks make it clear that banks need to integrate these tools in their business processes.

2.9 OPERATIONAL RISK TOOLS AND BUSINESS PROCESSES

Fundamental principles of Operational Risk Management calls for the integration of the risk management processes into the business process (Bank for International Settlements, 2010). This principle is based on the fact that bank management need to be aware of their environment and complication of the risks intrinsic in their products and services.

In order for banks to achieve a competitive advantage it is of utmost importance that they render quality customer services and effectively manage their business processes. Breakdowns in business processes has become a serious threat to businesses since customers are now more demanding and do not compromise when it comes to expected quality of service and products. Jallow

et al. (2007) stated that the integration of Operational Risk tools with business processes aims to mitigate or eliminate business processes breakdowns and help banks achieve competitive advantage.

Van Greuning (2009) highlighted that in running a banks day-to-day activities it is of utmost importance to ensure that these activities are coordinated in line with established risk appetite and corporate objectives. Van Greuning (2009) appreciated the relationship between shareholders, bank management, the board and other stakeholders as important in ensuring the soundness of the banking system and a key driver in attracting investments due to perceived good management of risks/ lower levels of risks.

Laeven and Levin (2009) suggested that there is a relationship between how the risk management processes are embedded within the banks and the ownership of the banks. Laeven and Levin (2009) furthermore suggested that banks which are controlled by the owners with larger controlling stake will take more risks than the banks controlled by owners with small shareholding which could then result in a possible conflict over the risk behaviour within the organisation.

The implementation of Operational Risk tools requires board and senior management buy-in and participation in order to ensure the general success of effective Operational Risk Management within financial institutions (Sheen, 2005).

Research by Cernauskas and Tarantino (2009) stated that a concern for many banks remains integration of Operational Risk tools in their business processes. The study highlighted the fact that risk tools should be integrated with the business processes in order to achieve risk transparency and reduce Operational Risks. Cernauskas and Tarantino (2009)further stated that the need for integration is due to the fact that Operational Risk tools should be used to improve business processes from which the key risk and performance can be used to indicate quality process performance.

The other consideration is that in a dynamic business environment, Operational Risk becomes a key tool in assessing and implementing business processes in order to ensure successful responses to changes and ultimate achievement of business objectives (Azvine, Cui, Majeed & Spott, 2007)

Barnier (2009) perceived the integration of Operational Risk tools with business processes as a way of “connecting the dots” where Operational Risk officers are expected to work side by side with other areas such as Information technology risk, human resources and all other relevant business lines.

CHAPTER 3: RESEARCH QUESTIONS

The research questions are aimed at gaining a better understanding of Operational Risk tools usage in defining a banks Operational Risk profile and regulatory capital calculation under AMA.

Banks using the AMA approach calculate capital using their own internal measurements, which are subjected to supervisory assessment. Banks may implement systems and processes which are different from one another; however, each bank needs to meet the minimum standards presented by the Basel II Accord (Bank for International Settlements, 2006). What causes concern is that there are challenges in implementing these tools and the failure to implement them correctly may have serious financial consequences, fail to present the true Operational Risk exposure/profile and lead to the incorrect Operational Risk regulatory capital.

Given the above, a case for evaluation of Operational Risk tools was investigated. This was accomplished through empirical testing of survey data. The following questions were investigated:

Research Question 1: Are Internal loss data and external data collection and reporting, key risk indicators identification, Risk and Controls Self assessment, Audit findings and Risk scenarios in line with the Basel II minimum requirements?

Research Question 2: Are Operational Risk Management tools integrated into day-to-day business processes and used as business risk management tools versus just regulatory capital calculation methods?

In answering the above two research questions, the following questions were also addressed.

Research Question 3: Do Operational Risk tools reliably measure Operational Risk regulatory capital?

Research Question 4: Does the Operational Risk tools, truly reflect banks Operational Risk exposure and profile?

CHAPTER 4: RESEARCH METHODOLOGY

4.1 INTRODUCTION

This section deals with the rationale for the proposed research method. The research design, population, sample and data collection tools, additionally possible limitations of the research are discussed.

The purpose of the research was to evaluate the application of Operational Risk tools used in regulatory capital calculation by the Advanced Measurement Approach (AMA) banks. The research was limited to the 3 major banks in South Africa, who had obtained approval to use the Advanced Measurement Approach for the calculation of regulatory capital.

4.2 RESEARCH DESIGN

Data collection techniques for assessing Operational Risk tools can be classified as either qualitative or quantitative methods (Saunders, Lewis, & Thornhill, 2009). Qualitative measures make use of non-numerical data and include focus groups and personal interviews. Quantitative measures use numerical assessments such as questionnaires (Buglear, 2005).

This study was quantitative in nature, and used primary data to determine whether the Operational Risk tools used by banks truly reflect their Operational Risk profile and reliably measure the Operational Risk regulatory capital.

Blumberg, Cooper, & Schindler (2008) regarded a quantitative research approach to be objective in nature which concentrates on measuring phenomena and therefore includes collecting and analysing numerical data and applying statistical tests.

The quantitative approach used in this study was descriptive, which Blumberg, Cooper, and Schindler (2008) describes as research conducted when the "hypothesis is clearly stated".

4.3 PRIMARY DATA

Nicholson & Bennett (2009) defined primary data as data gathered and collected by the researcher to address the current needs of the research. Primary data was used in this study as the problem under investigation was current and there was no secondary data available.

Given the considerations of time and practicality a questionnaire survey was used and responses were collected electronically through the use of emails. Saunders et al. (2009) stated that the use of primary data as oppose to secondary data, may allow the researcher to be able to achieve the research goals since data is collected for the specific problem under study and the researcher can create own definitions.

4.4 PROPOSED UNIT OF STUDY

Blumberg, Cooper, and Schindler (2008) distinguished between five different unit of analysis that are common in designing reseach: individuals, organisations, divisions, departments and general groups. This study focused holistically on risk management within banks as organisations and more particularly, from an embedded focus point, on the Operational Risk Management function.

The study analysed the use of the Operational Risk tools for the 3 AMA banks in South African, namely:

1. FirstRand banking group
2. Nedbank banking group and
3. ABSA banking group

These banks were chosen as they were AMA banks and consequently they needed to implement tools in their Operational Risk Management, as the tools are mandatory to implement in order to meet the regulatory requirements (South African Reserve Bank) and the AMA requirements (Moosa, 2008). The unit of analysis chosen was the organisations (the banks).

4.5 POPULATION OF RELEVANCE

The target population consisted of the Operational Risk managers, which included embedded segments/business units risk managers and senior Operational Risk managers in the enterprise risk management department (banking group level). The total population size differed per the structure of the banks risk management within each of the 3 banks. The minimum estimated population size (N) of senior Operational Risk managers for the 3 banks was 32.

Figure 4.1: AMA banks ORM structure

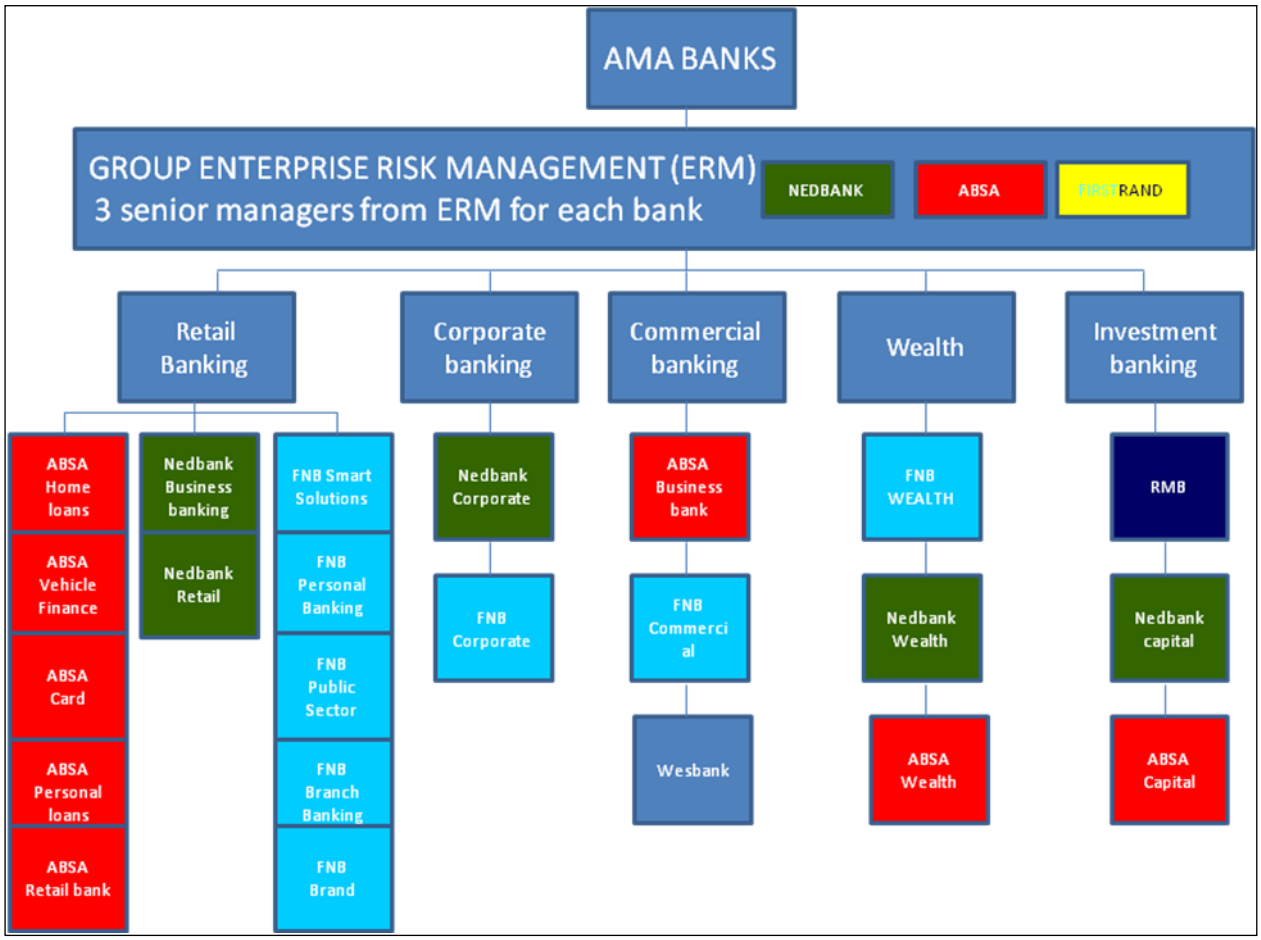


Table 4.1: AMA banks responses

Bank	Heads of Operational Risk Management in Business Units
FIRSTRAND (Including – FNB, Wesbank & RMB)	Thirteen (13)
ABSA	Eleven (11)
NEDBANK	Eight (8)

4.6 SAMPLING METHOD AND SIZE

The sampling frame, also known as the working population chosen is a non-probability sampling method, containing units or people who are most conveniently available (Saunders et al., 2009). In this study, the most conveniently accessibly units were the senior Operational Risk managers of the 3 banks identified. The sample came from the following segments of population:

i) A non-random selection of segments/ business units Operational Risk managers from major business lines, namely:

- Retail Banking
- Corporate Banking
- Commercial Banking
- Wealth management, and
- Investment banking

ii) Senior Operational Risk managers at the banking group level / enterprise risk management department.

The Operational Risk managers from the lower level of the business were excluded, as similar processes are cascaded down or a top down approach is followed and their responses were not expected to be different from the responses of the segment/business units risk managers. The sample was conviniet, since the researcher had access to senior management in the 3 banks group enterprise risk management.

4.7 DATA COLLECTION TOOL

The research instrument used was a questionnaire. The questionnaire was phrased in a simpler way to accommodate ease of reading and understanding with the sample group. The following documents were used to design the questionnaire:

- Principles for the Sound Management of Operational Risk (BIS, June 2011)
- Sound Practices for the Management and Supervision of Operational Risk (BIS, Dec 2010), and
- The Internal Convergence of Capital Measurement and Capital Standards (BIS, 2006).

The questionnaire items were put on a 5-point scale ranging in this order:

- 1 (strongly disagree), 2 (Disagree), 3 (Uncertain), 4 (Agree), 5 (Strongly agree).
- 1 (To a very small extent), 2 (To a small extent), 3 (Somewhat), 4 (To a great extent), 5 (To a very great extent). and
- “Yes” or “No”

A pilot study was conducted to validate the questionnaire. The questionnaire was distributed to subject experts who included Heads of Operational Risk Management of the three banks selected for review and feedback.

A total of 40 questionnaires were distributed. The questionnaires were distributed to each bank’s group head of Operational Risk Management for circulation within their organisations.

4.8 THE QUESTIONNAIRE

The survey questionnaire consisted of two parts. The first section focused on the 5 Operational Risk tools (Internal and External data, Key Risk Indicators, Risk and Controls Self Assessment, Risk Scenarios and Audit Findings) used in the regulatory capital calculation. The Questions were asked on each tool and analysed separately.

The second section focused on the integration of these Operational Risk tools into business processes.

4.9 DATA ANALYSIS

It is important to understand the kind of data involved before one undertakes A quantitative analysis. Smith, Thorpe, and Lowe (1999) make a distinction between 3 types of data, namely;

- Nominal
- Ordinal, and
- Interval

Nominal data is used where different categories can be “labelled” for example, gender characteristics classification, man or woman. Ordinal data is used where data can be ordered, for example, strongly agree, agree, neither agree nor disagree, disagree, strongly disagree. Interval data is used where the interval between 2 points or classification can be determined, for example, classification made on age or salaries.

The data collected from the questionnaire was ordinal data. The data collected from the returned questionnaires were captured onto an Excel spreadsheet for analysis. The data was sorted to group questions according to applicable tool under the test and analysed as such.

4.10 RESEARCH LIMITATION

The following aspects are limitations to this study-;

The research focused only on the top 3 banks in South Africa which had obtained an approval from South African Reserve Bank to use the AMA Operational Risk tools. The research could have been extended to the other 2 banks which are part of the top 5 banks to get a better understanding of the use of Operational Risk tools, however these banks have not obtained an approval to use the tools and as such the implementation methods and rigour may differ.

The research used survey, and is open to response bias, with the possibility of respondents giving perceptions they feel the researcher may want to see reflected. To minimise the effect of this, the respondents were requested to fill in the questionnaire based on what their first natural response to the statement were.

To gain a more in depth picture of the use of the Operational Risk tools, it would have been interesting to send survey to all Operational Risk managers including business units Operational Risk managers and not only segments risk managers. This is not practical given time constraints and the risk that they may not complete the questionnaire accurately given their level of seniority (experience) and interpretation of the questions / data.

CHAPTER 5: RESEARCH RESULTS

5.1 INTRODUCTION TO THE RESULTS

The previous chapter presented a description of the methodology applied to test the research questions outlined in chapter 3. This chapter presents the results of this research in the form of tables and graphs to allow a better and easier understanding of the research findings. Results of the questionnaire are presented as per data collected as defined in chapter 4. This chapter presents the responses as collated from the 3 Advanced Measurement Approaches (AMA) banks in South Africa.

5.2 RESEARCH PROCESS OUTLINE

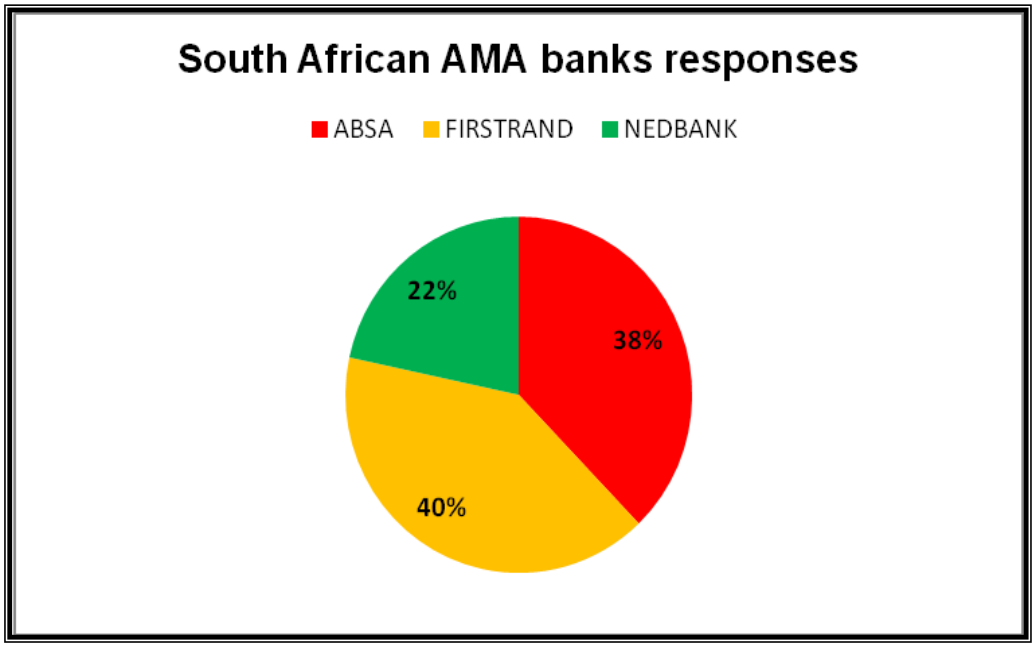
5.2.1 Sample size and response rate

Forty (40) questionnaires were prepared and circulated. A total of 40 responses were received. As a result of data completeness and data integrity checks one of the response had to be discarded due to an incomplete questionnaire. Thus the sample comprised of a total of 39 respondents was used for analysis. This exceeded the minimum required sample of 32. The extra responses were used as a larger sample added more value and enhance the quality of the results. The usable response rate amounted to 100% (based on the total responses), which was satisfactory.

5.2.2 Demographic representation

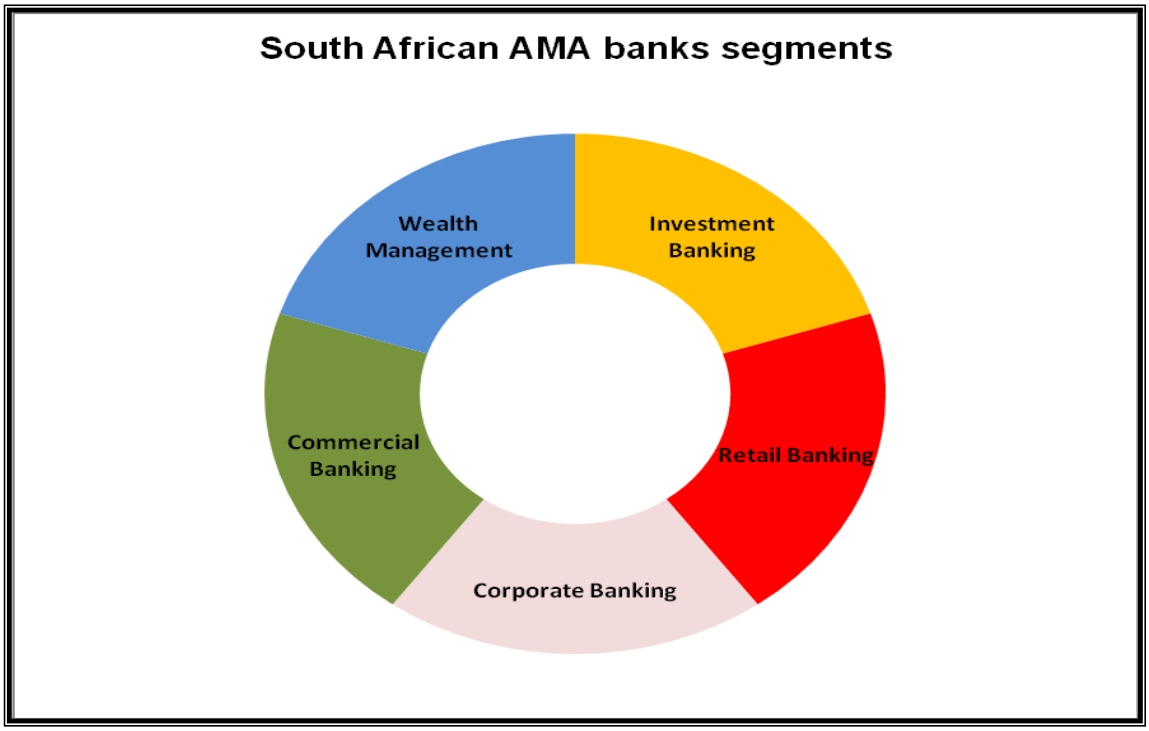
This section describes the demographic profile of the valid responses. Anonymity of the respondents was assured by not asking for, nor recording any easily identifiable personal information or information representing a particular bank. The questionnaires were distributed to senior managers in Operational Risk Management business units of the 3 banks in South Africa who have obtained approval to use the Advanced Measurement Approach for Operational Risk capital calculations as explained in chapter 4. Figure 5.2:1 below indicates the percentage of the respondents per bank.

Figure 5.1: South African AMA banks responses



FirstRand had the highest responses with 40%, while the next highest was ABSA with 38% and then Nedbank with 22%. The responses where mainly driven by the way each banks enterprise risk management departments were structured. At least one response from head of Operational Risk / Operational Risk manager of each segment was required. Figure 5.2:2 below provides the bank segments which participated in the data collection.

Figure 5.2: South African AMA Banks Segments



5.3 RESULTS PRESENTATION

The objective of the research was to evaluate whether the Operational Risk tools are being used effectively by the AMA banks in meeting the supervisory soundness standards as set out in the Basel II AMA requirements and truly reflects the banks Operational Risk exposure and profile. Furthermore the objective was to determine whether these tools are integrated into banks day-to-day management process and are inputs into management decision making. The above objectives help ascertain whether the Operational Risk tools reliably measure the Operational Risk regulatory capital.

