PRINCIPLES FOR AN OPERATIONAL RISK APPETITE FRAMEWORK FOR A BANK: A SOUTH AFRICAN PERSPECTIVE

by

SUNÉ MARÉ

Submitted in accordance with the requirements
for the degree of

MASTER OF COMMERCE

in the subject

BUSINESS MANAGEMENT

at the

UNIVERSITY OF SOUTH AFRICA

SUPERVISOR: PROF J YOUNG

January 2019

Student number: 55516106

DECLARATION

I declare that **PRINCIPLES FOR AN OPERATIONAL RISK APPETITE FRAMEWORK FOR A BANK: A SOUTH AFRICAN PERSPECTIVE** is my own work and that all the sources that I have used or quoted have been indicated and acknowledged using complete references.

24/01/2019

_____ _____

MS S MARÉ **DATE**

ACKNOWLEDGEMENTS

I want to give thanks to my Lord and Saviour who gave me the strength and courage to complete my dissertation.

A special thank you to my supervisor, Professor Jackie Young, for mentoring and supporting me throughout this process and all the valuable time you have devoted to my study. Special appreciation goes to Professor Ashley Mutezo who has encouraged me to stay positive and steadfast throughout the study and never to give up. A word of thanks also goes to Ilze du Plooy who advised me on how to conduct my statistical analysis.

I am deeply grateful for all the support and prayers that I have received from my family (Mariétha, Frans, Darius, and Theresa) and friends, especially Joané, Chantélle, Mareliese, Catherine, Retha and Cecile for encouraging me throughout my research journey. Your moral support and love have kept me steadfast and motivated. Thank you for believing in me.

I wish to thank all my colleagues at the Department of Finance, Risk Management, and Banking at the University of South Africa for their support and inputs during the study. This has been an incredible learning experience for me as an academic researcher.

ABSTRACT

The significance for a bank to determine its risk appetite has become crucial over the years, based on past and recent risk events in the financial services sector. Regulatory pressure, a focus on corporate governance and risk management have been stimuli for many changes in the financial industry. An example is the need to establish an operational risk appetite framework. It is against this background that the study aimed to identify guiding principles for an operational risk appetite framework that can be used to determine the operational risk appetite of a bank.

The study entailed a literature review and an empirical analysis of the principles for an operational risk appetite framework for the banking industry of South Africa. A survey was used to collate the data. Also, the researcher endeavoured to establish a gap between the principles and the current status of implementation of the confirmed principles. The descriptive and inferential results indicated that most of the identified principles were viewed as important and crucial for an operational risk appetite framework for a South African bank, although some were not yet fully implemented. The study also confirmed the principles for an effective operational risk appetite framework to comply with regulatory requirements and to ensure a sound risk management process to support the achievement of business objectives.

KEYWORDS: operational risk; risk appetite; operational risk appetite; operational risk appetite framework; operational risk appetite statement

OPSOMMING

Dat 'n bank in staat is om sy risikoaptyt in die finansiëledienstesektor vas te stel, is betekenisvol en dit het oor jare heen vanweë vorige en onlangse risikogebeurtenisse van kritieke belang geword. Die druk van regulering, 'n fokus op korporatiewe bestuur en risikobestuur is stimuli vir talle veranderinge in die finansiële bedryf. 'n Voorbeeld hiervan is die noodsaaklikheid daarvan om 'n operasionele risikoaptytraamwerk op te stel. Teen hierdie agtergrond het die studie beoog om riglyne te identifiseer vir 'n operasionele risikoaptytraamwerk wat gebruik kan word om 'n bank se operasionele risikoaptyt te bepaal.

Die studie omvat ’n literatuuroorsig en ’n empiriese ontleding van die beginsels van ’n operasionele risikoaptytraamwerk vir die bankbedryf in Suid-Afrika. ’n Opname is gebruik om die ingesamelde data te vergelyk, en die navorser het gepoog om ’n leemte tussen die beginsels en die huidige stand van implementering van die bevestigde beginsels uit te wys. In die beskrywende en inferensiële resultate word aangedui dat die meeste van die geïdentifiseerde beginsels beskou word as belangrik en kritiek vir ’n operasionele risikoaptytraamwerk vir ’n Suid-Afrikaanse bank, al word sommige beginsels nog nie ten volle geïmplementeer nie. Die studie bevestig die beginsels van ’n effektiewe operasionele risikoaptytraamwerk met die oog daarop om aan reguleringsvereistes te voldoen en ’n deurdagte risikobestuursproses te verseker en sodoende die verwesenliking van sakedoelwitte te ondersteun.

SLEUTELWOORDE: Operasionele risiko; risikoaptyt; operasionele risikoaptyt; operasionele risikoaptytraamwerk; operasionele risikoaptytverklaring

ISISHWANKATHELO

Ngokuhamba kweminyaka kuya kubaluleka kakhulu ukuba ibhanki iwujonge ngononophelo umngcipheko enokuwuthatha, ngenxa yokubona iziganeko zomngcipheko ezenzekileyo kwicandelo leenkonzo zoqoqosho. Uxinzelelo lolawulo, ugxininiso kulawulo lweenkampani kunye nolawulo lomngcipheko zizinto eziphembelele iinguqu ezininzi kurhwebo lokwenza imali. Umzekelo sisidingo sokuseka uphahla lokusebenza ngomngcipheko. Zezi zinto ezibangela ukuba esi sifundo sijolise ekufumaniseni iinqobo ezisisikhokelo sokuqwalasela umngcipheko onokuthathwa, nesinokusetyenziselwa ukulinganisela umngcipheko onokuthathwa yibhanki.

Esi sifundo siphengulule uluncwadi olukhoyo ngalo mbandela kunye nohlalutyo olunobungqina lweenqobo ezinokusetyenziselwa ukulinganisela umngcipheko onokuthathwa licandelo leebhanki zoMzantsi Afrika. Kwenziwa uhlolo zimvo ekuqokeleleni iinkcukacha zolwazi. Umphandi wabuya wazama ukubonisa umahluko phakathi kweenqobo ezimiselweyo nemeko ekuyiyo ekusetyenzisweni kweenqobo ezivunyiweyo. Iziphumo ezichazayo nezicingelwayo zibonise ukuba uninzi lweenqobo zibonwa njengamanqaku abalulekileyo nangundoqo okwenza uphahla lokusebenza ngomngcipheko onokuthathwa yibhanki eMzantsi Afrika, nangona ezinye zingekasetyenziswa ngokupheleleyo. Esi sifundo siphinde sangqinisisa iinqobo zophahla olululo lokusebenza ngomngcipheko onokuthathwa ezimele ukuthobela imigaqo elawulayo nokuqinisekisa inkqubo yomgcipheko eqinileyo yokuxhasa ukufunyanwa kweenjongo zoshishino.

AMAGAMA APHAMBILI: umngcipheko womsebenzi; umngcipheko onokuthathwa; umngcipheko womsebenzi onokuthathwa; uphahla lokusebenza ngomngcipheko onokuthathwa; inkcazelo yophahla lokusebenza ngomngcipheko onokuthathwa

LIST OF ABBREVIATIONS AND ACRONYMS

AMA	advanced measurement approach
APRA	Australian Prudential Regulation Authority
BCBS	Basel Committee on Banking Supervision
BCM	business continuity management
BIS	Bank for International Settlements
BSD	Bank Supervision Department
CEO	Chief Executive Officer
CFO	Chief Financial Officer
COSO	Committee of Sponsoring Organisations of the Treadway Commission
CRO	Chief Risk Officer
ERM	enterprise risk management
EUI	Economist Intelligence Unit
EY	Ernst and Young
FRC	Financial Reporting Council
FRRSC	Financial Regulatory Reform Steering Committee
FSA	Financial Services Authority
FSB	Financial Stability Board
G10	Group of Ten
HR	human resource
IACPM	International Association of Credit Portfolio Managers
ICAAO	Initial Internal Capital Adequacy Assessment Process

IFF	Institute of International Finance
IMF	International Monetary Fund
IoDSA	Institute of Directors in Southern Africa
IOR	Institute of Operational Risk
IRM	Institute of Risk Management
ISO	International Standards Organisation
IT	information technology
JSE	Johannesburg Stock Exchange
KCI	key control indicator
KPI	key performance indicator
KRI	key risk indicator
LDA	loss distribution approach
OECD	Organisation for Economic Co-operation and Development
OpRisk	operational risk
ORAF	operational risk appetite framework
ORAS	operational risk appetite statement
ORMF	operational risk management framework
OSFI	Office of the Superintendent of Financial Institutions of Canada
PEST	political, economic, social and technological
PRA	Prudential Regulation Authority
PwC	PricewaterhouseCoopers
RAF	Risk Appetite Framework
RA-RA	Risk Appetite–Risk Attitude

RAS	Risk Appetite Statement
RCSA	risk and control self-assessment
RIMS	Risk and Insurance Management Society
RM	risk management
RMA	Risk Management Association
SARB	South African Reserve Bank
SPE	special purpose entities
SREP	supervisory review and evaluation process
SSG	Senior Supervisors Group
SWOT	strengths, weaknesses, opportunities and threats
UK	United Kingdom
US	United States

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1: INTRODUCTION TO THE STUDY

1.1 INTRODUCTION

The proposal titled, “Principles for an operational risk appetite framework for a bank: A South African perspective” served as an introduction to the problem that was addressed in the study. A brief background of the banking industry in South Africa and the importance of managing risk within the industry is followed by the problem statement of the study.

The problem statement was substantiated by research objectives. The primary objective is to determine guiding principles to formulate an operational risk appetite framework for a South African bank. An empirical study was conducted to establish a framework that can be used in determining the operational risk appetite of a bank.

The purpose of the research methodology was to analyse the current approach taken by various South African banks to determine their operational risk appetite. The research focused on the analysis of the current underlying theoretical knowledge base for developing and implementing the concept of an operational risk appetite framework as a risk management tool in the South African banking industry.

The research investigated the different international, and national risk management frameworks and processes developed over the years to assist a bank in developing an appropriate operational risk appetite framework.

The research design of the study included a literature review to verify the importance of a bank to implement an operational risk appetite process in order to formulate an operational risk appetite framework and statement. The empirical study aimed to collate data from a predetermined target population, which was used to support valid and applicable conclusions and recommendations.

1.2 BACKGROUND

Risk management has become increasingly important over the past few years, due to many adverse events such as high-level fraud cases, terrorist attacks, the global financial crisis of 2008 and other critical global trends (Du Randt, 2011). Most of the incidents led to huge losses for banks, because of the mismanagement of operational risk exposures

(Young, 2012:172). The downfall of one of the largest and oldest banks in the United Kingdom (UK), Barings Bank, can directly be linked to one individual, Nick Leeson. As a result of this event, which could be attributed to the mismanagement of operational risk, operational risk became a focal point for many businesses. (Young, 2010:177). According to Apostolik, Donohue, and Went (2009:18), the collapse of Barings Bank was due to the failure of the internal procedures and processes of the bank. Nick Leeson was able to authorise his trades and capture them into the banking system without supervision. The trader's unauthorised actions were an excellent example of people risk, which forms part of operational risk.

In recent years, the world has witnessed significant risk events, such as the 2008 financial crisis and the sovereign debt crisis, which led to significant consequential financial damages and knock-on effects (Institute of Risk Management [IRM], 2011:11). The number of recent losses, which occurred in the financial crisis led to various banks being liquidated (Young, 2012:172). The events mentioned above raised the question as to why boards failed to see it coming (IRM, 2011:11). These events also emphasised the importance of a focused approach to operational risk management. According to Young (2012:172), it is crucial for a bank to maintain a sound risk management approach to ensure future growth.

The banking industry was one of the first industries to adopt a focused approach to operational risk management, based on the guidelines issued by the Basel Committee on Banking Supervision (BCBS), with the emphasis on the measurement of operational risk in terms of expected and unexpected losses for a bank (Young, 2010:177). The BCBS implemented Basel II in 2006. BCBS has stated that "the Basel II Accord does not aim at changing the global level of capital in the banking industry, but rather at creating an incentive to encourage banks to adopt what they consider "best practice" for risk management" (Moosa, 2007:37). Basel II focused on three pillars (refer to Figure 1.1) which illustrate the inclusion of operational risk.

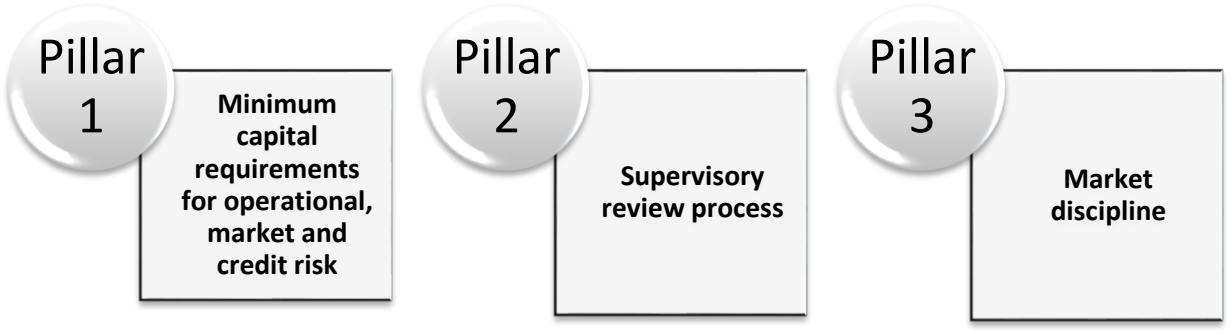


Figure 1.1: Basel II Pillars

Source: Adapted from *Operational Risk Management* (Moosa, 2007:42)

For this study, it is essential to understand the strategic positioning of risk management as a management discipline within the banking environment. This issue will be dealt with in detail in the ensuing chapters on the literature of risk management. The next section will discuss the banking industry and the importance of managing risk within the industry.

1.2.1 Risk management

This study only focused on banks, since they act as the backbone of modern business, and the development of any country depends on a sound banking system. One crucial question that must be asked is: “Why are banks more important than other financial and non-financial institutions?” (Moosa, 2007:30).

White (2004, cited in Moosa, 2007:30) argues that banks are more vulnerable and unstable because they are structurally fragile since they have illiquid assets (loans) and liquid liabilities (deposits) which could make a bank vulnerable to potential excessive withdrawals under certain circumstances. These circumstances could be a result of poor risk management. The recent African Bank fiasco in 2014 (Business Report, 2014) can also be attributed to poor risk management and demonstrates how unstable and vulnerable a bank can be. African Bank Investments Limited, one of the largest unsecured lenders in South Africa was placed under curatorship on 10 August 2014. The collapse of African Bank (Business Report, 2014) has placed approximately R4 billion of government pension money at risk (Business Report, 2014:1). According to Cameron (2014:1), the cost-saving drive of the bank itself proved hopelessly ineffective, and the

main cost inflators were people, processes and systems. The bank had around R17 billion of bad loans when it failed (Business Report, 2014:1).

The second argument by White (2004, cited in Moosa, 2007:31) is that banks are in the middle of the payment system because they can generate money. Banks deal with money, which is seen as a valuable commodity, and the risk of criminal activity (which can lead to operational risk exposure), is much higher for banks than other businesses (Moosa, 2007:31).

As part of the core business processes of a bank, risk is taken on a daily basis. Apostolik et al. (2009:13–14) provide the following practical examples of the risks banks might encounter:

- Borrowers may submit payments late or fail altogether to make payments, resulting in a bank losing some of its assets. This threat will affect the equity of the bank and reduce the shareholders' stake in the bank.
- Depositors may demand the return of their money at a faster rate than for which a bank has reserves, causing a possible negative influence on the state of liquidity of the bank.
- Interest rates may change and influence the value of the loans of a bank. For example, if interest rates rise, the value of the long-term assets will tend to fall more than the value of the shorter-term liabilities.
- Operational risk, such as human error or technology risk events and fraud in computer systems, could lead to losses for a bank.

According to the BCBS (2002:2), the increase in sophisticated financial technology, globalisation and the reduction of government power (deregulation) within the financial services industry in certain countries, has given rise to complex and diverse banking activities, which can influence the risk profile of a bank. BCBS also highlights the following examples of new risks faced by banks:

- the emergence of banks acting as large-volume service providers creates the need for continuous maintenance of internal controls and back-up systems;
- the use of highly automated technology has the potential to transform risks from manual processing errors to system failure risks;

- the growth of e-commerce also leads to new, not yet fully understood, potential risks, such as system security issues and external fraud;
- banks can implement mitigation controls to decrease their exposure to credit and market risk, but this can lead to other unidentified risks for a bank (BCBS, 2002:2).

As seen above, banks are faced with a set of unique risks and can assume more risks in order to increase their profits. Various authors classify risk faced by a bank differently. For example, Heffernan (2005:104) groups banking risks into eight types of risks (refer to Figure 1.2 below).

Figure 1.2: Types of risks in the core business of banking
Source: Adapted from *Modern Banking* (Heffernan, 2005:104)

Based on the above figure, it is evident that operational risk is identified as one of the primary risks a bank can face. Apostolik et al. (2009:14–18) classify risks related to banks into the following three key risk areas:

- credit risk;
- market risk;
- operational risk.

The BCBS also recognises the three main risk types as mentioned above, but they also recognise other types of risks that must be managed appropriately. For example, liquidity risk, business risk, and reputational risk. It is evident from the above-identified risks that operational risk is seen as one of the primary core risks a bank may encounter. Failing to understand the operational risks faced by a bank will increase the likelihood that risks will go unrecognised and uncontrolled, resulting in potentially devastating losses for the bank

(BCBS, 2002:6). For this study, only operational risks faced by a bank were focused on, due to the enormous impact this type of risk can have on a bank if such risk is not managed correctly. According to Moosa (2007:80), the extensive range of the scope of operational risk is one feature that differentiates operational risk from other risk types, such as market and credit risk. Market and credit risk are more widely appreciated and understood as risk types, whereas the diversity of operational risk makes it difficult to limit the number of dimensions required to describe it (Moosa, 2007:80). Operational risk in the banking industry will be discussed in the next section.

1.2.2 Operational risk in the banking industry

Operational risks are present in virtually all banking transactions and activities and are a significant concern for supervisors, regulators and bank management (Du Randt, 2011:4). As stated previously, operational risk has become a focus area for banks as an independent management discipline. For example, according to Heffernan (2005:104), banks have started to address their operational risks, such as fraud and theft, in the same formal manner banks address credit and market risks (Heffernan, 2005:104).

The BCBS (2002:2) defines operational risk 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 reputational, systemic and strategic risk. According to Casu, Molyneux, and Girardone (2006:272), the operational risk of a bank can also relate to the failure of the operating system, controls or other management failures of a bank, for example, human error. Also, Apostolik et al. (2009:182) demonstrate operational risk in terms of events (refer to Figure 1.3 below).

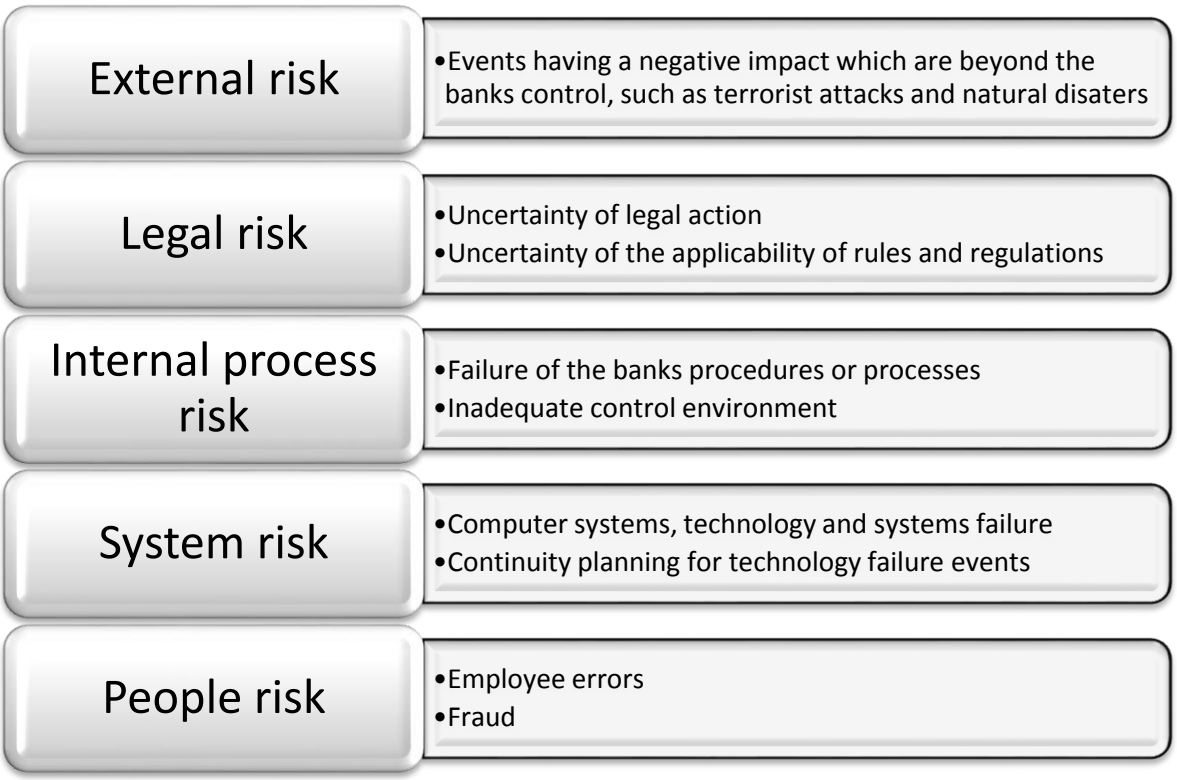


Figure 1.3: Operational risk categories and examples
Source: Adapted from *Foundations of banking risk: an overview of banking, banking risks, and risk-based banking regulation* (Apostolik et al., 2009:182)

Upon analysing Figure 1.3, it is evident that operational risk has a diversity of risk factors, which can be identified as people, process, system and legal risks. It also includes external risk factors threatening a bank, which could result in losses.

The management of operational risk is now widely accepted by most banking industries worldwide (Young, 2012:172). It is imperative that banks maintain a sound operational risk management approach. For the purpose of this study, it was important to understand the environment in which the South African banking industry is operating. The next section will discuss the current South African banking industry and the new changes that will be implemented by the banks in South Africa.

1.2.3 The South African banking industry

Banks play an essential role in maintaining the stability and security of the financial system of a country and are strictly regulated. In 2007, the South African government

launched a formal review of the financial regulatory system of South Africa. In 2011, the Minister of Finance published a policy document called “A safer financial sector to serve South Africa better” (Financial Regulatory Reform Steering Committee [FRRSC], 2013:2). This document outlined the impact of the financial crisis on South Africa (FRRSC, 2013:2). It noted that the domestic financial sector had weathered the global financial crisis reasonably well due to sound macroeconomic fundamentals in South Africa and a robust regulatory framework. Even though South Africa survived the financial crisis, there is a need to have minimum international standards integrated into the financial sector, as well as coordination between different national regulators. It was decided that South Africa would commit itself to implement refined global financial standards for the financial sector (FRRSC, 2013:2).

Against this background, it is the objective of the FRRSC to establish new reforms in South Africa. One of the reforms is the twin peaks system in financial sector regulation. The system deals with system-wide macro-prudential risks. In order to achieve this, the oversight of market conduct regulation (regulating how firms price and design their products, conduct their business and treat their customers) must be separated from prudential regulation (regulating the solvency and liquidity of financial institutions) (FRRSC, 2013:3).

The twin peaks system (FRRSC, 2013:13) is to be implemented in two phases. The first phase commenced in 2013 and dealt with the development of legislation to assist the South African Reserve Bank (SARB) and the Financial Services Board with their new additional responsibilities (FRRSC, 2013:13). The SARB is responsible for maintaining financial stability, together with the market conduct regulator to oversee systemic risks that may arise from financial markets. The Financial Services Board was established as the new market conduct regulator and is responsible for supervising and regulating the market conduct of the financial services sectors (FRRSC, 2013:14–15). The second phase was implemented on 1 April 2018, which concerns the implementation of a specific financial sector regulatory and supervisory framework and system (FRRSC, 2013:13).

Due to the ongoing financial crisis and new twin peak requirements established by the Financial Stability Board (FSB), the BCBS also issued a new document entitled “Basel III:

a global regulatory framework for more resilient banks and banking systems" (Hannoun, 2010:1) in 2010. The new Basel III framework focuses on the strengthening of the global capital framework and liquidity standards of banks (Hannoun, 2010:1). For this study, Basel III is only discussed briefly, since the focus was on operational risk, which is covered in Basel II.

The Basel III framework was implemented in South Africa on a phased-in basis, commencing on 1 January 2013, and completed in 2018. The framework replaces the previous capital framework with an amended capital framework, as set out in the proposed amended regulations relating to banks. The new reforms strengthen the supervision, regulation and risk management of the banking sector (Hannoun, 2010:3).

As seen in the discussion above, all of these changes occurring in the South African banking industry have become imperative since South Africa is striving towards meeting international standards. It is important for South African banks to understand national and international guidelines developed to assist banks in managing risks. The importance of risk management around the world has driven various countries and committees to develop frameworks, standards, and reports to assist organisations in managing risk.

For the purpose of this study, the following frameworks, standards and reports were compared to gain an understanding of global trends in operational risk management and the importance of risk appetite, namely the Basel II framework (BCBS, 2011), the framework of COSO (COSO, 2004), the ISO 31000 standard (ISO, 2009) and the King III Report (IoDSA, 2009). These are dealt with in the next section.

1.2.4 Comparison of global risk frameworks, standards, and reports

It is imperative for this study to compare global risk frameworks, standards, and reports to assist the South African banking industry in meeting international standards on operational risk management. The following frameworks, standards, and reports will be compared:

- Basel II framework;
- COSO framework;
- ISO 31 000 standard;
- King III Report.

The following information is compared in Table 1.1:

- background;
- aim;
- objective;
- definition of risk management;
- process or framework;
- principles;
- roles and responsibilities;
- definition of operational risk or enterprise risk management;
- definition of risk appetite.

Table 1.1: Comparison of global risk frameworks, standards, and reports

	Basel II framework	COSO framework	ISO 31000 standard	King III Report
Background	Implemented to "establish a flexible banking sector, which can support long-term sustainable growth. Implemented in 2006 to include operational risk, disclosure requirements and supervisory review processes. This inclusion resulted in banks to increase their focus on operational risk, internal risk measures and approaches to measuring credit for capital purposes" (BCBS, 2011:1).	The Committee of Sponsoring Organisations of the Treadway Commission (COSO) in America has "established comprehensive guidelines and frameworks for organisations to manage and govern enterprise risk management, internal controls, and fraud deterrence since 1992. As from 2013, COSO released an updated version of its Internal-control Integrated Framework due to the new requirements of the Sarbanes–Oxley Act. As from 15 December 2014, the 1992 framework became outdated" (McNally, 2013:2).	ISO 31000 was published in "2009 and is an internationally agreed standard for the implementation of risk management principles" (ISO, 2009:1).	The King III report was "implemented due to changes in international governance standards. King III was implemented in February 2009 and issued by the Institute of Directors in Southern Africa" (IoDSA) (Young, 2014:33).
Aim	To "strengthen the stability of international banking systems" (BCBS, 2011:1).	To "improve organisational performance through better integration of strategy, risk, control, and governance" (McNally, 2013:2).	It focuses on the "need for an organisation to manage its risk according to its own needs and structure" (ISO, 2009:v).	"Focuses on corporate governance in South Africa" (Young, 2014:33).
Objective	"To establish operational risk regulation towards a narrow risk management practice over time" (BCBS, 2011:1).	**1992 framework** *"Four objectives:* *Strategic* – high-level goals, aligned with and supporting its mission *Operations* – effective and efficient use of its resources *Reporting* – reliability of reporting *Compliance* – compliance with applicable laws and regulations" **2013 framework**: *"Operations* – effective and efficient use of its resources *Reporting* – reliability of reporting *Compliance* – compliance with applicable laws and regulations" (McNally, 2013:2 & 5).	The "international standard provides for principles and generic guidelines on risk management" (ISO, 2009:v).	"To draft governance principles applicable to all organisations. One of the principles is the governance of risk, which is divided into ten sub-principles that are mainly aimed at the role of the board of directors" (Young, 2014:33).
Definition of risk management		"A process effected by the board of directors, management and other personnel of an entity, applied in strategy and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives" (COSO, 2004:2).	"Coordinated activities to direct and control risk in an organisation" (ISO, 2009:2).	"Is the identification and evaluation of actual and potential risk areas as they pertain to the company as a total entity, followed by the process of either avoidance, termination, transfer, tolerance (acceptance), exploitation, or mitigation (treatment) of each risk, or a response that is a combination or integration" (IoDSA, 2009:56).