The presentation of these results is divided into two parts as explained below:

Part 1: below presents the research results in systematic order starting with the assessment of the use of the Operational Risk tools, where feedback relating to each tool as presented in chapter 2 is discussed. The results from the assessment of the Operational Risk tools answered the first research Objective.

Research Question 1: Are Internal and External loss data collection and reporting, Key Risk Indicators Identification, Risk and Control Self-Assessment, Audit findings and Risk Scenarios in line with the Basel II Requirements?

Part 2: provides the results as they relate to the integration of the Operational Risk tools into day-to-day management processes. The intention with the

presentation of the results in this section was to answer the second research objective.

***Research Question 2*:** Are Operational Risk Management tools integrated into day-to-day business processes and used as business risk management tools versus just regulatory capital calculation methods?

The results of the objectives set above assisted in determining whether the Operational Risk tools reliably measure the Operational Risk capital as per Basel II requirements.

As mentioned above, the objective of this section is to present feedback relating to each Operational Risk tool. There were 5 tools under consideration and results are presented according to the following sequence:

- Internal and External data
- Key Risk Indicators
- Risk and Control Self Assessments
- Audit Findings
- Risk-Scenarios

5.3.1 Internal and External loss data

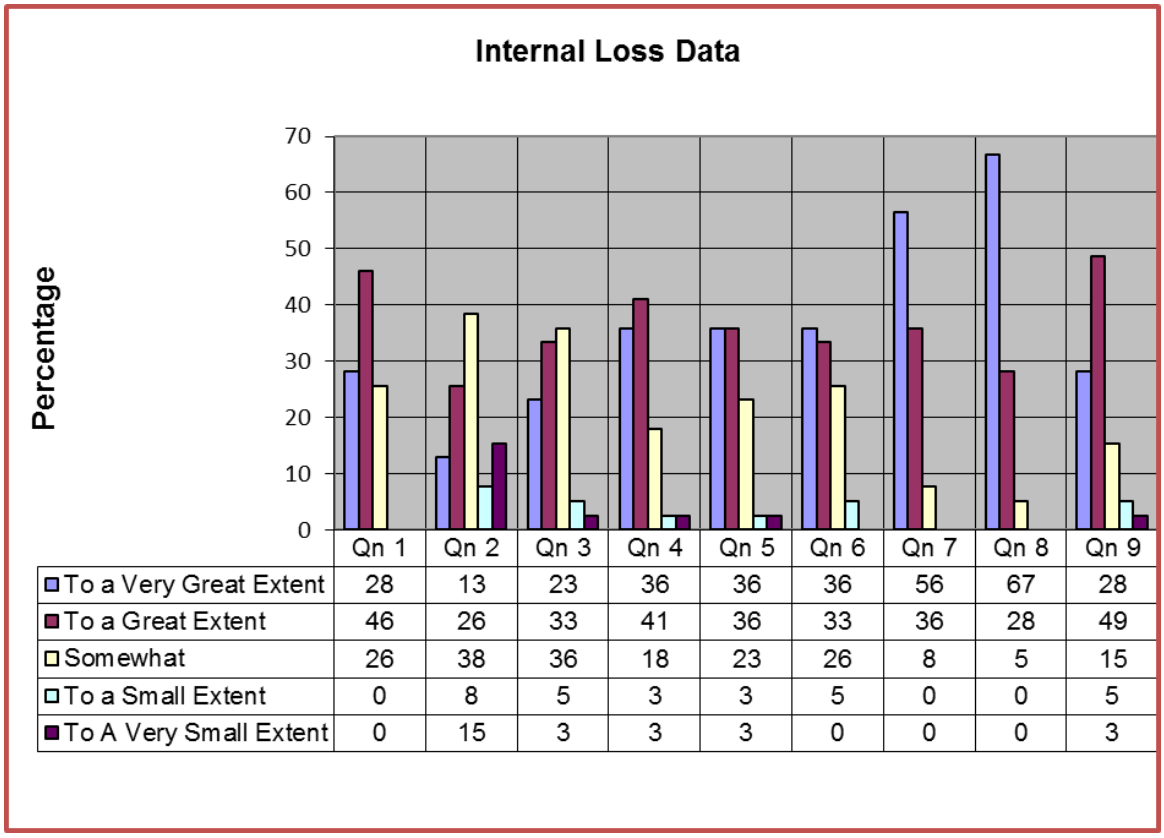
To manage Operational Risk effectively Basel II prescribes the use of internal and external loss data. The following questions were used to determine the use of internal and external data:

Table 5.1: Internal and External Loss Data Questions

Q 1	To what extent is internal loss data considered to be accurate?
Q 2	To what extent are internal losses taken into account in the budget process / are budgeted for?
Q 3	To what extent are Operational Risk managers involved in management of boundary events?
Q 4	To what extent are recoveries linked to Operational Risk losses?
Q 5	To what extent are Operational Risk losses used to inform KRIs?
Q 6	To what extent are Operational Risk losses used to inform RCSAs?
Q 7	To what extent are Operational Risk losses used to inform Risk Scenarios?
Q 8	To what extent are materials or significant losses identified brought to attention of senior management?
Q 9	To what extent does the actual loss data align to financial data?
Q 10	To what extent does a bank's Operational Risk measurement system use relevant external data (either public data and/or pooled industry data)?
Q 11	To what extent does a bank have a systematic process for determining the situations for which external data must be used and the methodologies used to incorporate the data (e.g. scaling, qualitative adjustments, or informing the development of improved scenario analysis?

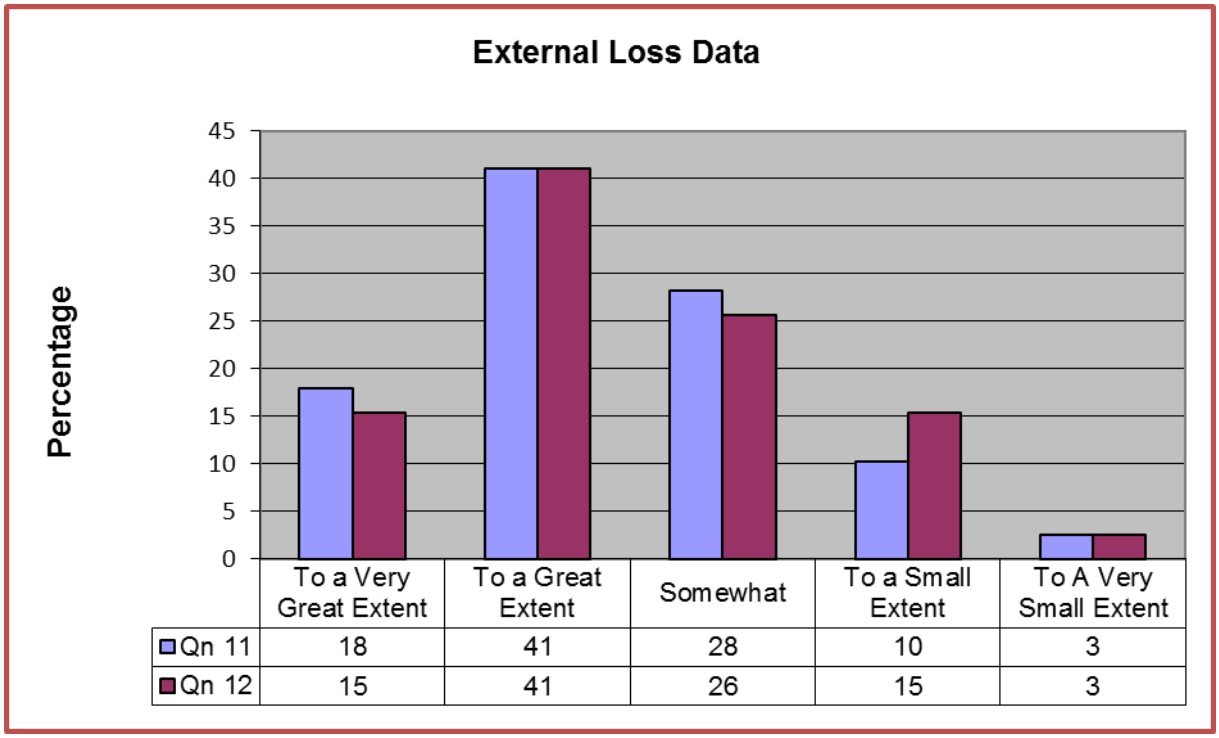
The overall results of the above questions for internal and external loss data are presented below. Each question is discussed and results for each are presented in the following sections. The figure below presents the consolidated results for the internal and external data based on the responses given in our survey.

Figure 5.2 Internal Loss Data



	Qn 1	Qn 2	Qn 3	Qn 4	Qn 5	Qn 6	Qn 7	Qn 8	Qn 9
To a Very Great Extent	28	13	23	36	36	36	56	67	28
To a Great Extent	46	26	33	41	36	33	36	28	49
Somewhat	26	38	36	18	23	26	8	5	15
To a Small Extent	0	8	5	3	3	5	0	0	5
To A Very Small Extent	0	15	3	3	3	0	0	0	3

Figure 5.3: External Loss Data



The next section discusses each of the above questions and presents the results of each.

5.3.1.1 To what extent is internal loss data considered to be accurate?

In order to use internal data effectively, the data recorded has to be accurate and the table below shows the responses given by the sample in regards to the accuracy of internal loss data.

Table 5.3.1.1: The Extent in which loss data is considered to be accurate

	To a Very Great Extent	To a Great Extent	Somewhat	To a Small Extent	To A Very Small Extent
n	11	18	10	0	0
%	28%	46%	26%	0%	0%

As shown in table 5.3.1.1 majority of respondents indicated that banks loss data is accurate, 46% of respondents indicate that internal loss data is accurate “To a Great Extent”, 28% indicate the accuracy of loss data “To a very Great Extent”. Despite the fact that majority of the responses considered loss data to be accurate, 26% indicated that loss data is “somewhat” accurate and no respondents considered loss data to be accurate “To a Small Extent” or “To a Very Small Extent”.

5.3.1.2 To what extent are internal losses taken into account in the budget process / are budgeted for?

To effectively ascertain that internal loss data was being used effectively as an Operational Risk Management tool, the extent to which internal loss data is taken into account in the budgeting process is important. The results are summarised as below:

Table 5.2. The extent in which internal losses are taken into account in budget processes

	To a Very Great Extent	To a Great Extent	Somewhat	To a Small Extent	To A Very Small Extent
n	5	10	15	3	6
%	13%	26%	38%	8%	15%

As shown in table 5.3.1.2 above, 38% of respondents demonstrate that internal loss data is Somewhat budgeted for, with 26% showing that the loss data is included in budget processes To a Great Extent. 15% of the respondents showed that the loss data is included in budget processes To a Very Small Extent, 13% show loss data to be included To a very Great Extent and 8% show that the loss data is included To a Small Extent.

5.3.1.3 To what extent are Operational Risk managers involved in management of boundary events?

In order to effectively manage the risk, Operational Risk managers need to be involved in the management of boundary events, the table below demonstrates the extent in which the Operational Risk managers were involved in management of the boundary events according to the sample.

Table 5.3.1.3: Involvement of Operational Risk Management in Boundary events

	To a Very Great Extent	To a Great Extent	Somewhat	To a Small Extent	To A Very Small Extent
n	9	13	14	2	1
%	23%	33%	36%	5%	3%

Table 5.3.1.3 above indicates that majority of respondents' show that Operational Risk managers are involved in the management of the boundary events, 33% show the involvement To a Great Extent, 23% show To a very Great Extent. However 36% of the respondents showed that Operational Risk managers are Somewhat involved in management of boundary events, with a very low percentage showing involvement To a Small Extent (5%) and To a Very Small Extent (3%).

5.3.1.4 To what extent are recoveries linked to Operational Risk losses?

In order to show a true picture of the Operational Risk loss amounts, recoveries as a result of Operational Risk losses should be linked to the said loss amounts and a net of recoveries be calculated. The table below show the responses with regard to the extent in which recoveries were considered in the calculation of the Operational Risk losses.

Table 5.3.1.1: Recoveries Linked to Operational Risk Losses

	To a Very Great Extent	To a Great Extent	Somewh at	To a Small Extent	To A Very Small Extent
n	14	16	7	1	1
%	36%	41%	18%	3%	3%

According to Table 5.3.1.4 above, a very high percentage of respondents indicated that recoveries are linked to the Operational Risk losses To a Great Extent (41%), followed by 36% of respondents who indicated To a Very Great Extent. Only 18% indicate that Operational Risk losses are somewhat linked to recoveries and a low percentage indicated To a Small extent (3%) and 3% showed To a Very Small Extent.

5.3.1.5 To what extent are Operational Risk losses used to inform KRIs, RCSAs and Risk Scenarios (this section covers Question5, 6 and 7)

Basel II requires that internal and external loss data be used to validate outputs of other Operational Risk tools such as KRIs and RCSAs. It is also critical for banks to have collated internal loss data and use external loss data as inputs to risk scenario calculation. Tables below summarises the extent to which the internal and external loss data was used as input into other Operational Risks tools, notably KRIs, RCSAs and risk scenarios.

Table 5.3.1.2: Operational Risk Losses used to inform KRIs

	To a Very Great Extent	To a Great Extent	Somewhat	To a Small Extent	To A Very Small Extent
n	14	14	9	1	1
%	36%	36%	23%	3%	3%

Table 5.3.1.5 show that the majority of respondents indicated that Operational Risk loss data is used to inform KRIs both To a Very Great Extent (36%) and To a Great Extent (36%). Only 23% of respondents showed that Operational Risk data is Somewhat used to inform KRIs and a very small percentages indicated the use of loss data to inform KRIs To a Small Extent (3%) and To a very Small Extent (3%).

5.3.1.6 To what extent are Operational Risk losses used to inform RCSA?

Table 5.3.1.3: Operational Risk Losses used to inform RCSAs

	To a Very Great Extent	To a Great Extent	Somewhat	To a Small Extent	To A Very Small Extent
n	14	13	10	2	0
%	36%	33%	26%	5%	0%

As per table 5.3.1.6 above, majority of respondents indicated that Operational Risk loss data is used to inform RCSAs To a Very Great Extent (36%) and To a Great Extent (33%). Only 26% of respondents showed that Operational Risk data is Somewhat used to inform RCSAs and a very small percentages indicated the use of loss data to inform RCSAs To a Small Extent (5%) and one of the respondents indicate the use of loss data to inform RCSAs To a very Small Extent.

5.3.1.7 To what extent are Operational Risk losses used to inform Risk Scenarios?

Table 5.3.1.4 Operational Risk losses used to inform Risk Scenarios

	To a Very Great Extent	To a Great Extent	Somewhat	To a Small Extent	To A Very Small Extent
n	22	14	3	0	0
%	56%	36%	8%	0	0

Table 5.3.1.7 above indicate that an overwhelming majority of respondents showed that loss data is used to inform Risk Scenarios To a Very Great Extent (56%) and To a Great Extent (36%). Only 8% of the respondents indicated that loss data is Somewhat used to inform Risk Scenarios and 0% indicated the use of loss data both To a Small Extent and To a Very Small Extent.

5.3.1.8 To what extent are material or significant losses identified brought to attention of senior management?

It is important for management to be aware of significant losses in order to put mitigating controls or manage the risks from recurring. The table below provides a summary of the extent to which material losses were brought to the attention of the senior management.

Table 5.3.1.5 Material / Significant losses brought to management attention

	To a Very Great Extent	To a Great Extent	Somewhat	To a Small Extent	To A Very Small Extent
n	26	11	2	0	0
%	67%	28%	5%	0%	0%

The results presented in table 5.3.1.8 above show that, a great majority of respondents showed that material or significant losses are brought to management attention, with 67% indicating To a Very Great Extent and 28% showing To a Great Extent. Only 5% of the respondents indicated that material losses are Somewhat brought to management attention. None of the responses indicated that losses are brought to management either To a Small Extent or To a Very Small Extent.

5.3.1.9 To what extent does the actual loss data align to financial data?

It is imperative that Operational Risk data align to financial information as recorded in financial system such as general ledger. It is vital for management to ensure alignment of Operational Risk losses and financial data when making business decisions. The table below presents the response with regard to the extent in which Operational loss data align to financial data.

Table 5.3.1.6: Operational loss data alignment to financial data

	To a Very Great Extent	To a Great Extent	Somewhat	To a Small Extent	To A Very Small Extent
n	11	19	6	2	1
%	28%	49%	15%	5%	3%

Table 5.3.1.9 above show that, a high percentage of respondents indicated that Operational loss data align to financial data to To Great Extent (49%) and 28% showing To a Very Great Extent. 15% of respondents indicated that Operational Risk loss data Somewhat align to financial data. Only 5% of responses indicated that loss data aligns to financial data To a Small extent and 3% show alignment To a Very Small Extent.

5.3.1.10 To what extent does a bank's Operational Risk measurement system use relevant external data (either public data and/or pooled industry data)?

It is key that a bank only use the relevant external data, since the publicly available data is often varied. Table 5.3.1.10 below provides the responses given by the sample with regard to the use of relevant external data.

Table 5.3.1.7: Use of relevant external loss data

	To a Very Great Extent	To a Great Extent	Somewhat	To a Small Extent	To A Very Small Extent
n	7	16	11	4	1
%	18%	41%	28%	10%	3%

Table 5.3.1.10 illustrate that overall responses show that relevant external loss data is used To a Great Extent (41%) and To a Very Great Extent (18%). 28% indicate that relevant external data is Somewhat used and 10% indicate external data is used To a Small Extent with only 3% indicating the use of external data To a Very Small Extent.

5.3.1.11 To what extent does a bank have a systematic process for determining the situations for which external data must be used and the methodologies used to incorporate the data (e.g. scaling, qualitative adjustments, or informing the development of improved scenario analysis)?

In most cases, external data is used for scenario analysis or analysis of the internal control environment, as such it is important to ensure that data that feeds into the above analysis is credible and there are methodologies which provide guidance in how to use the data. The table below shows the responses given by the sample with regards to the use of systematic processes and methodologies in selecting external loss data.

Table 5.3.1.8: Systematic processes in place and methodologies available on how to use external loss data

	To a Very Great Extent	To a Great Extent	Somewhat	To a Small Extent	To A Very Small Extent
n	6	16	10	6	1
%	15%	41%	26%	15%	3%

Table 5.3.1.11 above shows that responses to this question are almost similar to the question above on the use of relevant external data. Most of the respondents (41%) show that systematic processes and methodologies on how to use external data are available to To a Great Extent and To a

Very Great Extent (15%). However 26% indicate that systematic processes and methodologies are Somewhat available, with 15% indicating that these processes and methodologies are availability To a Small Extent and only 3% indicating To a Very Small Extent.

5.3.2 Key Risk Indicators (KRIs)

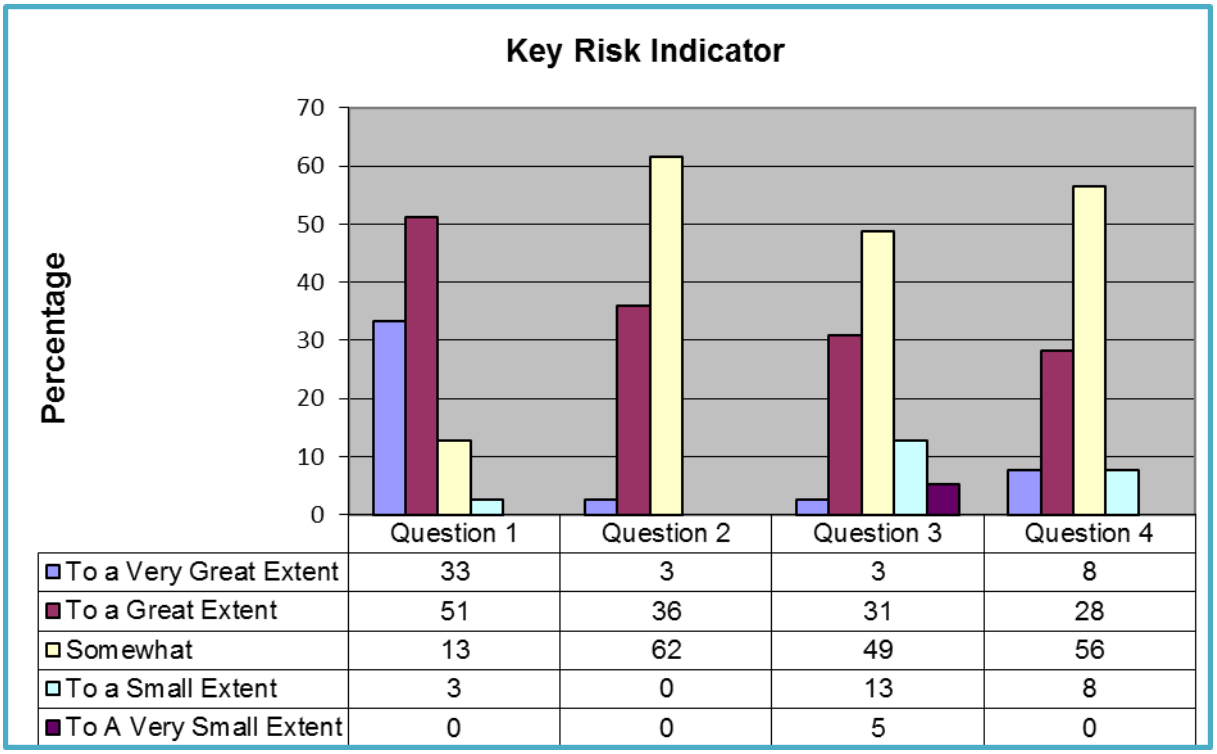
Key Risk Indicators remains a key tool in Operational Risk Management since they provide early warning of a potentially serious risk which is about to materialise. In order to assess whether the Basel II requirements pertaining to KRIs are being met by South African banks who are using Advanced Measurement Approach for Operational Risk capital calculations, the following questions were asked:

Table 5.2: Key Risk Indicators Questions

Question 1	To what extent are the risks identified key to the business i.e. if they materialise will have significant impact to the business?
Question 2	To what extent do indicators adequately reflect the underlying risk i.e. an effective KRI will be correlated to risk exposure? For example, does an increase in the number of complaints received provide adequate reflection of the risk of an inefficient process?
Question 3	To what extent does management make decisions based on the defined KRIs i.e. the KRIs provides relevant information which is able to produce tangible results from which to make decisions?
Question 4	To what extent does the change in the KRI reflect a change in the level of risk to the business in line with agreed appetite and tolerance levels i.e. threshold are not set too high/low?

The consolidated results per the above questions are graphically presented below:

Figure 5.4: Overall Key Risk Indicator Responses



	Question 1	Question 2	Question 3	Question 4
To a Very Great Extent	33	3	3	8
To a Great Extent	51	36	31	28
Somewhat	13	62	49	56
To a Small Extent	3	0	13	8
To A Very Small Extent	0	0	5	0

The next section discusses the results of the above questions. The interpretation of these results per question and per tool will be discussed in the next chapter.

5.3.2.1 To what extent are the identified risks key to the business i.e. if they materialise will have significant impact to the business?

In order for management to focus their attention on material risks it is important that only risks that are key to the business are identified, indicated, assigned and tracked periodically. The table below provides a summary of feedback received from respondents on the identification of risks which were key to the business.

Table 5.3.2.1: Risks identified is key to the business

	To a Very Great Extent	To a Great Extent	Somewhat	To a Small Extent	To A Very Small Extent
n	13	20	5	1	0
%	33%	51%	13%	3%	0%

The results in table 5.3.2.1 above show that majority of respondents indicated that risks identified are To a Great Extent (51%) and To a Very Great Extent (33%) key to the business. Only 13% of respondents indicated that risks identified are Somewhat key to the business and 3% show that To a Small Extent risk identified are key to the business. None of the respondents show that risks identified are To a Very Small Extent key to the business.

5.3.2.2 To what extent do indicators adequately reflect the underlying risk i.e. an effective KRI will be correlated to risk exposure? For example, does an increase in the number of complaints received provide adequate reflection of the risk of an inefficient process?

In order for a KRI to be relevant and add value to the Operational Risk Management, it needs to present useful information about risks exposures and it should be used to observe the risks associated with them, the extent in which the indicators adequately reflect the underlying risks was taken into account. The results are presented below:

Table 5.3.2.2: Reflection of underlying risk

	To a Very Great Extent	To a Great Extent	Somewhat	To a Small Extent	To A Very Small Extent
n	1	14	24	0	0
%	3%	36%	62%	0%	0%

Table 5.3.2.2 above illustrates that an overwhelming majority (62%) of respondents showed that indicators “Somewhat” adequately reflect the underlying risk. Only 36% and 3% showed that the indicators adequately reflect the underlying risk “To a Great Extent” and “To a Very Great Extent” respectively. None of the response indicated “To a Small Extent” and “To a Very Small Extent”.

5.3.2.3 To what extent does management make decisions based on the defined KRIs i.e. the KRIs provides relevant information which is able to produce tangible results from which to make decisions?

To effectively ascertain that KRIs provided relevant information for decision making, the extent that management make decisions based on defined KRIs was considered. The results are summarised below:

Table 5.3.2.3: Management makes decisions based on the defined KRIs

	To a Very Great Extent	To a Great Extent	Somewhat	To a Small Extent	To A Very Small Extent
n	1	12	19	5	2
%	3%	31%	49%	13%	5%

Table 5.3.2.3 above indicate that a large number (49%) of respondents indicated that management "Somewhat" make decisions based on the defined KRIs. 31% and 3% showed that management make decisions based on the defined KRIs To a Great Extent and To a very Great extent respectively. A 13% of respondents indicated that management make decisions based on the defined KRIs To a Small Extent and 5% showed To a Very small extent.

5.3.2.4 To what extent does the change in the KRI reflect a change in the level of risk to the business in line with agreed appetite and tolerance levels i.e. threshold are not set too high/low?

In order for a KRI to be effective, it should truly reflect a level of risk to the business and the table below shows the responses given by the sample with regard to correlation of KRIs and the underlying risk to the business.

Table 5.3.2.4: Change in the KRI reflect a change in the level of risk

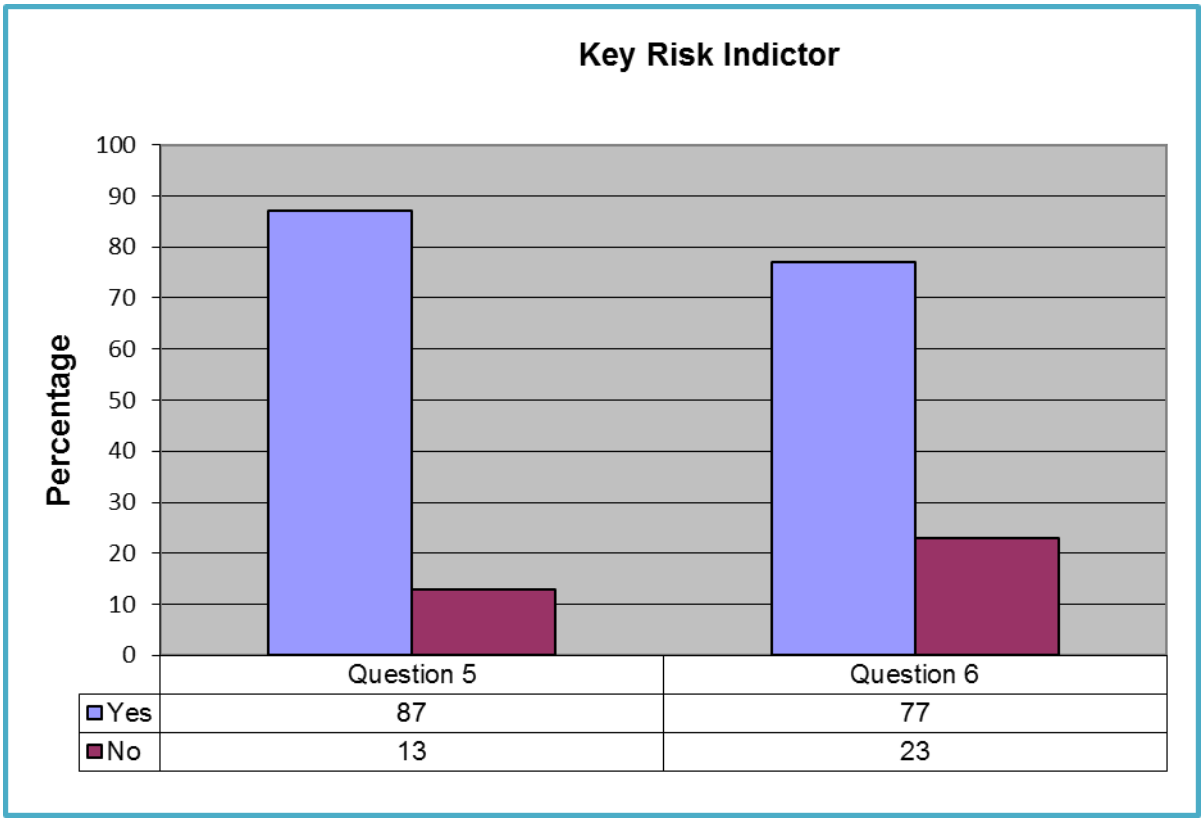
	To a Very Great Extent	To a Great Extent	Somewhat	To a Small Extent	To A Very Small Extent
n	3	11	22	3	0
%	8%	28%	56%	8%	0%

The table above shows that majority (56%) of the respondents indicated that Somewhat a change in KRIs reflect a change in the level of risk to the business in line with agreed appetite and tolerance levels. Only 28% of the respondents indicated that To a Great Extent a change in KRIs reflect a change in the level or risk, followed by 8% of respondents who indicated To a small extent and To a very Great extent. 0% indicated To a Very Small Extent.

5.3.2.5 Does the bank have a system (reliable source) where KRIs are captured?

To ascertain that the KRIs information used is credible, the bank use of Operational Risk Management information to capture KRIs was considered. The results are presented below:

Figure 5.5 Systems available to capture KRIs



According to figure 5.5 above a large number (87%) of respondents said "yes" there are systems to capture KRIs, and only 13% indicated that there are "no" systems to capture KRIs.

5.3.2.6 Does KRIs result in risk management actions within other AMA elements, for example, a KRI breach should be used to verify the RCSA values, and possible reassessment of the RCSA?

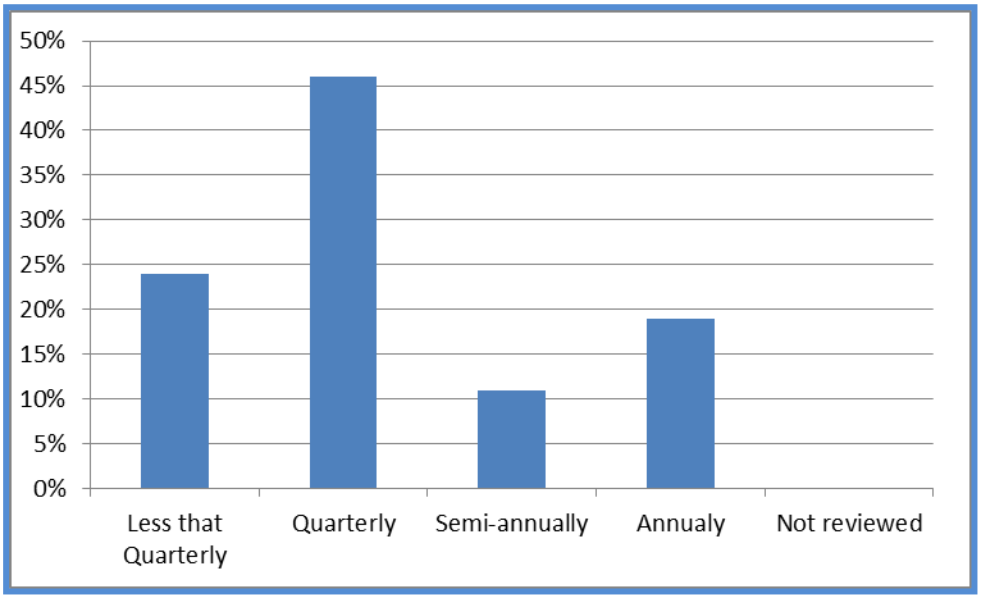
In order to manage Operational management effectively, Operational Risk tools should be aligned with one another. The table below shows the responses given by the sample with regard to the alignment of the KRIs to other Operational Risk tools.

As shown in figure 5.3.2.2 above a high percentage (77%) of respondents said “yes” KRIs result in risk management actions within other AMA elements, and only 23% answered “No”.

5.3.2.7 At what frequencies are KRIs reviewed to ensure relevancy?

In order to ensure relevancy, KRIs need to be reviewed and updated periodically and the graph below show the responses given by the sample with regard to frequency of the review.

Figure 5.6 Review of KRIs



A large number (46%) of respondents declared that KRIs are review quarterly, as shown in the figure above, followed by 24% of respondents indicating that KRIs are reviewed less that quarterly. 19% of respondents indicate that KRIs are reviewed annually and 11% indicated a bi (semi) annual review.

5.3.3 Risk and Controls Self-Assessment (RCSA)

Risk and Controls Self-Assessment (RCSA) is one of the key tools in Operational Risk Management as mentioned in the literature review. This tool is used where banks internal processes are assessed against threats and weaknesses and the effectiveness of the control environment is considered (BCBS, 2011). In order to assess whether the Basel II requirements pertaining to KRIs are being met by South African banks who were using the Advanced Measurement Approach for Operational Risk capital calculations, the following questions were asked:

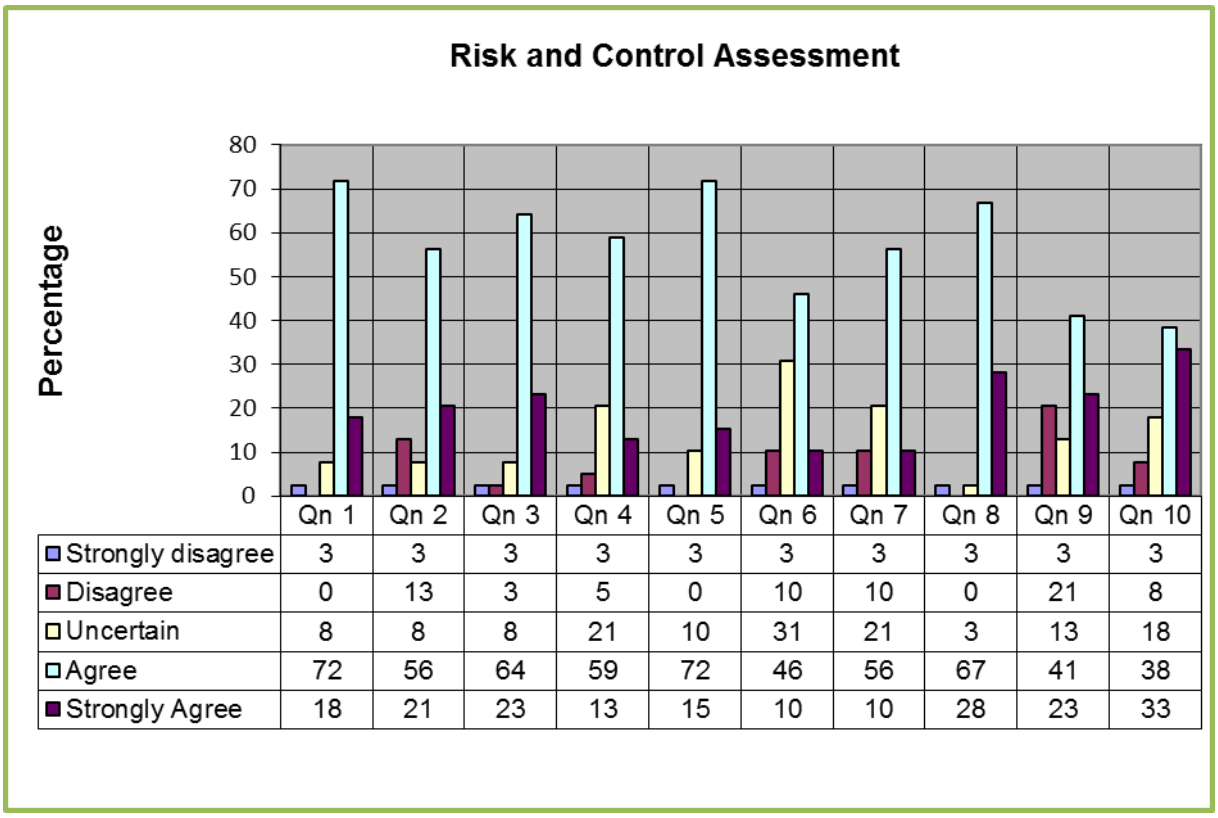
Table 5.3 Risk and Controls Self Assessment Questions

Question 1	Impact and the likelihood are adequately reflected in the inherent risk levels and reflect the market and operating conditions of the business. For example: does a change in the business environment, such as a new legislation, reflect an increase in the likelihood of the risk of a regulatory fine?
Question 2	Inherent risk levels are re-assessed at least quarterly or when business environment and control factors change?
Question 3	All controls identified are actual and existing controls i.e. controls that identified are actually a measure that is in place to mitigate the risk and not an action plan?
Question 4	The effectiveness of controls are an accurate representation of

	the way the controls are functioning in the business?
Question 5	The inherent risk levels and the control effectiveness are adequately reflected in the residual risk level i.e. the residual risk assessment should not be higher than inherent risk levels?
Question 6	Residual risk levels are aligned to related findings by internal audit i.e. does internal audit rating of the risk and control align to the rating of the risk and control in the RCSA?
Question 7	RCSA's result in risk management actions within other AMA elements, for example do the actions result in a new/revised KRI, the creation/review of a risk scenario?
Question 8	RCSAs are subject to periodic review to ensure relevance and consistency?
Question 9	KRI's, Internal losses, Audit findings directly informative to the RCSA's?
Question 10	RCSAs are used as an input into the Risk Scenarios?

The overall results of the above questions for RCSAs are presented below and the results for each are presented in the following sections:

Figure 5.1 Risk and Control Self-Assessment overall results



	Qn 1	Qn 2	Qn 3	Qn 4	Qn 5	Qn 6	Qn 7	Qn 8	Qn 9	Qn 10
Strongly disagree	3	3	3	3	3	3	3	3	3	3
Disagree	0	13	3	5	0	10	10	0	21	8
Uncertain	8	8	8	21	10	31	21	3	13	18
Agree	72	56	64	59	72	46	56	67	41	38
Strongly Agree	18	21	23	13	15	10	10	28	23	33

Below is a discussion of the above questions relating to RCSAs.

5.3.3.1 Impact and the likelihood are adequately reflected in the inherent risk levels and reflect the market and operating conditions of the business. For example: does a change in the business environment, such as a new legislation, reflect an increase in the likelihood of the risk of a regulatory fine?

According to the Sounds Practices of Operational RiskRisk Management (2010) paper the business inherent risk level should fairly present the impact and likelihood of the risk; the table below provides the result of responses with regard to the fair presentation of the inherent risk levels in RCSAs processes.

	Strongly disagree	Disagree	Uncertain	Agree	Strongly Agree
n	1	0	3	28	7
%	3%	0%	8%	72%	18%

It is clear from table 5.3.3.1 above, that in overall respondents agreed that Impact and the likelihood are adequately reflected in the inherent risk levels and reflect the market and operating conditions of the business. A 72% Agreed, 18% Strongly Agreed and only 8% of the respondents were uncertain and 3% Strongly disagreed.

5.3.3.2 Inherent risk levels are re-assessed at least quarterly or when business environment and control factors change.

In order for the RCSAs to stay relevant and useful to the business, periodic update is important or an update whenever the business change is necessary. The results with regard to the continuous update and assessment of Inherent risk are summarised as follows:

Table 5.3.3.2 Inherent risk re-assessed when business environment and control factors change?

	Strongly disagree	Disagree	Uncertain	Agree	Strongly Agree
n	1	5	3	22	8
%	3%	13%	8%	56%	21%

Table 5.3.3.2 indicate that a large majority (56%) Agreed followed by 21% Strongly Agreed that the inherent risk levels are re-assessed at least quarterly when the business environment changes. A 13% of respondents disagreed, 8% were uncertain and only 3% Strongly disagreed.

5.3.3.3 All controls identified are actual and existing controls i.e. controls that identified are actually a measure that is in place to mitigate the risk and not an action plan?

In order to assess the residual risk, only existing controls were considered and the table below shows the responses given by the sample with regard to the use of actual and existing controls in completion of the RCSAs.

Table 5.3.3.3 *All controls identified are actual and existing controls?*

	Strongly disagree	Disagree	Uncertain	Agree	Strongly Agree
n	1	1	3	25	9
%	3%	3%	8%	64%	23%

Table 5.3.3.3 above show that a high percentage (64%) Agreed and 23% Strongly Agreed that controls identified are actual and existing controls. 8% of the respondents were Uncertain and 3% disagreed and another 3 Strongly disagreed.

5.3.3.4 The effectiveness of controls are an accurate representation of the way the controls are functioning in the business.

To effectively assess the residual risk in the RCSAs process, the effectiveness of controls should be assessed and the table below illustrates the responses given by the sample with regard to the true presentation of the control effectiveness.

Table 5.3.3.4 The effectiveness of controls are an accurate representation of the way the controls are functioning in the business?

	Strongly disagree	Disagree	Uncertain	Agree	Strongly Agree
n	1	2	8	23	5
%	3%	5%	21%	59%	13%

As per table 5.3.3.4 above, majority (59%) of the respondents Agree and 13% Strongly Agree that the effectiveness of controls are a true representation of the way controls are functioning in the business. A 21% of respondents were Uncertain and only 5% and 3% Disagreed and Strongly Disagreed respectively.

5.3.3.5 The inherent risk levels and the control effectiveness are adequately reflected in the residual risk level? i.e. the residual risk assessment should not be higher than inherent risk levels?

To effectively determine the residual risk levels, the inherent risk and control effectiveness should be aligned (Sounds practices for Operational Risk Management). The results on whether there is an alignment between the inherent risk and controls effectiveness are presented in table 5.3.3.5 below:

Table 5.3.3.5 The inherent risk levels and the control effectiveness are adequately reflected in the residual risk level? i.e. the residual risk assessment should not be higher than inherent

	Strongly disagree	Disagree	Uncertain	Agree	Strongly Agree
n	1	0	4	28	6
%	3%	0%	10%	72%	15%

Table 5.3.3.5 shows that an Overall majority Agree (72%) and Strongly Agree (15%) that the residual risk is a true reflection of inherent and control effectiveness. Only 10% were Uncertain and 3% Strongly Disagreed.

5.3.3.6 Residual risk levels are aligned to related findings by internal audit i.e. does internal audit rating of the risk and control align to the rating of the risk and control in the RCSA?

In order to improve the control environment, it is important that internal audit assessment aligns to the controls assessment by Operational Risk managers. The table below illustrates the responses received by the sample on the control environment assessment by internal audit and Operational Risk function.

Table 5.3.3.6 Residual risk levels are aligned to related findings by internal audit i.e. does internal audit rating of the risk and control align to the rating of the risk and control in the RCSA?

	Strongly disagree	Disagree	Uncertain	Agree	Strongly Agree
n	1	4	12	18	4
%	3%	10%	31%	46%	10%

Table 5.4.3.6 above indicates that a high percentage (46%) Agreed that RCSAs risk ratings align to Internal Audit controls assessment. However 31% were Uncertain and 10% Strongly Agreed and another 10% Disagreed. Only 3% Strongly disagreed.