Process or framework	Operational Risk Framework: 1. Risk identification and assessment 2. Risk quantification and measurement 3. Risk analysis, monitor and reporting 4. Risk capital allocation 5. Risk management and mitigation (BCBS, 2011:6).	1992 Integrated risk management framework: 1. "Internal environment 2. Objective setting 3. Event identification 4. Risk assessment 5. Risk response 6. Control activities 7. Information and communication 8. Monitoring" 2013 Integrated risk management framework: 1. "Control environment 2. Risk assessment 3. Control activities 4. Information and communication 5. Monitoring" (McNally, 2013:5)	Risk Management Framework: 1. "Mandate and commitment 2. Design the framework for managing risk. 3. Implementing risk management 4. Monitoring and review of the framework. 5. Continual improvement of the framework". The risk management process: 1. "Establish the context 2. Risk assessment: 2.1. Risk identification 2.2. Risk analysis 2.3. Risk evaluation 3. Risk treatment 4. Monitor and review 5. Communication and consultation" (ISO, 2009:vii).	King III focuses on the "adoption of an acceptable risk management approach or framework based on fundamental principles rather than prescriptive measures" (IoDSA, 2009:6).
Principles	1. "The board should take the lead in establishing a strong risk management culture. 2. Banks should develop, implement and maintain a framework that is fully integrated into the overall risk management processes of the bank. 3. The board should establish, approve and periodically review the framework. 4. The board should approve and review a risk appetite and tolerance statement for the operational risk that articulates the nature, types, and levels of operational risk that the bank is willing to assume. 5. Senior management should develop for approval by the board a clear, practical and robust governance structure with defined, transparent and consistent lines of responsibility. 6. Senior management should ensure the identification and assessment of the operational risk inherent in all products, activities, processes, and systems to	17 Principles (2013 framework): **"CONTROL ENVIRONMENT** 1. Demonstrates commitment to integrity and ethical values 2. Exercises oversight responsibility 3. Establishes structure, authority, and responsibility 4. Demonstrates commitment to competence 5. Enforces accountability **RISK ASSESSMENT** 6. Specifies suitable objectives 7. Identifies and analyses risk 8. Assesses fraud risk 9. Identifies and analyses significant change	Risk management (RM): 1. "Creates and protects value. 2. Is an integral part of all organisational processes. 3. Is part of decision-making. 4. Explicitly addresses uncertainty. 5. Is systematic, structured and timely. 6. Is based on the best available information. 7. Is tailored. 8. Takes human and cultural factors into account. 9. Is transparent and inclusive. 10. Is dynamic, iterative and responsive to change. 11. Facilitates continual improvement of the organisation" (ISO, 2009:vii).	Governance of risk: 1. "The board should be responsible for the governance of risk. 2. The board should determine the levels of risk tolerance. 3. The risk committee or audit committee should assist the board in carrying out its risk responsibilities. 4. The board should delegate to management the responsibilities to design, implement and monitor the risk management plan. 5. The board should ensure that risk assessments are performed on a continual basis. 6. The board should ensure that frameworks and methodologies are implemented to increase the probability of anticipating unpredictable risks.

	make sure the inherent risks and incentives are well understood. 7. Senior management should ensure that there is an approval process for all new products, activities, processes, and systems that thoroughly assess operational risk. 8. Senior management should implement a process regularly to monitor operational risk profiles and material exposures to losses. 9. Banks should have a robust control environment that utilises policies, processes and systems, appropriate controls and appropriate risk mitigation and transfer strategies. 10. Banks should have business resiliency and continuity plans in place to ensure an ability to operate on an on-going basis and limit losses in the event of severe business disruption. 11. The public disclosure of a bank should allow stakeholders to assess its approach to operational risk management" (BCBS, 2011:7–18).	**CONTROL ACTIVITIES** 10. Selects and develops control activities 11. Selects and develops general controls over technology 12. Deploys through policies and procedures **INFORMATION AND COMMUNICATION** 13. Uses relevant information 14. Communicates internally 15. Communicates externally **MONITORING** 16. Conducts ongoing and separate evaluations 17. Evaluates and communicates deficiencies" (McNally, 2013:5)		7. The board should ensure that management considers and implements appropriate risk responses. 8. The board should ensure continual risk monitoring by management. 9. The board should receive assurance regarding the effectiveness of the risk management process. 10. The board should ensure that there are processes in place enabling complete, timely, relevant, accurate and accessible risk disclosure to stakeholders" (Young, 2014:33)
Roles and responsibilities	Role of supervisors: 1. "Should conduct regular independent evaluations of the policies, processes, and systems related to the operational risk of a bank. 2. Supervisory evaluations of operational risk should include all the areas described in the principles for the management of operational risk. Supervisors should ensure that operational risk is managed in an appropriate and integrated manner. 3. Deficiencies identified during the supervisory review may be addressed through a range of actions. Supervisors may use the tools most suited to the particular circumstances of the bank and its operating environment. 4. Should continue to take an active role in encouraging ongoing internal development efforts by monitoring and evaluating recent improvements and plans for prospective developments of a bank. These efforts can be compared with those of other banks to provide the bank	1. "Everyone in an entity has a particular responsibility for Enterprise Risk Management (ERM). 2. The chief executive officer is ultimately responsible and should assume ownership. 3. Managers should support the risk management philosophy of the entity, promote compliance with its risk appetite, and manage risks within their spheres of responsibility, consistent with risk tolerances. 4. A risk officer, financial officer, and internal auditor must have key support responsibilities. 5. Other entity personnel is responsible for executing ERM following established directives and protocols. 6. The board of directors must provide meaningful oversight to ERM and is aware of and concurs with the risk appetite of the entity. 7. Some external parties, such as customers, vendors, business partners, external auditors, regulators, and financial	1. "RM responsibilities for the CEO or Board: - Determine strategic approach to risk and set risk appetite - Establish the structure for risk management - Understand the most significant risks - Manage the organisation in a crisis 2. RM responsibilities for the business unit manager: - Build risk aware culture within the unit - Agree on risk management performance targets - Ensure implementation of risk improvement recommendations -Identify and report changed circumstances or risks 3. RM responsibilities for individual employees:	According to King III, it is "the legal duty of directors to act in the best interest of an organisation" (Young, 2014:34). King III "focuses on defining roles and responsibilities for risk management" (IoDSA, 2009:35). King III also emphasises the fact that "risk must be included across the organisation (inclusive approach) and not just reside with one person or function, for example, the Chief Risk Officer (CRO)" (IoDSA, 2009:20).

	with useful feedback on the status of its work" (BCBS, 2011:2–5).	analysts often provide information useful in effecting enterprise risk management, but they are not responsible for the effectiveness of, nor are they a part of, the enterprise risk management of the entity" (COSO, 2004:6). Board oversight: 1. "Understand the risk philosophy of the entity and concur with the risk appetite of the entity. 2. Know the extent to which management has established effective enterprise risk management of the organisation. 3. Review the portfolio of risk and consider it against the risk appetite of the entity. 4. Be apprised of the most significant risks and whether management is responding appropriately" (COSO, 2009:3-4).	- Understand, accept and implement RM processes - Report inefficient, unnecessary or unworkable controls - Report loss events and near-miss incidents - Co-operate with management on incident investigations 4. RM responsibilities for the risk manager: - Develop a risk management policy and keep it up to date - Document the internal risk policies and structures - Co-ordinate the risk management (and internal control) activities - Compile risk information and prepare reports for the board 5. RM responsibilities for specialist risk management functions: - Assist the company in establishing specialist risk policies - Develop specialist contingency and recovery plans - Keep up to date with developments in the specialist area - Support investigations of incidents and near misses 6. RM responsibilities for internal audit manager: - Develop a risk-based internal audit programme - Audit the risk processes across the organisation - Receive and assure the management of risk - Report on the efficiency and effectiveness of internal controls" (AIRMIC et al., 2010:12)	
Definition of operational risk (OpRisk) or	OpRisk: "Risk of direct or indirect loss resulting from inadequate or failed internal processes, people, and systems or from external events. The definition includes	ERM: "Is a process, effected by the board of directors, management and other personnel of an entity, applied in strategy setting and across the enterprise, designed		

Enterprise risk management (ERM)	legal risk but excludes strategic, reputational and systemic risk" (BCBS, 2011:3).	to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives" (COSO, 2009:3).		
Definition of risk appetite	"Is a high-level determination of how much risk a firm is willing to accept considering the risk/return attributes; it is often taken as a forward-looking view of risk acceptance" (BCBS, 2011:6).	"Risk appetite is the amount of risk, on a broad level; an organisation is willing to accept in pursuit of stakeholder value" (COSO, 2012:1).	"Amount and type of risk that an organisation is willing to pursue or retain" (RIMS, 2012:3).	"The level of residual risk that the company is prepared or willing to accept without further mitigation action being put in place, or the amount of risk the company is willing to accept in pursuit of value. The risk appetite of a company will vary from risk to risk. Risk appetite is different from risk-bearing capacity" (IoDSA, 2009:58).

Source: AIRMIC, Alarm and IRM (AIRMIC et al., 2010:2), BCBS (2011:1–18), Committee of Sponsoring Organisations of the Treadway Commission (COSO) (2004:2–7; 2009:3–4; 2012:1), Institute of Directors Southern Africa (IoDSA) (2009:6,20,35, 56, 58), International Organization for Standardization [ISO] 31000 (2009:v-vii, 1,3, 7–8), McNally (2013:2–5), The Risk and Insurance Management Society (RIMS) (2012:5), Young (2014:31–34)

Based on the above information, it is evident from the various international and national frameworks, standards, and reports that operational risk management and risk appetite has become important processes for businesses all around the world. Risk appetite is defined and addressed by all these frameworks, standards and reports. These frameworks and standards have established a range of new risk management principles, processes, reports and roles and responsibilities for the board of directors to consider when implementing an effective operational risk management approach. The following question then remains: are current organisations managing their risk exposures effectively by setting a realistic risk appetite? The next section briefly discusses the concept of operational risk appetite, which was the primary focus of the current research.

1.2.5 Operational risk appetite

According to Young (2010:176), risk appetite is a trend in the modern risk management approach. One of the most critical decisions any organisation ought to make is to determine how much risk to take, in any given situation (Hillson, 2012:1). Over the years, risk appetite has become a global trend and is most commonly described as the level of acceptable risk (Hillson, 2012:1).

The Financial Reporting Council (FRC) in the United Kingdom included the concept of risk appetite in their latest revised Section C of the UK Corporate Governance Code. According to this code, the board of directors is tasked with the role of “determining the nature and extent of the significant risks it [the board] is willing to take in achieving its strategic objectives” (IRM, 2011:11). For this study, various national and international organisations and institutions were researched in the literature review to determine the different approaches to risk appetite.

According to Young (2010:176), an organisation can face different kinds of risks, for example, market, operational, liquidity and credit risk. Each of these types of risks should be controlled differently. As such, a risk appetite statement should be determined for each of these types of risks separately. According to Blunden and Thirlwell (2013:64), the risk appetite for market and credit risk are more easily quantified and articulated than operational risk appetite. According to Moosa (2007:80), because of operational risk having a distinct diversity feature, compared to market and credit risk, this unique feature

will give rise to different methods and approaches in determining what level of operational risk is acceptable (risk appetite). It is imperative that research needs to be conducted to determine how an organisation can set its operational risk appetite. This study aimed to identify guiding principles for an operational risk appetite framework for the banking industry in South Africa.

Numerous risk terms are used in relation to risk appetite, such as risk attitude, tolerance, capacity, exposure, perception, profile, threshold, preference, culture, and propensity. All of these risk terms need to be fully explained and clarified to recognise the overlaps, differences, and relationship to risk appetite (Hillson, 2012:1). Based on recent research by Young (2010:182), these different terms can be used to determine the principles that can be considered by an organisation to determine risk appetite. The current study aimed to examine the different principles and guidelines identified by various organisations and institutions to determine the principles of a typical operational risk appetite framework (ORAF) and statement (ORAS) for a bank.

A risk appetite statement (RAS) ought to provide a basis for an organisation to monitor and evaluate the amount of risk it faces. It is vital for an organisation to establish a well-structured RAS at the board, executive and operational levels. An organisation should be able to come to terms with what they believe to be their appetite for risk and establish an effective ORAF or process (Rittenberg & Martens, 2012:23).

According to Hillson (2012:1), significant business decisions need to consider risk. An organisation must be able to answer the following questions as part of their operational risk appetite process:

- How much risk can we take?
- How much risk do we want to take?
- How much risk do we face?
- How much risk will we take?
- How much risk should we take?
- How much risk are we taking? (Hillson, 2012:1)

The operational risk appetite process will be discussed further in more detail as part of the literature review. For an operational risk appetite process to work effectively, an

organisation needs to implement various methods to express, define and manage their operational risk appetite (Blunden & Thirlwell, 2013:68). According to Blunden and Thirlwell (2013:68–75), an organisation should consider the following methods to define and manage their operational risk appetite:

- absolute figures (risk appetite in relation to actual loss experiences);
- risk and control assessments (risk appetite using risk assessment scores);
- indicators (risk appetite using key risk indicators);
- number of losses (risk appetite using the number of losses); and
- economic capital (risk appetite using regulatory capital modelling).

Given the above, an organisation, such as a bank, must be able to identify its operational risks effectively. In line with Blunden and Thirlwell's (2013:68–75) methods, Young (2010:179) also recognises the same methods to identify operational risks, namely:

- key risk indicators (KRIs);
- scenarios;
- historical or actual losses;
- risk and control self-assessments (RCSAs).

Based on the above, it is clear that various methods have been established over the years to manage operational risk. All of these methods need to be identified and will be discussed in more detail during the literature review.

This section gave a brief overview of some concepts related to operational risk appetite. However, further research needs to be conducted to establish the processes to determine an operational risk appetite and the principles of a standard risk appetite framework and statement for a bank. This forms part of the literature review in Chapter 2.

1.3 PROBLEM STATEMENT

The events of the African Bank debacle have amplified the need for improved and efficient risk management processes in the South African banking industry. Even past events, for example, the financial crisis of 2008, has increased the global importance for an organisation to implement an operational risk management process effectively. Emphasis has been placed on the banking industry to adopt a focused approach to operational risk

management. For a bank to manage its operational risk, which is evolving and changing over time, a bank must know how much risk it is willing to take or accept. It is vital for a bank to develop an approach to determine its operational risk appetite and establish the principles for an ORAF.

Based on the research conducted by Young (2010:176), various role players have written a great deal on this topic of risk appetite with different opinions and views, which have resulted in the misunderstanding of what is the accepted definition for risk appetite.

Even though it is difficult to define the term ‘operational risk appetite’, it is an essential task during the management of operational risk. A bank ought to ensure that the operational risk appetite of the bank is aligned with its strategic business objectives, and provide criteria when the board makes crucial business decisions within a risk-taking environment.

1.4 RESEARCH OBJECTIVES

The study aimed to identify guiding principles for an operational risk appetite framework for the banking industry in South Africa. The following primary objective and secondary objectives were derived from the aim:

1.4.1 Primary objective

To determine guiding principles to formulate an operational risk appetite framework for a South African bank.

1.4.2 Secondary objectives

In support of the primary objective, three secondary objectives were identified:

Firstly, to research the current theoretical knowledgebase for operational risk appetite in order to identify relevant principles for an operational risk appetite framework.

Secondly, to highlight the importance of an operational risk appetite framework in terms of the identified principles.

Thirdly, to determine the current status of implementation of the identified principles for an operational risk appetite framework by South African banks.

1.5 SIGNIFICANCE AND PURPOSE

Various authors, institutions and regulators, based on recent risk events (financial crisis of 2008) in the financial services sector, have acknowledged the significance for an organisation to determine its risk appetite (Young, 2010:177). As early as 1979, Kahneman and Tversky (cited in Hillson & Murray-Webster, 2011:2) emphasised the importance of analysing decisions under risks and the impact of risk perception on decision-making because of uncertainty.

Various authors such as Tversky and Kahnemann (1981), Sitkin and Pablo (1992), Sitkin and Weingart (1995) and Weber and Milliman (1997) (all cited in Hillson & Murray-Webster, 2011:2) conducted research on risk psychology to address the influence of risk perceptions on decision choices under uncertainty. After the 2008 financial crisis, more authors recognised the need to study the concept of risk appetite, for example, Hillson and Murray-Webster (2011:16). Hillson and Murray-Webster start their exploration by considering the ill-defined concept of risk appetite. The outcome of the study led to the development of a clearly defined framework for the different roles of a range of risk-related factors and how they interact to adopt the most appropriate risk attitude. Govindarajan (2011:17) offers a simple process model for organisations to develop a risk appetite statement, while Hillson (2012:6) provides a practical way for decision-makers to answer the “How much risk ...?” question through implementing the Risk Appetite–Risk Attitude (RA–RA) model. Young (2010:186) proposes five guiding principles for managing operational risk appetite in the banking industry. According to Young (2010:186), if banking organisations adopt these guiding principles, it can lead to sound decision-making and improved corporate governance in an organisation.

The IRM (2011) developed a guidance paper on risk appetite and tolerance which was published as a booklet for all sectors in all geographies. The FSB (2013) developed a report on the principles for an effective risk appetite framework. The focus and aim of the Institute of Operational Risk (IOR) is to develop and promote the discipline of operational risk management (IOR, 2009). The Committee of Sponsoring Organisations of the Treadway Commission (COSO) developed a guidance paper on risk appetite entitled “Enterprise Risk Management – Understanding and Communicating Risk Appetite”. The

International Standards Organisation (ISO) published ISO 31000:2009, namely “Risk management – Principles and guidelines”. The BCBS developed the Basel reforms to strengthen the stability of the international banking sector. The King Committee developed the King reports on corporate governance in South Africa.

Based on the above information, it was important that the study should conduct empirical research on global and domestic trends in operational risk management and the importance of risk appetite. This would ensure analysis of the leading and best practices for an ORAF.

1.6 RESEARCH DESIGN AND METHODOLOGY

According to Leedy and Ormrod (2010:2), “research is a systematic process of collecting, analysing and interpreting information in order to increase an interested in or concern about a phenomenon.” Therefore, the literature review aimed to collate the most recent national and international information on the current trends and various methods in managing operational risks, different approaches to risk appetite and the different principles of a typical ORAF for a bank.

Creswell (2009) alternatively describes research designs as plans and procedures that cover the decisions from broad assumptions to particular methods of data collection and data analysis to form a conclusion. Slife and Williams (1995, as cited in Creswell, 2009) note that the underlying philosophical paradigms influence the research design. Creswell (2009) summarises the philosophical paradigms as a postpositive, social construction, advocacy or participatory and pragmatic. Saunders, Lewis and Thornhill (2012:128) on the other hand, state that the research philosophies are pragmatism, interpretivism, realism and positivism. This current study focuses on the postpositive paradigm, as the assumptions made in this paradigm applies to quantitative research. Phillips and Burbules (2000:26) indicate that postpositivism challenges the simple notion of the absolute truth of knowledge. The postpositivism philosophy is deterministic because it needs to identify and assess the causes that influence outcomes. This philosophy is also reductionistic, as the intent is to reduce a broad set of ideas into small and discrete variables that consist of hypotheses and research questions.

When a study must focus on the factors that may influence an outcome which needs to be identified or to gain an understanding of the best predictors of outcomes, it is recommended by Creswell (2009) to use the quantitative approach. According to Creswell (2009), quantitative studies use theory deductively and place the literature review towards the beginning of the study with the objective of testing or verifying a theory, rather than developing it. The theory then becomes the framework for the study that organises the research questions and the data collection procedure. The quantitative approach is the most appropriate for this study, as the literature relevant to operational risk management and operational risk appetite was reviewed to identify the research problem, objectives and questions.

Cooper and Schindler (2008:13) define proper research as reliable and dependable. According to them, to achieve the objectives of the study, a research design should be constructed. Based on this approach, the research design for this study is illustrated in Figure 1.4 below.

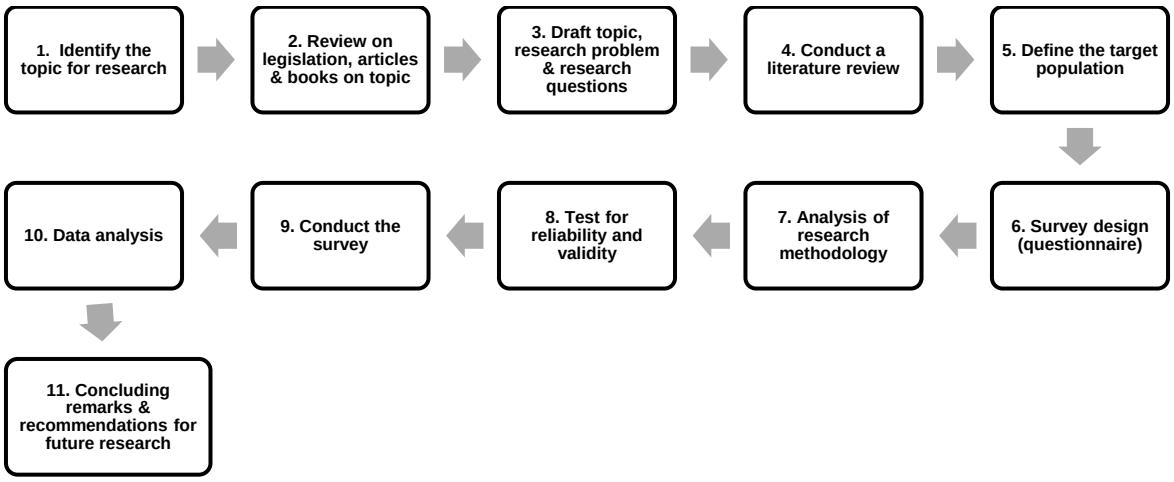


Figure 1.4: Research design to be followed
Source: Authors own compilation

1.6.1 Literature review

According to Kumar (2011:32), the literature review should be able to assist a researcher in the following functions:

- be able to bring clarity and focus to the research problem;
- improve the research methodology;

- broaden the researcher's knowledge base in the research area;
- assist in contextualising the research findings.

For this reason, the literature review forms a fundamental part of the study. It is essential that the literature review focuses on the most recent national and international information on the current trends and various methods of managing operational risks. The literature must also consider the different approaches to risk appetite and the different principles and guidelines identified by various authors and institutions to determine the principles of a typical operational risk appetite framework for a bank.

The current study includes the standards, frameworks and reports implemented over the years, to assist organisations in managing risks and to highlight the importance of an organisation to determine an operational risk appetite. The study also includes and highlights different views, statements and principles regarding the implementation of an operational risk appetite framework, which was used as a basis to establish guiding principles to formulate a realistic operational risk appetite framework for a bank.

1.6.2 Empirical research

The empirical research aims to determine and confirm the applicable risk management concepts by key participants in the South African banking industry. The research questions are the primary constructs for the research instrument, namely a questionnaire.

- **Data measurement**

Cooper and Schindler (2008:289) state that the characteristics of measures are reliability, validity and stability. These characteristics strengthen the research by acknowledging that the measurements derived from the research instruments can be used to reach a conclusion and make recommendations.

- Reliability and validity

It is essential that other researchers should be able to replicate a study. Crowther and Lancaster (2009:80) describe the extent to which the replication of a method would return similar results at a different time, is seen as the reliability of a study. Babbie (2008:160) defines validity as the ability to measure the significance of an empirical concept effectively and to determine to which extent the significance can be viewed as accurate.

For the current study, reliability was tested with Cronbach's Alpha reliability coefficient for Likert-type scales, which is regarded as a sophisticated measure of internal reliability and consistency. The survey questionnaire was pretested by a small team of experts to ensure face and content validity (DeVillis, 2011:105).

- Generalisation

The measurement instrument that was used is a 5-point Likert scale. DeVillis (2011:109) considers a Likert-type scale to be the most accurate and reliable measure when assessing the perspectives of a population. Normality (normal distribution of a data set) can also be tested when using a 5-point Likert-type scale.

- **Target population**

The target population of the research comprised participants in the South African banking industry. Gill and Johnson (2010:127) state that it would be unrealistic to distribute the questionnaire to the entire population, therefore sampling should be used. Moore, Neville, Murphy and Connolly (2010:71) suggest a stratified sampling method. The population has been determined by analysing the financial statements and risk management reports of various banks in South Africa to determine whether the board addresses the operational risk appetite of a bank. The population consisted of the six main banks, namely the Absa Group Limited, First National Bank, Nedbank Group, the Standard Bank of South Africa Limited, Capitec Bank and Investec South Africa. The six banks were identified based on their market share and asset value in the South African banking industry. These banks are also the leading practitioners based on the regulatory requirements in South Africa (SARB, 2018).

The sample was drawn from the participants across a variety of appropriate roles within the top management, board of directors, risk managers, internal auditors and business managers of the banks. The reason for using these role players is that they are instrumental in managing the operational risk exposures of a bank.

- **Data analysis**

The data collected from the sample was statistically analysed with Microsoft Office Excel 2010 and IBM SPSS Statistics. The results obtained from the survey were interpreted

with the use of descriptive and inferential statistics. In order to come to sound conclusions and recommendations, the study was approached in a structured way, based on the chapters as indicated in 1.9.

The next section discusses the main ethical considerations for the study to ensure ethical research and the ethical use of the research.

1.7 ETHICAL CONSIDERATIONS

As early as the 1920s, Watson and Rayner studied behaviourism, and they believed that all behaviour is the product of experience (Sarafino, 2005:63). When their study was undertaken in the 1920s, no ethical guidelines existed to conduct research. Over the years ethics has evolved to accommodate the changing ethos, needs, expectations and values in all professions (Kumar, 2011:241).

According to Kumar (2011:243), there are three stakeholders in research, namely the researcher, the funding body and the research participant or subject. A researcher is seen as anyone who collects information for the specific purpose of the understanding and development of professional knowledge while adhering to the accepted code of conduct. The researcher in the current study is employed by Unisa and receives financial support from the institution (the funding body). The integrity of the research will neither be influenced nor will it be changed in any way on the request of the institution. There is also no potential conflict of interest, as the researcher works in the Department of Finance, Risk management and Banking. The department is the most relevant department when researching topics in risk management and banking, as the department has specialists in this field.

If the researcher achieves the primary objective of the study, all participants and stakeholders will benefit, not only a predetermined sample.

Over the years ethical principles in research have been identified, developed and mentioned by various authors, such as Kumar (2011), Bryman and Bell (2011), Babbie (2008), Cooper and Shindler (2008), and Sarafino (2005). Based on these authors the ethical principles below were taken into consideration during the study and will be further discussed in Chapter 4:

- informed consent;
- avoidance of harm;
- deception;
- privacy, confidentiality and anonymity;
- coercion, incentives and sensitive information.

1.8 LIMITATIONS AND DELIMINATIONS

The first limitation was that the research study was limited to participants that are actively involved in the process of operational risk management in a bank in South Africa. The research was explicitly restricted to operational risk and any other risk types, for example, market and credit risk, fell outside the scope of the current study.

The second limitation was that the study had a limitation on the availability of data, which may be protected or may not be publicly available due to the sensitivity of the information in the banking industry. The number of participants in the operational risk management process in a bank may also be difficult to determine as banking institutions may make use of analysts, specialists or external consultants who might not be included in the sample.

Lastly, due to the limit on the number of questions that a questionnaire may contain, not all of the identified principles for an ORAF in the literature study were used. Only the most important principles were identified and tested in the survey.

1.9 STRUCTURE OF THE STUDY

The thesis consists of the following six chapters:

Chapter 1: Introduction to the study

This chapter consists of a brief overview of the literature, highlighting the current banking industry in South Africa and the importance of managing operational risk within the industry. The problem statement and research objectives have been set. A short description of the research methodology was explained, and the chapter addressed the ethical considerations, as well as limitations of the study.

Chapter 2: Theoretical overview of operational risk

This chapter provides a review of the relevant literature. The literature supported the primary and secondary research objectives, as well as the main constructs of the questionnaire. The chapter focuses on the background of operational risk management in an organisation. The different national and international frameworks, standards and reports developed to manage risk in an organisation, is explained and compared. Operational risks in a bank, the South African banking industry and international practices, is considered and explained. The chapter concludes by providing a relevant theoretical knowledge base to support the primary and secondary research objectives.

Chapter 3: Operational risk appetite

This chapter highlights the importance of determining operational risk appetite and implementing an ORAF and ORAS in an organisation. The chapter provides an overview of the various approaches and principles required to formulate an ORAF and ORAS. It also discusses the challenges that banks are experiencing with the implementation of an operational risk appetite framework and statement.

Chapter 4: Research design and methodology

This chapter focuses on the research design of the study and provides further details of the research methodology used to gather the data, as well as the statistical techniques used to analyse the data.

Chapter 5: Analysis of survey

This chapter presents the interpretation of the findings of the survey results based on the descriptive and inferential statistical analysis of the principles for an operational risk appetite framework for the banking industry in South Africa and the implementation status thereof.

Chapter 6: Summary, conclusion and recommendations

This chapter concludes with the findings, summary, research contribution and recommendations of the study. A conclusion is reached based on the findings of the survey regarding the crucial principles for an operational risk appetite framework in the

South African banking industry. The limitations of the study and suggestions for future research are also presented.

References

The reference section comprises all the sources referenced in the research on operational risk management and operational risk appetite in the South African banking industry and globally. The referencing technique used in the research complies with the standards of the Harvard referencing technique.

Appendices

Appendices are attached to this research report on operational risk appetite in the South African banking industry, namely the operational risk appetite questionnaire, informed consent letter, diagnostic questionnaire, ethical clearance certificate, confidentiality agreement with the statistician, descriptive statistics and correlation coefficient results and a checklist for an operational risk appetite framework.

1.10 CONCLUSION

Chapter 1 provided an introduction and outline of the study. The chapter introduced the reader to the importance of implementing the concept of operational risk appetite as a risk management tool in the South African banking industry. It presented a background for risk management, operational risk management, the South African banking industry and operational risk appetite. The chapter also compared global risk frameworks, standards and reports in order to assist the South African banking industry to meet international standards regarding operational risk management. It was also highlighted that a bank should implement an operational risk appetite process in order to formulate an ORAF and ORAS. The significance of establishing guiding principles to articulate an ORAF in a bank was also specified.

A problem statement was formulated. Based on the problem statement, the research questions were derived at, followed by the primary and secondary objectives. This study collected data from publicly available sources and participants in the South African banking industry, namely the top six banks. In order to accomplish the objectives of this study, the research methodology was presented, namely an outline of the research

design, the research instrument and the collection and analysis of data. Research questions were suggested in order to support the research objectives. Consideration was further given to the limitations of the study and research ethics. The chapter was concluded by presenting and clarifying the structure of the study.

The next chapter gives a theoretical overview of operational risk. It will focus on the definition of operational risk, the background and adoption of operational risk management and explain the ORAF and process for a bank. It will also highlight the different national and international frameworks, standards and reports developed to manage operational risk, the adoption of operational risk in the South African banking industry and international practices.

CHAPTER 2: THEORETICAL OVERVIEW OF OPERATIONAL RISK

2.1 INTRODUCTION

The significance of implementing the concept of operational risk appetite as a risk management tool in the South African banking industry was highlighted in Chapter 1. The purpose of this chapter is to focus on the definition of operational risk, the background and adoption of operational risk management, and to explain the ORAF and process for a bank. It is essential to understand the concept of operational risk management, which is used to identify, analyse, monitor and control operational risks. These activities rely on an underlying understanding of the risk appetite of a bank.

The chapter will also highlight the different national and international frameworks, standards and reports developed to manage operational risk, the adoption of operational risk in the South African banking industry, and international practices.

2.2 OPERATIONAL RISK DEFINITION

Different meanings and views regarding various definitions of operational risk have been established over the past few years in the banking industry. According to Kulpa and Magdoń (2012:37), a study by the British Bankers' Association, International Swaps and Derivative Association, PricewaterhouseCoopers LLP and the Risk Management Association were conducted of the different operational risk definitions by banks in 1999. When that study was concluded, the following four definitions emerged:

- "Operational risk is the risk that results from system maladjustments, operational problems, breaching guidelines developed by internal auditors, fraud and unpredicted catastrophes causing unpredicted losses for the organisation.
- Operational risk is endangering the company with financial and non-financial losses, caused by unpredicted events or failures in operational systems and processes.
- Operational risk is the risk of fraud committed by employees or persons outside an organisation, and the risk of conducting unauthorised transactions or errors caused by information technology (IT) systems.

- Operational risk should be viewed from the effectiveness and integrity of the systems of control and other mechanisms whose aim is the implementation of business processes" (Kulpa and Magdoń, 2012:37).

There are also various authors and institutions that have developed their own operational risk appetite definitions, which are shown in Table 2.1 below.

Table 2.1: Operational risk definitions

Author or institution	Operational risk definition
BCBS	"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 reputational, systemic and strategic risk" (BCBS, 2002:2).
The Hong Kong Monetary Authority	"Risk of direct or indirect loss resulting from inadequate or failed internal processes, staff and systems, or from external events" (The Hong Kong Institute of Bankers, 2013:5).
The British Bankers' Association	These are: • "risks associated with inadequate procedures and control, human error, fraudulent and criminal activity; • risks caused by technological shortcomings and system breakdowns; • all risks which are arising from business decisions, such as competitive action and pricing; • legal risks and risks to business relationships, failure to meet regulatory requirements or adverse influence on the bank's reputation; and • 'external factors', such as natural disasters, terrorist attacks and fraudulent activity" (Moosa, 2007:90).
Blunden and Thirlwell	"Operational risk covers all the internal and external sources of operational risk" (Blunden & Thirlwell, 2013:11).
JPMorgan Chase	"Operational risk is the risk of loss resulting from inadequate or failed processes or systems, human factors or external events" (Girling, 2013:179).
Young	"Operational risk is the exposure of an organisation to potential losses, resulting from shortcomings and failures in the execution of its operations. These losses may be caused by internal failures or shortcomings of people, processes and systems, as well as the inability of people, processes and systems to cope with the adverse effects of external factors" (Young, 2014:21).
Deutsche Bank	"Operational risk is the potential for failure (including the legal component) with regards to employees, contractual specifications and documentation, technology, infrastructure and distastes, external influences and customer relationships" (Girling, 2013:179).
Peccia	"The potential for loss due to failures of people, processes, technology and external dependencies" (Chapman, 2011:268).
Kendall	"The risk connected with a loss as a result of defective systems operations, insufficient control, improper management or human error" (Kulpa & Magdoń, 2012:36–37).
Turing	"The risk that deficiencies in information systems or internal controls will result in an unexpected loss".

	"The risk that a firm will suffer loss as a result of human error or deficiencies in systems or controls". "The risk run by an organisation that its internal practices, policies and systems are not rigorous or sophisticated enough to cope with untoward market conditions or human or technological errors". "The risk of loss resulting from errors in the processing of transactions, breakdown in controls, errors or failures in system support" (Moosa, 2007:95–96).

Based on the definitions above, it is evident that there is a common understanding of what is meant by operational risks and how to define it. The Financial Services Authority (FSA) (2002, as cited in Chapman, 2011:269) states:

> "[U]ltimately firms need to decide for themselves what operational risk means to them, and any firm needs to consider a more specific definition of operational risk that is appropriate to the range and nature of its business activities and its operating environment."

Even though a business can define operational risk in its own terms, the most widely adopted definition by most financial industries is the definition set out by the BCBS (2002:2), which explains that operational risk is "the risk of loss resulting from inadequate or failed internal processes, people, and systems or from external events." The BCBS definition is based on the occurrence of certain events that cause loss to the bank, but cannot be explicitly assigned to credit or market risk (Ghosh, 2012:389). For the purposes of this study, the BCDS definition of operational risk was accepted.

According to Girling (2013:178), the BCBS definition can be broken down into specific components, namely:

- Risk of loss: For an operational risk to exist there must be an associated loss anticipated.
- Causes of the loss that might give rise to an operational risk event:
    - inadequate or failed processes;
    - inadequate or failed people;
    - inadequate or failed systems; or
    - external events.

Mestchian (2003, cited in Moosa, 2007:92) suggests the unravelling of the definition of the BCBS into the following components:

- Process risks, for example, ineffectiveness or inefficiencies in the numerous business processes within an organisation. These include value-driven processes, such as product development and customer support, sales and marketing, and value-supporting processes such as human resources (HR), information technology (IT), and operations.
- People risks, for example, employee misdeeds or error, employee absence, inadequate employee development and recruitment.
- System or technology risks, for example, data quality and integrity issues, system failures caused by breakdown, poor project management and inadequate capacity.
- External risks, for example, macroeconomic and socioeconomic events and the risk of loss caused by the actions of external parties (for example, regulatory changes, competitor behaviour and external fraud).

It is evident that a bank should have a clear understanding of what is meant by the term ‘operational risk’ and the definition of a bank should include the full range of operational risk components (processes, people, systems and external events) encountered, and the most significant causes of operational losses (BCBS, 2002:2). It is important for employees of a bank to understand the definition and the components of operational risk to determine its operational risk appetite. A bank should also communicate its operational risk definition within its operational risk management framework, which will promote the understanding of operational risk by the staff and enhance the risk awareness across an organisation (Ghosh, 2012:400). It is furthermore important for the employees of a bank to understand the origin of operational risk and what operational risk management is comprised of in order to manage and measure operational risks effectively to ensure that the organisation is in line with its risk appetite (Young, 2014:17). The next section will discuss the background of operational risk management in the banking industry.

2.3 THE BACKGROUND OF OPERATIONAL RISK MANAGEMENT IN THE BANKING INDUSTRY

As quoted by Samad-Khan (2010, cited in Chapman, 2011:267):

> "[O]rganisations that choose to remain blissfully ignorant of operational risk will continue to operate under a false sense of security. They will remain "under-controlled" in areas where they have the most risk and "over-controlled" in areas where they have the least risk. So, without addressing operational risk head-on, recognising and understanding it and acknowledging the crucial role that it plays, we face the prospect of another global financial crisis in the not too distant future."

Based on this quote, it seems evident that more attention should be given to manage and embed operational risk management effectively into an organisation to lessen the impact of financial failures.

According to the British Bankers Association (1999, cited in Teplý, Chalupka & Černohorský, 2009:692), operational risk management is not a new risk but has developed over the past few years into a discipline in its own right with newly established tools, processes and management structures. The operational risk management discipline became imperative in 1988 when the BCBS started to emphasise operational risks in banks (Young, 2014:ix). Before 1988, operational risk was seen as a residual risk category (any risk that is not market or credit risk), because it was considered to be too difficult to manage, quantify or insure in a traditional way (Teplý et al., 2009:692). Even though operational risk was in the past perceived as a residual risk, it was still being implemented by a bank in some way, for example, banks have always been trying to maintain the integrity of internal controls, prevent fraud and reduce risks and errors in their transaction processes (BCBS, 2002:3).

The significance of operational risk management within banks was also confirmed by a survey conducted by the British Bankers Association, and Coopers and Lybrand (1997, cited in Kulpa & Magdoń, 2012:35), which indicates that 70% of the surveyed banks perceived operational risk management as equal or even more important than credit or market risk. This perception is also accepted by the BCBS, which recognises the role of operational risk management as an essential aspect of sound risk management practices

in financial institutions (Schwartz Gârliste, 2013b:173). Since the formulation of the Basel II Accord by the BCBS in 2001, the importance of categorising operational risk as a separate main risk type in a bank was emphasised (Young, 2014:ix). With the implementation of Basel II in 2006, it became increasingly important for a bank to understand how operational risks link with the other risk categories, and how to control and monitor these risks (Kulpa & Magdoń, 2012:35). If operational risks are not managed or measured accordingly, they can affect the soundness and stability of the banking system (Bostander, 2007:12).

It is imperative for a bank to identify and manage operational risks within all the processes and activities in a bank. This view is supported by Nâstase and Unchiaşu (2013:105), who mention that operational risk is an inherent factor of any business activity or the environment, internal procedure, technical infrastructure and corporate governance framework. This view is also supported by the FSA, which states that operational risk is present in all firms and can affect the solvency of a firm, the fair treatment of its customers and the occurrence of financial crime (Chapman, 2011:267). Due to the nature and impact of operational risks, an organisation can be destroyed in the event of an operational risk incident, because it can lead to the loss of operating capabilities, reputational damage or a decrease in monetary value (Martin, 2009:75). According to Young (2014:1), the continuous improvement of sophisticated technology, the increasing vulnerability of organisations to operational losses, the complexity of products, the rapid expansions of business areas across international borders and major incidents attributed to operational failures, this also resulted in increased attention to operational risk events. As a result, the need for an organisation to determine its operational risk appetite, as discussed in Chapter 1(see 1.2.5), has become extremely significant, which supports the purpose of this study. Against this background, the different financial failures and operational risk events, which contributed to the emphasis on operational risk management, will be discussed in the next section.

2.3.1 Financial failures and operational risk events

The increasing financial problems of global organisations and frequent bankruptcies have made operational risk management one of the most important topics currently in the

financial industry (Kulpa & Magdoń, 2012:47). History has shown that various crises over the last few years started with operational problems (Kulpa & Magdoń, 2012:35). Financial fiascos involving Barings Bank, American International Group, Citigroup, HBOS plc, Northern Rock and the financial crises of 2008 illustrate failures in risk management or corporate governance (Martin, 2009:79). These debacles have increased the importance of effective operational risk management within an organisation. Table 2.2 illustrates various corporate collapses and scandals over a number of years, where risk management and corporate governance failed.

Table 2.2 Examples of corporate collapses and scandals

Year	Country	Company	Underlying cause
1974	Germany	Herstatt Bank	Settlement risk, lead to the bankruptcy of the bank.
1995	United Kingdom	Barings Bank	A derivatives trader, Nick Leeson, managed to hide unreported losses for over two years, which led the bank to bankruptcy. This was due to mismanagement and weak internal controls. Shareholders' wealth lost (US $): 1.3 billion
1996	Japan	Sumitomo Corporation	Copper trader, Yasuo Hamamaka, known as 'Mr Five Per Cent' piled up unreported losses over three years, because of the proportion of the copper market he controlled. Reputational damage. Shareholders' wealth lost (US $): 2.6 billion
2000	United States	Tyco	Accounting fraud
2001	United States	Enron	Accounting fraud and fictitious SPEs (special purpose entities) Created off-balance sheet exposures to hide debts and losses. Shareholders' wealth lost (US $): 80 billion Jobs lost: 4 500
2001	Australia	HIH Insurance	Mismanagement and poor strategic decisions.
2002	United States	Worldcom	Mismanagement and weak internal controls. Arthur Anderson hid expenses ($3.9 billion) to raise the bottom line. Shareholders' wealth lost (US $): 100 billion Jobs lost: 17 000
2002	United States	Allied Irish Bank	Trader, John Rusnack, hid three years of losing trade on the yen/dollar exchange rate. Reputational damage occurred. Shareholders' wealth lost (US $): 691 billion

2002	United States	Xerox	Improper reports of $6.5 billion in revenue over five years. Shareholders' wealth lost (US $): 3 billion Jobs lost: 13 600
2002	United States	Merck & Co.	$14 billion in revenue reported over many years but was never collected. Shareholders' wealth lost (US $): 43 billion
2003	Netherlands	Royal Ahold	Accounting fraud; fictitious earnings were created.
2003	Italy	Parmalat	Accounting fraud and a kickback scheme; fictitious earnings were created.
2004	Singapore	China Aviation Oil	Mismanagement and poor strategic decisions.
2005	South Africa	Regal Treasury	Accounting fraud and mismanagement.
2006	South Africa	Leisurenet	Mismanagement.
2008	India	SATYAM	Accounting fraud, by inflating earnings and assets.
2008	Europe	Société Générale	Trader (Jérôme Kerviel) was systematically deceiving systems by taking unauthorised positions in stock index futures. (IT risk). Shareholders' wealth lost (Euro €) 4.9 billion. Bank managed to absorb the loss, but reputational damage occurred.
2008	United States	Lehman Bros	The largest bankruptcy in US history. The mark-to-model valuations of the company for securitised mortgage portfolios were untrustworthy.
2009	South Africa	Fidentia	Accounting fraud and mismanagement.
2011	Switzerland	UBS	Trader, Kweku Adoboli, traded on fraudulent and unauthorised exchange-traded fund transactions. Shareholders' wealth lost (US $): 2.3 billion.

Sources: Hendrikse and Hefer-Hendrikse (2012), and Jednak and Jednak (2013:72).

As illustrated in Table 2.2, some scandals were due to internal fraud, rogue traders, management failures, operational losses not monitored, and market or operational risk failures. The cost of these failures can be high and catastrophic, due to the complexity, increased size and interconnectedness of financial institutions. The impact of an operational risk event can have a much more destructive and more significant consequence than any other risk category; this is due to the difficulty of quantifying and measuring the performance of operational risks within business areas, which can magnify system-wide risk levels (Jobst, 2010:47).

The above-mentioned operational risk events caused internal and external events such as bankruptcy, massive monetary losses, trivial development strategies, decreased the market value of shares, reputational damage and job losses which led to the deterring of growth within the global financial economy (Jednak & Jednak, 2013:72). The importance of effective operational risk management within a financial institution is growing because, if financial institutions fail, they fail considerably, which leads to huge shocks and ripple effects in all the global financial systems (Grody & Hughes, 2008: 54). According to Martin (2009:84), organisations in the banking industry must start to demonstrate that they can learn from past failures and not repeat the same mistakes, and they need to start taking operational risk management more seriously. If the operational risks of a bank are not adequately managed, it can lead to substantial financial problems. Based on this discussion, it can be concluded that the importance of strong operational risk management is becoming more vital every day. With robust operational risk management processes, a bank should be able to avoid bad surprises and prepare itself to respond swiftly when an operational risk event occurs (Girling, 2013:24).

The next section presents a discussion on the different international operational risk frameworks, standards and reports, and how these can be implemented in the South African banking industry.

2.4 INTERNATIONAL OPERATIONAL RISK FRAMEWORKS, STANDARDS AND REPORTS IN THE SOUTH AFRICAN BANKING INDUSTRY

Based on the comparison of the global risk frameworks, standards and reports in Chapter 1, this section will further discuss which international practices were implemented to manage operational risk in a South African bank. The following frameworks, standards and reports were compared in Chapter 1: Basel II Framework, COSO ERM Framework, ISO 31000 Standard and the King reports. The comparison in Chapter 1 considered the following information, namely the background, aim, objective, a definition of risk management, process or framework, principles, roles and responsibilities, the definition of operational risk or enterprise risk management and definition of risk appetite. Based on the comparison, it is evident from the various international and national frameworks,

standards and reports that operational risk management and operational risk appetite has become an essential process for organisations all around the world.

Two main role players, from a South African perspective, are the King Committee on Corporate Governance and the BCBS. The King Committee on Corporate Governance was formed to consider corporate governance in the context of South Africa (IoDSA, 2009:4). The BCBS, on the other hand, formulated broad supervisory guidelines and standards and recommended statements of best practice for operational risk management for use by banks and supervisory authorities (BCBS, 2002:1). The International ISO 31000 Standard: Risk Management – Principles and guidelines, was developed in 2009 by the ISO, and has strongly influenced the risk management field.

Lastly, COSO published in 2004 the COSO ERM Integrated Framework, which focuses on the importance of understanding and embracing ERM in an organisation. For the purpose of the current study these practices, approaches and recommendations will be dealt with in more detail in the ensuing sections.

2.4.1 The King reports

Financial institutions, and particularly banks, are critical for any economy to flourish. It is therefore crucial that banks have strong corporate governance structures (Hendrikse & Hefer-Hendrikse, 2012:143). It is essential for the employees of a bank to understand the meaning of corporate governance. The UK Cadbury Commission Report on Corporate Governance, 1992, gives the following definition: "corporate governance is the system by which businesses are directed and controlled" (Chapman, 2011:34). In 2004, the Organisation for Economic Co-operation and Development (OECD) expanded the definition to:

> "[C]orporate governance involves a set of relationships between a company's management, its board, its shareholders and other stakeholders. Corporate governance also provides the structure through which the objectives of the company are set, and the means of attaining those objectives and monitoring performance are determined" (Chapman, 2011:34).

It is clear from these definitions that corporate governance is the practice by which organisations are managed and controlled. Corporate governance in South Africa was established by the publication of the King Report on Corporate Governance in 1994. The

King Committee on Corporate Governance (headed by Dr Mervyn King) was formed in 1992 under the authority of the Institute of Directors in Southern Africa (IoDSA), to consider corporate governance due to increasing interest all around the world, in the context of South Africa (Hendrikse & Hefer-Hendrikse, 2012:5–6). The purpose of the King Report (1994) was to promote the highest standards of corporate governance in South Africa. After legislative developments, locally and internationally, the King I Report was revised and replaced by the second King Report on Corporate Governance for South Africa. The King II Report was published in 2002 with the following six sections, namely board and directors, risk management, internal audit, integrated sustainability reporting, accounting and auditing, and compliance and enforcement (Valsamakis, Vivian & Du Toit, 2010:83).

Unlike the King I report, which covered only one element of risk management, namely internal control, the King II report addresses risk management as a core element of corporate governance (Valsamakis et al., 2010:83). The following are seen as the most critical recommendations in the King II Report regarding risk management (refer to Table 2.3 below).

Table 2.3: King II risk management and recommendations

	Recommendations:
1	"The ultimate responsibility for the total process of risk management resides with the board. The King II report acknowledges accountability of management towards the board for implementing, designing and monitoring the risk management process."
2	"The board in liaison with senior management should set the risk strategy policies and ensure that the assessment of the risk processes is undertaken. This risk assessment should address the exposure of the organisation to the following: - operational and physical risks; - technology risks; - market and credit risks; - human resource risks; - compliance risks; and - business continuity and disaster recovery."
3	"A board committee needs to oversee the entire risk management process and must determine the effectiveness of the process."
4	"The internal audit function should not assume the systems, processes and functions of risk management, but should give assurance about management's assertions surrounding the effectiveness of internal control and risk management."

5	"A comprehensive system of control should be established by the board to ensure that risks are mitigated and risks should be assessed on an ongoing basis."
6	"An organisation must develop a risk management system and internal control measures which build a more robust business operation and delivers: - a commitment by management to the risk management process; - a system of documented risk communications; - a demonstrable system of risk identification; - a system of documenting the cost of non-compliance and losses; - a demonstrable system of risk mitigation activities or techniques; - a register of key risks that could affect shareowners and relevant stakeholder interests; - an alignment of assurance of efforts to the risk profile."
7	"The board must identify key risk areas and key performance indicators."
8	"In the annual report of an organisation, the directors must disclose that they are accountable for the risk management process and that an active process, which is regularly reviewed, has been instituted. The directors should also provide assurance regarding the procedures, which will assist the organisation to continue with its core business processes in the event of a disaster. The effectiveness of the internal controls of an organisation must be disclosed."

Source: IoDSA (2002:75–85)

Based on the recommendations as mentioned above, it is evident that the King II report repeatedly emphasises the accountability and responsibility of the board towards the overall risk management process. By complying with the corporate governance principles, an organisation must consider the importance of an integrated risk management framework, which covers all the risks in an organisation (Valsamakis et al., 2010:83–84). According to Bhargava (2014:65), the incorporation of strong operational risk management with well-developed and effective corporate governance structures are considered best industry practice for banks.

The implementation of the Companies Act (No. 71 of 2008) (South Africa, 2008), and changes in international governance developments necessitated the third report on corporate governance in South Africa. King III, which was published in 2009, is a recommended code of corporate conduct for all entities (private, public and non-profit sectors) (IoDSA, 2009:16). Even though the King III report applies to all entities, it is still a non-legislated compliance framework. However, as of June 2010, the Johannesburg Stock Exchange Institute (JSE) requires listed companies to comply with King III (IoDSA, 2009:5). The King III report has widened the range of corporate governance in South

Africa with its fundamental philosophy regarding sustainability, corporate citizenship and leadership (Hendrikse & Hefer-Hendrikse, 2012:101). The King III report on corporate governance, conduct, practices and principles were established to be used by South African banks when developing a corporate governance and risk management framework. The King III report consists of ten principles for corporate governance. One of these principles is the governance of risk, which is discussed in Table 2.4 below.

Table 2.4: King III principle 4: The governance of risk

Governance element	Principle	Recommended practice
The responsibility of the board for risk governance	"The board should be responsible for the governance of risk."	"The board should develop a risk management policy and plan to implement a system and process for risk management. The board should comment in the integrated report on the effectiveness of the system and process of risk management. The responsibility of the board for risk governance should be expressed in the board charter. The induction and ongoing training programmes of the board should incorporate risk governance. The responsibility of the board for risk governance should manifest in a documented risk management policy and plan. The board should approve the risk management policy and plan. The risk management policy should be widely distributed throughout the company. The board should review the implementation of the risk management plan at least once a year. The board should ensure that the implementation of the risk management plan is monitored continually."
	"The board should determine the levels of risk tolerance."	"The board should set the levels of risk tolerance once a year. The board may set limits for the risk appetite. The board should monitor that risks taken are within the tolerance and appetite levels."
	"The risk committee or audit committee should assist the board in carrying out its risk responsibilities."	"The board should assign a committee responsible for risk. The risk committee should: - consider the risk management policy and plan and monitor the risk management process; - have as its members executive and non-executive directors, members of senior management and independent risk management experts to be invited, if necessary; - have a minimum of three members; and - convene at least twice per year.

		The performance of the committee should be evaluated once a year by the board."
Management's responsibility for risk management	"The board should delegate to management the responsibility to design, implement and monitor the risk management plan."	"The risk strategy of the board should be executed by management using risk management systems and processes. Management is accountable for integrating risk in the day-to-day activities of the company. The Chief Risk Officer (CRO) should be a suitably experienced person who should have access to and regularly interact on strategic matters with the board and appropriate board committee and executive management."
Risk assessment	"The board should ensure that risk assessments are performed on a continuous basis."	"The board should ensure that adequate and ongoing risk assessments are performed. A systematic, documented, formal risk assessment should be conducted at least once a year. Risks should be prioritised and ranked to focus on responses and interventions. The risk assessment process should involve the risks affecting the various income streams of the company, the critical dependencies of the business, the sustainability and the legitimate interests and expectations of stakeholders. Risk assessments should adopt a top-down approach. The board should regularly receive and review a register of the key risks of the company. The board should ensure that key risks are quantified where practicable."
	"The board should ensure that frameworks and methodologies are implemented to increase the probability of anticipating unpredictable risks."	"The board should ensure that a framework and processes are in place to anticipate unpredictable risks."
Risk response	"The board should ensure that management considers and implements appropriate risk responses."	"Management should identify and note in the risk register the risk responses on which they decide. Management should demonstrate to the board that the risk response provides for the identification and exploitation of opportunities to improve the performance of the company."
Risk monitoring	"The board should ensure continuous risk monitoring by management."	"The board should ensure that adequate and continuous monitoring of risk management takes place. The responsibility for monitoring should be defined in the risk management plan."