5.3.3.7 RCSA's result in risk management actions within other AMA elements, for example do the actions result in a new/revised KRI, the creation/review of a risk scenario?

In order to manage Operational Risk, it is important that the results of Operational Risk tools are aligned. The results on whether RCSA results inform other Operational Risk tools are provided in table 3.7 below.

Table 5.3.3.7 RCSA's result in risk management actions within other AMA elements?

	Strongly disagree	Disagree	Uncertain	Agree	Strongly Agree
n	1	4	8	22	4
%	3%	10%	21%	56%	10%

Table 5.3.3.7 above shows that a large number (56%) “Agreed” and 10%”Strongly Agreed” that RCSAs result in risk management actions within other AMA elements. 21% of respondents were “Uncertain” and 10% “Disagreed”. Only 3% “Strongly disagreed”.

5.3.3.8 RCSAs are subject to periodic review to ensure relevance and consistency.

In order for the RCSAs to stay relevant, they need to be reviewed periodically and the table below show responses with regard to the periodic review of RCSAs.

Table 5.3.3.8 ***RCSAs review to ensure relevance and consistency?***

	Strongly disagree	Disagree	Uncertain	Agree	Strongly Agree
n	1	0	1	26	11
%	3%	0%	3%	67%	28%

Table 5.3.3.8 illustrate that an overwhelming majority (67%) Agreed and 28% Strongly Agreed that RCSAs are subject to a periodic review to ensure relevancy and consistency. Only 3% were Uncertain and another 3% Strongly Disagreed.

5.3.3.9 KRI's, Internal losses, Audit findings directly informative to the RCSA's.

To effectively assess that RCSA information, the use of other Operational tools data was taken into account. The results are summarised below:

Table 5.3.3.9 KRI's, internal losses, Audit findings directly informative to the RCSA's.

	Strongly disagree	Disagree	Uncertain	Agree	Strongly Agree
n	1	8	5	16	9
%	3%	21%	13%	41%	23%

According to table 5.3.3.9 above a vast majority (41%) “Agreed” and 23% “Strongly Agreed” that KRIs, Internal losses and Audit findings directly informs RCSAs. However 21% “Disagreed” with 13% “Uncertain” and only 3% “Strongly Disagreeing”.

5.3.3.10 RCSAs are used as an input into the Risk Scenarios.

To effectively assess the risk scenarios, the results of RCSA were used as an input and the table below provides a summary with regard to the use of RCSA input in Risk Scenarios analysis.

Table 5.3.3.10 RCSAs used as an input into the Risk Scenarios.

	Strongly disagree	Disagree	Uncertain	Agree	Strongly Agree
n	1	3	7	15	13
%	3%	8%	18%	38%	33%

Table 5.3.3.10 above shows that a high number (38%) Agreed and 33% Strongly Agreed that RCSA are input to Risk Scenario analysis. Only 18% were Uncertain, 8% Disagreed and 3% Strongly Disagreed.

5.3.4 Internal Audit Findings

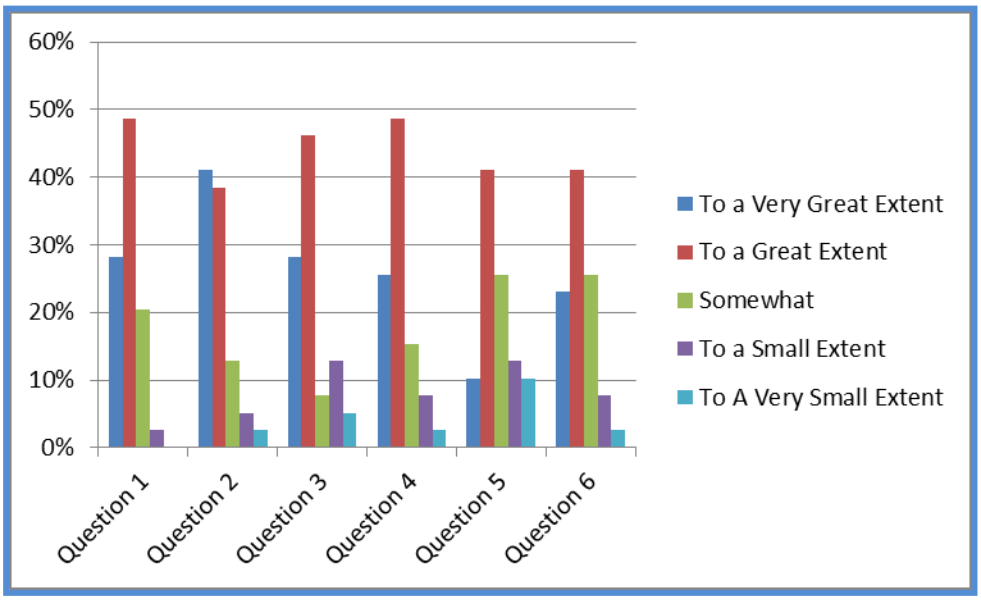
Effective risk management warrant internal audit to act as a third line of defense where an independent review of the Operational Risk Management, controls and systems is conducted. As such, internal audit findings are used as a tool in managing Operational Risk. In order to assess whether this tool was used effectively by AMA banks the following questions were asked:

Table 5.4: Internal Audit Findings Questions

Question 1	To what extent do you align the view of Internal Audit in Operational Risk Management?
Question 2	To what extent does Internal Audit review and challenge the bank's Operational Risk Management, controls, processes and systems.
Question 3	To what extent does Internal Audit take into account the result of RCSA when conducting audit reviews?
Question 4	To what extent does Internal Audit take into account Operational Risk breakdowns and losses during their audit review?
Question 5	To what extent does the result of RCSA align to Internal Audit findings?
Question 6	To what extent does Internal Audit evaluate whether Operational Risk Management frameworks meet organisational needs and supervisory expectations? For example, while Internal Audit should not be setting specific risk tolerance or appetite, it should review the robustness of the process of how the limits are set; including why and how they are adjusted in response to changing circumstances.

The overall results of the above questions for the use of Internal Audit findings are presented below and results for each are presented in the following sections:

Figure 5.7 Internal Audit Findings Consolidated Results



The next section discusses each of the questions in turn and presents the results of each. The interpretation of these results per question and per tool is discussed in the next chapter.

5.3.4.1 To what extent do you align the view of Internal Audit in Operational Risk Management?

In order to manage Operational Risk effectively, the internal audit view needed to be considered and the table below shows the responses given by the sample with regard to the alignment of the internal audit view in Operational Risk Management.

Table 5.3.4.1 Internal Audit's views aligned to Operational Risk Management

	To a Very Great Extent	To a Great Extent	Somewhat	To a Small Extent	To A Very Small Extent
n	11	19	8	1	0
%	28%	49%	21%	3%	0%

Table 5.3.4.1 shows that a high number of respondents answered that Internal Audit views are aligned to ORM To a Great Extent (49%) and To a Very Great Extent (28%). However 21% indicated that Somewhat the internal audit views aligns to ORM and only 3% showed that they align To a Small Extent.

5.3.4.2 To what extent does Internal Audit review and challenge the bank's Operational Risk Management, controls, processes and systems?

In order for the internal audit to provide an independent assurance, it is important for internal auditors to review and challenge the Operational Risk Management process, controls and systems. The responses on the internal audit review and challenge of Operational Risk processes, controls and system is provided in table 4.2 below.

Table 5.3.4.2 ***Internal Audit review and challenge Operational Risk Management practices***

	To a Very Great Extent	To a Great Extent	Somewhat	To a Small Extent	To A Very Small Extent
n	16	15	5	2	1
%	41%	38%	13%	5%	3%

Table 5.3.4.2 above shows that majority (41%) indicated that internal audit review and challenge ORM practices To a Very Great Extent and 38% indicated To a Great Extent. Only 13% showed that internal audit Somewhat challenges ORM practices, 5% and 3% showed To a Small Extent and To a Very Small Extent respectively.

In order to assess the Operational Risk control environment, it is important that internal audit considers all other factors and tools which had an

influence on their findings. To effectively assess the internal audit considerations of other factors tables 5.3.4.3, 5.3.4.4 and 5.3.4.5 provide summary of results provided by the sample on internal audit consideration of other factors:

Table 5.3.4.3 Internal Audit considers RCSA results when conducting audit reviews

	To a Very Great Extent	To a Great Extent	Somewhat	To a Small Extent	To A Very Small Extent
n	11	18	3	5	2
%	28%	46%	8%	13%	5%

Table 5.3.4.3 illustrate that a high number (46%) indicated that Internal audit considers RCSA results when conducting reviews To a Great Extent and 28% To a Very Great Extent. Only 13% responses showed To a Small Extent, followed by 8% indicating Somewhat and 5% showed To a Very Small Extent.

5.3.4.3 Internal Audit considers Operational Risk breakdowns and losses during their audit review

Table 5.3.4.4 Internal Audit considers Operational Risk breakdowns and losses during their audit review

	To a Very Great Extent	To a Great Extent	Somewhat	To a Small Extent	To A Very Small Extent
n	10	19	6	3	1
%	26%	49%	15%	8%	3%

According to table 5.3.4.4 a large percentage (49%) responded that Internal Audit considers Operational Risk breakdowns and losses during their audit To a Great Extent and 26% To a very Great Extent. A small percentage (15%) showed that Internal audit Somewhat consider Operational Risk breakdown and losses during their audit review and 8% and 3% indicated To a Small Extent and To a Very Small Extent respectively.

5.3.4.4 Result of RCSA align to Internal Audit findings

Table 5.3.4.5 Result of RCSA align to Internal Audit findings

	To a Very Great Extent	To a Great Extent	Somewhat	To a Small Extent	To A Very Small Extent
n	4	16	10	5	4
%	10%	41%	26%	13%	10%

Table 4.5 shows that a fair number (41%) of respondents indicate that results of RCSA align to Internal Audit Findings To a Great Extent and 10% answered To A Very Great Extent. However 26% of the respondents indicated that RCSA results Somewhat align to Internal Audit Findings. Only 13% and 10% indicate that RCSA align to Internal Audit Findings To a Small Extent and To a Very small Extent respectively.

5.3.4.5 To what extent does Internal Audit evaluate whether Operational Risk Management frameworks meet organisational needs and supervisory expectations? For example, while Internal Audit should not be setting specific risk tolerance or appetite, it should review the robustness of the process of how the limits are set; including why and how they are adjusted in response to changing circumstances.

Internal audit need to provide assurance on the organisations functions. They need to evaluate whether or not Operational Risk Management meet both the organisational need and supervisory expectation. A summary of responses on the internal audit evaluation of Operational Risk Management is provided on table 4.6 below:

Table 5.3.4.6 Internal Audit evaluates ORM frameworks against banks need and supervisory requirements

	To a Very Great Extent	To a Great Extent	Somewhat	To a Small Extent	To A Very Small Extent
n	9	16	10	3	1
%	23%	41%	26%	8%	3%

Table 5.3.4.6 above indicates that a large percentage (41%) responded that Internal Audit evaluates ORM Frameworks against banks need and supervisory requirements To a Great Extent and 23% To a very Great

Extent. However 26% showed that Internal Audit Somewhat evaluates ORM Frameworks against banks need and supervisory requirements. Only 8% and 3% indicate Internal Audit evaluates ORM frameworks against banks need and supervisory requirements To a Small Extent and To a Very small Extent respectively.

5.3.5 Results on Risk Scenarios

Risk Scenarios play an important role in the Operational Risk capital modeling, especially for banks that are on the Advanced Measurement Approach of Operational Risk. Risk Scenarios remain a key Operational Risk tool and in order to assess the use of this tool, the following questions were asked:

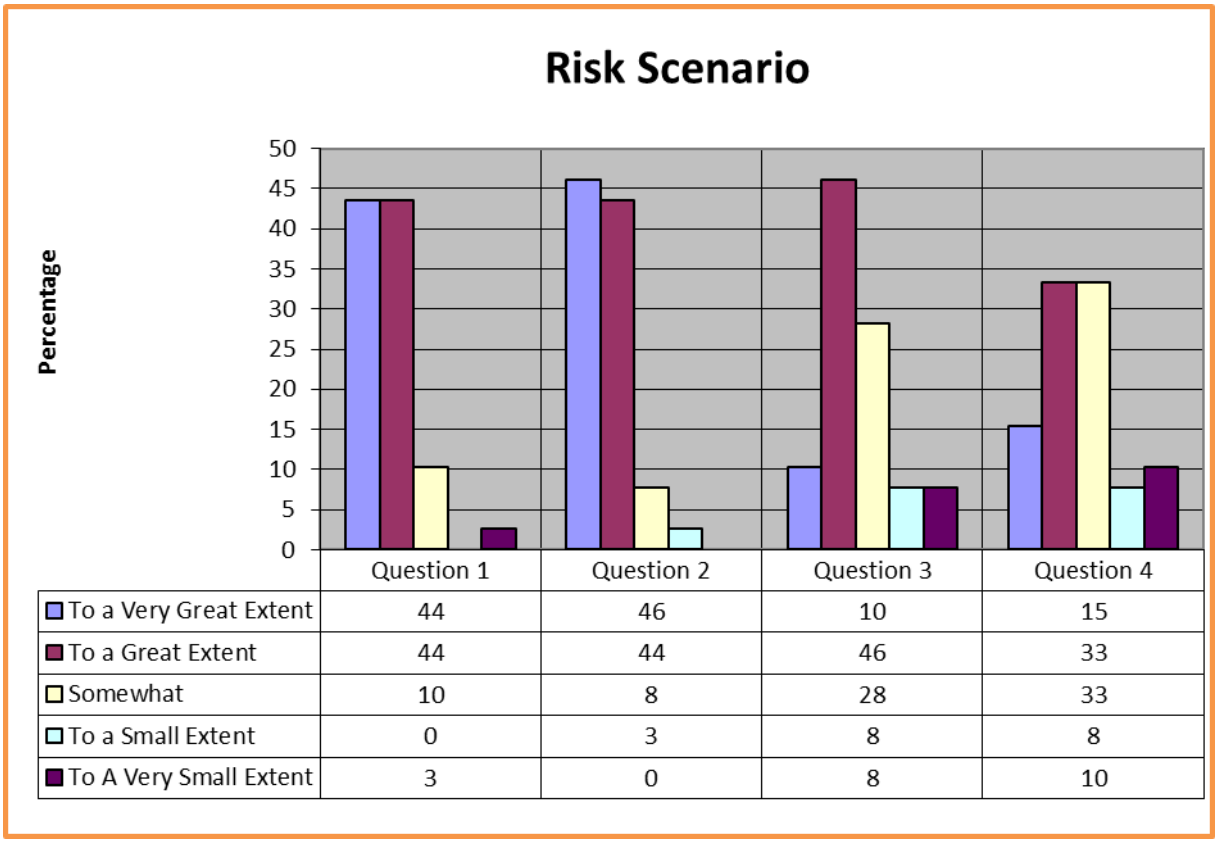
Table 5.5 Risk Scenarios Questions

Question 1	To what extent are Risk scenarios a reflection of the significant risks to your business?
Question 2	To what extent are all the risk information sources considered when defining risk scenarios i.e. internal and external data, RCSA, KRIs?
Question 3	To what extent is the Risk scenario information used to manage your business i.e. in risk reporting and decision-making (risk scenarios should inform other risk management processes i.e. KRI's, RCSA etc.)?

Question 4	To what extent do Risk scenarios result in management actions which are consistent with the output of the other AMA elements? For example, risk management actions point to the same actions as listed for KRI's, RCSA etc?
Question 5	Are Risk scenarios subject to periodic (semiannually/annually) review to ensure alignment with the results of the AMA i.e. the results of the RCSA, loss data and KRIs data etc.
Question 6	Are Risk scenarios based on the business expert judgment?
Question 7	Are Risk scenarios free of bias?
Question 8	Are Risk scenarios forward looking?
Question 9	Are Business Risk Scenarios subjected to independent validation e.g. by ERM, internal audit?

The overall results of the above questions for Risk Scenarios are presented

Figure 5.8 Overall Risk Scenarios Results



	Question 1	Question 2	Question 3	Question 4
To a Very Great Extent	44	46	10	15
To a Great Extent	44	44	46	33
Somewhat	10	8	28	33
To a Small Extent	0	3	8	8
To A Very Small Extent	3	0	8	10

The next section discusses each of the questions.

5.3.5.1 To what extent are Risk scenarios a reflection of the significant risks to your business?

To ascertain that Risk Scenarios are used effectively, only catastrophic risks should be taken into account .The table below present the result on consideration of significant risks in Risk Scenarios identification:

Table 5.3.5.1 Risk scenarios reflection of the significant risks to your business

	To a Very Great Extent	To a Great Extent	Somewhat	To a Small Extent	To A Very Small Extent
n	17	17	4	0	1
%	44%	44%	10%		3%

Table 5.3.5.1 shows that a majority (44%) indicated that Risk Scenarios reflect the significant risks To a Very Great Extent and 44% showed To a Great Extent. A very small percentage (10%) indicated that Risk Scenarios Somewhat reflect the significant risks to business with only 3% indicated To a Very Small Extent.

5.3.5.2 To what extent are all the risk information sources considered when defining risk scenarios i.e. internal and external data, RCSA, KRIs?

In order for Risk Scenarios to be meaningful all other risk sources should be considered, the extent of this consideration was taken into account and the results are presented in a table below:

Table 5.3.5.2 All the risk information sources are considered when defining risk scenarios i.e. internal and external data, RCSA, KRIs

	To a Very Great Extent	To a Great Extent	Somewhat	To a Small Extent	To A Very Small Extent
n	18	17	3	1	0
%	46%	44%	8%	3%	

Table 5.3.5.2 above indicate that a large number (46%) showed that all risk information sources are considered when defining risk scenarios To A very Great Extent and 44% indicated To a Great Extent. Only 8% indicated that risk information sources are Somewhat considered when defining risk scenarios and 3% indicated that risk information is considered To a Small Extent.

5.3.5.3 To what extent is the Risk scenario information used to manage your business i.e. in risk reporting and decision-making (risk scenarios should inform other risk management processes i.e. KRI's, RCSA etc.)?

In order to manage the Operational Risk, the Operational Risk results/ output has to be in such a way that allows for use in decision making. The table below shows the responses given by the sample with regards to the use of Risk Scenarios information in managing the business.

Table 5.3.5.3 Risk scenario information is used to manage your business

	To a Very Great Extent	To a Great Extent	Somewhat	To a Small Extent	To A Very Small Extent
n	4	18	11	3	3
%	10%	46%	28%	8%	8%

Table 5.3.5.3 above shows that a high number (46%) of responses indicated that risk scenario information is used to manage their business To a Great Extent. However 28% indicated that risk scenario information is Somewhat used to manage their business. 10% showed that the risk scenarios information is used to manage their business To a Great Extent. 8% mention that risk scenario information is used To a Very small Extent and another 8% indicated the use To a Small Extent.

5.3.5.4 To what extent do Risk scenarios result in management actions which are consistent with the output of the other AMA elements? For example, risk management actions point to the same actions as listed for KRI's, RCSA etc?

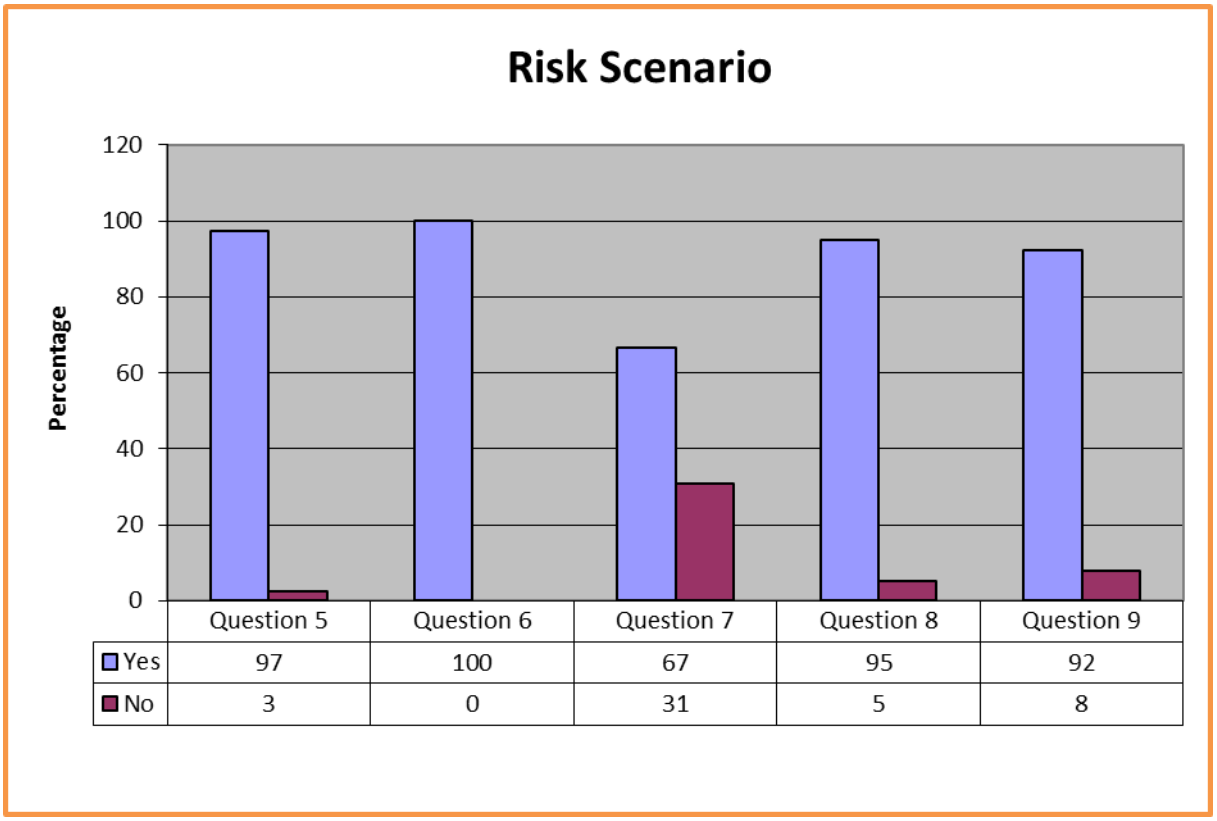
In order for the Risk Scenarios to remain current, the information taken into account in assessing them should be in line with information considered in other Operationalm risk tools. The table below provides a summary of the results with regard to the consistency of information used in Risk Scenarios and other Operational Risk Management tools.