Risk assurance	"The board should receive assurance regarding the effectiveness of the risk management process."	"Management should assure the board that the risk management plan is integrated into the daily activities of the company. An internal audit should provide a written assessment of the effectiveness of the system of internal controls and risk management to the board."
Risk disclosure	"The board should ensure that there are processes in place enabling complete, timely, relevant, accurate and accessible risk disclosure to stakeholders."	"Undue, unexpected or unusual risks should be disclosed in the integrated report. The board should disclose its view on the effectiveness of the risk management process in the integrated report."

Source: IoDSA (2009:35–39)

It is clear from Table 2.4 that the governance and management of risk are seen as the responsibility of the board. It is also vital for the board to set the levels for risk appetite and risk tolerance of the organisation, and monitor that the risks taken are within the appetite and tolerance levels.

King III is also based on the following two aspects, namely inclusive stakeholder approach and integrated reporting. With an inclusive stakeholder approach, the interest and expectations of stakeholders are considered when decisions are taken in the best interest of an organisation (IoDSA, 2009:11–12). By issuing integrated reports, which holistically indicate the performance of an organisation in terms of both its finance and sustainability, an organisation will be able to increase the confidence and trust of its shareholders, enhance the legitimacy of its business operations, increase business opportunities and improve its risk management processes (IoDSA, 2009:11–12).

On 1 November 2016, the IoDSA released the King IV report on Corporate Governance for South Africa. King IV replaces King III in its entirety, and the application of King IV is effective in respect of financial years starting on or after 1 April 2017 (PwC, 2016:2). King IV builds on the positioning of its predecessor regarding sound corporate governance as an essential element of good corporate citizenship (PwC, 2016:2). According to Deloitte (2016:1), King IV provides a more practical, outcome-based approach to good corporate

governance and incorporates both global public sentiment and international regulatory changes since the incorporation of King III. The objectives of King IV are the following:

- Promote corporate governance as integral to running an organisation and delivering governance outcomes such as an ethical culture, good performance, effective control and legitimacy.
- Reinforce corporate governance as a holistic and interrelated set of arrangements to be understood and implemented in an integrated manner.
- Broaden the acceptance of King IV by making it accessible and fit for implementation across a variety of sectors and organisational types.
- Present corporate governance as concerned with, not only structure and processes, but also with an ethical consciousness and conduct.
- Encourage transparent and meaningful reporting to stakeholders (IoDSA, 2016:22).

As seen above, King IV has moved away from “apply and explain” to a more outcome-based approach. The new code has reduced the 75 principles in King III to 17 basic principles. For this study, the focus is on principle 11, which explains the governance of risk. As in King III, King IV is still focusing on the governance of risk, but the code is now recognising the complexity of risks and the need to strengthen risk oversight (IoDSA, 2016:30). One of the significant changes in the recommendation is that the risk committee comprises of a majority of non-executive members as part of the governing body. This recommendation goes beyond what was required in King III (IoDSA, 2016:30).

Principle 11 focuses on the governing body’s process regarding how to govern risk in a way that supports the organisation in setting and achieving its strategic objectives (IoDSA, 2016:41). The following are recommended practices for the governance of risks based on King IV:

- “The governing body should assume responsibility for the governance of risk by setting the direction for how risk should be approached and addressed in the organisation. Risk governance should encompass both:
    - the opportunities and associated risks to be considered when developing strategy; and

  - the potential positive and negative effects of the same risks on the achievement of organisational objectives.
- The governing body should approve a policy that articulates and gives effect to its set direction on risk.
- The governing body should treat risk as integral to the way it makes decisions and executes its duties.
- The governing body should evaluate and agree on the nature and extent of the risks that the organisation should be willing to take in pursuit of its strategic objectives. It should approve in particular:
  - the risk appetite of the organisation, namely its propensity to take appropriate levels of risk; and
  - the limit of the potential loss that the organisation can tolerate.
- The governing body should consider the need to receive periodic independent assurance on the effectiveness of risk management.
- The governing body should exercise ongoing oversight of risk management and, in particular, oversee that it results in the following:
  - an assessment of risks and opportunities emanating from the triple context in which the organisation operates and the capital that the organisation uses;
  - an assessment of the dependence of the organisation on resources and relationships as represented by the various forms of capital;
  - an assessment of the potential upside, or opportunity, presented by risks, with potentially adverse effects, on achieving organisational objectives;
  - the design and implementation of appropriate risk responses;
  - the integration and embedding of risk management in the business activities and culture of the organisation;
  - the establishment and implementation of business continuity arrangements that allow the organisation to operate under conditions of volatility, and to withstand and recover from severe shocks.
- The governing body should delegate to management the responsibility to implement and execute effective risk management.

- The nature and extent of the risks and opportunities the organisation is willing to take should be discussed without compromising sensitive information.
- Also, the following should be disclosed concerning risk:
    - an overview of the arrangements for governing and managing risk;
    - critical areas of focus during the reporting period, including objectives, the key risks that the organisation faces, as well as undue, unexpected or unusual risks and risks, are taken outside of risk tolerance levels;
    - actions are taken to monitor the effectiveness of risk management and how the outcomes were addressed;
    - planned areas of future focus" (IoDSA, 2016: 61–62).

From the mentioned recommended practices, the importance of an organisation to agree on the nature and extent of the risks the organisation is willing to pursue in order to achieve objectives is evident. An organisation should approve its risk appetite and the limit of the potential loss the organisation is willing to tolerate to achieve good risk governance.

Based on the above, it can be highlighted that corporate governance involves the way in which the affairs and business of banks are overseen by their senior management and the board, affecting how banks:

- determine objectives (generating economic returns to owners);
- consider the interests of recognised stakeholders;
- run the daily operations of the bank;
- protect the interest of depositors; and
- align business behaviours and activities with the expectation that banks will operate safely and soundly, and comply with appropriate laws and regulations (Hendrikse & Hefer-Hendrikse, 2012:143).

It is evident from the above mentioned that corporate governance should consider the interests of all stakeholders (for example savers, depositors and policyholders), and the stability of the banking system as a whole. When an organisation implements corporate governance, it should align its practices with that of the board of directors, its shareholders, the risk strategy, appetite and profile of the bank (Hendrikse & Hefer-

Hendrikse, 2012:144). In conclusion, it is clear that the practice of good corporate governance in a bank includes the responsibility of the board to determine the limits for risk appetite and to monitor that the risks that are taken are within the appetite levels of the bank.

The next section discusses Basel II in order to highlight best practices for operational risk management for use by banks and supervisory authorities.

2.4.2 The Basel accords

The Basel II framework is an international standard and best practice guide that defines the minimum capital requirements for internationally active banks (Hendrikse & Hefer-Hendrikse, 2012:69). Basel II aims to promote stability in the banking sector and to minimise the possibility of bank failures (protect banks from operational loss events). The Basel frameworks are issued and updated by the BCBS, which falls under the Bank for International Settlements (BIS). The committee has no formal global authority and only recommends standards of best practice (Sweeting, 2011:473). Only the banks in the Group of Ten (G10) countries (which have now become 11 countries[1]) should implement the Basel frameworks. Currently, more than 100 other countries (including South Africa) have volunteered to adopt these principles or to take them into account and to use them as a foundation for national rulemaking and regulation processes (Hendrikse & Hefer-Hendrikse, 2012:69).

In support of the implementation of the Basel II framework in banks across various countries, Moosa (2007:36) highlights the need for minimum capital requirements under the following points:

- e-commerce carries the risk of external and internal fraud, system security issues and authentication problems;
- credit and market risk mitigation techniques (for example, credit derivatives) which may result in another kind of risk (for example, legal risk);
- if not adequately controlled, the increasing use of automated technology can alter risk from labour-intensive processing errors to system failure risks;

[1] Canada, Italy, Japan, Belgium, Sweden, the Netherlands, France, the United Kingdom, Switzerland, Germany and the United States

- the participation in settlement and clearing systems and outsourcing arrangements can mitigate some risk while generating other kinds of risks;
- during the ten years ending early in the 21st century, there were more than 100 operational loss events, exceeding $100 million each; and
- when banks act as wholesale service providers, the need arises for the maintenance of back-up systems and internal controls.

Based on the points mentioned above, it is evident that the attention of Basel II is to align capital requirements to the various types of risks (such as credit, market and operational) which can result in losses (Hendrikse & Hefer-Hendrikse, 2012:69).

Basel II deals with the minimum regulatory capital requirements for credit, market and operational risks in banks (Pillar 1). Banks must calculate their minimum capital requirements for operational risks by using any one of the following approaches:

- Basic indicator approach. This approach links the capital charge to the annual gross income of the bank (Hendrikse & Hefer-Hendrikse, 2012:69). In this approach, the basic indicator will be the annual gross income. Each bank will hold capital for operational risks equal to the amount of a fixed percentage, which is then multiplied by the individual amount of gross income of the bank (Khan, 2015:88). According to Schwartz Gârliste (2013a:172), the basic indicator approach is much more straightforward than the alternative approaches and is recommended for banks not operating internationally. By contrast, Khan (2015:88) states that this approach is not recommended for implementation, because it is unable to identify all of the operational risk exposures in a bank.
- Standardised approach. Banks rely on external measures of credit risk (like the credit rating agencies) to assess the credit quality of their borrowers (Hendrikse & Hefer-Hendrikse, 2012:69). The standardised approach consists of eight business lines, namely retail banking, corporate finance, payment and settlement, agency services, retail brokerage, trading and sales, asset management and commercial banking, which is then divided into a beta factor. For capital assessment purposes the gross income of a bank will be multiplied with the beta factor of the business of which the capital charge is calculated (Khan, 2015:88). According to Schwartz

Gârliste (2013a:172), the “total allocation of capital is calculated as an average three-year simple summation of the regulatory capital allocation to each of the business lines in each year”.

- The Advanced Measurement Approach (AMA). This approach is based on internal models and years of loss experience (Hendrikse & Hefer-Hendrikse, 2012:69). This method involves using internal and external data to determine the expected size of the loss and the probability of loss events, given that an event has occurred (Sweeting, 2011:476). Before the AMA approach can be implemented in a bank, a database of internal loss data should be kept for at least three years. In order to implement the AMA approach, the bank must get approval from local regulatory authorities and also satisfy the banking supervisor that, at a minimum:
    - it has an operational risk management system that is theoretically sound and is implemented with integrity;
    - it has sufficient resources allocated to the major business lines and the audit and control areas;
    - senior management and the board are actively involved in the oversight of the operational risk framework (Khan, 2015:89).

  The AMA approach does not require the use of a particular modelling technique, but the over-all method taken by the banking industry is the Loss Distribution Approach (LDA) (Schwartz Gârliste, 2013a:173). By implementing this method, a bank divides its operational losses in, similar divisions which are called units. For each measure, the bank constructs a loss distribution which represents expectations to total losses that may materialise during a one-year time-period (Schwartz Gârliste, 2013a:173).

The above discussion emphasises the need for banks to allocate capital to cover operational risks, which include the risk of loss because of errors, disruption of IT systems, fraud, litigation or external events (Hendrikse & Hefer-Hendrikse, 2012:69). According to Khan (2015:88), the AMA is mostly adopted by banks because it is more reliable and risk sensitive than the other approaches. With the application of the recommended guidelines

from Basel II, it has become an international standard that banks are required to hold at least 8% of their exposure in base capital (Pelzer, 2013:142).

Basel II also focuses on the principles for effective supervision (Pillar 2). Supervisors should ensure that banks have sufficient capital to make provision for all the risks that a bank can face and to assist banks to develop risk management techniques in managing and monitoring their risks (BCBS, 2004:218). There are four fundamental principles:

- "Principle 1: Banks should have a process for assessing their overall capital adequacy with their risk profile and a strategy for maintaining capital levels.
- Principle 2: Supervisors should review and evaluate the internal capital adequacy assessments and strategies of banks, as well as their ability to monitor and ensure their compliance with regulatory capital ratios. Supervisors should take appropriate supervisory action if they are not satisfied with the result of this process.
- Principle 3: Supervisors should expect banks to operate above the minimum regulatory capital ratios and should have the ability to require banks to hold capital in excess of the minimum.
- Principle 4: Supervisors should seek to intervene at an early stage to prevent capital from falling below the minimum levels required to support the risk characteristics of a particular bank, and should require rapid remedial action if capital is not maintained or restored" (BCBS, 2004:219–226).

According to Sweeting (2011:477), market discipline (Pillar 3) covers transparency and the commitment of banks to release meaningful information to all stakeholders such as their risks, their capital and how they manage risks. Basel II aims to encourage market discipline through industry training and developing a set of disclosure requirements which will allow market participants to gain access to information such as risk exposure, capital and risk assessment processes (Sweeting, 2011:477).

When a bank implements the processes mentioned above into its banking environment, it also needs to comply with the BCBC guidance paper on "Sound Practices for the Management and Supervision of Operational Risk" which was published in 2003 and was revised in 2011 (BCBS, 2011:1). The guidance paper aims to incorporate the evolution of

sound industry practice and specifies eleven principles of sound operational risk management, which covers governance, the risk management environment and the role of disclosure (BCBS, 2011:1). Refer to Table 2.5 below.

Table 2.5: Fundamental principles of operational risk management

Principle	Sound Practice
1	"The board should take the lead in establishing a strong risk management culture. The board of directors and senior management should establish a corporate culture that is guided by robust risk management and that supports and provides appropriate standards and incentives for professional and responsible behaviour. In this regard, it is the responsibility of the board of directors to ensure that a robust operational risk management culture exists throughout the whole organisation."
2	"Banks should develop, implement and maintain a framework that is fully integrated into the overall risk management processes of the bank. The framework for operational risk management chosen by an individual bank will depend on a range of factors, including its nature, size, complexity and risk profile."
3	"The board should establish, approve and periodically review the framework. The board of directors should oversee senior management to ensure that policies, processes and systems are implemented effectively at all decision-making levels."
4	"The board should approve and review a risk appetite and tolerance statement for the operational risk that articulates the nature, types and levels of operational risk that the bank is willing to assume."
5	"Senior management should develop for approval by the board a clear, practical and robust governance structure with defined, transparent and consistent lines of responsibility. Senior management is responsible for consistently implementing and maintaining throughout the organisation, policies, processes and systems for managing operational risk in all of the material products, activities, processes and systems of the bank, consistent with the risk appetite and tolerance."
6	"Senior management should ensure the identification and assessment of the operational risk inherent in all products, activities, processes and systems to make sure the inherent risks and incentives are well understood."
7	"Senior management should ensure that there is an approval process for all new products, activities, processes and systems that thoroughly assess operational risk."
8	"Senior management should implement a process regularly to monitor operational risk profiles and material exposures to losses. Appropriate reporting mechanisms should be in place at board, senior management and business line levels that support proactive management of operational risk."
9	"Banks should have a healthy control environment that utilises policies, processes and systems, appropriate controls and appropriate risk mitigation and transfer strategies."
10	"Banks should have business resiliency and continuity plans in place to ensure an ability to operate on an ongoing basis and limit losses in the event of severe business disruption."
11	"The public disclosure of a bank should allow stakeholders to assess its approach to operational risk management."

Source: BCBS (2011:5–6)

The principles mentioned earlier are essential reference tools for banks to consider when developing operational risk processes, policies and risk management systems. These principles should not be viewed in isolation but should be integrated into the overall framework for managing operational risks across a bank (BCBS, 2011:1–2). By creating an operational risk awareness culture, banks will be able to enhance their ability to achieve objectives, and improve their business practices, technology and processes. Sustainable operational risk practices can lead to higher profitability, reduced losses and improved employee and customer satisfaction. It can also demonstrate to regulators that careful consideration to operational risk management is given by banks, which can lead to relief of capital charges and reduced corporate insurance premiums (Harmantzis, 2003:9). The next section discusses the 2014 review, conducted by BCBS, of the principles of operational risk to enhance international practices.

2.4.2.1 Review of the Basel II operational risk principles

Due to the importance of operational risk management principles, and to keep up with international best practices, the Basel Committee conducted a review of the implementation of its Operational Risk Principles in 2014. The review involved 60 systemically important banks (South African Banks were also included), in 20 jurisdictions and covered all eleven operational risk principles (BCBS, 2014:1). The objectives of the review were to establish the degree to which banks have applied the principles, identify significant breaches in their application of the principles and identify significant and emerging operational risk management practices at banks that were not addressed previously (BCBS, 2014:1). The report indicates that overall, banks have made inadequate progress in applying the principles mentioned above (BCBS, 2014:1). Many banks are still in the process of implementing various principles, for example systemically important banks have initiated the principles and the operational risk management tools to varying degrees (BCBS, 2014:1). Table 2.6 below indicates the findings of the review regarding the critical areas of operational risk practices in a bank where the most scope for improvement exists.

Table 2.6: Recommendations for improving the operational risk management principles for banks

Area	Improvements
Risk identification and assessment	• "increase their use of external data for risk management; • participate in industry consortia, to enhance the availability of external loss data for all jurisdictions; • further, implement the use of business process mapping as an operational risk management tool; • further, implement the use of key risk and performance indicators; • further develop and implement comparative analysis processes that compare the outputs of each of the tools to assess the effectiveness of other tools within business lines, as well as that of tool assessments and outputs across similar business lines and geographies; • use operational risk scenarios for enterprise-wide risk management assessment purposes; • ensure that action plans from the operational risk identification and assessment tools are monitored; • ensure that there is a formal process to create, monitor and remediate action plans derived from all tools; and • consider formal processes for benchmarking operational risk management practices externally."
Change management	• "ensure that their change management programmes are comprehensive and fully implemented; • ensure that the roles and responsibilities for change management processes are fully implemented and aligned with the principle of the three lines of defence; and • ensure that post-approval monitoring and post-implementation reviews are fully implemented."
Three lines of defence	• "ensure that an effective three lines of defence model, which includes functions that own and manage risk, oversee risk management and compliance and provide independent assurance such as internal audit, is implemented appropriately to identify and manage operational risk; • assign roles and responsibilities of the three lines of defence to relevant departments; • including business units, business unit operational risk managers, other corporate experts and operational risk managers; and • reinforce their operational risk management culture through an active communication strategy."
The first line of defence	• "further, refine and enhance the roles and responsibilities for business line management; and • ensure that refresher or follow-up training is provided to business line management."

The second line of defence	• "assign the roles and responsibilities for the three lines of defence to relevant departments, such as business units, business unit operational risk managers, other corporate experts and corporate operational risk managers; and • implement a quality assurance programme within the second line of defence to ensure that an independent challenge is consistently applied."
The third line of defence	• "ensure that there is sufficient focus within the audit plan on the Operational Risk Management Framework (ORMF), and • enhance the execution and monitoring of the third line of defence responsibilities."
Operational risk appetite and tolerance	• "continue their work further to articulate and implement enhanced, and forward-looking operational risk appetite and tolerance statements."
Operational risk management framework (ORMF)	• "further, develop the integration of the operational risk management programme into the strategic decision-making process of the bank; • ensure that the ORMF or other relevant policy requires a robust operational risk assessment process within the new product and new initiative approval processes of the bank; • ensure that the ORMF specifies the use of all implemented operational risk identification and assessment tools; • ensure that the ORMF requires the use of the operational risk taxonomy of the bank in all operational risk tools, to allow for the aggregation and reporting of operational risks and control issues; • develop a quality assurance programme to ensure the independent review, applied by the second line of defence, results in consistent RCSAs."
Board of directors	• "ensure the scope of internal audit is on the full implementation and execution of the framework, rather than being limited to the operational risk capital model; • ensure the scope of internal audit includes a review of the effective implementation and execution of the ORMF at the business unit or legal entity levels, to complement the overall audit of the ORMF; and • consider periodically engaging a benchmarking analysis of the operational risk management framework of the bank, with the assistance of independent external advisors, as part of the regular assessment of the ORMF design and effectiveness at the bank."
Senior management	• "ensure that the ORMF is approved by the board or a committee of the board; • ensure that the ORFM has sufficient stature, resources and infrastructure, about other risk management functions, to implement the ORMF; • ensure that an Operational Risk Committee is established; • ensure that an effective independent challenge is applied by the second line of defence; and • further, develop and implement operational risk training and awareness programmes."
Monitoring and reporting	• "the timeliness and effectiveness of data-gathering and aggregation in a stressed condition need to be developed or tested;

	• flexible processes to extract data on demand need to be further developed; and • the timeliness and quality of information related to external events or environments need to be improved."
Control and mitigation	• "broaden the scope of outsourcing oversight beyond internal or related-party providers; • further, develop the consideration of IT risk within the operational risk appetite and tolerance statement; and • ensure that the risk and insurance management programme of the bank is subject to regular board and senior management oversight."
Business resilience and continuity	• "ensure that all businesses and groups are subject to the business continuity management (BCM) programme; and • increase, using a risk-based approach, their participation in disaster recovery and business continuity testing with key service providers."
Operational risk culture	• "continue their work further to align compensation policies with the operational risk appetite and tolerance statement; and • further, implement and develop their operational risk training and awareness programmes".
Role of disclosure	• "develop a comprehensive disclosure policy that is subject to approval and oversight by the board, and also subject to independent review, and enhance disclosure on how the bank manages its operational risk exposures, and on the status of the operational risk management programme."

Source: BCBS (2014:40–42).

The above review is indicating that many banks are not adequately managing and identifying their operational risk exposures (BCBS, 2014:2). The banks need to improve their articulation and implementation of operational risk appetite and tolerance statements. These improvements and recommendations for operational risk appetite principles will be further discussed in Chapter 3. The importance for a South African bank to implement the sound principles and practices of the BCBS for operational risk management is becoming more and more crucial, due to the recent operational risk-related losses incurred by banks, as mentioned previously.

The importance of the implementation of the Basel frameworks globally has been highlighted in the discussion mentioned above, but how did the South African banking industry implement the Basel frameworks? The next section will discuss the adoption of the Basel Accords by the banking industry in South Africa.

2.4.2.2 The adoption of the Basel Accords in the South African banking industry

The adoption of operational risk management has significantly increased over the past few years, to a greater extent where international best practices have emerged to address operational risk management and view it as an inclusive discipline (BCBS, 2002:3). In order to achieve a sound South African banking system, the regulation and supervision of banks are based on international standards and best practices (Government Gazette No. 35880, 2012:26). In 2006, Basel II was entirely executed by the BCBS by adding supervisory review processes, operational risk and disclosure requirements. This reform showed the way for banks to apply operational and internal risk control measures and how to implement new approaches to measure operational and credit risk for capital allocation purposes in a bank (Hannoun, 2010:2).

The SARB implemented Basel II, "The Basel Committee's revised capital framework", on 1 January 2008 and was one of the first jurisdictions who adopted it (International Monetary Fund [IMF], 2014:56). The regulation and supervising of banks in South Africa lie with the SARB, and the total process of implementing Basel II into the regulatory framework of South Africa was a significant exercise undertaken over several years. The following elements of Basel II had to be taken into consideration by the SARB during the implementation process:

- Pillar 1: The primary focus of this pillar is the establishment of the minimum required regulatory capital for South African banks regarding market, operational and credit risk. It also includes the formation of the approval and application processes that need to be followed in respect of operational and credit risk. It also focuses on the determination of the targeted approach of a bank, other than the base approaches, conducting quantitative impact studies, field testing and parallel runs, and the recognition of eligible external credit assessment institutions for banks.
- Pillar 2: The development of capital management, which includes the Initial Internal Capital Adequacy Assessment Process (ICAAO) assessments and the updating of the Supervisory Review and Evaluation Process (SREP).

- Pillar 3: This pillar incorporates the market discipline for banks, which also includes industry training (SARB, 2016:1).

The Basel II Framework was established to reinforce the stability of international banking structures, and the BCBS foresees that operational risk regulation will move towards a narrow risk management practice in the near future (BCBS, 2010:2). The BCBS has stated that “the Basel II Accord does not aim to change the global level of capital in the banking industry, but rather to create an incentive to encourage banks to adopt what BCBS considers ‘best practice’ for risk management” (Moosa, 2007:37).

In order to facilitate the implementation of Basel II, the Bank Supervision Department (BSD) of the SARB also decided to amend the Banks Act and the Regulations in 2007, to incorporate the practices mentioned above. These amendments came into effect on 1 January 2008 (Government Gazette No. 35880, 2012:26). Even though the Banks Act was amended, the ongoing financial crisis and new requirements established by the FSB, the BCBS issued a new document entitled: “Basel III: a global regulatory framework for more resilient banks and banking systems” in 2010. The Basel III framework focuses on the strengthening of the global capital framework and liquidity standards of banks (Government Gazette No. 35880, 2012:27).

As a result of these changes it became necessary for South Africa to amend the Banks Act to include these new practices, and to:

- “align the provisions of the Banks Act to the 2008 Companies Act;
- comply further with the requirements of the Basel Committee on Banking Supervision; and
- align the Banks Act to changing supervisory policy, market developments and practical considerations” (Government Gazette No. 35880, 2012:27).

According to the SARB (2016:1), the Basel III framework will be implemented in South Africa with a phased-in approach and have commenced on 1 January 2013, and will continue until 2018. The framework will replace the current capital framework with a revised capital framework as set out in the suggested amended regulations relating to banks. With the implementation of the new capital framework, Basel III aims to:

- improve risk management and governance processes in banks;

- strengthen transparency and disclosures of banks;
- increase the ability of the banking sector to absorb shocks arising from economic and financial pressure, whatever the source (SARB, 2016:1).

These new reforms will strengthen the supervision, regulation and risk management of the banking sector by raising the resilience of banking institutions to periods of stress and targeting system-wide risks, which can occur across the banking sector, as well as the intensification of these risks over time (SARB, 2016:1). It is evident that Basel III focuses more on risk coverage, for example, credit risk (counterparty credit risk and reliance on external credit ratings), compared to Basel II (Kubat, 2014:350). It is still crucial for a bank to incorporate the above-mentioned sound practices and principles of Basel II for operational risks, which also emphasise the need for the board to approve and review the risk appetite, and tolerance statement for operational risk in a bank. These principles regarding operational risk appetite will be further discussed in the next chapter.

In conclusion, the Basel Accords have been adopted by numerous global financial institutions (including in South Africa) and have resulted in global regulatory changes (Girling, 2013:32). According to Kulpa and Magdoń (2012:35), the survival of a bank and its activities depends on the success of its operational risk management system. In support of this, Matiş (2009:593) emphasises that a bank must manage its operational risks throughout all the organisational levels and integrate it within all banking activities to accomplish a successful operational risk management system. To achieve this integration, the Basel II and III frameworks will need to lead the way for banks to address their capital and operational risk requirements. The next section will deal with the ISO 31000 international standard.

2.4.3 ISO 31000

The ISO 31000: Risk management – Principles and guidelines, is a risk management standard published in 2009 by the ISO (Knight, 2010:68). ISO 31000 incorporates new principles and a generic framework for risk management, as well as discussing the different methods to enhance the way in which an organisation can manage its risks (Knight, 2010:68). The implementation of ISO 31000 has been formally accepted by many countries (25 countries voted for the standard, including South Africa) to replace their

domestic standards and is causing other standard-setting bodies to revise their documents (Purdy, 2010:886).

The ISO 31000 standard recommends that an organisation should have a risk management framework which integrates its risk management processes into the overall strategy, policies, culture, management, governance and reporting processes of the organisation (Standards Australia/New Zealand, 2009:iv). The standard can be applied to any risk, for example, operational risk, whatever its nature or consequence (negative or positive) in any organisation, for example, a bank (ISO, 2009:1). The standard supports a new, simple way of considering risk and risk management, and it intends to resolve the discrepancies and uncertainties which exist between many different definitions and approaches (Purdy, 2010:881). According to ISO 31000 (2009:7–8), the principles for effective risk management aim to:

- create and protect value;
- be part of the decision-making process;
- be systematic, structured and timely;
- be an integral part of all organisational processes;
- be transparent and inclusive;
- facilitate continual improvement of the organisation;
- be tailored, dynamic, iterative and responsive to change;
- explicitly address uncertainty;
- be based on the best available information;
- take human and cultural factors into account.

Purdy (2010:883) concurs with the above principles and states that the necessary result of effective risk management is to assist an organisation to have a correct, current and comprehensive understanding of the risks encountered and the risks which are within the risk criteria and risk appetite of the organisation. According to ISO 31000 (2009:7), for risk management to be effective, an organisation should comply at all levels with the above principles. These principles must also be linked to and incorporated within the risk management framework and risk management process to ensure integrated risk management. The risk management framework ensures that information about risk

resulting from the risk management process is sufficiently reported and used as a source for accountability and decision-making at all appropriate organisational levels (ISO, 2009:8). The components of the framework are shown in Figure 2.1 below.

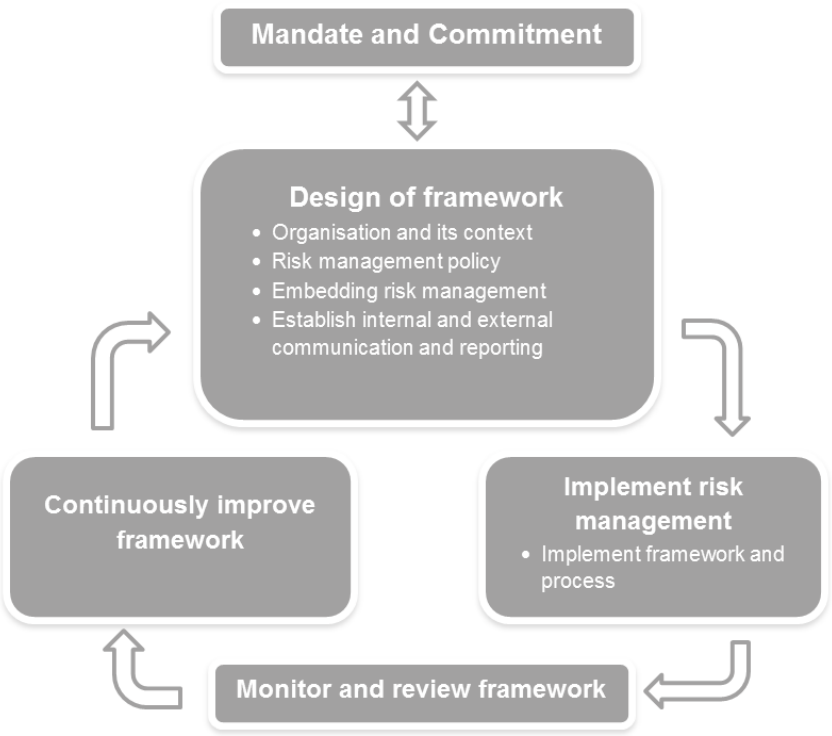


Figure 2.1: ISO 31000 framework for managing risk
Source: ISO (2009:9)

Figure 2.1 illustrates the required components of the framework for managing risks and the way in which they interrelate iteratively. The components of an ISO 31000 risk management implementation framework will be briefly discussed in the next sections.

- **Mandate and commitment**

According to ISO 31000 (2009:9), to achieve ongoing effective risk management, senior management must have a strong commitment and mandate to achieve risk management objectives at all levels. Management should:

- "define and endorse risk management;
- ensure that the culture and risk management policy of the organisation are aligned;

- determine risk management performance indicators that align with performance indicators of the organisation;
- align risk management objectives with the objectives and strategies of the organisation;
- ensure legal and regulatory compliance;
- assign accountabilities and responsibilities at appropriate levels within the organisation;
- ensure that the necessary resources are allocated to risk management;
- communicate the benefits of risk management to all stakeholders;
- ensure that the framework for managing risk continues to remain appropriate" (ISO, 2009:9–10).

- **The design of a framework for managing risk**

The design and implementation of the framework are vital for effective risk management. According to ISO 31000, the design of the framework for managing risk should include:

- An understanding of the internal and external contexts of an organisation which can considerably influence the design of the framework.
- A risk management policy which clearly states the objectives of the organisation and the commitment to risk management.
- Accountability for the management of risk. This process should ensure that the risk management process is implemented and maintained and that the controls are efficient, effective and adequate.
- The integration of risk management throughout the processes and practices of the organisation. The risk management process should become part of the objectives, policies, strategies, review and change management processes of the organisation.
- The allocation of resources for the implementation of risk management within the organisation.
- The establishment of internal communication and reporting mechanisms in order to support and encourage accountability and ownership of risk.

- The establishment of external communication and reporting mechanisms in order to communicate with external stakeholders regarding risk information (ISO, 2009:10–12).

- **Implementing risk management**

Based on ISO 31000, in implementing the framework for managing risk, the organisation should:

- "define the appropriate timing and strategy for implementing the framework;
- apply the risk management policy and process to the organisational processes;
- comply with legal and regulatory requirements;
- ensure that the decision-making, including the development and setting of objectives, is aligned with the outcomes of the risk management processes;
- hold information and training sessions;
- communicate and consult with stakeholders to ensure that the risk management framework remains appropriate;
- implement the risk management process through a risk management plan at all relevant levels and functions of the organisation, as part of the practices and processes of the organisation" (ISO, 2009:12–13).

- **Monitoring and review of the framework**

In order to ensure that risk management is effective and continues to support organisational performance, the organisation should:

- "measure risk management performance against indicators, which are periodically reviewed for appropriateness;
- periodically measure progress against, and deviation from, the risk management plan;
- periodically review whether the risk management framework, policy and plan are still appropriate, given the external and internal context of the organisation;
- report on risk, progress with the risk management plan and how well the risk management policy is being followed;
- review the effectiveness of the risk management framework" (ISO, 2009:13).

- **Continual improvement of the framework**

According to ISO (2009:13), decisions should be made regarding how the risk management plan, policy and framework can be improved, based on the results of the review and monitoring processes. These decisions should lead to improvements in the management of risk in the organisation, and a well-established risk management culture.

From the discussion above, it is evident that the risk management framework is also linked with the risk management process. According to ISO 31000 (2009:13), a risk management process should be a central part of management, entrenched in the practices and culture, and personalised to the business processes of the organisation. Figure 2.2 indicates the activities for a risk management process.

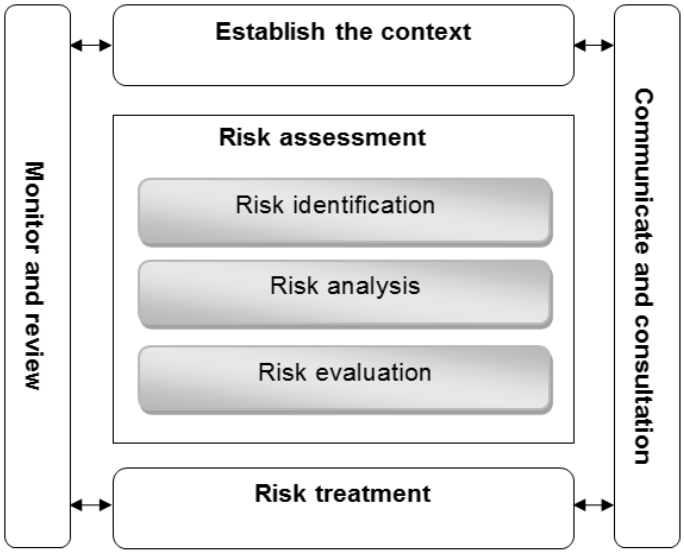


Figure 2.2: ISO 31000 risk management process
Source: ISO (2009:14)

The ISO 31000 risk management process activities will only be briefly explained in the next section because the operational risk management process will be discussed in more detail later in the study. Based on Figure 2.2 the activities include:

- Establishing the context of the organisation by articulating the objectives, defining the internal and external restrictions to be considered when managing risk, and setting the scope and risk criteria and risk appetite.

- Risk assessment, which is the overall process of risk identification, analysis and evaluation. Risk identification establishes the exposure of the organisation to risk and uncertainty. Risk analysis can be used to establish a risk profile which gives a rating of significance to each risk and provides an instrument for prioritising risk treatment procedures. Risk evaluation will assist in making decisions regarding the risk response techniques to implement, namely, treat, terminate, tolerate and transfer.
- Risk treatment, which involves selecting and implementing appropriate control measures to control the risk. A significant element in the risk treatment stage is risk control, but it also includes other elements such as risk avoidance, transfer and financing.
- Monitoring and review that ensures that the organisation is monitoring risk performance and learns from current and past experiences.
- Communication and consultation with internal and external stakeholders during all stages of the process (ISO, 2009:14–20)

The risk management process should take place within the risk management context of an organisation. From the above discussions, it is evident that the ISO 31000 standard is a generic framework for risk management, or according to AIRMIC, Alarm and IRM (2010:2), it can also be seen as an enterprise-wide framework, which can be applied to any organisation. An enterprise-wide risk management approach will allow an organisation to consider the potential impact of all types of risks on all activities, stakeholders, processes, products and services (AIRMIC et al., 2010:2).

To conclude, enhanced risk management includes fully defined and accepted accountability for risks, controls and risk treatment activities by an organisation (ISO, 2009:22). It is essential for senior management to take full accountability for organisational risks and understand the application of risk management in all decision-making processes (ISO, 2009:23). According to ISO 31000 (2009:23), all decision-making within the organisation must be done within the level of importance and significance of risk; this can then assist an organisation to determine its risk appetite. Another enterprise-

wide approach to risk management is the COSO ERM framework, which will be discussed in the following section.

2.4.4 COSO ERM framework

COSO is a voluntary, private sector initiative, which is devoted to improving organisational performance and governance through effective ERM, internal controls and fraud prevention (McNally, 2013:2). COSO published an Enterprise Risk Management – Integrated framework standard in 2004 with the aim to set an enterprise-wide foundation for ERM and embedding it across an organisation. The COSO ERM cube is a common risk framework for risk practitioners and provides clear practices on how to establish ERM in an organisation.

COSO (2009:3) states that ERM is a process, which indicates a holistic and robust top-down view of key risks encountered in an organisation. The COSO ERM framework was developed to assist the board and senior management in understanding the critical elements of an enterprise-wide risk management approach (COSO, 2009:3). According to COSO (2004:1), ERM comprises the following activities:

- Reducing operational losses and surprises. Through this activity, an organisation will be able to identify potential events and establish responses to these loss events, as well as reducing surprises and associated costs or losses.
- Enhancing risk response decisions. ERM provides the rigour to identify and select risk responses namely risk reduction, acceptance, avoidance and sharing. These decisions will be discussed later in the study.
- Identifying and managing multiple and cross-enterprise risks. Every organisation faces numerous risks, which affect different parts of the organisation. ERM facilitates effective responses to interconnected impacts of different risks and integrates responses for multiple risks.
- Improving the distribution of capital. Through obtaining comprehensive risk information, it will assist senior management effectively to assess the overall capital needs and enhance capital allocation.

- Aligning risk appetite and strategy. It is crucial for management to consider the risk appetite of the organisation. Through this activity, management must evaluate alternative strategies, develop mechanisms to manage related risks and set objectives, which are aligned with the risk appetite of the organisation.
- Seizing opportunities. By considering an assortment of potential events, senior management can identify opportunities and achieve success.

Through the above-identified components of an enterprise-wide risk management approach, COSO developed the ERM cube. Refer to Figure 2.3 below.

Figure 2.3: COSO ERM Cube
Source: COSO (2011:9).

The COSO ERM cube addresses the context and scope of risk management by defining it in terms of a three-dimensional matrix. According to COSO (2004:3), the first of these dimensions is the range of areas that a risk management framework should cover, namely:

- operational: effective and efficient use of the resources of an organisation.
- compliance: complying with applicable laws and regulations;
- reporting: continuously evaluating the reliability of reporting;
- strategic: high-level goals, supporting and aligned with the mission of the organisation.

The second dimension described in the framework covers eight components of ERM (COSO, 2004:3–4):

- Internal environment: The internal environment sets the tone at the top as well as the basis regarding how risks are viewed and addressed by the employees of the organisation, but also includes the operating environment, risk appetite and risk management philosophy, and integrity and ethical values.
- Objective setting: Business objectives must be determined before management can identify potential risk events which can affect achieving organisational objectives. ERM ensures that management implements a process to define objectives and that the identified objectives supports and aligns with the organisational mission, and are consistent with the organisational risk appetite statement.
- Event identification: External and internal risk events which can affect an organisation achieving its objectives, must be identified and then be classified as a risk or opportunity. Opportunities that were identified also need to be reported to top management and incorporated in the organisational strategic and objective setting processes.
- Risk assessment: Risks must be analysed according to their impact and likelihood so that the organisation can determine how these risks should be managed.
- Risk response: Management needs to determine which risk response strategies to implement, namely reducing, accepting, sharing or avoiding the risk. Management also needs to develop strategies to align risks with the organisational risk appetite or tolerance level.
- Control activities: Policies and procedures must be determined and implemented to assist with the execution of risk response strategies.
- Information and communication: Relevant information needs to be identified, communicated and captured to assist employees in carrying out their tasks and responsibilities. Effective communication also occurs in a broad sense: flowing up, down and across the organisation.

- Monitoring: The entire ERM process must be continuously monitored, and adjustments need to be made if necessary. Monitoring is accomplished through ongoing management activities or separate evaluations.

Based on the components as mentioned above, it is evident that the internal environment of an organisation sets the tone at the top regarding risk appetite, and the objectives and strategies of an organisation must be aligned with the risk appetite and risk appetite statement of the organisation.

The final dimension in the framework is the level of application. This dimension highlights the need for risk management to be applied to all the levels in an organisation, namely the business units, subsidiaries and internal divisions. It is vital for an organisation to understand the dynamic nature of the ERM framework because it can assist the board and management in making risk-informed strategic decisions (COSO, 2009:4). According to COSO (2009:4), robust and continued engagement by the board in ERM oversight will strengthen the resilience of an organisation to substantial risk exposures. ERM can assist in providing the following:

- a path of awareness of the risks that an organisation encounter;
- the inherent-related nature of the risks;
- a proactive risk management process; and
- a transparent decision-making process concerning risk/reward trade-offs, which can then contribute towards the possibility of achieving business objectives (COSO, 2009:4).

Based on the discussions above, it is evident that the COSO ERM integrated framework emphasises the need for an organisation to align its risk appetite and strategy by determining which risk responses to implement, namely reducing, accepting, sharing or avoiding the risk (COSO, 2004:1). An organisation needs to understand how much risk it is willing to accept and to what extent should the risks which are accepted, mirror the stakeholders' objectives and attitudes towards risks (COSO, 2012:1).

In conclusion, based on the discussions in 2.3, it is evident that concerning the management of risks, there are connections between King III, Basel II, ISO 31000 and the COSO ERM frameworks. The importance of a risk management framework and

process is highlighted by ISO 31000. The COSO ERM framework indicates that the internal environment, objective setting, event identification, risk assessment, risk responses, control activities, information and communication, and risk monitoring are essential components for the effective management of risk within an organisation. King III and Basel II emphasise corporate governance and internal controls. The principles and practices for effective risk management in an organisation are stressed by Basel II, ISO 31000 and the COSO ERM framework. The importance of the board to determine and aligning risk appetite and tolerance levels to the strategy of an organisation was also highlighted by King III, Basel II and the COSO ERM frameworks.

The standards mentioned above also identify different components of a risk management framework and process. It is important for a bank to understand that these different components could also be adapted to implement an operational risk management framework and process, which will be dealt with in the next section.

2.5 OPERATIONAL RISK MANAGEMENT FRAMEWORK

According to the IOR (2016:5), the primary objective of an ORMF is to identify, assess, monitor and report the risks to which an organisation may, currently or potentially, be exposed. For the ORMF to be effective, it is necessary for the framework to be interrelated, consistently applied and integrated with business processes in an organisation (IOR, 2016:5). According to Rosenthal (2014:72), an ORMF can deliver valuable and actionable information to make informed decisions when executed and embedded correctly.

Chapman (2011:14) explains that the purpose of the risk management framework is to assist an organisation in embedding risk management into its management structures and processes so that it becomes a routine activity. The IOR (2016:5) also highlights that the purpose of an ORMF is to assist an organisation to embed risk management into its daily activities, to integrate the framework into an organisation and to align it with business processes and objectives. Also, Schwartz Gârliste (2013b:175) mentions many reasons why a bank should have an ORMF, namely to ensure that:

- operational efficiency is improved;
- the focus on operational risk management is increased;

- massive unexpected losses are avoided;
- the return on capital for a bank can be improved;
- there are human resource allocation and information management in a bank;
- a large number of low-value losses can be avoided by the bank;
- the bank can allocate capital;
- there is an improvement of the customer service at a bank (Schwartz Gârliste, 2013b:175).

Ghosh (2012:399–400) emphasises that the design of the ORMF should be oriented towards the individual requirements of a bank, by the size and complexity of the business, risk appetite, targeted level of capital and working environment. He states that an ORMF for a bank should aim to:

- familiarise staff with operational risk events;
- describe the operational risk philosophy and appetite or tolerance level;
- disclose business operational risk limits per unit;
- explain potential sources of operational risks to staff;
- promote risk awareness;
- classify operational risk loss events into appropriate categories for operational risk management;
- familiarise staff with key operational risk management processes;
- map each activity into a prescribed business line for operational capital assessment;
- facilitate switchover to the AMA;
- explain the procedure for operational risk identification;
- entrust to business heads the responsibility to identify operational risks in their specific lines of business;
- establish a methodology for operational risk assessment and measurement;
- assess capital requirements and to comply with capital adequacy requirements;
- adhere to prescribed policies, procedures and limits;
- detect deficiencies in the operational risk management process;
- assess the effectiveness of the operational risk management system;

- minimise the impact of operational risks;
- establish structured procedures and policies to deal with risks from the outsourcing of services and other residual risks, for example, reputational risks;
- formulate business continuity plans in the event of disruptions;
- provide to top management with an assurance of compliance regarding policies and procedures;
- establish an organisational structure in alignment with operational risk management activities.

If an operational risk management framework is correctly implemented, it can assist with the reporting of risks to senior management for informed decision-making (Chapman, 2011:14). According to Blunden and Thirwell (2013:29), one of the benefits of a framework is to clarify the operational risk policy and confirm whether the approved risk appetite of the board is aligned with the objectives and policy of the bank, as well as simplifying the risk and control accountability and ownership within the bank.

Table 2.7 below highlights the components of various risk management frameworks developed over the years, namely the ISO risk management framework, the COSO ERM framework, and the Risk Management Association (RMA) framework and the IOR ORMF.

Table 2.7: Components of a risk management framework based on ISO, COSO, RMA and IOR

ISO 31000 risk management framework	COSO ERM framework	RMA framework	IOR ORMF
Mandate and commitment: "There must be a strong commitment and planning process from management to introduce risk management within an organisation, for example, the implementation of a risk policy and process" (ISO, 2009:9).	**The first dimension** of "a risk management framework should cover the effective use of operational resources, determine if an organisation is complying with applicable laws and regulations, stress continuous reporting, and ensure that strategic goals are aligned with objectives" (COSO, 2004:3).	**Strategy:** "Sets the overall tone and approach for risk management regarding the business objectives, policy and governance model" (Haubenstock, 2001:26–29).	**Operational risk governance:** "Risk governance is the manner within which operational risk management operates in an organisation. It will reflect, and seek to sustain and evolve, the risk culture of an organisation. Operational risk management encompasses everyone in the organisation; this means that the framework for risk governance should incorporate everyone. The ORMF can only operate if there are compelling and strong lines of communication both up and down the organisation and a culture in which good and bad news are allowed to travel freely" (IOR, 2016:17).
Design of framework: - "Understanding the organisation and its context. - Establishing a risk management policy. - Accountability towards the management of risks. - Integrating risk management into the process of an organisation. - Resources should be allocated to risk management.	The **second dimension** described in "the framework covers eight components of ERM, namely risk assessment, internal environment, control activities, objective setting, risk response strategy, event identification, information and monitoring and communication" (COSO, 2004:3–4).	**Process:** "Describes the steps and decisions for managing operational risks in day-to-day activities" (Haubenstock, 2001:26–29).	**Operational risk appetite:** "Operational risk appetite involves defining what is acceptable and what is not in an organisation. This could be accomplished by deciding, for each type of risk, what is acceptable, what is unacceptable, and the range between the two, i.e. what is tolerable. This approach can be applied across all ORMF components (including RCSA, scenario analysis and internal loss event reporting) and offers a

- Internal and external communication and reporting mechanisms should be established" (ISO, 2009:10-12).			perfect indication of the relative response to the apparent materiality of the associated risk" (IOR, 2016:17).
Implement risk management: "An organisation must implement the framework for managing risk as well as the risk management process" (ISO, 2009:12-13).	The **third dimension** in the framework is the level of application (risk culture). This dimension highlights "the need for risk management to apply to all levels of an organisation, from the organisation as a whole, all through to the business units, subsidiaries and divisions" (COSO, 2004:5).	**Infrastructure:** "Identifies the tools used during the management process, for example, data and systems" (Haubenstock, 2001:26–29).	**Categorisation:** "The approach to risk categorisation is essential to the active management of operational risk. It is applied across all ORMF components and risk management activities, crucially providing a standard frame of reference for reporting, which is the foundation for ensuring action and attention upon which significant quantification will rely on" (IOR, 2016:17).
Monitor and review framework: An organisation must "ensure that risk management is effective and continuous to support organisational performance" (ISO, 2009:13).		**Environment:** "Refers to the risk culture in an organisation" (Haubenstock, 2001:26–29).	**Culture, attitudes and behaviours:** "The risk culture of an organisation. The organisation should seek to enhance its risk culture by integrating the management of operational risk into its business processes" (IOR, 2016:17).
Improve framework: "Decisions should be made on how to improve the framework, policy and plan" (ISO, 2009:13).			**Operational risk management toolkit:** An ORMF aims to "identify, assess, monitor and report operational risk (applying control and mitigation as required to avoid exceeding appetite) and to champion effective reporting of risk and emerging risk issues, this can be achieved through the following: - loss events (internal and external); - risk and control self-assessment; - key risk indicators;

			- scenario analysis and stress testing" (IOR, 2016:18).
			Environment: "The organisation must understand its internal and external environments" (IOR, 2016:12-13).
			Business strategy and objectives: The ORMF must be "aligned with the business strategy, objectives, policies and processes" (IOR, 2016:11).
			Operational risk management process: The ORMF must be "linked with the operational risk management process of the organisation, namely: - Identification. Identification of all key risks and related controls. - Assessment. Evaluation of risks and controls and formulation of appropriate actions. - Monitoring. Regular review of the risk profile and exposure to risk appetite. - Reporting: Articulating the risk profile for internal governance and external reporting requirements" (IOR, 2016:19).

Sources: COSO (2004:3–5), Haubenstock (2001:26–29), IOR (2016:11-13 & 17-19), ISO (2009:9-13).

Based on the Operational Risk Management Frameworks (ORMFs) above, it is evident that a framework needs to include an operational risk management policy and procedure, risk management strategy, risk management process, risk governance, risk culture, risk structure, risk taxonomy (categorisation of risks) and risk appetite and tolerance thresholds. Young (2014:42) also explains that an ORMF is developed to integrate operational risk management practices inside the activities of a bank and that an ORMF should consist of the following components:

- operational risk management culture, which are the main principles for managing operational risk and value-adding activities;
- operational risk management strategy or policy, which determines the overall risk management goals, mission, vision and objectives of the bank;
- operational risk management structure which establishes the governance and compliance structure, as well as the responsibilities and roles of managing operational risks within a bank;
- operational risk management process, which is the process to be followed when managing operational risk exposures and losses (Young, 2014:42).

Based on the discussion above, it is evident that the general components of an operational risk management framework can be seen as follows:

- Operational risk governance structure – a governance structure defines the responsibilities and roles of the head of the operational risk function and the team that manages the framework, the operational risk managers in lines of business, the committee that oversees and makes critical decisions about risk management and every employee who may encounter operational risk within an organisation (Girling, 2013:41).
- Operational risk culture – the organisational norms, attitudes and behaviours interrelated to risk awareness, risk-taking and risk management (FSB, 2014:1).
- Operational risk management policy – the policy that establishes the minimum requirements and controls to address business strategy, compliance with laws,

rules, regulations and mitigation of other identified risks. The policy must be actionable and enforceable (Girling, 2013:69).

- Operational risk management process – “the systematic application of management procedures, practices and policies to activities of establishing the context, identifying, analysing, evaluating, treating, communicating and consulting, monitoring and reviewing risks” (ISO, 2009:3).

In conclusion, the BCBS (2011:7–8) also supports the importance of an operational risk framework by explaining that a bank should establish a framework for managing operational risk and assess the adequacy of capital given in the framework. Based on the Basel II principles, a bank should develop, implement and maintain a framework that is fully incorporated into the overall risk management activity of the bank and is developed based on the nature, size, risk profile and complexity of the bank (BCBS, 2011:7). It should also include policies outlying the process of the bank to identify, assess, monitor and control or mitigate the risk (BCBS, 2011:7–8).

An ORMF also provides a multidimensional view of the risk exposure in an organisation, and assist senior management with the weighing of high-level risks against the risk appetite of the organisation (Rosenthal, 2014:72). The framework should cover the appetite and tolerance for operational risk of the bank, as specified through the policies for managing risks, including the manner and extent in which operational risk is transferred from outside the bank (BCBS, 2011:7–8). According to Girling (2013:43), the whole ORMF is held together by risk appetite. To express a risk appetite for operational risk is difficult, but not impossible. It can take a while for a framework to mature to the stage where risk appetite can be agreed up and discussed successfully (Girling, 2013:43). Effective risk governance requires a clear articulation of risk appetite, and risk appetite can be set when robust governance and a risk culture is in place (Girling, 2013:43). The IOR (2016:7) also highlights that a risk culture, which is aligned with the stated values and appetite for risk of an organisation is likely to improve risk-taking and control decisions that enable the achievement of organisational objectives.

For this study, only the operational risk management process which forms part of the operational risk management framework will be discussed to establish how an operational

risk appetite a bank fits into the process. The process is the foundation for an organisation to use to determine its operational risk appetite. The process determines the operational risks faced by an organisation, which will assist senior management or the board to determine the operational risk appetite for the organisation.

2.6 OPERATIONAL RISK MANAGEMENT PROCESS

According to Valsamakis et al. (2010:145), the purpose of an operational risk management process is to offer a structured approach to operational risk management so that the risk exposures are identified and effectively managed and it aims to ensure the formulation of realistic operational risk appetite. The operational risk management process is essential for a bank to ensure that all of the operational risks are effectively managed and that business objectives are achieved (Young, 2014:46). According to ISO 31000 (2009:13), the risk management process should be a central part of management, must be entrenched in the culture and practices and be tailored to the business processes of an organisation. Various views and models regarding a risk management process have been established over the years. For example, Gardener and Ayling (1984:16) state that previous risk management literature provided a model which included the identification, evaluation and handling of risk in the process. Over the years this process has evolved to a complex one, for example the ISO 31000 (ISO, 2009:3) expanded to a systematic application of a risk management process by including activities such as the establishment of the context, identification, evaluation, analysis, monitoring and reviewing, treatment, communication and consultation of risks. The Hong Kong Institute of Bankers (2013:29–31) also divides the process of operational risk management into the following broad activities:

- defining the scope and objectives of the programme;
- identifying and assessing critical risks;
- measuring and analysing risks;
- mitigating and controlling risks through management actions;
- monitoring risks with regular reporting to management.

According to Taylor (2014:22), the activities mentioned above in the risk management process can also be achieved by continuously asking the following questions:

- Context: What is the objective or goal the organisation wish to review?
- Identify: What are the risks associated with a specific objective or goal?
- Analyse: What is the impact and likelihood of a risk event happening?
- Evaluate: What are the capacity, tolerance and risk appetite of the organisation and which risks need the most attention?
- Treat: What does the organisation do to deal with a risk or how does the organisation respond to risk?

Based on the discussions above, it is evident that there are five steps in the operational risk management process, namely operational risk identification, evaluation, control, financing and monitoring. All of these steps are connected and must be monitored continuously throughout the process as illustrated in Figure 2.4 below.

Figure 2.4: Operational risk management process
Source: Young (2014:47)

The different components of an operational risk management process will now be briefly discussed in the following sections.