Table 5.3.5.4 Risk scenarios result in management actions which are consistent with the output of the other AMA elements

	To a Very Great Extent	To a Great Extent	Somewhat	To a Small Extent	To A Very Small Extent
n	6	13	13	3	4
%	15%	33%	33%	8%	10%

Table 5.3.5.4 above show that the results on this questions were evenly spread with 33% of the responses indicating that risk scenario result in management actions To a Great Extent, another 33% shows that risk scenarios result Somewhat result in management actions which are consistent with the output of the other AMA elements. 15%, 10% and 8% show that risk cenarios result in management actions which are considered

with other output of the AMA elements To a Very Great Extent, To a Very Small Extent and To a Small Extent respectively.



5.3:2 Risk Scenarios – questions 5 to 9 overall results

5.3.5.5 Are Risk scenarios subject to periodic (semiannually/annually) review to ensure alignment with the results of the AMA i.e. the results of the RCSA, loss data and KRIs data etc.

In order for the Risk Scenarios to remain relevant, they need to be reviewed periodically and the table below shows the respondes on whether Risk Scenario were reviewed and updated periodically.

Table 5.3.5.5 Risk scenarios subject to periodic (semiannually/annually) review to ensure alignment with the results of the AMA

	Yes	No
n	38	1
%	97%	3%

Table 5.3.5.5 shows that 97% of the respondents answered “Yes” that risk scenarios are subject to periodic review, only 3% answered “No”.

5.3.5.6 Are Risk scenarios based on the business expert judgement?

In order for Scenarios to be effective, expert judjement should be used. The table below provides the responses given by the sample with regard to the use of the experts in defining Risk Scenarios.

Table 5.3.5.6 Risk scenarios based on the business expert judgement

	Yes	No
n	39	0
%	100%	0%

Table 5.3.5.6 shows that All the respondents agreed 100% that Risk Scenarios are based on the business expert judgement.

5.3.5.7 Are Risk scenarios free of bias?

To effectively ascertain the quiality of risk scenarios, the possible bias in the scenario identification was considered and the results are summarised below:

Table 5.3.5.7 Risk scenarios free of bias

	Yes	No
n	26	13
%	67%	33%

Table 5.3.5.7 above shows that majority (67%) of responses are of the view that Risk Scenarios are free of bias and only 33% answered “No”.

5.3.5.8 Are Risk scenarios forward looking?

Basel II requires risk scenarios to be forward looking, the extent into which rsk scenarios were forward looking was taken into accout and the results are summarised below in Table 5.3.5.8:

Table 5.3.5.8 Risk scenarios forward looking

	Yes	No
n	37	2
%	95%	5%

Overwhelming number (95%) indicate that Risk Scenarios are forward looking, and only 5% indicate that they are not.

5.3.5.9 Are Business Risk Scenarios subjected to independent validation e.g. by ERM, internal audit?

In order to ensure that Risk Scenarios represent the risks that the business was exposed to, the data presented should be validated independently and the table 5.9 shows the results of responses:

Table 5.3.5.9 Business Risk Scenarios subjected to independent validation e.g. by ERM, internal audit

	Yes	No
n	36	3
%	92%	8%

Table 5.3.5.9 above show that a high number (92%) of the respondents answered “Yes” that Risk Scenarios are subjected to independent validation and only 8% answered “No”.

Research question two: Part 2

5.3.6 Are Operational Risk Management tools integrated into day-to-day business processes and used as business risk management tools versus just regulatory capital calculation methods?

In order for management to be aware of their environment and risks intrinsic in their products and services, Operational Risk tools need to be integrated in business processes. In order to assess whether the Operational Risk tools are integrated into business processes the following questions were asked:

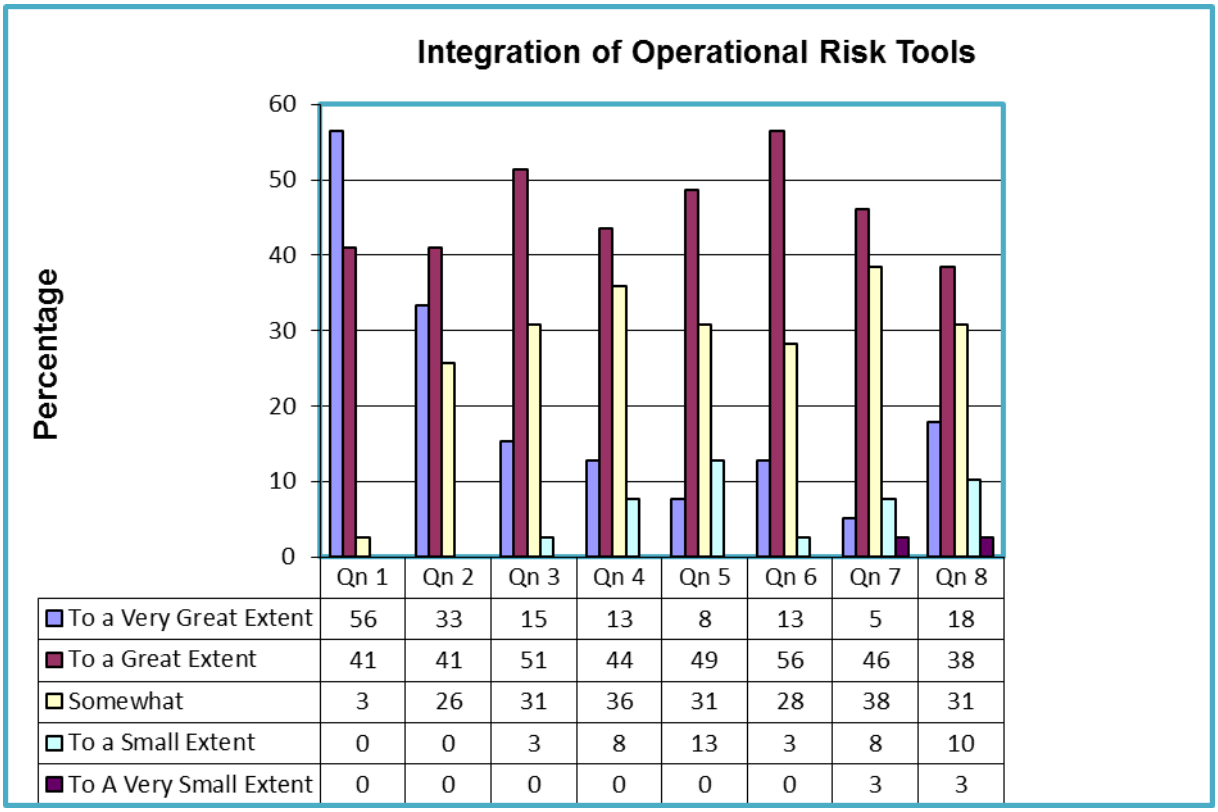
Table 6 Integration of Operational risk tools into day to day business processes

Question 1	To what extent does the bank have an independent Operational Risk Management function that is responsible for the design and implementation of the bank's Operational Risk Management framework?
Question 2	To what extent does the bank management understand the nature and complexity of Operational Risk inherent in portfolio of bank products, services and activities?
Question 3	To what extent is the Operational Risk culture embedded in the business?
Question 4	To what extent are the results of the bank's Operational Risk assessment incorporated into the overall bank business strategy development processes?

Question 5	To what extent does the bank business processes documented and regularly updated with changes to the business?
Question 6	To what extent are Operational Risk reports comprehensive, accurate, consistent and actionable across business lines and products?
Question 7	To what extent do Operational Risk staffs communicate effectively with staff responsible for managing credit, market and other risks?
Question 8	To what extent is Operational Risk training available throughout the business unit/organisation?

The overall results of the above questions for the Integration of the Operational Risk into business process are presented below but each question is discussed and results for each are presented in the following sections:

Figure 5.3:3 Integration of the Operational Risk tools into business process overall results



	Qn 1	Qn 2	Qn 3	Qn 4	Qn 5	Qn 6	Qn 7	Qn 8
To a Very Great Extent	56	33	15	13	8	13	5	18
To a Great Extent	41	41	51	44	49	56	46	38
Somewhat	3	26	31	36	31	28	38	31
To a Small Extent	0	0	3	8	13	3	8	10
To A Very Small Extent	0	0	0	0	0	0	3	3

The next section discusses each of the questions in turn and presents the results of each. The interpretation of these results per question and per tool is discussed in the next chapter.

5.3.6.1 To what extent does the bank have an independent Operational Risk Management function that is responsible for the design and implementation of the bank's Operational Risk Management framework?

To effectively ascertain that the bank Operational Risk Management frameworks are effective, the extent to which an independent Operational management function is established was taken into account and the results are summarised below:

Table 5.3.6.1 Independent Operational Risk Management (ORM) function

	To a Very Great Extent	To a Great Extent	Somewhat	To a Small Extent	To A Very Small Extent
n	22	16	1	0	0
%	56%	41%	3%	0%	0%

Table 5.3.6.1 above shows that a high percentage (56%) of respondents indicated that banks have an independent ORM function responsible for the design and implementation of the Operational Risk Management frameworks To a Very great extent. The second largest group (41%) indicated that banks have independent ORM function to a great extent. Only 3% of responded showed that banks “Somewhat” have independent ORM function. None of the respondents indicated that banks have ORM function “To a Small Extent” or “To a very Small Extent”.

5.3.6.2 To what extent does the bank management understand the nature and complexity of Operational Risk inherent in portfolio of bank products, services and activities?

To effectively ascertain management understanding of Operational risk, the extent in which they understand the nature and complexity of Operational Risk inherent in their products and services was also taken into account. The results are summarised below:

Table 5.3.6.2 Management understand the nature and complexity of Operational Risk inherent in bank products

	To a Very Great Extent	To a Great Extent	Somewhat	To a Small Extent	To A Very Small Extent
n	13	16	10	0	0
%	33%	41%	26%	0%	0%

Table 5.3.6.2 above indicate that a majority of the respondents (41%) show that management understand the nature and complexity of Operational Risk inherent in bank products to “A great extent”, followed by (33%) respondents who indicate that management understand complexity of Operational Risk in bank products to “A very Great extent”. The remaining group (26%) indicated that management “somewhat” understand Operational Risk inherent in bank products. None of the respondents indicated that banks understand the nature

and complexity of Operational Risk inherent in products to “A Small Extent” or to “A very Small Extent”.

5.3.6.3 To what extent is the Operational Risk culture embedded in the business?

In order to effectively manage Operational Risk effectively, the risk cultures has to be embedded in the business and the table below shows the responses given by the sample with regard to the embedding of the risk culture within the business.

Table 5.3.6.3 Operational Risk culture embedded in business

	To a Very Great Extent	To a Great Extent	Somewhat	To a Small Extent	To A Very Small Extent
n	6	20	12	1	0
%	15%	51%	31%	3%	0%

Table 5.3.6.3 above indicate that a high percentage (51%) of responses show that the Operational Risk culture is embedded in business “To a great Extent”, followed by a 31% group which show that the Operational Risk culture is “somewhat” embedded in the business. 15% indicate that it is embedded “To a very great extent” and only 3% indicated that the Operational Risk culture is embedded in business “To a Small Extent”.

5.3.6.4 To what extent are the results of the bank's Operational Risk assessment incorporated into the overall bank business strategy development processes?

In order to manage the business effectively, the results of Operational Risk assessment should be incorporated in the strategy development and the table below shows the summary of the responses with regard to incorporation of Operational Risk assessment in business strategies.

Table 5.3.6.4 Operational Risk assessments are incorporated into the overall business strategy

	To a Very Great Extent	To a Great Extent	Somewhat	To a Small Extent	To A Very Small Extent
n	5	17	14	3	0
%	13%	44%	36%	8%	0%

According to table 5.3.6.4 above, majority of respondents (44%) indicate that the Operational Risk assessments are incorporated into the overall business strategy To a Great extent, followed by 36% of respondents indicating that Operational Risk assessment are Somewhat incorporated into the overall business strategy. Only 13% of respondents' show that Operational Risk assessments are implemented To a Very great extent and 8% show the incorporation To a small extent.

5.3.6.5 To what extent does the bank business processes documented and regularly updated with changes to the business table below provide a summary of the extent in which business processes are documented and regularly updated?

As part of the effective Operational Risk Management, the bank has to document and update its business processes regularly.

Table below illustrates that a large number (49%) of respondents showed that business processes are documented and updated regularly “To a Great extent”, followed by 31% of respondents indicating that business processes are “somewhat” documented and updated regularly. Only 13% of respondents’ indicated that business processes are documented and regularly updated “To a Small extent” and 8% showed “To a Very extent”.

Table 5.3.6.5 *Bank business processes documented and regularly updated*

	To a Very Great Extent	To a Great Extent	Somewhat	To a Small Extent	To A Very Small Extent
n	3	19	12	5	0
%	8%	49%	31%	13%	0%

5.3.6.6 To what extent are Operational Risk reports comprehensive, accurate, consistent and actionable across business lines and products?

To effectively ascertain that accurate and consistent data is used in managing the Operational Risk, the extent in which the reports produced provides comprehensive, accurate, consistent and are actionable across business lines and products were taken into account. The results are summarised below:

Table 5.3.6.6 Operational Risk reports comprehensive, accurate, consistent and actionable across business lines and products

	To a Very Great Extent	To a Great Extent	Somewhat	To a Small Extent	To A Very Small Extent
n	5	22	11	1	0
%	13%	56%	28%	3%	0%

Table 5.3.6.6 shows that a high percentage (56%) of respondents indicated that Operational Risk reports are comprehensive, accurate, consistent and actionable across business lines and products “To a Great extent”, followed by 28% of respondents indicating that Operational Risk reports are “somewhat” comprehensive, accurate, consistent and actionable across business lines and products. Only 13% showed that Operational Risk reports are comprehensive, accurate, consistent and actionable across business lines and products “To a Very Great extent” and 3% showed “To a Small extent”.

5.3.6.7 To what extent does Operational Risk staff communicate effectively with staff responsible for managing credit, market and other risks?

In order to manage Operational Risk, Operational Risk managers need to communicate with other risk managers within the bank and the table below shows the responses provided on whether there is a communication between risk managers.

Table 5.3.6.7 Operational Risk staff communicate effectively with staff responsible for managing credit, market and other risks

	To a Very Great Extent	To a Great Extent	Somewhat	To a Small Extent	To A Very Small Extent
n	2	18	15	3	1
%	5%	46%	38%	8%	3%

According to table 5.3.6.7 majority of respondents (46%) indicated that Operational Risk staff communicate effectively with staff responsible for managing credit, market and other risks “To a Great extent”, followed by 38% of respondents indicating that Operational Risk staff “somewhat” communicate with staff responsible for managing other risks. Only 8% of respondents’ show that Operational Risk staff communicates effectively with staff responsible for managing other risk types “To a Small extent”. 5% and 3% of the respondents showed “To a Very great extent” and “To a very small extent” respectively.

5.3.6.8 To what extent is Operational Risk training available throughout the business unit/organisation?

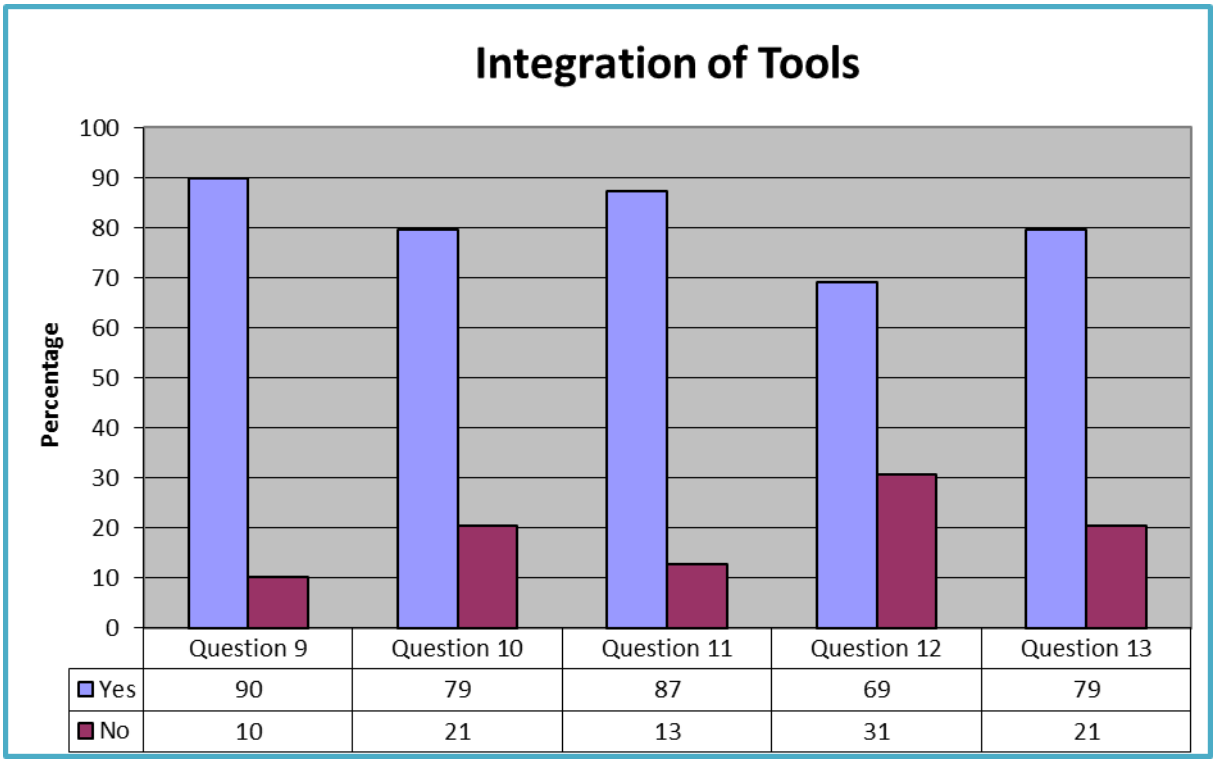
To effectively ascertain that Operational Risk is management is properly managed, the extent in which Operational Risk training is available throughout the organisation was taken into account. The results are summarised below:

Table 5.3.6.8 Operational Risk training available throughout the business unit/organisation

	To a Very Great Extent	To a Great Extent	Somewhat	To a Small Extent	To A Very Small Extent
n	7	15	12	4	1
%	18%	38%	31%	10%	3%

Table 5.3.6.8 above shows that a fair number (38%) of respondents indicate that Operational Risk training is available throughout the organisations “To a Great extent”, followed by 31% of respondents who showed that Operational Risk training is “Somewhat” available throughout the organisation. 18% of respondents showed that Operational Risk training is available “To a Very Great Extent” and 10% indicated “To a Small Extent”. Only 3% showed “To a Very Small extent”.

5.3:4 Integration of the Operational Risk tools – overall results (questions 9 to 12)



	Question 9	Question 10	Question 11	Question 12	Question 13
Yes	90	79	87	69	79
No	10	21	13	31	21

In order to manage Operational Risk effectively, the tone has to be set from the top i.e the board level, table 5.3.6.9 below shows the responses given by the sample with regard to the key content contained in the board approved policies:

Table 6.1 Questions on Board policies

Does the bank have board approved policies which defines the following?:		Yes	No
Question 9	The bank's acceptable Operational Risk profile.	90%	10%
Question 10	The banks' permissible threasholds or tolerances for inherent and residual risk, and approved risk mitigation strategies and instruments.	79%	21%
Question 11	Risk reporting and management information system (MIS)?	87%	13%
Question 12	The policies to be revised whenever a material change in the Operational Risk profile of the bank occurs?	69%	31%
Question 13	Bank approval processes for new products, when entering unfamiliar markets, when implementing new business processes or technology system?	79%	21%

Each response is discussed below:

5.3.6.9 Board approved policies which defines the bank's acceptable Operational Risk profile.

As per the table above, an overwhelming number (90%) of respondents answered “yes” that banks have board approved policies which define acceptable Operational Risk profile, only 10% answered “No”.

5.3.6.10 Board approved policies which defines banks' permissible thresholds or tolerances for inherent and residual risk

Table 5.3.6.9 shows that majority (79%) of respondents answered “yes” that banks have policies that define permissible thresholds or tolerances for inherent and residual risk, only 21% answered “No” to this question.

5.3.6.11 Board approved policies which defines risk reporting and management information system (MIS)

A high number (87%) of the respondents answered “Yes” that banks have approved policies which define risk reporting and information systems and only 18% answered “No”.

5.3.6.12 Board policies are revised whenever a material change in the Operational Risk profile of the bank occurs

Table 5.3.6.9 illustrates that majority (69%) of respondents answered “yes” that board policies are revised whenever a material change in Operational Risk profile occurs. However 31% of respondents answered “No”.

5.3.6.13 Bank approval processes for new products, when entering unfamiliar markets, when implementing new business processes or technology system

Table 5.3.6.9 shows that a high number (79%) of the respondents answered “Yes” that banks have approval processes for new products, when entering unfamiliar markets or when implementing new business processes or technology system. Only 21% answered “No” to this question.