2.6.1 Operational risk identification

According to Valsamakis et al. (2010:145), operational risk identification is the first step in the process, and it aims to analyse the objectives, processes and strategies in the organisation regarding its risk exposure. ISO 31000 (ISO, 2009:17) also emphasises the need for an organisation to identify sources of risks, areas of influence, events (including

changes in circumstances), and their potential consequences and causes. The importance of risk identification which considers both internal and external risk factors encountered by a bank is also emphasised by the Basel II principles (BCBS, 2011:11). The operational risk identification process is where skilled personnel are responsible for recognising and identifying the risk event (downside risk) and risk opportunity (upside risk), which then need to be recorded in a risk register (Chapman, 2011:159).

A risk register lists all the risks identified according to its risk category (Blunden & Thirwell, 2013:87). The risk register will be used and updated throughout the operational risk management process. The operational risk identification process will be discussed in the next section.

2.6.1.1 The operational risk identification process

A bank should apply risk identification techniques and tools throughout the operational risk identification process which are suited to the capabilities, objectives, and risks faced by a bank (ISO, 2009:17). According to Chapman (2011:163–169), the risks and opportunities in an organisation can be identified through any of the following techniques and tools:

- Risk prompt list: A list that categorises each risk into a type or area. The organisation will be able to categorise the key risks experienced within the organisation through this list.
- Risk checklist: This checklist lists all of the risks identified on previous projects within the organisation.
- Risk taxonomy classification: This is a structured checklist to breakdown the risks and opportunities into manageable components and then aggregated for reporting, exposure measurement and management.
- Political, economic, social and technological (PEST) prompt list: The PEST analysis method is used to identify the external environmental risk exposure of the organisation.
- Gap analysis: A gap analysis identifies the main risks linked to a particular project or activity of the organisation. This method will aid the organisation to determine

where the gap is in the risk associated with the project or activity in order to implement reactive or pro-active risk measures.

- Risk database: A risk database can be used to capture information of each risk identified in the organisation and assists in monitoring all of the risks and actions used in the risk control process.
- Strengths, weaknesses, opportunities and threats (SWOT) prompt list: A SWOT analysis is a straightforward method for an organisation to identify the risks and opportunities in the business. Such an analysis of the strengths, weaknesses, opportunities and threats brings together the results of an analysis of both the internal and external environments of the organisation.
- Risk questionnaire: This questionnaire is used when an organisation needs to identify the risks and concerns arising from a business project or activity through the various risk management stages. The responses received from the questionnaire will show how the employees of the organisation react to risk.
- Business risk breakdown structure: This technique is used to identify all the sources of risk within activities and projects in the organisation.

The BCBS (2011:11–12), on the other hand, identifies the following tools that a bank can use to identify operational risks:

- Internal loss data collection and analysis: Internal operational loss data provides meaningful information for assessing the success of internal controls of a bank and operational risk exposures.
- External data collection and analysis: External data consist of gross operational loss amounts, dates, recoveries and relevant causal information for operational loss amounts and loss events occurring at organisations other than a bank.
- Audit findings: The primary focus of audit findings is on vulnerabilities and control weaknesses, but these reports can also provide insight into inherent risks due to internal or external factors.

- Business process mapping: This technique identifies the crucial steps in business activities, processes and organisational functions.
- Risk assessment: In a risk assessment process, which can also be referred to as a risk control self-assessment (RCSA), a bank evaluates the processes underlying its banking operations against potential threats, vulnerabilities and their impact.
- Scenario analysis: Scenario analysis is used to identify potential operational risk events and assess their potential outcomes through obtaining expert opinions from the risk and business line managers.
- Risk and performance indicators: Key risk indicators (KRIs) are risk statistics and metrics that provide insight into the critical risk exposures of a bank. Key performance indicators (KPIs) provide clarity into the status of operational processes and weaknesses.
- Comparative analysis: This analysis compares the results of the various risk assessment tools to provide a broad overview of the operational risk profile of a bank.
- Measurement: Banks can quantify their operational risk exposure by using the outputs of the risk assessment tools as inputs into a model that measures the exposures.

After the risks and opportunities have been identified through any of the above-mentioned mechanisms, a bank can classify its operational risk events as expected and unexpected losses or internal and external losses, which will then assist a bank to define and understand the nature and effect of its risk exposure, which also affects its risk appetite (Young, 2014:88). In order to achieve this, a bank needs to categorise its operational risks, which will be discussed in the subsequent section.

2.6.1.1.1 Operational risk categorisation

Operational risk categorisation may be one of the first challenges a bank can encounter in the operational risk management process because if a bank wants to manage its risks holistically, they must understand the inter-relationships between different risk types (IOR, 2011:1). For example, the occurrence of an operational risk could precipitate a

consequence that encompasses another risk type, and the combination could lead to a ripple effect elsewhere (IOR, 2011:1). It is essential for a bank to understand the following operational risk concepts (Nâstase & Unchiaşu, 2013:105):

- Event: the incident associated with the risk type, for example, a system failure (event) caused by a human error (operational risk).
- Consequence: the bank defines this as the potential or actual loss.
- Control: a process, policy or an IT system used to mitigate risk.
- Impact: can be tangible (financial impact) or intangible (business efficiency or reputational impact).
- Cause: operational risk causes include processes, people, systems and external factors.

Based on the above information a bank needs to categorise an event based on the cause and effect, as well as the controls to mitigate an event (IOR, 2011:2). These concepts can also be explained through the following example: an IT system failure occurred in a bank due to an employee error, which led to the loss of business because of downtime. The event can be seen as the IT system failure, the cause was employee error, and the effect was the loss of business. As illustrated by the example, it is imperative for a bank to understand the different operational risk causes, effects and events. Otherwise, it can lead to confusion within its processes and activities (Young, 2014:17). For the purpose of the current study, it is important to understand that operational risk categorisation should be applied across all of the risk management activities and needs to be tailored according to each organisation (IOR, 2011:1). If the risk categorisation is done correctly, it will assist a bank to determine its operational risk appetite for every operational risk decisively. In order to achieve this, a bank should categorise the different operational risks by adopting one of the five approaches mentioned below, according to the needs and preferences of the bank.

2.6.1.1.2 Different approaches to risk categorisation

The first approach is the categorisation of operational risk events. According to the IOR (2011:2), the categorisation of operational risk events is the most widely recognised approach used to categorise operational risk losses. This approach is adopted and

recognised for many reasons. Namely, it is linked to business and financial performance, it supports the analysis of loss events and is widely adopted by loss data associations to facilitate the flow of information between participating organisations (IOR, 2011:2).

The second approach is to address the cause of an event which is seen as the action to avoid or mitigate a recurrence. If a bank analyses some events which share the same underlying cause, it can assist the bank to manage these risks correctly (IOR, 2011:3). The four primary operational risk causes (as adopted by the financial industry) are people, systems, processes and external events. It is crucial for a bank first to establish the operational risk cause and then determine the effect because a combination of causes can lead to an effect (Young, 2014:17). According to the IOR (2011:3), this approach can be challenging to achieve in practice, because there has, up to date, been no recognised standards developed for determining the cause of an event. Even though this approach can be difficult to implement, a bank can consider classifying operational risks into internal and external factors, which is the underlying operational risk causes mentioned above. Table 2.8 illustrates examples of operational risk causes, namely people, processes, systems and external events, which a bank can use to classify internal and external factors.

Table 2.8: Internal and external risk factors

Internal factors			External factors	
Systems	**People**	**Processes**	**External**	**Physical**
System capacity	Employee error	Capacity risk	Tax	Theft
System compatibility	Employment law	Project risk	Legal	Fire
System unsuitability	Industrial action	Contract risk	External sources	Terrorism
System delivery	Loss of important personnel	Error reports	Political	Physical security
Strategic risk	Employee fraud	Transaction error	Supplier risk	Natural disasters
Security breach	Employer responsibility	Accounting error	Money laundering	
Data quality	Employee misdeed	Settlement or payment error	Regulatory	
Programme error	Health and security	Product complexity		
	Lack of skills	Selling unsuitability		

Source: Adapted from Jednak and Jednak (2013:66)

The third approach is to categorise the function of controls, which are already established. The bank will be able to establish controls that deter or prevent the underlying cause (e.g. widely publicised penalties for actual or attempted fraud) or detect the appearance of the risk (e.g. validation of details to identify fraudulent transactions), and will be able to recover from adverse consequences (IOR, 2011:3). This approach can assist a bank to determine if it has too few of one type of control or even too many of another, which can result in an ineffective control framework (IOR, 2011:3).

The fourth approach is for a bank to categorise the effect of risk events. This approach will assist in mitigating and prioritising activities to utilise time and effort within the organisation optimally during the risk management process. The effects can also be categorised according to financial and non-financial categories. Financial effects are, for example, easier to incorporate and to evaluate organisational business decisions and objectives, than non-financial effects (IOR, 2011:3). Non-financial effects could include, for example, customer service degradation or damage to the brand or reputation, which is potentially more significant than a quantifiable direct financial loss (IOR, 2011:3).

The fifth approach is to break down operational risk events into expected and unexpected losses. Expected losses are losses that are expected during a specific period. Unexpected losses are potential losses, which could be experienced in extreme cases (Young, 2014:88). See Figure 2.5 below for examples of expected and unexpected losses in a bank.

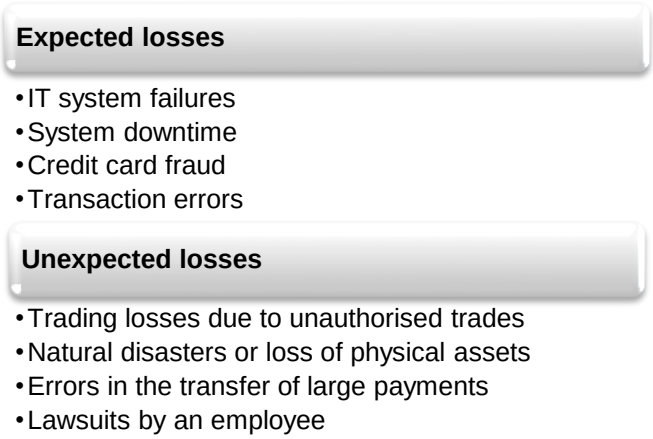


Figure 2.5: Expected and unexpected losses

Source: Bostander (2007:32)

Based on the nature and impact of expected and unexpected losses, a bank should reserve regulatory capital for both categories of losses. This measure increases the importance for a bank to control and manage expected operational losses effectively by correctly categorising the losses (Bostander, 2007:32).

It is also important to note that the outcomes of any of the categorisation approaches mentioned above can be grouped and analysed according to their effect and frequency.

- Low-frequency/high-impact events: Losses resulting from floods, theft, fire and robberies.
- High-frequency/low-impact events: Losses from cheque or card fraud.
- Low-frequency/low-impact events: Petty cash theft/shortages.
- High-frequency/high-impact events: A high number of losses linked to trading and investments in high-risk shares (Young, 2014:97)

By analysing the impact and frequency of risk events, the bank will be able to offer a judgement on the likelihood of the opportunities and risks occurring and their effects, should they occur (Chapman, 2011:185). For the purpose of the current study, it is essential to understand that a bank needs to establish the likelihood and effect of operational risk events because it will assist in determining the levels of risk-taking that are acceptable, according to the risk appetite statement (Taylor, 2014:76). The next subsection will discuss the difference between a cause and effect in order to analyse operational risk events effectively.

2.6.1.1.3 The difference between a cause and effect

It is imperative that the outcome of a chain of events is determined in order to manage the root cause of risk. Managers in business tend to focus more on the effect of the risk, rather than the cause (Young, 2014:17). It is essential for a bank to manage its operational risks through the recovering of a loss and then to fit the cause to that specific loss because some causes may contribute to either one or more losses (Young, 2014:17). In order for a bank to accomplish this, it is essential to understand the difference between a cause and effect (loss). Refer to Figure 2.6 below.

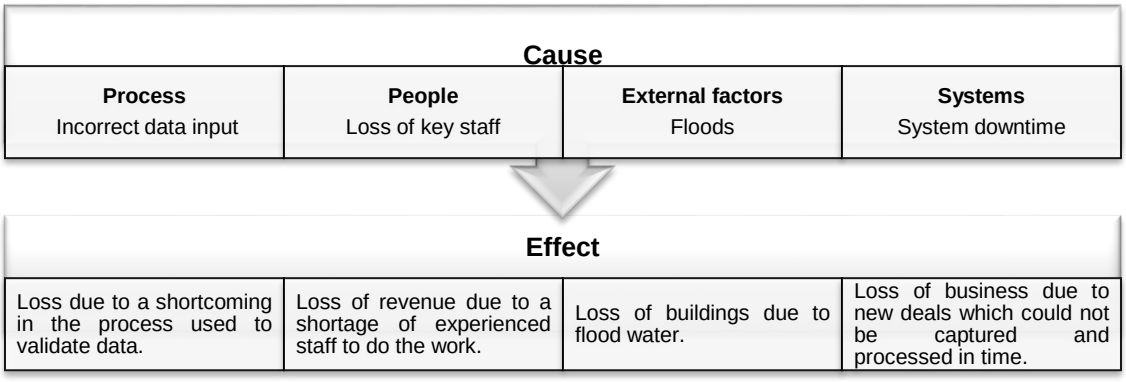


Figure 2.6: Difference between a cause and effect
Source: Adapted from Young (2014:17).

As seen from Figure 2.6, the cause of a loss can usually be traced to a specific source, for example, a flood, where the effect is the damage to a building, which resulted in a financial loss (Valsamakis et al., 2010:27–28). Based on the definition of operational risk by the BCBS (2002:2) and the figure above, the following four operational risk causes can be noted:

- processes: the processes operated by a bank;
- people: the employees of a bank to assist in managing processes;
- systems: systems used to support the process;
- external events: the risks resulting from the external environment of the bank.

According to Kulpa and Magdoń (2012:37–38), there can also be the following operational risk causes, which can be identified by banks, namely:

- products: the method of new-product implementation, the preparation of the portfolio in respect of business, law and IT;
- people: the ability to use appliances and equipment correctly, the vastly understood quality of resources, skills, motivation, and the conditions of work;
- safety connected to client service of a bank (bank information access channels and personal data protection) and HR systems;
- crimes: fraud, theft and corruption;
- outsourcing: external contracting of processes and services;

- processes and systems: IT and technical processes and the integrity of the business;
- failures, catastrophes and disasters;
- links between clients: the relationship between the client and the bank.

As seen in Figure 2.6, the starting point of risk may not cause a loss without the interaction of inadequate systems, processes or controls. It is important for a bank to link potential events to their causes and effects (Young, 2014:17–18). In order to accomplish this, a bank ought to identify the different events that can occur within the bank, which will be discussed in the next section.

2.6.1.1.4 Operational risk events

It appears for banks effectively to manage operational losses; they should identify future operational risk events and also rely on past events to recognise future events. A past event can often be traced to a specific time and place, for example, a fire which occurred, or it can be recorded for statistical analysis, for example, the number of system errors or thefts (Valsamakis et al., 2010:27–28). Based on a study conducted by the BCBS, the following seven operational risk events can lead to financial losses in a bank (see Table 2.9):

Table 2.9: Operational risk events according to the BCBS

Operational risk event category	Examples
1. **Workplace safety and employment practices, which can lead to discrimination issues.**	Violation of employee health and safety rules, organised labour activities, general liability, work assignments that overwhelm the employee's knowledge and workers compensation claims.
2. **External fraud by a third party to side-step or defraud the law.**	Forgery, fake banknotes or coins in the bank by clients, cheque kiting, computer hacking and robbery.
3. **Internal fraud by an internal party to defraud or circumvent regulations, company policies or the law.**	Money or material theft, intentional misreporting of positions, the performance of illegal banking operations not in the employee's responsibility, insider trading.
4. **System failures and business disruptions.**	Utility outages, viruses in the banking informatics system, telecommunication problems, software and hardware (data) failures and electronic banking failures.
5. **Failed delivery, transaction and process management.**	Incomplete legal documentation, vendor disputes, data entry errors, unapproved access given to client accounts, collateral

	management failures, inadequate transportation of cash between banks and ATMs.
6. Clients, products and business practices. Negligent behaviour towards clients or failure to meet a professional obligation to clients.	Misuse of confidential client or customer information, not investigating a client's data, money laundering, fiduciary breaches, the sale of illegal products, incorrect use of IT applications by clients and improper trading activities on the banks account.
7. Damage to physical or tangible assets from natural events or catastrophes.	Vandalism, floods, earthquakes, terrorism, fires and unpredicted events by third persons.

Source: BCBS (2002:2–3)

In addition to the seven operational risk event types identified above, the BCBS also established under the standardised approach (as previously discussed in 2.3.2), eight business lines into which banks are required to categorise operational risk events, namely:

1. retail banking
2. corporate finance
3. commercial banking
4. agency services and custody
5. brokerage
6. trade and sales
7. managing assets
8. payment and settlement (Bostander, 2007:31).

For each of the eight business lines as mentioned above, their gross income is seen as a general indicator which scales the business operations, which then, in turn, will scale operational risk exposures within each of the lines (Schwartz Gârliste, 2013a:172). The reason why the BCBS decided to classify operational risk events in terms of the seven-event types and eight business lines, is to enable banks to determine precisely where the operational risk losses occurred so that they can implement control measures to prevent losses from recurring (Bostander, 2007:32).

Matiş (2009:593–594) also agrees with the events mentioned above and adds that the security of the electronic banking system, for example, fabrication of electronic money,

and improper activities performed in the system, can also be seen as an operational risk event.

As discussed previously, when a bank identifies operational risk events, the bank needs to establish the underlying operational risk causes. The following example illustrates this process: an employee in a bank committed internal fraud; the risk event will be the internal fraud, and the cause will be the employee committing the fraud. For more examples, refer to Table 2.10 below.

Table 2.10: Linking operational risk causes and events

Risk Cause	Risk event	
Systems (technology)	- System failure - System integrity - System suitability	- Out-dated systems - System support
Legal/regulatory	- Contractual failures - Non-compliance with standards	- Changes in regulatory standards
People/employees	- Internal fraud - Wrongful trading - Employment law	- Employer's liability - Errors - Absence or loss of key staff
External environment/factors	- Natural disasters - External fraud	- Third-party theft - Business interruption

Source: Adapted from Young (2014:18)

It is evident from the discussion above that a bank needs to understand how to align its operational risk causes, effects and events in the risk identification process (Young, 2014:35). This action should assist a bank to control and manage perceived operational risks effectively. The following key points regarding the risk identification process should also be considered:

- It is sometimes better to use a combination of approaches to ensure that the identification of risks is complete because the use of one approach only is unlikely to be enough to identify all of the risk exposures.

- It is imperative to establish which approach will work the best in that particular industry because certain approaches might be more useful in some industries than others.
- The risk identification process is enhanced by consultation with many people, which fall outside the risk management department.
- The identification of risks is a continuous process and should not be seen as a once off or isolated exercise.
- Finally, risk identification must involve a certain degree of creativity (Valsamakis et al., 2010:121)

In conclusion, the importance of effective risk identification allows a bank to allocate risk management resources efficiently and establish its risk profile (BCBS, 2011:11). If a bank does not consider all the operational risks, risk-taking incentives might not be properly aligned with the risk appetite and tolerance of a bank (BCBS, 2011:12).

Based on the discussion of the operational risk identification process, it is evident that a bank needs to capture the identified operational risks on a constant basis and also need continuously to identify new risks (present and future) which can arise (Tchankova, 2002:293). One of the methods to capture these risks is through a risk register. It is essential to record the operational risk exposures and opportunities in a risk register, but a bank can also consider using a risk register to keep a record of the performance of the exposure or opportunity and its control measures. A bank can also include in the risk register, an anticipated timeframe in which the opportunity or exposure will reach its peak, or indicate the changing effect and likelihood at specific points in time, for example over one, five or ten years (Taylor, 2014:34). By implementing a risk register, it can be used as a critical communication tool in the operational risk evaluation process, which will be discussed next.

2.6.2 Operational risk evaluation

The results of the operational risk identification process which is captured in the risk register should be used in the operational risk evaluation process. According to Chapman (2011:187), this process will give a clear view of the likely risk exposures or potential

opportunities arising from the activities of a bank. In support of this view, Valsamakis et al. (2010:123) also describe it as a process that can lead to the expression of risks in numerical terms. The operational risk evaluation process entails the measurement (quantitative) and assessment (qualitative) of the identified operational risk events (Young, 2014:102). The purpose for the risk evaluation process is to indicate the size of the different risks and their impact on earnings, capital, cash flow or other key performance indicators, for instance, the reputation of the organisation (Valsamakis et al., 2010:123). The following methodologies are some of the most popular methods used to evaluate operational risks.

- **Loss event database**

This database accumulates historical information on previous risks or losses (internal and external) that occurred in a bank which will assist a bank to take appropriate preventive measures for losses exceeding the tolerance levels of the bank (Breden, 2008:160). Internal operational loss data delivers information on the assessment of the exposure to internal operational risks of a bank, and the effectiveness of internal controls. External operational loss data offers information on external operational loss events, which occurred at other organisations, and not the bank (BCBS, 2011:11). By collecting and analysing internal and external operational risk events, or loss data, it will deliver valuable insights into the current operational risk exposure of a bank (Girling, 2013:75).

- **Audit findings**

Audit findings focus on control vulnerabilities and weaknesses within an organisation, as well as providing insight into inherent risks due to internal or external factors (BCBS, 2011:11).

- **Risk and control self-assessment (RCSA)**

Each banking unit must identify and rate the degree and nature of operational risks by establishing the frequency and impact of the loss (Jednak & Jednak, 2013:74). This method also determines the existing risk control measures in place and how the risks are currently managed. The tools used are facilitated workshops, issue-orientated lists or forms, scorecards and questionnaires (Jednak & Jednak, 2013:74). This method has the

advantage of using risk and control data which have already been agreed on and are linked to the business objectives or processes (Blunden & Thirlwell, 2010:119). The RCSA method will assist a bank in the assessment of risks and controls against the risk appetite threshold established by senior management for those risks (Blunden & Thirlwell, 2010:92).

- **Key risk indicators (KRIs)**

KRIs are used to provide a reliable basis for determining the likelihood and impact of current operational risk events or losses. KRIs will monitor, anticipate and measure operational risk exposures and serve as an early warning system for potential threats (Scandizzo, 2005:235–236). KRIs need to be linked to the objective, strategy and targeted performance levels of a bank, with a robust understanding of the sources of risk or risk drivers (Fraser & Simkins, 2010:128). Through the setting of escalation and threshold levels, KRIs can support and confirm the risk appetite and tolerance levels of a bank (Fraser & Simkins, 2010:134).

- **Key performance indicators (KPIs)**

KPIs are used to measure how well or how efficient something is performing (Hong Kong Institute of Bankers, 2013:75). KPIs provide an understanding of the status of operational processes, which may, in turn, provide comprehension into operational failures, potential losses and weaknesses (BCBS, 2011:12).

- **Scenario analysis**

Scenario analysis is the analysis of potential risk exposures which are identified through the use of scenarios by critical employees in a bank (Young, 2014:48). Scenario analysis uses descriptive models to determine how the future might turn out (Chapman, 2011:176). A bank can use various scenario analysis methods, for example, workshops, conduct interviews or the analysis of data in small teams (Girling, 2013:130). The results of scenario analysis can indicate the ‘top risks; of a bank and assist a bank to manage these risks through mitigating solutions (Girling, 2013:162).

- **Business or risk process flow analysis**

The business or risk process flow analysis identifies the key steps and risk points in business activities, processes and organisational functions (BCBS, 2011:12). Information can be gathered through the use of focus groups, workshops, interviews, and facilitated meetings. The results of the analysis can be illustrated in a risk map, which displays the relationship between the likelihood of a risk occurrence and the severity of the impact thereof, once the controls are in place (Young, 2014:91–92).

- **Comparative analysis**

This method compares the results of all the various methods used to evaluate the risks, for example, the frequency and severity of internal data are compared with RCSAs, which can assist a bank to determine whether the self-assessment processes are functioning effectively. This method provides a more comprehensive view of the exposure of a bank to potential risk events and operational risk profile (BCBS, 2011:12).

Based on the above discussion, it is imperative that some or a combination of these methods form part of the operational risk evaluation process of a bank and is essential to use in the monitoring the operational risk appetite of a bank. It is also crucial for a bank to re-evaluate the risk register to determine whether any significant risks were overlooked (Blunden & Thirlwell, 2010:71). After the risk exposures of the bank have been evaluated using the above methods, the residual risks remain, which are the risks that remain after control measures were implemented (Valsamakis et al., 2010:123). The operational risk control process aims to address the residual risks which remain a threat to the bank this will be discussed in the next section.

2.6.3 Operational risk control

Operational risk control is the cyclical process of evaluating a risk treatment measure and determining whether residual risk levels are tolerable. If these levels are not tolerable, the bank must generate a new risk treatment measure, and assess the effectiveness of that treatment (ISO, 2009:19). For a bank to control an operational risk event, it must mitigate and map the operational risk loss. Through operational risk control, the bank should be able to avoid catastrophic losses and anticipate operational risk events (Young,

2014:105). As discussed previously, one of the fundamental operational risk management principles in Basel II is control and mitigation. This principle underlines the importance for a bank to have a healthy control environment that utilises systems, processes and policies, appropriate internal controls, and suitable risk mitigation and transfer strategies (BCBS, 2011:6). Operational risk controls consist of various techniques designed to minimise and treat operational risks exposures through loss control and prevention measures (Moosa, 2007:21). The various views and techniques will be discussed next.

According to Young (2014:118), there are four pillars of a risk control process, namely policies and procedures, organisational structure, risk reporting and internal controls. A bank must establish these components to ensure that adequate risk control measures are achieved. For a bank to be able to control risk, it needs to decide whether to accept, treat, transfer or avoid the operational risk. For example, acts of God can be insured against, and virus controls can be implemented to prevent inadequate systems security in a bank (Young, 2014:105). Mapping the identified risks according to their frequency and impact on a risk map can be used during the risk control process (see Figure 2.7).

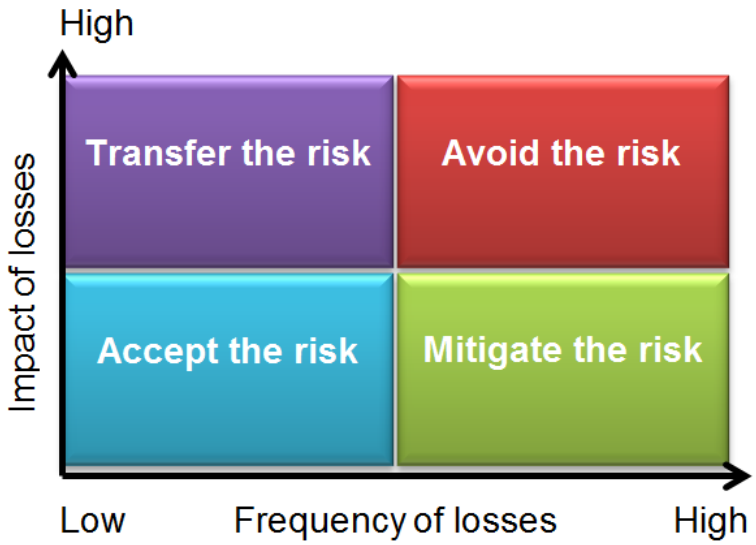


Figure 2.7: Key risk mitigation decisions
Source: Young (2010:178)

As seen in the figure above, some of the categories for risk control decisions are:

- Risk acceptance or tolerance is where the bank accepts the consequence of a risk event because the losses incurred are of such a nature that it is accepted and disregarded.
- Risk treatment or mitigation is when a bank needs to develop and implement control measures to minimise or prevent losses.
- Risk transfer is when the bank transfers potential effects of a loss to a third party (insurance) because there will always be residual risks which remain within the bank.
- Risk avoidance/termination is where a bank needs to avoid a business decision which could result in unacceptable losses and have a catastrophic impact on the bank (Young, 2014:107).

In concurrence with the risk control decisions mentioned above, the Hong Kong Institute for Bankers (2013:123–135) recommends the following risk control interventions:

- Loss prediction of the events that may cause future losses.
- Contingency management of the company-wide aftermath following significant loss events.
- Loss reduction by reducing the impact of a specific event.
- Risk avoidance by reducing the engagement in the activities that expose the bank to identified operational risks or removing risk by eliminating the risk when an unfavourable outcome or impact or high-risk exposure is anticipated.
- Loss prevention by redesigning business activities and processes to make a loss event less likely to occur in the future.
- Internal controls by implementing mechanisms to limit exposures. It is a measure to identify risk exposures and avert them from turning into loss events.
- Risk financing to ensure that the bank can finance the losses by either transferring the loss to an external party better able to manage the risks for a fixed premium (insurance) or restructuring the organisation to be able to handle the risk.
- Loss control by changing the causal paths by which high-impact events happen. It curbs the tendency of relatively frequent and insignificant events to become more critical.

According to ISO 31000 (2009:19), risk control measures can be seen as the following:

- Removing the risk source: *treat – prevent*.
- Changing the consequence: *treat – reduce*.
- Avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk: *terminate*.
- Retaining the risk by an informed decision: *tolerate*.
- Changing the likelihood: *treat – reduce*.
- Sharing the risk with another party or parties (including contracts and risk financing): *transfer the financial impact of the threat*.
- Taking or increasing the risk in order to pursue an opportunity: *take the risk for reward*.

Based on the above, it is evident that a decision must be made on whether to accept or avoid certain risks and how the bank will manage key risk factors that affect the profit and loss position of the bank (Hong Kong Institute for Bankers, 2013:30). After a bank executes the control decisions as mentioned above, it should also implement preventive and detective control measures to eliminate or minimise the effect of operational risk events. Detective controls are measures that address the effects of an operational risk event, and preventive controls are measures which are in place to prevent a loss from occurring (Thirwell & Blunden, 2010). Operational risk management must be incorporated into the internal control system of a bank (Croitoru, 2014:24). The risk control and reporting process should be effective to ensure timely decision-making regarding risk control measures (Young, 2014:118). To conclude, the operational risk control process is used for the treatment of risk by determining if the risk is tolerable and within the limits of the risk appetite of the organisation. The next step, operational risk financing, which is interrelated with operational risk control, will be discussed in the next section.

2.6.4 Operational risk financing

Operational risk financing is one of the most crucial steps in the risk management process and forms a close link with operational risk control because it needs to ensure that the cost of risk management does not exceed the benefits (Valsamakis et al., 2010:145). The operational risk financing process aims to determine the funds available to assist an

organisation when operational risk losses occur (Moosa, 2007:21). According to Young (2014:121), effective operational risk financing should ensure optimal financing and cost-efficiency for a bank when dealing with the cost of risk management.

According to the Hong Kong Institute for Bankers (2013:129), there are various approaches for a bank to finance its losses, namely:

- Corporate diversification: The acquisition or investment in other firms or projects whose cash flows are not perfectly correlated with the other cash flows of the organisation.
- Hedging: Where financial derivatives are used by an organisation to offset losses, which could occur from movements in interest rates, commodity prices and forex rates.
- Financial restructuring: Debt is seen as the cheapest form of external financing, and could allow an organisation to capture tax benefits, as well as essential economies of scale and scope. Increased debt, however, means an increased risk of default. Techniques, such as credit management and asset-backed financing, assist in managing this trade-off by restructuring both short- and long-term liabilities.
- Contractual risk transfers: Risks which are transferred using contracts, for example, outsourcing or using independent contractors.
- Asset-liability management. Focusing on restructuring the portfolio of assets and liabilities will assist in minimising the sensitivity of a bank to liquidity and interest-rate risks.
- Insurance. An external insurer promises to provide funds to cover specified losses in return for a premium from the purchaser at the commencement of the contract.

Young (2014:132) also stresses that a bank needs to establish certain financing instruments such as insurance, internal funding and capital reserves, which should be available as control measures in the event of a loss. Refer to Table 2.11 below regarding how a bank can implement certain risk financing instruments for certain operational risk events.

Table 2.11: Financing instruments for operational risk events

Risk category	Example of event	Risk financing mechanism
Low-frequency/high impact	Catastrophic or unexpected events, for example, fire or floods	Third party insurance or self-insurance (captives).
High-frequency/low impact	Expected or unexpected events, for example, credit card fraud	Third party insurance.
Low-frequency/low impact	Expected events, for example, losses due to staff or transaction errors and petty cash theft.	Part of operations and part of risk appetite levels which is accepted and written off by the bank.
High-frequency/high impact	Expected events, for example, many losses linked to trading and investments in high-risk shares.	Internal funding or capital provision.

Source: Young (2014:130)

A bank should always measure the financial impact of an operational risk event against its acceptable risk appetite. If the financial impact of a specific operational risk is higher than the bank's acceptable risk appetite level for that risk, the bank should either retain (assume) or transfer the risk (Moosa, 2007:21). It is fundamental for a bank first to determine its capacity limits and then its risk appetite (Young, 2014:129). Operational risk appetite is seen as the level of risks an organisation is willing to accept to achieve its strategic objectives (PwC, 2014:3). Operational risk appetite forms an essential component of risk financing because a bank needs to determine its risk appetite and inform the board of directors and senior management about the risk culture in which it operates (Chapman, 2011:229). The concept of operational risk appetite will be adequately addressed in Chapter 3. Operational risk monitoring as a component of a risk management process will be dealt with in the next section.

2.6.5 Operational risk monitoring

Risk monitoring is another critical component of the operational risk management process. It is essential for a bank continuously to review and monitor all the steps in the operational risk management process because new information may become available or circumstances may have changed at the bank (Chapman, 2011:233). The BCBS (2011:5) also emphasises the need to monitor risks as one of their sound practice principles. The BCBS (2011:5) states that senior management should develop a process to monitor operational risk profiles and material exposures to losses frequently. As such,

suitable reporting mechanisms should be in place at the business line, senior management and board level to support proactive management of operational risk (BCBS, 2011:5).

The importance of continually monitoring and reporting on all the steps in the operational risk management process will ensure that corrective actions against risk exposures are taken by a bank (Young, 2014:138). According to the BCBS, the reporting of operational risks should include the following:

- Information regarding relevant external events and potential effects or losses on a bank and its operational risk capital.
- Details of current internal operational risk events.
- Breaches of the tolerance levels or risk appetite thresholds of a bank (BCBS, 2011:14)

Hain (2009, cited in Young, 2015:886), also concurs by stating that risk reporting plays a central role in operational risk management, and internal and external risk reporting is essential to ensure the provision of accurate and suitable risk information for decision-making and operational risk management. Risk monitoring and risk reporting go hand in hand because risk reports need to cover the results of the monitoring activities and can assist in the communication of the overall operational risk profile (Young, 2015:886).

ISO 31000 (ISO, 2009:20) also highlights the importance of monitoring risk as part of the risk management process for:

- obtaining further information to improve risk evaluation;
- identifying emerging risks;
- analysing and learning the lessons from events (including near-misses), trends, changes, failures and successes;
- ensuring that risk controls are efficient and effective in both design an operation;
- detecting changes in the internal and external environment, including changes to risk criteria and the risk itself, which can require adjustment of risk priorities and treatments.

The operational risk monitoring process must be carried out with the purpose of increasing the success of the implementation of the operational risk management

process, as well as enhancing operational risk practices, policies and procedures (Chapman, 2011:233). The risk monitoring process also extends to the evaluation of the culture, preparedness and performance of the organisation, as well as the risk improvement recommendations, the evaluation of embedding risk management activities into the organisation, and the routine monitoring of risk performance indicators (AIRMIC et al., 2010:15).

As seen in the discussions above, it is crucial for a bank to implement an operational risk management process effectively. The result of an effective operational risk management process is the creation of various risk reports that can be used to determine the risk profile of a bank. The risk profile, in turn, will indicate the risks, which will serve as an input to determine a realistic operational risk appetite (Valsamakis et al., 2010:147).

In conclusion, in order for a bank to determine its operational risk appetite, it is necessary for a bank to understand the operational risk management process and how it must be aligned with the business objectives of a bank. According to Blunden and Thirlwell (2013:64), it is important for the operational risk management process to be undertaken with the business objectives and risk appetite of an organisation. This section now concludes the discussion on the operational risk management process.

2.7 CONCLUSION

This chapter provided an overview of the literature regarding operational risk in the financial and banking industry. The chapter aimed to focus on the definition of operational risk, the background and adoption of operational risk management and explained the operational risk management framework and process for a bank. The chapter also discussed the different national and international frameworks, standards and reports developed to manage operational risk, the adoption of operational risk in the South African banking industry and international practices. A bank must know all of these topics because it will enable the bank to get an underlying understanding of its operational risk appetite.

The literature review revealed that it is essential for a bank to implement operational risk management measures throughout its business processes and activities. The range of new risk management principles, processes, frameworks, and roles and responsibilities

that have been established international role players, namely the ISO, COSO, the Basel Committee on Banking Supervision and the King Committee on Corporate Governance, was discussed. Basel II, King III, ISO 31000 and the COSO ERM framework was explained to gain an understanding of best practices and approaches for effective operational risk management.

Based on relevant literature, the operational risk management framework and process was discussed. A risk management framework, policy, strategy and process need to be embedded in the overall objectives and activities of a bank to enable a bank to determine its risk appetite effectively. It is also crucial for a bank to manage the five steps in the operational risk management process effectively, namely risk identification, evaluation, control, financing and monitoring. These steps are essential components in the determination of the risk appetite levels for identified risks of a bank. Literature also suggests that a bank needs to categorise its operational risks into causes, events and effects and that there are different approaches to the categorisation of risks. If a bank correctly categorises the identified operational risks, the bank should be able to distinguish between the high-impact and low-impact operational risks, which could steer the bank to determine its operational risk appetite towards each risk. The literature also highlights operational risk appetite as an essential component of the risk-financing step, because it is fundamental for a bank first to determine its capacity limits and then its risk appetite. From the literature in the chapter, the following conclusions can be made:

- it is crucial for a bank to understand the definition and the components of operational risk to determine its operational risk appetite;
- a bank needs to understand the origin of operational risk and what operational risk management is comprised of in order to manage and measure operational risks effectively, to ensure that the bank is in line with its operational risk appetite;
- an operational risk management framework, policy, strategy and process need to be embedded in the overall objectives and activities of a bank to enable the bank to determine its operational risk appetite effectively;

- It is crucial for a bank to implement a useful operational risk management framework and process because it can assist a bank to understand the operational risks encountered, to determine its operational risk appetite;
- An ORMF can provide a multidimensional view of the risk exposure in an organisation and assist senior management with the weighing of high-level risks against the operational risk appetite of the bank.
- The operational risk management process must be undertaken with the business objectives and operational risk appetite of a bank.
- It is also essential for a bank to manage the five steps in the operational risk management process effectively, namely risk identification, evaluation, control, financing and monitoring because it will assist a bank to determine the operational risk appetite levels of the bank for identified operational risks.
- Operational risk appetite is as an important component of the risk-financing step because it is fundamental for a bank to determine its capacity limits first and then its operational risk appetite.

To conclude, the following question in Chapter 1 remains: Are current organisations managing their risk exposures effectively by setting a realistic risk appetite? The next chapter will discuss the literature regarding the concept of operational risk appetite, which is the primary focal point of the research.

CHAPTER 3: OPERATIONAL RISK APPETITE

3.1 INTRODUCTION

Chapter 2 focused on the background and adoption of operational risk management, and the explanation of an operational risk management process in a bank. It also highlighted the different national and international frameworks, standards and reports developed to manage operational risk in a bank, the adoption of operational risk in the South African banking industry and international practices.

This chapter will highlight the importance of determining an operational risk appetite and implementing an operational RAF in a bank. It will provide an overview of the various approaches and principles to formulate an operational RAF and statement. This chapter will also discuss the challenges that banks are experiencing with the implementation of an operational RAF and statement.

3.2 OPERATIONAL RISK APPETITE

As discussed in the previous chapters, many of the crises at financial institutions over the past years were based on the failure of operational risk management processes, coupled with inadequate capital or unsuitable funding structures Jednak and Jednak (2013:72). Goldstein and McElligott (2014:2), on the other hand, ask the question whether it is not also possible that many financial institutions involved in these crises did not align their strategy or objectives with their risk capacity and risk appetite? According to COSO (2012:5), one immense problem which led to the financial crisis of 2008 was that although objectives were created, there was no identification of those responsible when risks were sustained or the articulation of risk appetite within the organisation. The Risk and Insurance Management Society (RIMS) executive report (2012:5) concurs and states that many of the organisations involved in the financial crises had not established or enforced acceptable risk appetite levels and did not communicate or define risk appetite. Organisations that did define their risk appetites and risk tolerances did not communicate or enforce the risk limits across their organisations.

Furthermore, these organisations had no clear mechanism or risk governance structure in place to view the effect of individual risk taking on an enterprise-wide level or an individual business unit (RIMS, 2012:5). Some of these organisations also did not have suitable governance structures in place to ensure that risk takers were conforming with the defined risk appetites and tolerances of the organisations (RIMS, 2012:5). After the financial crisis of 2008, financial institutions have started to increase their efforts to strengthen their risk appetite frameworks (RAFs) in response to new standards provided by the FSB and other regulators (PwC & IACPM, 2014:1). According to a study undertaken by PricewaterhouseCoopers LLP (PwC) and the International Association of Credit Portfolio Managers (IACPM) (2014:1), financial institutions and supervisors agree that an RAF is a crucial component of an effective risk governance process. The RAF will be fully discussed in the following sections.

The financial crisis also led board members and senior managers to increase the risk management discussions, regarding risk appetite and the acceptable risk boundaries for an organisation, at board meetings (RIMS, 2012:5). It is crucial for the board and senior management of a bank to understand what is meant by the term ‘risk appetite’ because the risk appetite of a bank should link with the strategy, objectives and risk governance processes of a bank (Hillson, 2012:3). In order to do this, the bank must be able to define risk appetite. The ability to express and understand what is meant by risk appetite in a bank will allow decision-makers at all levels to decide how much risk they should take in any particular situation (Hillson, 2012:3).

Even though the term ‘risk appetite’ has been in use for many years, the challenge remains that there is not a single agreed-upon definition of risk appetite. Various authors and institutions have developed their risk appetite definitions, which are shown in Table 3.1.

Table 3.1: Various definitions of risk appetite

Author or institution	Risk appetite definition
IoDSA: King III	"The level of residual risk that the company is prepared or willing to accept, without further mitigation action being put in place, or the amount of risk the company is willing to accept in pursuit of value" (IoDSA, 2009:58).
BCBS	Basel operational risk definition: "Risk appetite is a high-level determination of how much risk a firm is willing to accept considering the risk-return attributes; it is often taken as a forward-looking view of risk acceptance" (BCBS, 2011:6). Basel corporate governance definition: "Risk appetite is the level and type of risk a firm is able and willing to assume in its exposures and business activities, given its business objectives and obligations to stakeholders. Risk appetite is generally expressed through both quantitative and qualitative means and should consider extreme conditions, events and outcomes. In addition, risk appetite should reflect the potential impact on earnings, capital, and funding or liquidity" (Girling, 2013:171).
ISO	"Amount and type of risk that an organisation is willing to pursue or retain" (RIMS, 2012:3).
COSO	"Risk appetite is the amount of risk, on a broad level an organisation is willing to accept in pursuit of stakeholder value" (COSO, 2012:1).
FSB	"The aggregate level and types of risk a financial institution is willing to assume within its risk capacity to achieve its strategic objectives and business plan" (FSB, 2013:3).
IRM	"The amount of risk that an organisation is willing to seek or accept in the pursuit of its long-term objectives" (IRM, 2011:15).
IOR	"Operational risk appetite can be described as the operational risk it is prepared to tolerate" (IOR, 2012:5).
RIMS	"The total exposed amount that an organisation wishes to undertake by risk-return trade-offs for one or more desired and expected outcomes" (RIMS, 2016:3).
BIS	"Risk appetite reflects the level of aggregate risk that the board is willing to assume and manage in the pursuit of the business objectives of the bank. Risk appetite may include both quantitative and qualitative elements, as appropriate, and encompass a range of measures" (Girling, 2013:168).
PwC	"The amount of risk an organisation is willing to accept in pursuit of strategic objectives" (ERM Initiative Faculty & Cox, 2014:1).
Blunden and Thirlwell	"The amount and type of risk that an organisation is willing to take to achieve its strategic objectives (over a specified time horizon at a given level of confidence)" (Blunden & Thirlwell, 2010).
Girling	"The view of the firm on what risks it is willing or unwilling to take or the amount of risk the company chooses to take" (Girling, 2013:167).
Taylor	"It is a combination of capacity to take treats and opportunities and the willingness or tolerance towards the taking of risks" (Taylor, 2014:74–75).

Young	"Operational risk appetite is the amount of risk an organisation is prepared to tolerate at a given point in time concerning losses in pursuit of business objectives" (Young, 2014:50).
Aven	"It is the willingness to take on risky activities in pursuit of value" (Aven, 2013:465).
Chapman	"The amount of risk a business is prepared to tolerate (be exposed to) at any point in time" (Chapman, 2011:226).
Hillson	"The tendency of an individual or group to take a risk in a given situation" (Hillson, 2012:2).

After analysing the abovementioned definitions, the following main concepts can be identified, relating to risk appetite:

- risk acceptance;
- stakeholder value;
- business or strategic objectives;
- tolerance for risk;
- amount of risk;
- types of risks; and
- capacity for risk.

Based on the above definitions and identified concepts, the common thread linking these definitions is that risk appetite is based on the fact that a bank must accept a certain level of risk to realise its strategic objectives. Some of the definitions also refer to risk appetite as the willingness to accept or tolerate risk.

According to the IOR (2012:4), risk appetite definitions can vary according to the following:

- context: industry sector (for example financial services, construction, insurance, health and retail);
- risk type (for example credit risk versus market risk versus operational risk); and
- stakeholder perspective (for example internal management versus board members versus external investors).

Young (2014:48) also supports the idea that the variety of meanings and interpretations of risk appetite definitions could lead to confusion. The challenge lies in the fact that

specific risk appetite definitions are defined according to the different individual risk types, or based on a broad view of all the risk types. According to Young (2010:182), a one-fits-all definition could lead to misunderstanding, and it is crucial for a bank to define risk appetite for each risk type instead. Goldstein and McElligott (2014:2–3), by contrast, state, that the board should agree and identify a single definition of risk appetite, risk tolerance and risk limits for use through all business units in the organisation. According to them, it is sound practice to establish a central risk appetite definition supported by a number of risk limits, which are contextualised by the nature of the risk category to which the risk relates.

Gorzeń-Mitka and Wieczorek-Kosmala (2013:115) argue, on the other hand, that the core problem when defining risk appetite, is the understanding of the term 'risk' which influences the approaches to risk management. For example, if the risk is seen as a threat, then the risk appetite is associated with the acceptable and realistic level of risk exposure for a particular organisation, whereas, if the risk is perceived to be an opportunity, risk appetite is expressed as a proactive approach to risk. Aven (2013:466) states that if an organisation wants to implement the concept of risk appetite properly within its organisational environment, it is vital for the organisation to understand the measurement dimension of risk. He also explains that risk appetite is defined as the willingness to take on risky activities in pursuit of value. By using this definition, it becomes clear that it is important for an organisation to clarify what the term 'risk' means as well. It is vital to have risk perspectives that also support the risk appetite concept in an organisation (Aven, 2013:466).

As seen above, there are various views of and opinions on how an organisation should define its risk appetite, and that is why Marsh Risk Consulting and the University of Nottingham in 2009 embarked on a study that was devoted to the problem of defining risk appetite (Marsh, Nottingham University Business School & AIRMIC, 2009). The study evaluated the definitions, challenges, approaches and insights into the concept of risk appetite. The findings indicated the following:

- Definitions of risk appetite vary across organisations/practitioners. There is no single 'one size fits all' approach to risk appetite, as this depends on the industry,

data availability, degree of de-centralisation, culture and risk management maturity.

- Certain organisations choose to make a distinction between risk appetite (amount of risk that is taken for reward) and risk tolerance (the maximum risk that can be taken before financial distress).
- Some organisations use a combination of different definitions as a basis for their risk appetite statement.
- Most of the risk managers of the organisation have developed a unified risk appetite statement, and only a minority have risk appetite statements for different risk types (Marsh, Nottingham University Business School & AIRMIC, 2009:5–6, 19, 46)

One of the reasons to why most of the organisations only have a consolidated risk appetite statement and not one for each risk type as was found in the study mentioned above might be that risk appetite definitions for market and credit risks are much easier to determine than for operational risks. This challenge can be due to the following causes:

- Operational risk is pervasive because it is managed throughout the organisation and is often merely a consequence of operating activities (PwC, 2014:3). Operational risks (for example, external fraud or IT system failures) may be inherent in operational activities but are seldom intentionally sought out (IOR, 2012:4).
- Operational risks have been more difficult to quantify than market and credit risks because there is no ‘common currency’ for operational risks (PwC, 2014:3). There is no material upside regarding income/return generation because of an operational risk event (IOR, 2012:4). For example, some operational risks which cannot be measured quantitatively may have no appetite in the organisation whatsoever, such as employee injuries or deaths as a result of inadequate health and safety procedures (Blunden & Thirlwell, 2013:66).
- Operational risks are likely to be mitigated downwards to the stated appetite level by senior management as long as the cost of mitigation does not exceed the

expected loss, whereas taking market or credit risks is likely to be encouraged up to the stated appetite level by senior management (IOR, 2012:4).

- Operational risks are unavoidable. Though an appetite for loss is agreed upon, it is likely to be exceeded, despite the controls and other mitigating factors that are in place (Blunden & Thirlwell, 2013:63).
- Operational risks cannot be capped as with credit or market risks. Once an organisation enters into business, it needs to manage the associated operational risks of the business activities (IOR, 2012:5).

It is imperative that senior management of an organisation defines operational risk appetite in a way that is understood and accepted throughout the organisation. By achieving this, an organisation will reach its objectives through informed decision-making (PwC, 2014:3). By drawing on the above literature review on various definitions of risk appetite and the challenges faced to define a suitable definition, the following definition is accepted for the purposes of this study:

Risk appetite is the amount of operational risks an organisation is willing to accept or tolerate in order to achieve strategic objectives.

The above definition should indicate the quantitative (the overall financial appetite of the organisation) and qualitative (operational risk types related to the business portfolio) expressions which relate to the amount of operational risks that the organisation is willing to accept or tolerate to achieve strategic objectives. A clear definition of operational risk appetite should enable senior management and the board to understand the quantity and type of operational risks the organisation is willing to accept or tolerate and indicate the trade-offs between risk and return, as well as the capacity to manage the operational risks to achieve objectives (PwC, 2014:4). The definition also indicates the link between operational risk appetite and the strategy of an organisation through its desirable and undesirable risk exposures (Goldstein & McElligott, 2014:2–3). According to Blunden and Thirlwell (2013:62–63), an organisation can also decide to form individual risk appetite statements/definitions for each operational risk type/loss category, for example:

- the organisation has no appetite or a zero tolerance for financial crime and will implement appropriate mitigating measures to control it;

- the organisation has no appetite or a zero tolerance for adverse media coverage and will use every effort to ensure that events that could potentially lead to such losses are avoided; and
- the organisation has no appetite or a zero tolerance for individual operational risk losses above a certain amount and cumulative losses of a specified amount within a specified period.

If operational risk appetite is clearly defined in an organisation, the organisation can convert risk metrics and methods into strategic decisions, sound reporting systems and day-to-day business decisions (Barfield, 2007:2). An operational risk appetite could also set the boundaries to form a dynamic link between operational risk management, strategy and objectives (Barfield, 2007:2), and could facilitate the identification and management of risks and opportunities (Goldstein & McElligott, 2014:5).

According to Barfield (2007:2), if a financial institution has achieved a clear definition of its operational risk appetite, it will have accomplished the following:

- the basis for consistent communication to different stakeholders, for example, the board, senior management, chief risk officers, external stakeholders and regulators;
- clarity over the operational risks that the financial institution wishes to assume; and
- clear articulation of the attitudes to operational risks of the board and senior management.

The 2012 RIMS Executive Report, “Exploring risk appetite and risk tolerance” (RIMS, 2016:3), also explains that a clear and well-organised risk appetite and tolerance practice can provide many benefits:

- align stakeholders, including the board, senior management and shareholders, regarding the amount and type of risk the organisation is willing to take;
- motivate organisations to take measured risks in order to create value and avoid unbearable losses; and
- create awareness about and actions to prevent extreme levels of risk that could lead to adverse consequences.

Young (2010:182–183) also emphasises the importance of having a realistic operational risk appetite and states that the following benefits will be realised:

- A culture of risk awareness throughout the organisation.
- Better mitigating strategies to reduce risks in order to bring them within the defined risk appetite of the organisation.
- Alignment of strategic objectives and business activities. This activity will ensure that there are strategic alternative routes that could be taken to avoid the risk appetite being breached or to maximise the upside potential.
- Sound decision-making by the board and senior management.
- Enhanced corporate governance of the organisation.
- Improved reputation of the organisation.
- The involvement of all stakeholders to provide risk information and make sound decisions to achieve business objectives.
- A healthier view of the risk expenses which will ensure that the cost of risk does not exceed the benefits. It will, therefore, ensure that the potential rewards associated with the course of action do not breach the risk appetite levels.

The IOR (2012:5–6) also highlights the importance for a financial institution to define operational risk appetite. Through defining operational risk appetite, the financial institution will increase its operational performance, enhance its value to stakeholders and achieve the following benefits:

- Providing a means of expressing the attitude of senior management and the board to risk, which can then be communicated all the way through the organisation as part of encouraging a risk-aware culture (for example, clarifying the relationship profitable business and risk).
- Aligning operational activities and strategic objectives by improving the balance between business development/returns/growth and the related operational risks inherent in pursuing those objectives.
- Establishing a framework for business and risk decision-making (for example which operational risks can be accepted/tolerated, which risk should be mitigated and by how much), as well as ensuring a proper balance between being risk-

averse and risk-seeking. Operational risk appetite can represent a powerful instrument for managing the business, for instance not only when a breach occurs, but also where a potential breach can be predicted and averted.

- Ensuring an improved view of risk expenditure so that the cost of risk does not exceed the benefits.
- Encouraging more conscious and active operational risk management practices, for example, prioritising risk-related issues for escalation and action.
- Enabling the board to exercise appropriate corporate governance and oversight by defining the nature and level of operational risks it considers acceptable or unacceptable as well as setting limits for business behaviours and activities.
- Improving the allocation of operational risk management resources by bringing attention to higher priority problems (for example areas where appetite thresholds are under threat) (IOR, 2012:6).

Based on the benefits identified above, it is evident that if a bank clearly defines its operational risk appetite, it will be able to identify the operational risks it wishes to accept and tolerate, achieve business objectives and express the risk appetite of the board and senior management throughout the bank. While it is important to define risk appetite, it is also crucial to consider the different concepts that are related to risk appetite, for example risk capacity, risk tolerance or threshold, risk profile, risk culture and risk limits to enable an organisation to understand the differences, as well as how these concepts are interchangeable. Setting risk appetite without considering these concepts can lead to severe consequences, for example, there will be a disconnect between the risk appetite, tolerance and capacity of the organisation, which could disrupt decision-making. The different concepts will be briefly discussed below to indicate the differences between them and risk appetite, but also how they are interconnected.

3.2.1 Risk tolerance

According to COSO (2012:4), “risk tolerance relates to risk appetite, but differs in one fundamental way: risk tolerance represents the application of risk appetite to specific objectives”. Risk tolerance is defined as the boundaries of risk-taking from which the

organisation is not prepared to undertake in the pursuit of its long-term goals (IRM, 2011:15). RIMS (2016:3), on the other hand, defines risk tolerance as “the amount of uncertainty an organisation is prepared to accept in total within a certain business unit, a particular risk category, or for a specific initiative”. It is seen as specific parameters or boundaries within the overall risk appetite the organisation chooses to follow, providing a clear definition of the number of risks the organisation is willing to take (RIMS, 2016:3). It is expressed in quantitative terms that can be monitored and is communicated in terms of unacceptable and acceptable outcomes or as limited levels of risk (RIMS, 2012:3).