CHAPTER 6: DISCUSSION OF RESULTS

6.1 INTRODUCTION

The objective of the research was to evaluate whether the Operational Risk tools are being used effectively by the AMA banks in meeting the supervisory soundness standards as set out in the Basel II AMA requirements and truly reflects the banks Operational Risk exposure and profile. The research involved collecting data from the 3 AMA banks and the results were presented in chapter 5. The purpose of this chapter is to interpret and discuss the results gathered.

The interpretation of the results was informed by the insight gained in the literature review and the data is validated against requirements of the Basel II Framework (2006) and the recently published Principles for the Sound Management of Operational Risk (Banking for International Settlements, 2011).

The results are discussed in two parts. Part I provides feedback based on research question 1, where analysis of each Operational Risk tool is undertaken in order to answer the first research objective. Part II addresses the second research question in answering research objective number two.

This chapter provides an opportunity to assess Operational Risk data and practices across the 3 AMA banks in South Africa. It also identifies areas where the AMA banks are doing well in complying with the principles of Operational

Risk Management as per the feedback gathered, and also highlights the areas of improvement.

6.2 RESEARCH QUESTION 1: Are Internal loss data and external loss data collection and reporting, Key Risk Indicators, Risk and Controls Self Assessment, Audit Findings and Risk Scenarios in line with the Basel II minimum requirements?

The results of each tool are discussed and interpreted in the sections below.

6.2.1 Use of Internal and External loss data

In order to best discuss the results and understand the use of Internal and External loss data, questions with common themes are grouped together and discussed as such.

Association of the internal loss data accuracy and the use thereof in budgeting processes, in other Operational Risk tools as well as the alignment to financial data is discussed below:

6.2.1.1 Extent in which internal loss data is considered to be accurate

There was widespread agreement among the respondents that the internal loss data used in Operational Risk Management is accurate, despite 26% of respondents indicating that the loss data was somewhat accurate. It is worrying

to see such a large percentage of respondents indicating that loss data is somewhat accurate, since it is vital for the loss data to be accurate for the following reasons:

- According to the principles of sound Operational management (BIS, 2011) loss data is used to identify or assess the internal control weaknesses.

- Loss data assist in calculating the Operational Risk regulatory capital (BIS, 2006),

- It informs management of the actual loss occurrences and serves as an input in the calculation of other Operational Risk tools.

Therefore it is important to have very high accuracy of loss data to ensure the above is done accurately. The impact of incorrect loss data is huge as it could lead to an incorrect calculation of regulatory capital and incorrect business decisions.

6.2.1.2 Extent in which internal losses are taken into account in the budget process / expected losses are budgeted for

The use of loss data in budgeting processes responses varied from “Somewhat” 38% to a great extent (34%). The Basel II Framework is not explicit in that loss data should be included in financial budgets, however regulatory

capital can be calculated based on unexpected losses only where banks budget for expected losses (as opposed to being calculated on both expected and unexpected losses).

Basel II framework also recommends that management must be aware of their expected losses and connect these losses into their business processes. A study by Ernst & Young (Making strides in financial services risk management, 2010) indicated that the majority of organisations are striving to tie the risk and financial data in order to make better and informed decisions. As such, it is not surprising to see a move towards budgeting for Operational Risk losses as indicated by 39% of responses who showed that Operational Risk losses are budgeted to a great extent. Therefore banks who are able to demonstrate that expected loss data are budgeted for, will be allowed to exclude such losses in their regulatory capital calculations (BIS, 2006).

6.2.1.3 Extent in which Operational Risk managers are involved in management of boundary events

Involvement of Operational Risk manager in management of boundary events has been highlighted by the Basel II accord as critical. From the responses collated majority (55%) showed the involvement to Great extent; however it appears that improvement is required for most responses as 36% showed that Operational Risk manager are somewhat involved in the management of boundary events.

In a case where Operational Risk managers do not flag the Operational Risk events related to credit risk, or the Operational Risk events related to market risk are not included in the calculation of Operational Risk capital charge, then banks will be in contravention of the AMA requirements and the Operational Risk capital charge somehow not accurate (Girling, 2009).

6.2.1.4 Extent to which recoveries are linked to Operational Risk losses

Many banks use insurance to transfer the risk of loss exposures. The Basel II framework allows the banks a reduction on the capital charge of up to 20% in case insurance is used to transfer the risk. In response to the question above, majority (77%) of responses indicated that recoveries are linked to the Operational Risk losses to a great extent. These results support the case study by Wood & Humphries (2009) where the use of insurance is shown as having value in the management of Operational Risk losses.

6.2.1.5 Extent to which Operational Risk losses are used to inform KRIs, RCSAs and Risk Scenarios

In chapter 2 (literature review) the Basel II framework explains that internal loss data may be used as input or validation of other Operational Risk Management tools. The use of internal loss data in informing other Operational Risk tools is increasingly common as indicated by responses received.

Key risk indicators provide early warning of the possible control failures or emerging risks (Osborne, 2006). Increase in Operational Risk losses may indicate breakdowns in processes or control failures; as such loss data may provide useful contribution in informing KRIs. A high percentage (72%) of respondents indicates that loss data is used as an input in Key Risk Indicator identification processes.

Risk and Controls Assessments are designed to help the business in assessing the inherent risk and effectiveness of controls in their business (Joseph & Engle, 2005). As such the internal loss data can assist in indicating the risks inherent in the business and weakness or robustness of internal controls. From the feedback received on the use of loss data in RCSA processes, responses showed that 71% use the loss data to a great extent.

Risk Scenarios identification heavily rely on the expert judgment of the business and risks. However it is recommended that business experts consider loss data when formulating scenarios (Palmer, 2005). An overwhelming majority (92%) showed that loss data is used as an input in Risk Scenarios analysis.

These results demonstrate a positive approach by Advanced Measurement Approach banks in meeting supervisory requirements. The fact that majority of responses regard the loss data as accurate demonstrate the banks significant effort in improving the quality of data used which in turn leads to accuracy in the regulatory capital calculations.

6.2.1.6 Extent in which material or significant losses identified are brought to attention of senior management

Risk governance is possibly viewed as the most significant area in management of the Operational Risk. There was a very strong agreement (97%) that significant Operational Risk losses are brought to the attention of management. This requirement is emphasised in principle 1 of the Principles for sound management of Operational Risk (Banking for International Settlements, 2011) in that senior management must establish a strong risk culture, where Operational Risk losses are escalated to appropriate bodies in ensuring proper treatment and integration in business processes.

The escalation of the significant Operational Risk losses to management aligns to the modern Operational Risk Management (ORM) approach, where the Operational Risk Management is not only about the risk quantification but the integration of the Operational Risk losses in management key decision making and business processes (Khan, 2008).

6.2.1.7 Extent to which the actual data align to financial data

In assessing the alignment of the actual Operational Risk data to financial data; a high percentage (77%) of respondents agreed that Operational Risk actual losses are aligned to financial data to a great extent. This confirms the notion by Garrity (2007) in that some of the obvious Operational Risk losses (for

example, interest claims) maybe identified in the Accounting systems (GL) with ease, whereas Operational Risk losses which are not easily identifiable in Accounting systems maybe hidden in accounts with different classification. Therefore, the alignment will ensure that the actual Operational Risk losses are accounted in accounting systems and reconciled to Operational Risk Systems.

Therefore, the results show that management does see a common goal of truth in the financial data presented and the Operational Risk losses quantified. The fact that 23% of respondents showed that somewhat loss data align to financial data could explain the reason why majority of respondents do not include loss data in their financial budgets as highlighted in section 6.2.1.2 above.

6.2.1.8 External loss data – Extent in which the bank use relevant external data, and have systematic processes for determining the situations for which external data must be used

Although 59% of respondents indicated that banks use relevant external data to a great extent and almost the same percentage (57%) showed that banks have systematic processes and methodologies on how to use external data. These results are positive considering the fact that Cope (2010) highlights challenges with the collation of published external data. He mention that the key challenge is the fact that data is varied given the need for banks to carefully choose data that is relevant and applicable to their environment.

Therefore, the results above indicate improvements in banks external data collection and use. This can be attributable to the fact that AMA banks subscribes to the external databases such as ORX, First Case studies etc where the quality of external loss data has improved.

6.2.2 Key Risk Indicators (KRIs)

6.2.2.1 Extent to which the risks identified are key to the business (i.e. if they materialise will have significant impact to the business) and the extent in which the indicators adequately reflect the underlying risks

Key Risk Indicators are an important tool in helping management to consider and assess the full range of factors that could potentially harm their business. Principles for Sound Management of Operational Risk (BIS, 2011) make a reference to the identification of the indicators that are “key” to the business.

Majority (84%) of respondents indicated that they consider risks that are key to the business, however 62% of respondents indicated that the indicators “somewhat” reflect the underlying risk. The literature (Scandizzo, 2005) highlighted the fact that there is a minimal guidance available on KRIs identification, this could explain disconnect between the risk identified as key and the underlying indicator used to tract them as demonstrated by the responses. Therefore, if the indicator is not linked to a risk driver then it may not

identify the possible weaknesses in the business processes or inadequacy of controls and it becomes ineffective as a risk tool.

Davies, Finlay, McLenaghen and Wilson (2006) reported that the Risk Management Association survey in 2005 showed that KRIs are critical in informing risk profiles of many financial institution, however many organisation still struggle with ensuring the completeness, accuracy and validity of the indicators identified.

The results above demonstrate that AMA banks in South African still have challenges in ensuring that the indicators identified reflect the underlying risks and therefore improvements to the Key Risk Identification process is required.

6.2.2.2 Extent in which management make decisions based on the identified KRIs

The role of Key risk indicators is amongst other, to provide an input in strategic decision making processes. Management use Key Risk Indicators to assess performance of key activities and base their plans on the output of the Key Risk Indicators (Institute of Operational Risk, 2010). The majority (49%) of respondents indicate that management somewhat make decision based on the Key Risk Indicators, with only 33% agreeing that management consider KRIs in their decision making to a great extent and 18% shows to a small extent.

The results are not surprising as McDermott and Davies (2008) mentions that there are challenges in obtaining management buy-in when it comes to Key Risk Indicators and there is a lack of strong governance to ensure that KRIs are part of management decision making processes. This could also be attributable to the fact that there are disconnect between the indicators and the underlying risks as highlighted in section 6.2.2.1 above.

6.2.2.3 Extent in which a change in the KRI reflect a change in the level of risk to the business in line with agreed appetite and tolerance levels i.e thresholds are not set too high/low

Principles for Sound Management of Operational Risk (BIS, 2011) clearly state that indicators may present evidence of the Operational breakdown which could result in a loss. Only 32% of responses agreed that there is a link between the change in KRI and the level of the risk, and majority (56%) of responses indicated that there is “somewhat” a link.

Therefore, the result shows that the KRIs may be irrelevant overtime, that is, if do not change as the risk exposure changes. Osborne (2006) clearly states that Key Risk Indicators should provide early warning of potential hazard and they should be kept relevant in reflecting risk exposures. Failure to update Key Risk Indicators renders them inadequate.

6.2.2.4 Banks have system where KRIs are captured

Majority (87%) responses indicated that banks have systems for capturing and tracking of Key Risk Indicators. This is a positive outcome given the fact that risk management relies on robust data and IT infrastructure as enabler. Many regulators expect banks to demonstrate that they have robust IT infrastructure before AMA application can be approved.

Petria and Petria (2009) declare that an institution‘s ability to have sound system in the management of Operational Risk is important in the overall risk management. The fact that banks have systems to capture KRIs may help address issues of aligning indicators to underlying risk as highlighted in section 6.2.2.1. This can be achieved as the IT system will make it easier to monitor indicators and identify possible disconnect over time.

6.2.2.5 KRIs result in risk management actions within other AMA elements

Operational Risk Management maturity levels have increased significantly, mainly as a result of the Basel II requirements. Basel II requires Operational Risk tools to be integrated and be used as inputs or be used to validate the results of other tools in order to ensure an accurate risk profile. Feedback received on the above question showed that a high majority (77%) indicated

that KRI results are used as an input in risk management action within other AMA elements.

The fact that the KRIs are used in other AMA component is critical, however the challenge is that KRIs output may not be credible as highlighted above where majority of respondents do not link the identified indicators to the underlying risk exposures. If an indicator is assigned to incorrect risk, then the output will be incorrect leading to wrong decisions being taken.

6.2.2.6 Frequencies of KRIs review to ensure relevancy

The frequency of conducting KRIs reviews to ensure relevancy varies from less than quarterly (24%), quarterly (46%) and annually (19%) as indicated from responses.

Basel II framework does not prescribe the frequencies in which Key Risk Indicators are to be reviewed, however Immaneni, Mastro and Haubenstock (2004) are of the opinion that the Key Risk Indicators should be updated whenever there is a change in the underlying risk or whenever there risk self assessment is undertaken.

In support of the above statement Scandizzo (2005) state that management should ensure that the Key Risk Indicators remain relevant and applicable in managing the Operational Risk.

6.2.3 Risk and Controls Self Assessment (RCSA)

6.2.3.1 Impact and the likelihood are adequately reflected in the Inherent risk levels and reflects the market and operating conditions of the business, and the Inherent risk levels are re-assessed at least quarterly or when business environment and control factors change

Principles for Sound Management of Operational Risk (BIS, 2011) makes it clear that RCSA are intended for banks to make assessments of possible factors which could harm their businesses, and to perform an impact analysis should such activities occur. An overwhelming (90%) majority of responses agreed that the impact and the likelihood of such factors are adequately reflected in their business processes.

These results therefore provide an affirmation that the RCSA are being be used as an effective tool for improving the business controls as highlighted by Joseph and Engle (2007).

However, when asked if the inherent risk is re-assed when the business environment and control factors change, only 77% agreed. The fact that inherent risk is not reassessed with the changes to the business can be seen as a weakness, as highlighted by Jallow et al. (2007) that inherent risk assessment is critical in order to ensure business continuity. Lack of regular

assessment of inherent risk levels may result in an failure to notice emerging risks or weaknesses in controls.

6.2.3.2 All controls identified are actual and existing controls and the effectiveness of controls are an accurate representation of the way the controls are functioning in the business

Based on the feedback received, 87% of responses agreed that controls which are identified are existing controls and not planned controls. According to Power (2005) the use of planned actions and not actual controls may provide a false view of the control environment as the control effectiveness cannot be assessed on a planned action but only on the actual control.

Therefore, the results demonstrate Operational Risk managers understanding of the assessment and analysis of the controls used in the RCSA processes. The understanding of controls assessment has a direct impact on the residual risk ratings.

6.2.3.3 Residual risk levels are aligned to related findings by Internal Audit controls

Principles for Sound Management of Operational Risk (BIS, 2011) make a reference to a need for comparative analysis. It indicates that by comparing outcomes of different “assessment tool” may allow for a more inclusive

observation of the Operational Risk profile. RCSAs outcomes were compared to the internal audit review in order to determine if there is a common view of the banks control assessments. 56% of respondents agreed that there is an alignment, with 31% indicating uncertainties when it comes to the alignment of RCSAs to Internal audit controls assessments.

Sarens and De Beelde, (2006) research found that internal audit plays a significant role in the risk assessment and in identifying control improvements; as such the current internal audit reviews adopt a risk based approach.

Therefore the results above do not demonstrate this alignment as 31% are uncertain whether the results of RCSA align to the internal audit assessment. There is a clear indication that internal audit, risk expert and management assessment of the control environment needs to be aligned somehow. The misalignment may lead to a different interpretation of controls weaknesses or different views on risk exposures and impacts to the banks.

6.2.3.4 RCSA's result in risk management actions within other AMA elements, for example, actions result in a new/revised KRI, or the creation/review of a risk scenario

A large number (66%) of respondents agreed that RCSA results in a management action within other AMA elements. However 21% were uncertain of whether this is the case. Karwowski and Orlowski (2009) regard RCSA as a

tool which provide a practical analysis of possible risks supported by the experts' experience of the business. As such the risks identified should be used in other AMA components such as Risk Scenarios.

Even though a large number agree that the information derived from RCSA result in management action within other AMA elements the fact that 21% of the respondents is uncertain support the findings by Shojai (2008) that RCSA may not be used in other AMA components due to their subjective nature and the fact that the values used are estimates which cannot be used for comparison purposes. This problem is viewed as a serious challenge in the management of Operational Risk as the Operational Risk tools need to be integrated (BIS, 2011).

6.2.3.5 RCSAs are subject to periodic review to ensure relevance and consistency

The results show that most (95%) respondents agree that RCSA are subjected to a periodic review. Yong and Kook (2007) state that Operational Risk tools need to be reviewed and kept up to date in order to ensure reliability and consistency of data quality. The results also meet the requirements of the Basel II framework.

Therefore the results show Operational Risk managers understanding of the importance of periodical review of RCSA to ensure relevancy and assessment of inherent risks and controls effectiveness.

6.2.3.6 Internal losses, KRIs, Audit findings are directly informative to the RCSAs

Lubbe and Snyman (2009) mention that risk tools cannot be used in separation but should be correlated and aligned for efficient risk management. Majority (74%) of respondents agreed that tools such as internal losses, KRIs and Audit findings are used to inform RCSA.

However, the results also showed some uncertainties from the respondents on whether these other tools are used to inform RCSAs. This can be attributable to the fact that expert judgement / senior management who have an intimate understanding of the business environment is used when identifying RCSAs as highlighted by Karwowski and Orlowski (2009). Their expertise and understanding of the internal and external business factors may be seen as sufficient in RCSA processes.

6.2.3.7 RCSAs are used as an input into the Risk Scenarios

Heikkinen and Korhonen (2006) are of the opinion that RCSA should be used as an input in the Risk Scenarios quantification; since both RCSA and Risk

Scenarios identifications and processes are based on the business experts' judgement.

Majority (71%) agree that the RCSAs are an input in Risk Scenarios computation. Therefore the results align with the effective risk management practices and the correct processes followed in the Risk Scenario computation, even though Basel II framework is not explicit about the need to use RCSAs as an input into Risk Scenarios processes.

6.2.4 Internal Audit Findings

6.2.4.1 Extent to which internal audit view is align Operational Risk Management

Respondent's feedback indicated that majority (77%) align the view of the internal audit in Operational Risk Management to a great extent. Goodwin and Kent (2006) assert that internal audit play a significant role in risk management, since it provides assurance that the risk management practices are properly understood and controlled by the organisation.

Therefore the fact that majority of respondents align the view of audit in the Operational Risk Management is a positive indication of the Operational Risk Management practices by the AMA banks.

6.2.4.2 Extent in which internal audit review and challenge the bank's Operational Risk Management, controls, processes and systems

The results showed that a large number of respondents (79%) are of the opinion that internal audit reviews and challenges the bank's Operational Risk Management, controls, processes and systems to a great extent.

The results are in line with Fernandez, (2007)'s recommendation that in order for the organisations to implement the effective ORM framework, internal audit should be vigilant to the business environment and be able to challenge where there are deficiencies.

6.2.4.3 Extent to which internal audit take into account Operational Risk breakdowns and losses during their audit review

In order for internal audit to suggest improvement to the banks control environment, the Operational Risk breakdowns and losses should be considered during their review. From the responses collated majority (75%) showed that internal audit does consider the Operational Risk breakdowns and losses to a great extent, however it appears that improvement is required as 15% of the respondents showed that internal audit somewhat considers the Operational Risk breakdowns and losses during their review.

Sarrens and De Beadle's (2006) study found that management place a great reliance on internal audit to uncover the weaknesses in control environment. Therefore buy not considering Operational Risk breakdowns and losses, weakness that led to such breakdowns and losses might be overlooked.

6.2.4.4 Extent to which the result of RCSA align to Internal Audit Findings

Osborne (2006) declare that internal audit approaches are now risk based, as such it is expected that risk tools such as RCSA should be more or less align to internal audit findings since the same approach to review the control environment is adopted.

Although 51% of the respondents showed that RCSAs align to internal audit findings, 26% indicated that they are somewhat aligned and 23% showed the alignment to a small extent. This is however not surprising as the results of the alignment of internal audit findings and RCSA above, also showed that there is a little misalignment.

6.2.4.5 Extent to which internal audit evaluate whether Operational Risk Management frameworks meet organisational needs and supervisory expectations

Staciokas and Rolanders (2005) proclaim that internal audit is used by management to enhance their business processes and by regulators to obtain assurance on the organisation's functions.

The results showed that 26% of respondents indicated that internal audit somewhat evaluate the Operational Risk Management frameworks to assess whether they meet the organisational needs and supervisors/regulators expectation. This calls for concern, despite the fact that majority (64%) agreed that internal audit evaluate the Operational Risk Management frameworks to assess whether they meet the organisational needs and supervisors/regulators expectation.

The main concern is the fact that internal audit function is to add value to the organisation and act as a third line of defence in providing an independent review and assurance of Operational Risk Management, controls and systems (BIS, 2011).

Therefore, internal audit function should ensure that they assign employees who understand the business environment to audit review where the audit findings will highlight areas of non-compliance with organisational frameworks

6.2.5 Risk Scenarios

6.2.5.1 Extent to which Risk scenarios a reflection of the significant risks to your business

Lynn (2006) emphasised that banks should consider catastrophic risk when completing Risk Scenario reviews. This is mainly due to the fact the fact that scenarios should be forward looking and not only consider the current losses.

An overwhelming majority (88%) of responses indicated that risk scenarios reflect significant risks to their business. For that reason it can be assumed that risk scenarios identification meets the requirements on Basel II framework.

6.2.5.2 Extent in which all the risk information sources are considered when defining risk scenarios i.e. internal and external data, RCSA, KRIs

Rippel and Teply (2011) assert that other risk information such as internal loss and external loss data make a considerable contribution in defining risk scenarios. Despite the fact that scenarios are defined by the business experts, consideration of all sources of risk information assist in identifying some of the events which have not yet been experienced by the business, but have a potential of occurring.

A high number (90%) of respondents agreed that all other risk information is considered when completing Risk Scenarios, which means that the risk calculations are comprehensive. The results provide comfort that the information used for regulatory capital calculation is a reflection of the banks risk profiles or exposures.

6.2.5.3 Extent in which Risk scenario information is used to manage the business i.e. in risk reporting and decision-making (risk scenarios should inform other risk management processes i.e. KRI's, RCSA etc.)

The results collected shows that 28% of respondents indicate that risk scenario information is somewhat used to manage their business. The number is fairly large, despite the fact that majority (56%) of respondents show that risk scenarios information is used to manage their business to a great extent.

The reason that some respondents may not be using the risk scenario information, may be attributable to the fact that the use of Operational Risk tools in capital modeling and managing the business is still immature (de Fontnouvelle, Rosengren and Jordan, 2007) since Operational Risk capital modeling was mainly introduced in 2008.

6.2.5.4 Extent to which Risk scenarios result in management actions which are consistent with the output of the other AMA elements, for example, risk management actions point to the same actions as listed for KRI's, RCSA etc

Barnier (2009) perceive the integration of Operational Risk tools as a way of "connecting the dots", not only within the risk tools themselves but also with business processes. Only 48% of the respondents indicated that risk scenarios result in management actions which are consistent with other output of the AMA elements and 38% showed that risk scenario somewhat result in actions which are consistent with other tools.

These results are not surprising since a study by Cernauskas and Tarantino (2009) showed that a concern for many banks remains integration of Operational Risk tools in their business processes. The lack of integration of Operational Risk tools was also highlighted under the use of RCSA in other risk tool in the previous section.

6.2.5.5 Risk scenarios subject to periodic (semiannually/annually) review to ensure alignment with the results of the AMA i.e. the results of the RCSA, loss data and KRIs data etc.

Risk Scenarios need to be constantly reviewed taking into account changes in the business environment (BIS, 2010). The periodic review will ensure that the capital requirements truly reflect the risk exposures.

The results showed that 97% agrees that risk scenarios are subjected to periodic review. This review is important as it feeds into the regulatory capital modeling and ensures completeness.

6.2.5.6 Risk scenarios based on the business expert judgment

Scenario identification should be based on experts' opinions. The respondents agreed 100% that scenarios identification is done by the business experts. This is a positive outcome in meeting the AMA requirements since Risk Scenario identification is subjective and heavily reliant on the people who understand the business environment.

6.2.5.7 Risk scenarios free of bias

According to the requirements of Basel II framework, Risk Scenarios should be forward looking and free of bias. Majority (67%) of respondents showed that

risk scenarios are free of bias; however 33% indicated that scenarios are not free from bias.

This confirms a study by Tchernobai (2006), which found that there is a "reporting bias" when using own or Internal loss modeling mechanisms. Operational Risk managers are required to challenge the scenarios identified by the business in order to avoid bias. As the bias in scenario identification may lead in risks which are relevant to the business not being considered or inaccuracy in the capital modeling processes.

6.2.5.8 Risk scenarios forward looking

According to AMA requirements, risk scenarios need to be forward looking and not only consider historical events (BIS, 2010) in order to ensure appropriate coverage of risks. A high percentage (95%) agreed that risk scenarios are forward looking. These results show risk managers and business experts understanding of extreme risks, their control and business environment.

6.2.5.9 Business Risk Scenarios subjected to independent validation e.g. by Enterprise Risk Management, internal audit e.t.c

Since risk scenarios identification is subjective, an independent review and validation is required. Majority (92%) of the respondents agreed that risk scenarios are subjected to an independent validation by either Enterprise Risk

Management function or Internal Audit. This is in line with the requirements of the sound management of Operational Risk (BIS, 2010), where it requires the governance body that ensures the reliability of risk scenario data.

6.3 RESEARCH QUESTION 2: Are Operational Risk Management tools integrated into day-to-day business processes and used as business risk management tools versus just regulatory capital calculation methods?

6.3.1 Extent in which the bank have an independent Operational Risk Management function that is responsible for the design and implementation of the bank's Operational Risk Management framework

Business management is expected to act as a first line of defense, followed by an independent risk function which acts as second line of defense. The risk management function is expected to design and oversee the Operational Risk frameworks and practices (BIS, 2011).

Majority (97%) of respondents indicated that an independent risk management functions exist in their organisations. These results demonstration an understanding by AMA banks of the Operational Risk governance requirements and good risk governance practices.

6.3.2 Extent in which the bank management understand the nature and complexity of Operational Risk inherent in portfolio of bank products, services and activities

According to Sheen (2005) management need to obtain an understanding of Operational Risk inherent in their products in order to ensure effective Operational Risk Management. Majority (74%) the respondents indicated that management understand the nature and complexity of Operational Risk inherent in portfolio of bank products to a great extent, and 26% showed that there is somewhat understanding by management.

Even though majority agrees with the above question, the 26% which showed somewhat management understand the inherent risk in the products raises questions since management understanding of the inherent risk is essential in order to ensure that risk and rewards relationships are understood.

6.3.3 Extent to which the Operational Risk culture embedded in the business

According to a survey conducted by Moosa (2007), Operational Risk success depends primarily on entrenching the risk culture within the business. A large percentage (69%) of the respondents show that Operational Risk culture has been embedded in the business to a great extent, despite the 31% which

shows that the Operational Risk culture is somewhat embedded in the business.

These results demonstrate that AMA banks have made a good progress in embedding Operational Risk in their business, given the fact that AMA requirements were formally adopted and implemented for the first time in South Africa in 2008. These results also illustrate the need to enhance Operational Risk initiatives targeted in improving the understanding of Operational Risk throughout the organisation.

6.3.4 Extent to which results of the bank's Operational Risk assessment are incorporated into the overall bank business strategy development processes

In the light of recent Operation risk failures it is important for management to consider Operational Risk assessment in developing business strategies, only 57% of respondents reported that Operational Risk assessment are incorporated into the bank overall business strategy development processes with 36% indicating that they are somehow considered in this processes.

These results show that more work need to be done in incorporating Operational Risk assessment into bank strategies to avoid future failures. Currie (2004) mentions that reasons behind the introduction of Operational Risk in the Basel II framework, was to allow management to consider the results of

Operational Risk assessments in their strategies in order to improve their control environment.

6.3.5 Extent to which bank business processes are documented and regularly updated with changes to the business

Documentation of business process is critical in the Operational Risk Management. Jallow et al. (2007) state that business process documentation allow the business to understand their processes better and to identify Operational Risk inherent in the processes. Not much progress has been made in the business processes documentation as 57% of the respondents indicated that processes are documented to a great extent, with 31% showing that they are somehow documented.

The results give an indication that improvement is required when coming to documentation of the processes.

6.3.6 Extent to which Operational Risk staffs communicate effectively with staff responsible for managing credit, market and other risks

In order to ensure that there are no gaps in the overall risk management within the bank, the staff responsible for Operational Risk should communicate with credit risk managers, market risk managers and other risk managers (BIS, 2011). In responding to this question, 51% of respondents showed that there is

a communication with other risk managers to a great extent; however 38% indicated that somewhat communication with other risk managers exist.

The result shows that the need for communication with other risk managers need to improve in order to close the possible gaps and possible overlie in bank risk management programmes to allow effective management of risk.

6.3.7 Extent to which Operational Risk reports are comprehensive, accurate, consistent and actionable across business lines and products

Operational Risk reporting needs to be accurate, consistent and comprehensive in order to allow for the appropriate examination of Operational Risk exposures and profiles (BIS, 2010). Despite the fact majority of the respondents (69%) who agreed that the reports are comprehensive, accurate and consistent, 28% indicated that these reports are somehow accurate, consistent and comprehensive.

Considering the high reliance placed by senior management on the accurate reporting of Operational Risk, improvement is required to ensure that the quality of data allows for accurate decision making or risk management processes.

6.3.8 Extent to which Operational Risk training is available throughout the business unit/organisation

In order to embed the Operational Risk Management culture, practices and systems within the bank, training programmes should be designed to suit specific audience and training be rolled out the entire organisation (BIS, Feb 2010). A fair number (56%) reported that Operational training is available throughout the organisation; however 31% still indicate that training is somewhat available throughout the organisation. Based on this result, banks need to improve on the training initiatives.

6.3.9 The bank has board approved policies which defines the following:

Dowling (2006) declare that the board is eventually responsible for the management of risks in the bank. He further mentions that the results of the recent corporate failures were mainly due to the board lack of awareness of the main risks facing their organisations. As such board of directors is responsible for approving risk management policies within their organisations (BIS, 2011). Below are key features that Operational Risk policies need to have.

6.3.9.1 Acceptable Operational Risk profile

An overwhelming majoring (90%) of respondents agreed that banks risk management policies defines the bank's acceptable Operational Risk profile.

These results shows that board are keen and involved in providing risk management oversight.

6.3.9.2 Permissible thresholds or tolerances for inherent and residual risk, and approved risk mitigation strategies and instruments

Although a high number (79%) indicated that board policies defines the banks' permissible thresholds or tolerance for inherent and residual risk, 21% answered no to this question.

The results show that AMA banks need to enhance their policies to include the permissible thresholds or tolerances and approve risk mitigation strategies and instruments. The thresholds or tolerances, as well as mitigating strategies are critical in managing the risks that can be emanate from the changes in the macroeconomic environment, new product and promises (BIS, 2011).

6.3.9.3 Risk reporting and management information system (MIS)

Only 87% of the responded agreed that board policies define the risk reporting and information management system. The AMA banks are expected to have policies which define the risk reporting and information management system.

These results show a clear indication that improvements need to be done in order to incorporate this information.

6.3.9.4 Policies are revised whenever a material change in the Operational Risk profile of the bank occurs

Only 69% of respondents agreed that that risk policies are revised whenever a material change in the Operational Risk profile of the bank occurs. It is important that risk policies are kept relevant and upto date, in order to ensure continuity from any business disruption (BIS, 2011).

6.3.9.5 Bank approval processes for new products, when entering unfamiliar markets, when implementing new business processes or technology system

To understand the risks in new products, board policies should define the approval processes before products are launched or before entering unfamiliar markets. Seventy nine percent of the respondents indicated that their policies do define the approval processes, with 21% answering “no” to this question.

The new products approval processes is required since in most cases, taking on new products or entering unfamiliar processes increase risks (BIS, 2011). As such it critical that a thorough assessment is conducted before products are taken on, so that controls can be put in place.

6.3.10 Summary of Results

In conclusion, based on the results or feedback received from AMA banks, there was strong evidence to suggest that responses obtained across the 3 banks represent the Operational Risk Management practices in the major segments/divisions of these banks. This also talks to the relevance of this study where the intention was to test the use of the Operational Risk tools against the Basel II Advanced Measurement Approach requirements.

The findings affirmed the analysis of Imeson (2006), where it was highlighted that banks adopting the Advanced Measurement Approach need to ensure that their internal practices truly reflect their Operational Risk exposures and regulatory capital calculations. The main reason behind the need for Operational Risk data accuracy is the fact that under AMA, banks use their internal models to calculate Operational Risk capital and the regulators rely on banks to produce valid and complete data in order for them to carry out their duties of safeguarding financial systems. The inaccurate calculation of Operational Risk capital could lead to huge reputational and financial risk for these banks.

CHAPTER 7: CONCLUSION

7.1 INTRODUCTION

Based on the findings of the research questions, this chapter looks at the conclusions that can be drawn and provides recommendations based on the research findings and the literature review. The recommendation on what improvements can be implemented is discussed per Operational Risk tool analyses. Furthermore the chapter finally explores ideas for future research.

The respondents may use the results of this research to benchmark themselves to their peers or also used by the regulator to understand areas they need to provide guidance on, in order to ensure improvements and better implementation of the Operational Risk tools.

7.2 MAIN FINDINGS AND CONCLUSION

The South African banks that have obtained an approval for the use of Advanced Measurement Approach (AMA) for Operational Risk, have shown significant progress in the effective use of Operational Risk tools. The feedback received from respondents illustrates that significant efforts are underway to address the deficiencies in Operational Risk Management even though there are some gaps in implementing certain tools.

The results suggest that the AMA banks recognise that improving their internal Operational Risk practices is fundamental to creating a robust Operational Risk Management system and creating a more resilient banking environment. This can also be attributable to strong supervision by the South African Reserve Bank (SARB) and well experienced Operational Risk managers.

The conclusion is discussed per tool and then an overall conclusion is provided in the following section.

7.3 RESEARCH QUESTION 1

Analysis of each Operational Risk tool was completed in order to answer the first research question. Below is a conclusion on each tool.

7.3.1 Internal and External loss data

The requirements of the Basel II framework with regard to internal and external data have substantially been implemented by the AMA banks. However some elements of the internal and external loss data may need to be re-assessed and validated in order to ensure data quality and completeness. The main gaps identified were with regard to the accuracy of loss data and Operational Risk managers' involvement in management of boundary events and budgeting for Operational loss data.

The accuracy of the internal loss data remains fundamental given its impact on the overall risk management decision making, influence on other Operational Risk tools and Operational Risk regulatory capital calculations.

Improving the accuracy of internal and external loss data, will require banks to reassess their loss data collection processes. This includes the analysis of the nature of losses collected (e.g. boundary events, internal fraud, external fraud etc), quality of the Operational Risk Management systems and the overall risk management culture within the organisation. Root cause analysis of losses such as boundary events will ensure that Operational Risk managers work closely with the relevant parties in designing mitigating controls. Transparency and proactive reporting of the internal loss data should be encouraged throughout the organisation.

Gaps with regard to budgeting for Operational Risk losses could be improved once the accuracy of data is achieved. Accurate data plays a prominent role in budgeting for typical or expected losses and in the identifying Operational Risk appetite.

7.3.2 Key Risk Indicators (KRIs)

.The results showed that banks have processes and systems in place to capture, monitor and report on Key Risk Indicators. Regardless of the processes and systems in place the feedback received pointed towards the fact that identified indicators do not reflect the underlying risks. Even though KRIs are reviewed periodically, the results showed that the KRIs do not reflect a change in the level of risk to the business.

Banks need to ensure that senior management and employees that understand the business are involved in the identification of the key risk indicators in order to ensure that indicators reflect the underlying risks to the business. The indicators need to be assessed continuously in order to ensure that they assist management with emerging risks so that improvements can be designed to mitigate weaknesses in controls.

7.3.3 Risk and Control Self Assessment (RCSA)

It was clear from discussion of the results that there were inadequacies in the implementation of the RCSA processes. This situation may well persist until banks put interventions in place to ensure RCSA processes are enhanced to a much higher degree.

Reform initiatives with regard to the implementation of RCSA processes, should focus particularly on ensuring that inherent risk levels are re-assessed when the business environment or control factors changes. The residual risk rating should align to the internal audit rating and findings, in order to ensure that both lines of defences have a single view of the business risks and controls.

The research findings, pointed to effective and adequate identification and use of internal audits in Operational Risk Management. To ensure effective use of this tool; internal audits need to increase their consideration of the Operational Risk losses suffered in the review processes.

Despite impressive use of internal audits in Operational Risk Management; the internal audit process needs to enhance their review procedures when evaluating banks Operational Risk Management frameworks in an effort to meet the organisational needs (strategies) and supervisory expectation.

7.3.4 Risk Scenarios

There was an overwhelming positive response to the implementation of the Operational Risk scenarios. However, the use of risk scenario information in managing the business and business decision making remains a challenge and needs to be improved. Risk scenarios need to be integrated into day-to-day business activities and their output considered when making business decisions.

7.3.5 Summary on the Use of Operational Risk tools

The findings of this research suggested that the 5 key Operational Risk tools were being used by AMA banks in South Africa as intended, and substantially met the Basel II requirements and sound practices of Operational Risk. Although ultimately there was evidence to suggest that each tool has a unique role to play in Operational Risk Management – the tools need to be integrated and reinforce one another; this is an area in which an improvement is required.

7.4 RESEARCH QUESTION 2

The second objective of the research was to evaluate whether the Operational Risk Management tools are integrated into day-to-day business processes. The integration of Operational Risk Management tools into day-to-day management of the business appeared to be immature. In some cases, managements understanding of the nature and complexity of Operational Risk inherent in portfolio of bank products, services and activities was still a challenge. Well identified Operational Risk and clear communication of risks in products and services will help management in understanding the inherent risks and assist in connecting the overall products and services strategy and the risk management practices.

Documentation of the business processes remains a challenge. There should be rigorous governance around documentation of business processes to

ensure that risk identification and control measures are completed for all business processes. Such documentation should include approval processes for new products, when entering unfamiliar markets or when implementing new technologies or processes.

7.5 Overall summary

The results indicated that AMA banks have substantially complied with the minimum requirements of Basel II Framework. The current gaps can be attributable to the fact that for most the banks AMA approval had been obtained recently and on-going refinements were underway.

The bottom line is that the AMA banks understood the implications of not complying fully with the AMA requirements and that inaccurate calculation of Operational Risk capital could lead to huge reputational and financial risk. Notwithstanding the current gaps in the results, it can be deduced that the Operational Risk tools are largely integrated in to day-to-day business processes and represent the Operational Risk exposures and profile of the AMA banks.

7.6 Future research ideas

The future research ideas are based on a combination of research limitations of this study and some of the insights gained from the literature review and findings. The following research ideas can be pursued:

- Research on the time period it takes AMA banks to implement and fully embed the Operational Risk tools within their businesses, upon the AMA approval by their regulators.
- Further explore whether the characteristics of Operational Risk tools Implementation and maturity is somewhat similar among banks segment / divisions.

REFERENCES

Akhter, W. (2010). Risk management in takaful. *Enterprise Risk Management, 2*(1), 128-128-144. Retrieved from http://search.proquest.com/docview/845921496?accountid=14717

Altman, E. I., & Sabato, G. (2005). Effects of the new basel capital accord on bank capital requirements for SMEs. *Journal of Financial Services Research, 28*(1-3), 15-15. doi:10.1007/s10693-005-4355-5

Azvine, B., Cui, Z., Majeed, B., & Spott, M. (2007). *Operational risk management with real-time business intelligence* Springer Science & Business Media. doi:10.1007/s10550-007-0017-5

Bank for international settlements: Committee on banking regulations and supervisory practices' consultative paper on proposals for international convergence of capital measurement and capital standards. (1988). *International Legal Materials, 27*(2), 524-524. Retrieved from http://search.proquest.com/docview/60751591?accountid=14717

Bank for International Settlement (2006). *International Convergence of Capital measurement and Capital Standards:* Basel Committee on Banking Supervision. Retrieved from http://www.bis.org/publ/bcbs128.htm

Bank for International Settlement (2011). *Principles for the Sound Management of Operational Risk:* Basel Committee on Banking Supervision. Retrieved from

http://www.bis.org/publ/bcbs195.htm

Bank for International Settlement (2010). Basel Committee on Banking Supervision consultative paper on the *Sound Practices for the Management of Operational Risk*. Retrieved from http://www.bis.org/publ/bcbs183.htm

Barnier, B. G. (2009). *Ten questions in operational risk today and insight from other industries* Robert Morris Associates. Retrieved from http://search.proquest.com/docview/209775976?accountid=14717

Beans, K. M. (2010). *Perspectives on operational risk management* Robert Morris Associates. Retrieved from http://search.proquest.com/docview/723399677?accountid=14717

Beans, K. M. (2007). *Chief operational risk officers discuss: Basel II and the development of the operational risk discipline* Robert Morris Associates. Retrieved from http://search.proquest.com/docview/209774240?accountid=14717

Bergmark, D., & Tattam, D. (2005). Operational risk management. *JASSA,* (4), 31-34. Retrieved from http://search.proquest.com/docview/89139917?accountid=14717

Berley, S. (2006). Erm: Time to catch the wave. *Risk Management, 53*(4), 12-14,16,18. Retrieved from http://search.proquest.com/docview/226997338?accountid=14717

Birade, L., & Mark, R. (2009). In Reuvid J.,ed (Ed.), Investing in an operational risk framework Sixth edition. London and Philadelphia: Kogan Page; distributed by Ingram Publisher Services, LaVergne, Tenn. Retrieved from http://search.proquest.com/docview/753927052?accountid=14717

Boris B,. Donald R. Cooper, & Pamela S. Schindler (Eds.). (2007). *Business research methods* McGraw-Hill. doi:DOI: 10.1016/j.intacc.2007.06.005

Catarineu-Rabell, E., Jackson, P., & Tsomocos, D. P. (2005). Procyclicality and the new basel accord--banks' choice of loan rating system. *Economic Theory, 26*(3), 537-537-557. Retrieved from http://search.proquest.com/docview/56589831?accountid=14717

Cernauskas, D., & Tarantino, A. (2009). Operational risk management with process control and business process modeling. *The Journal Of Operational Risk, Northern Illinois University* , 3-17.

Chavez-Demoulin, V., Embrechts, P., & Neslehova, J. (2006). Quantitative models for operational risk: Extremes, dependence and aggregation. *Journal of Banking and Finance, 30*(10), 2635-2658. doi:10.1016/j.jbankfin.2005.11.008

Cleary, S., Valleret, T., & Fényes, T. (2007). Resilience to risk; business success in turbulent times. *South African Journal of Economics, 75*(4), 728-728-729. Retrieved from http://search.proquest.com/docview/36842180?accountid=14717

Cope, E. W., Mignola, G., Antonini, G., & Ugoccioni, R. (2009). *Challenges and pitfalls in measuring operational risk from loss data* Incisive Media Plc. Retrieved from http://search.proquest.com/docview/223574011?accountid=14717

Cope, E. W. (2010). Modeling operational loss severity distributions from consortium data. *The Journal of Operational Risk, 5*(4), 35-64. Retrieved from http://search.proquest.com/docview/819287241?accountid=14717

Creswell, J.W. (2003). Research design: Qualitative, Quantitative and mixed methods approaches. California. Sage Publications

Cummins, Lewis & Wei (2006), The Market value impact of Operational loss events for US banks and Insurers, Journal of Banking & Finance Volume 30, Issue 10, October 2006, Pages 2605-2634, retrieved from http://www.sciencedirect.com.innopac.up.ac.za/science/article/pii/S0378426606000537

Danescu, T., & Muntean, A. (2005). *Adressing Operational Risk by Using a Risk Based Internal Audit Approach.* Romania: Faculty of Economics, Petru Maior University. Retrieved from http://www.wseas.us/e-library/conferences/2010/Tunisia/AEBD/AEBD-14.pdf

David Häger, Andersen, L., Aven, T., & Frode Bø. (2007). *The basel II capital accord and operational risk management; status and the way forward* Journal of American Academy of Business. Retrieved from http://search.proquest.com/docview/197303402?accountid=14717

Davies, J., Finlay, M & Wilson, D. (2006). *Key Risk Indicators – Their Role in Operational Risk Management and Measurement* Retrieved

http://d.yimg.com/kq/groups/12093474/1290864495/name/McLenaghenTara3.pdf

De Fontnouvelle, P., DeJesus-Rueff, V., Jordan, J., & Rosengren, E. (2006). *Capital and risk: New evidence on implications of large operational losses* Retrieved from http://search.proquest.com/docview/56313562?accountid=14717

Di Renzo, B., Hillairet, M., Picard, M., Rifaut, A., Bernard, C., Hagen, D., Maar, P. and Reinard, D. (2007), *Operational risk management in financial*

institutions: Process assessment in concordance with Basel II. Software Process: Improvement and Practice, 12: 321–330. doi: 10.1002/spip.322

Dowling, G. (2006). Reputation risk: It is the board's ultimate responsibility. *The Journal of Business Strategy, 27*(2), 59-68. Retrieved from http://search.proquest.com/docview/202681191?accountid=14717

Dutta, K., & Perry, J. (2007, January). *A Tale of Tails*: An Emperical Analysis of Loss Distribution Models for Estimating Operational Risk Capital. USA. Retrieved from http://irm.wharton.upenn.edu/F07-Dutta.pdf

Ernst & Young Survey (2010): *Making Strides in financial services risk management* (2010) EYGM Limited. Retrieved from http://www.ey.com/Publication/vwLUAssets/Making_strides_in_FSRM/$FILE/Making%20strides%20in%20financial%20services%20risk%20management.pdf

Eichengreen, B., Mody, A., Nedeljkovic, M., & Sarno, L. (2009). *How the subprime crisis went global: Evidence from bank credit default swap spreads.* Unpublished manuscript. Retrieved July 20, 2011, from http://search.proquest.com/docview/56917886?accountid=14717

Embrechts, P., Furrer, H., & Kaufmann, R. (2003). *Quantifying regulatory capital for operational risk* Palgrave Macmillan. Retrieved from http://search.proquest.com/docview/232032828?accountid=14717

Evans, J., Womersley, R., Wong, D., & Woodbury, G. A. (2008). *Operational risks in banks* Finsia - Financial Services Institute of Australasia. Retrieved from http://search.proquest.com/docview/89226977?accountid=14717

Errol Kruger*, 2005. Basel II Introduction and implementation in South Africa* Retrieved from http://www.nkonki.com/images/library/Basel_II_Workshop_One_Summary.pdf

Fernández, A. L (2007). Internal audit function role in operational risk management. *Journal of Financial Regulation and Compliance, 15*(2), 143-155. doi:10.1108/13581980710744039

Flamholtz, E. G. (2009). Towards using organizational measurements to assess corporate perfomance. *Journal of Human Resource Costing & Accounting Vol. 13 No.2* , 105-117.

Garrity, V. (2007). Developing and implementing an operational loss data collection program. *Bank Accounting & Finance,,* 3-9. Retrieved from http://search.proquest.com/docview/215048086?accountid=14717

Girling, P. (2009). Practical Operational risk management Garrat Graham Retrieved from http://www.garritygraham.com/CM/Custom/Part-4.pdf

Goodwin-Stewart, J., & Kent, P. (2006). The use of internal audit by australian companies. *Managerial Auditing Journal, 21*(1), 81-101. Retrieved from http://search.proquest.com/docview/274698994?accountid=14717

Helbok, G., & Wagner, C. (2006). *Determinants of operational risk reporting in the banking industry* Incisive Media Plc. Retrieved from http://search.proquest.com/docview/197281167?accountid=14717

Heikkinen, P., & Korhonen, K. (2006). Technology-driven efficiencies in financial markets Retrieved from http://www.suomenpankki.fi/fi/julkaisut/selvitykset_ja_raportit/yleistajuiset_selvitykset/Documents/A110.pdf

Herring, R. (2002). *The Basel 2 approach to bank operational risk: Regulation on the wrong track* Emerald, 60/62 Toller Lane, Bradford, West Yorkshire, BD8 9BY, UK, [URL:http://www.emeraldinsight.com]. doi:10.1108/eb022953

Imeson, M. (2006). *Special supplement: Operational risk - obeying the regulator - of all the forms of operational risk, compliance officers are most concerned with regulatory risk. why? because the consequences of getting it wrong can be*

so severe, writes michael imeson The Financial Times Limited. Retrieved from http://search.proquest.com/docview/225651313?accountid=14717

Immaneni, A., Mastro, C., & Haubenstock, M. (2004). A Structured Approach to Building Predictive Key Risk Indicators. *The RMA Journal* Retrieved from

http://d.yimg.com/kq/groups/12093474/1290864495/name/McLenaghenTara3.pdf

Jallow, A., Majeed, B., Vergidis, K., Tiwari, A., & Roy, R. (2007). Operational risk analysis in business processes. *BT Technology Journal, 25*(1), 168-177. doi:10.1007/s10550-007-0018-4

Jiménez-Rodríguez, E. J., Feria-Domínguez, J. M., & Martín-Marín, J. L. (2008). *Scenario analysis for modelling operational losses in the absence of data : The spanish bank in perspective** Om Sai Ram Centre for Financial Research. Retrieved from http://search.proquest.com/docview/215226436?accountid=14717

Jobst, A. (2007). The treatment of operational risk under the new basel framework: Critical issues. *Journal of Banking Regulation, 8*(4), 316-352. doi:10.1057/palgrave.jbr.2350055

Jobst, A. A. (2010). The credit crisis and operational risk - implications for practitioners and regulators Incisive Media Plc. Retrieved from http://search.proquest.com/docview/759257022?accountid=14717

Joseph, G. W., & Engle, T. J. (2005). The use of control self-assessment by independent auditors. The CPA Journal, 75(12), 38-38-43. Retrieved from http://search.proquest.com/docview/212337011?accountid=14717

Jorion, P. (2009). *Risk management lessons from the credit crisis* doi:10.1111/j.1468-036X.2009.00507.x

Karwowski, W., & Orlowski, A. (2009). *Information Systems in Management III.* Warsaw University of Life Sciences. Department of Informatics. Retrieved from

http://isim.wzim.sggw.pl/resources/ISIM_III_2009.pdf

Khan, A.S., Guharay, S., Franklin, B., Fischtrom, B., Scanlon, M., & Shimpi, P.2010). *A new Approach for Managing Operational risk* Canadian Institute of Actuaries. Retrieved from http://www.soa.org/files/pdf/research-new-approach.pdf

Kuritzkes, A., & Schuermann, T. (2006). *What we know, don't know and can't know about bank risks: A view from the trenches*. Rochester: Retrieved from http://search.proquest.com/docview/189871903?accountid=14717

Lynn, B. (2006). *Operational risk: Are you prepared?* Association for Financial Professionals. Retrieved from http://search.proquest.com/docview/226059258?accountid=14717

Lubbe, J. & Snyman, F. (2009. The advanced measurement approach for banks. Retrieved from http://www.bis.org/ifc/publ/ifcb33p.pdf

McDermott, P., & Davies, G. (2008). *Communicating operational risk results to senior management* Robert Morris Associates. Retrieved from http://search.proquest.com/docview/209776243?accountid=14717

McEachern, C. (2003). *Operational risk: An ongoing operation* United Business Media LLC. Retrieved from http://search.proquest.com/docview/206639879?accountid=14717

McKinsey & Co. (2009) *Operational risk management: The future of the discipline*. Robert Morris Associates. Retrieved from http://search.proquest.com/docview/209781488?accountid=14717

Moosa, I. A. (2008). A critique of the advanced measurement approach to regulatory capital against operational risk. *Journal of Banking Regulation, 9*(3), 151-151-164. doi:10.1057/jbr.2008.7

Nicholson, S. W., & Bennett, T. B. (2009). *Transparent practices: Primary and secondary data in business ethics dissertations: JBE* Springer Science & Business Media. doi:10.1007/s10551-008-9717-0

Osborne, P. (2006). *Which risks are 'blinking' on your dashboard?* American Bankers Association. Retrieved from http://search.proquest.com/docview/202666997?accountid=14717

Pablo, T (2011). Will higher bank capital requirements sink the world? *Corporate Finance Review, 15*(6), 42-47. Retrieved from http://search.proquest.com/docview/875636197?accountid=14717

Palmer, D. (2005). Using Scenario Analysis to estimate Operational Risk Capital. Retrieved from http://fic.wharton.upenn.edu/fic/papers/10/10-10.pdf

Petria, N., & Petria, L. (2009). Operational risk management and basel ii. *Land Forces Academy Review, 14*(4), 96-100. Retrieved from http://search.proquest.com/docview/89154194?accountid=14717

Point, B. (2005). *Addressing Operational Risk.* Wall Street and Technology. Retrieved from http://online.wsj.com/

Power, Michael (2005) *The invention of operational risk*, Review of International Political Economy, 12:4, 577-599

Sabatini, J. (2003). *Operational risk: An ongoing operation* United Business Media LLC. Retrieved from http://search.proquest.com/docview/206639879?accountid=14717

Sabatini, J. (2006). *Achieving excellence in operational risk management: A corporate staff perspective* Robert Morris Associates. Retrieved from http://search.proquest.com/docview/209774793?accountid=14717

Sandford, L. (2008, March). How to Manage Risk In a Global Economy. USA. Retrieved from www.qualityprogress.com.

Saunders, M., Lewis, P., & Thornhill, A. (2009). *Research Methods for Business Students.* United Kingdom: Person Professional Limited.

Scandizzo, S. (2005). *Risk mapping and key risk indicators in operational risk management* Blackwell Publishing Ltd. doi:10.1111/j.0391-5026.2005.00150.x

Sarens, G., & De Beelde, I. (2006). Internal auditors' perception about their role in risk management: A comparison between US and belgian companies. *Managerial Auditing Journal, 21*(1), 63-80. Retrieved from http://search.proquest.com/docview/274699291?accountid=14717

Sarens, G., & De Beelde, I. (2006). *The relationship between internal audit and senior management: A qualitative analysis of expectations and perceptions* Blackwell Publishing Ltd. doi:10.1111/j.1099-1123.2006.00351.x

Sheen, A. (2005). *Implementing the EU capital requirement directive - key operational risk elements* Emerald Group Publishing, Limited. Retrieved from http://search.proquest.com/docview/235027173?accountid=14717

Shojai, S. (2008). Minimise risk, Optimise success. *Journal of Financial Transformation* Retrieved from http://www.capco.com/sites/all/files/Journals28_Web.pdf

Staciokas, R., & Rupsys, R. (2005). Application of internal audit in enterprise risk management. *Inzineriné Ekonomika, 2*(42), 20-25. Retrieved from http://search.proquest.com/docview/36514707?accountid=14717

Staciokas, R., & Rolandas R. (2005). Internal audit and its role in organizational government. *Organizacijø Vadyba: Sisteminiai Tyrimai,* (33), 169-180. Retrieved from http://search.proquest.com/docview/222771420?accountid=14717

Tchernobai, A. (2006). In Jammalamadaka S. (Ed.), *Contributions to modeling of operational risk in banks*. United States -- California: University of California, Santa Barbara. Retrieved from http://search.proquest.com/docview/305349069?accountid=14717

Tozer-Pennington, V. (2010). *Chinese banks' AMA operational risk projects put on hold* Incisive Media Plc. Retrieved from http://search.proquest.com/docview/756808075?accountid=14717

Yeh, A. (2008). Key Motifs in the home-host mantra of operational risk management:Prudential Supervision Department. Retrieved from http://search.proquest.com/

Jong, Ko., Kook, S., (2007). *The Analysis on Operational Risk Profile of Korean Banks.* Retrieved from *http://www1.kdi.re.kr/data/download/attach/7884_a2_4.pdf*

Laeven, L., & Levine, R. (2009). Bank governance, regulation and risk taking. *Journal of Financial Economics, 93*(2), 259-259-275. doi:10.1016/j.jfineco.2008.09.003

Jarrow, R. A. (2007). A critique of revised basel II. *Journal of Financial Services Research, 32*(1-2), 1-1-16. doi:10.1007/s10693-007-0006-3

Jan Emblemsvåg. (2010). The augmented subjective risk management process. *Management Decision, 48*(2), 248-248-259. doi:10.1108/00251741011022608

Elizalde A & Repullo R. (2006). Economic and Regulatory Capital in Banking: What is the Difference? *International Journal of Central Banking*, Vol. 3, No. 3 (September 2007), pp. 87-117 http://www.defaultrisk.com/pp_super_41.htm

Sabatini, J. A. (2006). Achieving excellence in operational risk management: A corporate staff perspective. *The RMA Journal, 88*(5), 26-26-30. Retrieved from http://search.proquest.com/docview/209774793?accountid=14717

Grody, D., Harmantzis, F., Kaple, G. (2007), Operational Risk and Reference Data: Exploring Costs, Capital Requirements and Risk Mitigation *Journal of Operational Risk, Vol. 1, No. 3, 2006* Available at SSRN: http://ssrn.com/abstract=849224

Triana, P. (2011). Will higher bank capital requirements sink the world? *Corporate Finance Review, 15*(6), 42-42-47. Retrieved from http://search.proquest.com/docview/875636197?accountid=14717

Rippel, M., & Teply, P. (2011). Operational risk scenario analysis. *Prague Economic Papers, 20*(1), 23-39. Retrieved from http://search.proquest.com/docview/869563571?accountid=14717

APPENDIX A: Questionnaire

CRITICAL EVALUATION OF THE OPERATIONAL RISK TOOLS

Evaluation Questions — **INSTRUCTIONS: Please place a cross / mark in the box that you agree with.**

	Intergration of the the Operational risk tools into business process	To a Very Great Extent	To a Great Extent	Somewhat	To a Small Extent	To A Very Small Extent
1	To what extent does the bank have an independent Operational risk management function that is responsible for the design and implementation of the bank's operational risk management framework?					
2	To what extent does the bank management understand the nature and complexity of operational risk inherent in portfolio of bank products, services and activities?					
3	To what extent is the Operational risk culture embedded in the business?					
4	To what extent are the results of the bank's operational risk assessment incorporated into the overall bank business strategy development processes?					
5	To what extent does the bank business processes documented and regularly updated with changes to the business?					
6	To what extent are operational risk reports comprehensive, accurate, consistent and actionable across business lines and products?					
7	To what extent do Operational risk staff communicate effectively with staff responsible for managing credit, market and other risks?					
8	To what extent is Operational risk training available throughout the business unit/organisation?					
	Answer "Yes" or "No"	Yes	No			
	Does the bank have board approved policies which defines the following:					
9	i) the bank's acceptable operational risk profile.					
10	ii) the banks' permissible threasholds or tolerances for inherent and residual risk, and approved risk mitigation strategies and instruments.					
11	iii) risk reporting and management information system (MIS)?					
12	iv) the policies to be revised whenever a material change in the operational risk profile of the bank occurs?					
13	v) bank approval processes for new products, when entering unfamiliar markets, when implementing new business processes or technology system?					

Key Risk Indicators

Evaluation Questions

INSTRUCTIONS: Please place a cross / mark in the box that you agree with.

	Key Risks	To a Very Great Extent	To a Great Extent	Somewhat	To a Small Extent	To A Very Small Extent
1	To what extent are the risks identified key to the business i.e. if they materialise will have significant impact to the business?					
2	To what extent do indicators adequately reflect the underlying risk i.e. an effective KRI will be correlated to risk exposure? For example, does an increase in the number of complaints received provide adequate reflection of the risk of an inefficient process.					
3	To what extent does management make decisions based on the defined KRIs i.e. the KRIs provides relevant information which is able to produce tangible results from which to make decisions?					
4	To what extent does the change in the KRI reflect a change in the level of risk to the business in line with agreed appetite and tolerance levels i.e. threshold are not set too high/low?					
	Answer "Yes" or "No"	Yes	No			
5	Does the bank have a system (reliable source) where KRIs are captured?					
6	Does KRIs result in risk management actions within other AMA elements, for example, a KRI breach should be used to verify the RCSA values, and possible reassessment of the RCSA?					
7	At what frequency are KRIs reviewed to ensure relevancy?	less than Quarterly	Quarterly	Semi annually	Annually	Not reviewed

Risk and Control Self Assessment

Evaluation Questions

INSTRUCTIONS: Please rate how strongly you agree or disagree with each of the following statements by placing a cross / mark in the appropriate box.

	RCSA	Strongly disagree	Disagree	Uncertain	Agree	Strongly Agree
1	Impact and the likelihood are adequately reflected in the inherent risk levels and reflect the market and operating conditions of the business. For example: does a change in the business environment, such as a new legislation, reflect an increase in the likelihood of the risk of a regulatory fine?					
2	Inherent risk levels are re-assessed at least quarterly or when business environment and control factors change.					
3	All controls identified are actual and existing controls i.e. controls that identified are actually a measure that is in place to mitigate the risk and not an action plan.					
4	The effectiveness of controls are an accurate representation of the way the controls are functioning in the business.					
5	The inherent risk levels and the control effectiveness are adequately reflected in the residual risk level i.e. the residual risk assessment should not be higher than inherent risk levels.					
6	Residual risk levels are aligned to related findings by internal audit i.e. does internal audit rating of the risk and control align to the rating of the risk and control in the RCSA.					
7	RCSA's result in risk management actions within other AMA elements, for example do the actions result in a new/revised KRI, the creation/review of a risk scenario.					
8	RCSAs are subject to periodic review to ensure relevance and consistency.					
9	KRI's, Internal losses, Audit findings directly informative to the RCSA's.					
10	RCSAs are used as an input into the Risk Scenarios.					

Risk Scenario

INSTRUCTIONS: Please place a cross / mark in the box that you agree with.

Evaluation Questions

	Risk Scenario	To a Very Great Extent	To a Great Extent	Somewhat	To a Small Extent	To A Very Small Extent
1	To what extent are Risk scenarios a reflection of the significant risks to your business?					
2	To what extent are all the risk information sources considered when defining risk scenarios i.e. internal and external data, RCSA, KRIs?					
3	To what extent is the Risk scenario information used to manage your business i.e. in risk reporting and decision-making (risk scenarios should inform other risk management processes i.e. KRI's, RCSA etc.)?					
4	To what extent do Risk scenarios result in management actions which are consistent with the output of the other AMA elements? For example, risk management actions point to the same actions as listed for KRI's, RCSA etc?					
	Answer "Yes" or "No"	Yes	No			
5	Are Risk scenarios subject to periodic (semiannually/annually) review to ensure alignment with the results of the AMA i.e. the results of the RCSA, loss data and KRIs data etc.					
6	Are Risk scenarios based on the business expert judgement?					
7	Are Risk scenarios free of bias?					
8	Are Risk scenarios forward looking?					
9	Are Business Risk Scenarios subjected to independent validation e.g. by ERM, internal audit?					

Internal & External Loss Data

INSTRUCTIONS: Please place a cross / mark in the box that you agree with.

Evaluation Questions						
Internal loss data		To a Very Great Extent	To a Great Extent	Somewhat	To a Small Extent	To A Very Small Extent
1	To what extent is internal loss data considered to be accurate?					
2	To what extent are internal losses taken into account in the budget process / are budgeted for?					
3	To what extent are operational risk managers involved in management of boundary events?					
4	To what extent are recoveries linked to Operational risk losses?					
5	To what extent are Operational risk losses used to inform KRIs?					
6	To what extent are Operational risk losses used to inform RCSAs?					
7	To what extent are Operational risk losses used to inform Risk Scenarios?					
8	To what extent are material or significant losses identified brought to attention of senior management?					
9	To what extent does the actual loss data align to financial data?					
External loss data						
10	To what extent does a bank's operational risk measurement system use relevant external data (either public data and/or pooled industry data)?					
11	To what extent does a bank have a systematic process for determining the situations for which external data must be used and the methodologies used to incorporate the data (e.g. scaling, qualitative adjustments, or informing the development of improved scenario analysis)?					

Audit Findings

Evaluation Questions

INSTRUCTIONS: Please place a cross / mark in the box that you agree with.

	Audit Findings	To a Very Great Extent	To a Great Extent	Somewhat	To a Small Extent	To A Very Small Extent
1	To what extent do you align the view of Internal Audit in Operational risk management?					
2	To what extent does Internal Audit review and challenge the bank's operational risk management, controls, processes and systems.					
3	To what extent does Internal Audit take into account the result of RCSA when conducting audit reviews?					
4	To what extent does Internal Audit take into account operational risk breakdowns and losses during their audit review?					
5	To what extent does the result of RCSA align to Internal Audit findings?					
6	To what extent does Internal Audit evaluate whether operational risk management frameworks meets organisational needs and supervisory expectations? For example, while Internal Audit should not be setting specific risk tolerance or appetite, it should review the robustness of the process of how the limits are set; including why and how they are adjusted in response to changing circumstances.					