COSO (2012:4) also elaborates on the term ‘risk tolerance’ as “the acceptable level of variation relative to achievement of a specific objective, and often is best measured in the same units as those used to measure the stated objective”. In setting risk tolerance, the board and senior management consider the relative importance of the stated objective and align risk tolerance with risk appetite. Operating within risk tolerance levels ensures that the organisation remains within its risk appetite and, in turn, achieves objectives (COSO, 2012:4). According to Protiviti (2012:9–10), risk tolerance relates to the key matrices and targets used in realising the business objectives of the organisation.

Risk tolerances should be set in such a way that they stay within the risk appetite of the organisation, even if they are exceeded, but may be flexible enough to allow increased risk-taking in one or more business areas, without requiring an equal offset of risk from other business areas (Goldstein & McElligott, 2014:9). If the risk tolerance levels are surpassed by an organisation, it may not only endanger its overall strategy and objectives but may threaten its very survival. This can be because of the consequences regarding cost, disruption to objectives or reputational impact. Risk appetite and risk tolerance are determined by the board and are linked with the strategy and objectives of the organisation (RIMS, 2012:3). Risk appetite and risk tolerance are linked because they aim to capture the organisational philosophy desired by the board for managing and taking risks, assist in framing and defining the expected risk culture of the organisation and guide the overall resource allocation towards the management of risks (RIMS, 2012:3)

Risk targets may also accompany risk tolerance. According to Ernst & Young (EY) (2016:3), a risk target is seen as the optimal level of risk that an organisation wants to take in pursuit of a specific business goal. Setting the risk target should be based on the desired risk-return, which also needs to consider the risks that must be taken to achieve a specific business goal and the capability of a company to manage those risks (EY, 2016:3). According to RIMS (2012:4), a risk target is the preferred level of risk that the organisation considers ideal to meet objectives. This can be seen as a level within the risk tolerance boundaries, which can be shown on a risk or reward curve. According to RIMS (2012:5), it is also crucial for an organisation to determine the effectiveness and appropriateness in operating within the boundaries of the desired target levels.

Based on the above discussion, it can be concluded that the risk appetite and risk tolerance level of an organisation should be interrelated. An organisation should operate within its risk tolerance levels to ensure that it remains within its risk appetite and, in turn, achieves business objectives.

3.2.2 Risk capacity

Risk capacity is the assessment of the board and senior management of the maximum amount of risk that the firm can accept, given its liquidity, regulatory standing, capital structure, borrowing capacity or other factors (Deloitte, 2014a:3). The FSB (2013:2) defines risk capacity as the “maximum level of risk the financial institution can assume, given its current level of resources before breaching constraints determined by regulatory capital and liquidity needs, the operational environment (for example, the technical infrastructure, risk management capabilities and expertise) and obligations”. According to Sweeting (2011:386), risk capacity for financial institutions is a function of legislative and regulatory limits, and as such is part of the external risk setting of the organisation. Organisations should consider the risks to which they believe they are exposed, as well as the risks, which they are obliged to manage. Just because there is no regulatory limit in a specific business area, does not mean that risks should go unmanaged (Sweeting, 2011:386).

RIMS (2012:4) on the other hand define risk capacity as the amount of risk an organisation can bear. There is little benefit in having a considerable risk appetite or

tolerance for risk unless the capacity to manage it also exists. Risk capacity is seen as an enabler for risk-taking, as well as a cushion for risk losses (IRM, 2011:17). The board and senior management of an organisation may have a high-risk appetite, but not have enough capacity to deter the potential impact or volatility of a specific risk. Inversely, the risk capacity may be high, but the organisation may decide, based on strategy, objectives and stakeholder expectations to adopt a lower risk appetite (RIMS, 2012:4).

In conclusion, it can be said that an organisation needs to understand its risk capacity to enable it to determine a risk appetite. There is no benefit for an organisation to determine its risk appetite unless there is the capacity to manage the risk.

3.2.3 Risk limits

The FSB (2013:3) defines risk limits as the quantitative measures based on forward-looking assumptions, which assigns the risk appetite statement to specific business lines, legal entities, risk categories, concentrations, and other levels of the financial institution. Risk limits should set out the qualitative or quantitative parameters used in assessing a specific risk category and measure the aggregate amount of that specific risk. Risk limits should be measurable and specific (FSB, 2013:3).

According to Goldstein and McElligott (2014:7–8), risk tolerance refers to the acceptable variability around the risk limit. The board and senior management must understand how much risk it is willing to tolerate against a level of risk that it is willing to accept (Goldstein & McElligott, 2014:7–8). Deloitte (2014a:3) states that an emerging practice has come to light, which shows that certain organisations use an upper-risk appetite limit (level of risk that the organisation is willing to allow the risk appetite to rise to) and a lower-risk appetite limit (the minimum level of risk the organisation expect to take to achieve agreed objectives), providing a range of desired risk-taking strategies.

To conclude, it is important for an organisation to determine its risk limit by also considering its upper and lower risk appetite limit.

3.2.4 Risk profile

COSO (2012:4) defines a risk profile as the distribution and level of risks across the organisation and various risk categories. Whereas the ISO (2009:5) defines it as the

description of any set of risks (for example, risks that relate to the entire organisation or as part of the organisation). The FSB (2013:3), on the other hand, defines it as an assessment of the gross and net risk exposures (after considering mitigation strategies) of a financial institution, aggregated within and across each relevant risk category based on forward-looking assumptions. When the risk appetite is determined, the organisation also needs to assess the risk profile and the desired risk profile by allocating appetites for risks to various risk categories (Barfield, 2007:1–2). The organisation will need to determine the risks of the organisation, the likelihood and effect of these risks and the mitigating controls to enable them to set a realistic risk appetite (ERM Initiative Faculty & Cox, 2014:2).

Based on the risk profile discussion above, it can be concluded that an organisation needs to understand its risk profile to enable the organisation to determine its risk appetite.

3.2.5 Risk culture

Another influence on risk appetite is the risk culture of an organisation. The risk culture describes the set of mutual beliefs, values and knowledge that the group has about risk within an organisation (Hillson, 2012:3). A risk culture sets the standards and behaviours that are naturally accepted by the group when a particular situation is perceived as risky but is also seen as necessary (Hillson, 2012:3). According to the FSB (2014:1), risk culture is defined as the “norms of behaviour for individuals and groups within an organisation that determine the collective ability to identify and understand, openly discuss and act on the organisation’s current and future risks”. An organisation with a substantial risk culture is one where employees, senior management and the board undoubtedly apprehend which risks should be accepted and which risks should be avoided or minimised (Goldstein & McElligott, 2014:11).

In order for an organisation to have a clear picture of its risk culture, it must determine its attitude towards risks, which is a view held by the organisation or an individual of the perceived quantitative and qualitative value that may be gained in comparison to the possible loss (RIMS, 2012:4–5). ISO (2009:2) defines risk attitude as an organisation’s approach to access and eventually pursue, retain, take or turn away from risk. According to Chapman (2011:204), organisational decision-makers could have different attitudes

and preferences towards risks and returns. There might be risk-neutral, risk-averse and risk-seeking attitudes. Young (2014:36) agrees and explains these risk preferences as follows:

- *Risk-neutral:* the attitude towards risk that requires no changing of the risk/reward balance in return for an increase in risk. This attitude is usually not conducive for taking any risks to enhance the organisation.
- *Risk-averse:* the attitude towards risk that requires an increase in return for an increase in risk. This attitude is a conservative approach to risk management and usually requires detailed risk analysis before new ventures are undertaken. As such, the organisation is not prepared to take high risks for a potential increase in business or profits.
- *Risk-seeking:* the attitude towards risk whereby a decreased return would be accepted for an increase in risk. This attitude usually relates to speculation, and the organisation is prepared to take high risks in return for a potentially higher return over a short period. Due to a lack of detailed analysis and the quick reactions to market conditions, the organisation might encounter a loss when taking these business risks.

Taylor (2014:75), on the other hand, describes risk attitudes towards threats and opportunities as individuals who are unaware or ignorant of risks or individuals who are obsessed about threats and opportunities. Individuals who are ignorant towards risks will lead the organisation to be exposed to risks and destroy organisational growth and value. Taylor (2014:75) states that the ideal way for an organisation to obtain the best performance is to be neither ignorant about risk nor obsessed about it, but managing threats and opportunities to add value and growth.

Based on these opinions, it can be concluded that risk attitudes reflect a broad philosophy and method that are informed by the underlying beliefs, culture and collective comfort level of the individuals within the organisation as well as external stakeholders, while risk appetite and risk tolerance statements are intended to provide explicit guidance (RIMS, 2012:5). The extent to which the risk appetite of the organisation is demonstrated by the behaviour of individuals in that organisation is a critical factor for a sound risk culture

(Goldstein & McElligott, 2014:11). A sound risk culture should ensure that an appropriate risk-reward balance consistent with the risk appetite of a financial institution is achieved when taking on risks (FSB, 2014:1).

From the discussions above, it can be deduced that there is a clear link between risk appetite, tolerance, capacity and limits. Figure 3.1 below illustrates this relationship:

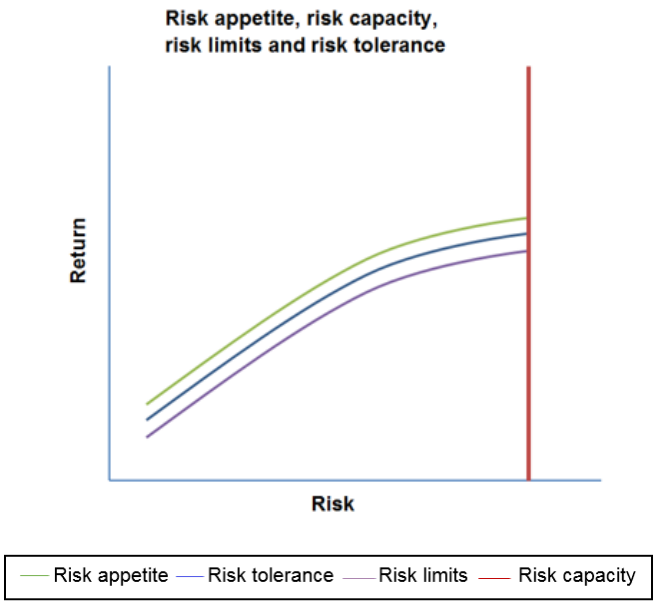


Figure 3.1: Relationship between risk appetite, tolerance, limits and capacity
Source: Goldstein and McElligott (2014:9)

In Figure 3.1, the red vertical line represents risk capacity, which is seen as the entire maximum amount of risk that the organisation can take at that specific moment, irrespective of the opportunity that is available. The purple line represents risk limits, and the green line represents risk appetite. The risk limits line is underneath the risk appetite line for all risk and return points. This is because risk appetite is the total of the organisation's risk limits plus a safeguard (risk tolerance) for caution. The blue line represents risk tolerance. The risk-return trade-off in the figure demonstrates that the strategic objectives of the organisation cannot be achieved without taking risks (Goldstein & McElligott, 2014:9–10). The amount of risk that an organisation can take is expected to be appropriate with the return available up to a maximum amount of risk that the organisation could bear at any time. It is the responsibility of the board and senior

management to consider what signifies an acceptable and an unacceptable risk within the framework of the organisation's strategy and objectives (Goldstein & McElligott, 2014:9–10).

It can also be established that there is a connection between risk appetite, profile, attitudes, tolerance and capacity. This link is summarised in Figure 3.2 below:

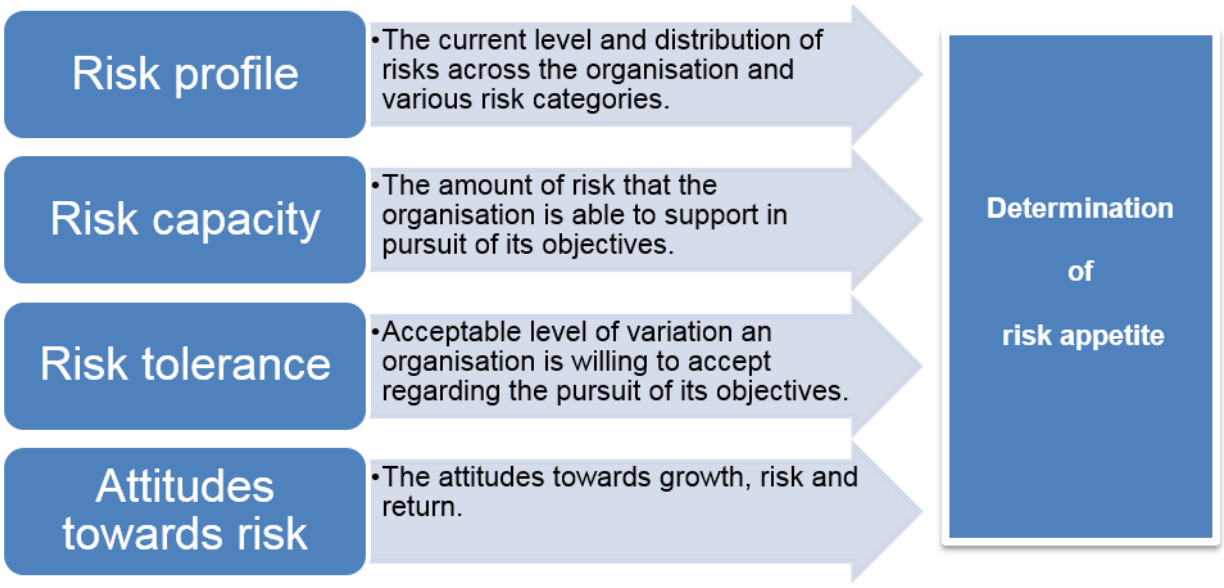


Figure 3.2: Overview of factors linked to risk appetite
Source: COSO (2012:4)

Based on Figure 3.2, it is clear that risk appetite is not developed in isolation from other factors. An organisation should also consider its capacity to take on extra risks in seeking its objectives, as well as its existing risk profile, not as a determinant of risk appetite but as an indication of the risks it currently addresses. According to COSO (2012:4), an organisation's risk appetite, strategy and objectives are interconnected, which means that senior management must take them into account when making business decisions.

Various factors connected to the risk appetite of an organisation were discussed in the sections above (see 3.2.1 to 3.2.5), but there could also be other internal and external factors to consider due to an ever-changing environment. It is essential for an organisation to keep abreast of these changes and to adjust its risk appetite accordingly.

To conclude, this section discussed the importance for a bank to define its risk appetite and its operational risk appetite. The section also defined the term 'operational risk appetite'. If a bank defines its operational risk appetite, it will be able to determine the amount of operational risks it is willing to take or tolerate in achieving its strategic objectives. The section also highlighted the importance of a bank to understand the link between risk appetite, capacity, profile, tolerance, culture and limits. Refer to Figure 3.3 below, which illustrates the importance of determining an organisation's risk appetite by also considering risk tolerance, capacity, profile, culture and limits.

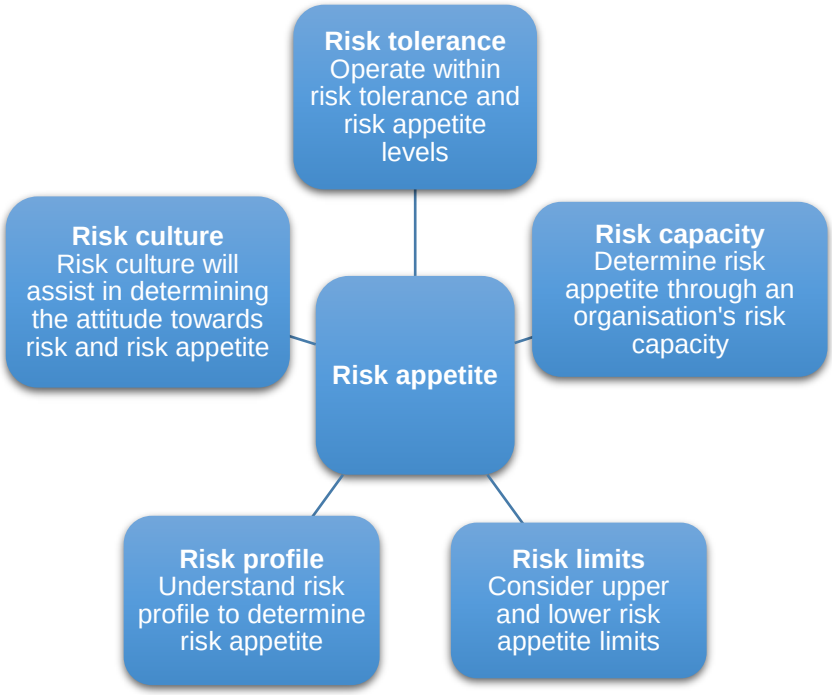


Figure 3.3: Link between risk appetite, tolerance, limit, culture profile and capacity
Source: Author's own compilation

As seen in Figure 3.3 above, each of the concepts (risk tolerance, culture, capacity, profile and limits) has an interconnected link with risk appetite. Through effective implementation and understanding of these concepts, the various components of the risk appetite framework (RAF) and the risk appetite statement (RAS) can be established. An appropriate RAF should enable an organisation to determine its risk capacity, risk appetite, risk limits, risk profile and risk tolerance in all business activities (FSB, 2013:1). The next section will discuss operational risk appetite practices, which will consider a

bank's operational risk appetite, regulatory pressure, and implementing operational RAFs and RASs in a bank. Sections 3.3.2 and 3.3.3 will illustrate how the concepts mentioned above form part of the components of an effective RAF and RAS.

3.3 OPERATIONAL RISK APPETITE PRACTICES

According to PwC (2014:8), effective use of operational risk appetite assumes a certain maturity in operational risk management practices and the overall risk culture and profile of an organisation. The articulation of operational risk appetite at the top level of an organisation and using operational risk appetite to drive business decisions throughout an organisation continue to be a challenge (PwC, 2014:9). The IOR (2009:3), on the other hand, states there could be immaturity of the operational risk appetite discipline since operational risk appetite is an area that attracts different views amongst practitioners because of the wide variety of backgrounds and contexts of operational risk appetite within different industries, for example:

- the different sizes and structures of organisations;
- the complexity of product or service offerings; and
- the regulatory jurisdictions within which organisations function.

It was important for this study to consider the different operational risk appetite practices in the financial industry and other organisations to determine which practices can be implemented in an operational risk appetite process of a bank. The next section will consider how a bank needs to determine its operational risk appetite.

3.3.1 Determining the operational risk appetite for a bank

Risk appetites are unique to every organisation because they are based on specific strategies and attributes that influence specific organisational behaviours this could lead to challenges when an organisation wants to determine its risk appetite (ERM Initiative Faculty & Cox, 2014:1). Risk appetite can be influenced by the nature of the organisation and the industry within which the organisation operates. It is therefore imperative for an organisation to understand the environment within which it operates to determine the risk appetite.

Organisations with a high-risk appetite are generally focused on the potential for significant increases in value and earnings rather than on a stable growth environment. As a result, these organisations may be willing to accept high-risks for high-returns (RIMS, 2012:4). Early-stage, high-potential, high-risk, growing or start-up organisations have a higher appetite for risk and are usually willing to accept greater uncertainty and volatility than organisations that have a moderate risk appetite (RIMS, 2012:4). On the other hand, organisations with a low-risk appetite generally are risk-averse, because their focus is on stable growth and earnings. They may be averse to market fluctuations and could be significantly influenced by legal and regulatory requirements (RIMS, 2012:4).

A bank is usually seen as an organisation with a low-risk appetite level, but some banks might have a high-risk appetite level. According to Ghosh (2012:57), a bank with a relatively low capital base and average risk management and risk control capabilities usually pursues a conservative approach to risk management and has a moderate risk appetite. These banks focus on loans and investments that involve less risk, they diversify their activities, and they also need to protect themselves against low retruns and underperformance (Ghosh, 2012:57). Banks with a high-risk appetite will prefer to do business mainly in financial instruments, real estate finance, gold and futures trading. These banks need to have high capital, rigorous risk management practices and effective control mechanisms in place (Ghosh, 2012:57). There are also banks that could have a balanced approach to risk appetite. They need to take up both speculative and traditional activities to strike a balance between high risk-return and low risk-return activities. For example, a bank could specify that 30% of its total business activities will be in the high-risk bracket, 40% in the moderate, and 30% in the low-risk bracket (Ghosh, 2012:57). It is also recommended by Ghosh (2012:56) that a bank cannot have an aggressive risk appetite level, partly because the nature of a bank is to do business with public deposits, and a bank is under strict regulatory and supervisory control.

According to Barfield (2007:1), risk appetite is also influenced by perspectives, which could vary in different sections of the organisation and by external stakeholders, for example, equity investors' appetite for risk will vary from that of rating agencies. Equity investors want to see a return, but rating agencies want to minimise the risk of default. Regulator perspectives on risk appetite differ from those of management, which in turn

differ from those of customers, employees and shareholders. Both Blunden and Thirlwell (2013:67) and Girling (2013:168) state that the board may see risk appetite in terms of capital while senior management may understand it in terms of risk and return. Business units may define risk appetite in terms of risk-control self-assessment, key risk indicators and loss data whereas the business support function may see it only in terms of key risk indicators and loss data.

According to Blunden and Thirlwell (2013:66), senior management's operational risk appetite is likely to be relatively short-term and focused on business opportunities, which generate an appetite that is inevitably bullish, for example, targets and thresholds are likely to be significant in size. The risk appetite of the board is likely to be longer-term and lower than senior management's risk appetite. The shareholders' risk appetite is likely to be the lowest of the three, and will probably be focused on the smaller possible volatility in earnings consistent with a reasonable return (Blunden & Thirlwell, 2013:66).

In a bank, risk appetite could also vary between different business activities, for example, corporate finance, real estate finance, wholesale banking, commercial banking, and retail banking. Likewise, it could also vary between operational, credit and investment activities (Ghosh, 2012:56).

To express or determine operational risk appetite in a bank is a question of defining what is acceptable to an organisation and what is not (IOR, 2009:4). As discussed in Chapter 2 (see 2.6.3), there are various ways in which operational risk can be measured or controlled. This is mapped according to a risk map, which indicates risk acceptance, risk transfer, risk mitigation and risk avoidance. The same principles can be followed when determining the operational risk appetite of a bank for a specific operational risk. This can be achieved by deciding, for each type of operational risk, what is acceptable, what is unacceptable and the parameters of the area between the two, for example, what is tolerable (IOR, 2009:4). According to the IOR (2009:4), it is common practice when monitoring performance against operational risk appetite to assign a 'RAG' status (**r**ed, **a**mber and **g**reen), indicated and explained in Table 3.2.

Table 3.2: Example of an operational risk appetite 'RAG' status

Status	Meaning	Required action
Green	Acceptable	No action required but continue monitoring.
Amber	Tolerable, but action required to avoid a red status	Investigate (to verify and understand underlying causes) and consider ways to mitigate or avoid risks within a specified period.
Red	Unacceptable; urgent attention is required	Investigate and take steps to mitigate or avoid risks within a specified short-term period.

Source: IOR (2009:4)

A bank needs to determine its operational risk categories (for example technology, people, corporate security, compliance and conduct risk) to enable the bank to map out the status of each of the operational risk categories in the above table (PwC & Strategy, 2009:8). On the other hand, Girling (2013:175) states that with operational risk, it may be inappropriate to consider having an appetite for certain operational risks. For example, should an organisation have a set appetite for internal fraud? For this reason, it can be helpful to consider risk tolerance instead. Which level of internal fraud will the organisation tolerate, even though its appetite is zero? (Girling, 2013:175). Blunden and Thirlwell (2013) concur with this statement, and indicate that operational risk includes elements that cannot be measured quantitatively, including certain risks for which there may be no appetite whatsoever, for example, there is a zero appetite for employee deaths or injuries due to poor health and safety procedures within the organisation. They also state that risk tolerance needs to be considered, for example, while there is no appetite for theft, a certain level can be tolerated (Blunden & Thirlwell, 2013).

Based on the above discussion, it can be concluded that it is essential that a bank consider its existing risk profile, desired risk appetite and risk tolerance range (for example within tolerance, slightly out of tolerance or out of tolerance) when determining operational risk appetite (PwC & Strategy, 2009:8). According to PwC and Strategy (2009:8), the aggregation of risk tolerances ensures that the bank operates in line with its desired overall risk appetite. The approach mentioned above can be applied to the overall operational RAF and will promote a consistent understanding of how to determine operational risk appetite across the organisation (IOR, 2009:4).

According to Young (2010:182), the following principles can be considered when determining operational risk appetite:

- “The process to determine risk appetite should include information regarding the number of financial losses due to operational risk exposures, which management is prepared to accept as a loss and as part of the operational and business process.
- Risk appetite should include the number of financial losses, which an organisation is prepared to tolerate as a loss notwithstanding control measures. The cost of these control measure must not exceed the potential benefits for the organisation at any given time.
- When considering risk appetite, it should be within the capacity limits of the organisation. An organisation should be able to afford premiums for insurance and absorb financial losses without impairing the sustainability of the organisation.
- All risk-bearing activities should be considered during the process to determine the risk appetite of the organisation.
- Risk appetite should indicate sufficient action required to manage the risk exposures by using the risk map effectively”.

PwC (2014:5) identified the following key challenges facing organisations concerning the determination of operational risk appetite:

- “expressing operational risk appetite at the top level of an organisation, given the many aspects and sub-types of operational risk, the absence of a ‘common operational risk currency’ (PwC, 2014), and the fact that operational risk is managed in a decentralised way across the organisation poses a challenge;
- the difficulty for an organisation to integrate operational risk appetite into decision-making, which requires the linking of high-level statements to more granular risks or performance indicators that are meaningful at a business level;

- the effort of allocating operational risk appetite across the organisation, especially in the case of qualitative and quantitative expressions of operational risk appetite that are subject to diversification benefits, such as capital; and
- the difficulty in linking operational risk appetite to operational risk capital, given the shortcomings of commonly used AMAs that could result in capital levels based on historical losses that far exceed the current appetite for operational risk."

Due to the challenges faced by organisations in setting risk appetite, as discussed above, regulators are setting new expectations for risk appetite with the focus on RAFs and RASs (Deloitte, 2014b:1). The next section will discuss these regulatory pressures and changes in the regulatory environment concerning risk appetite.

3.3.1.1 Regulatory pressure

Based on a survey conducted by the Economist Intelligence Unit (EIU) and KPMG in 2012, the greatest threats to organisations are regulatory pressure and changes in the regulatory environment (KPMG & EIU, 2013:6). The national regulators write the rules, enforce the rules and serve out the justice when these rules are broken. Various regulators for example European, UK and US regulators are exercising pressure on banks on everything related to conduct and the control environment (Imeson, 2014:1–2). This pressure is causing banks to take risk culture more seriously, and they are much more risk-aware than before (Imeson, 2014:1–2). This is also evident based on the enormous fines regulators are giving out to banks, for example the UK's Financial Conduct Authority fined Lloyds Banking Group £28 million for severe failings in controls over sales incentive schemes (the schemes led to operational risks, and sale staff were put under immense pressure to hit targets to get a bonus or avoid being demoted, rather than focusing on what consumers may want or need). It was the largest ever fine imposed by UK financial regulators for retail banking conduct failings, and the reputational damage done to the bank was immeasurable (Imeson, 2014:1). Another example is the case of Barclays Bank. Barclays Bank's reputation was severely damaged by its past operational conduct and unethical behaviour, which resulted in the departure of its chief executive, chairman and other senior directors in 2012 (Imeson, 2014:1).

Regulatory pressure, such as Basel II and emphasis on corporate governance has been a motivation for various changes in the financial industry. One of these was the acknowledgement of the necessity to articulate risk appetite more clearly (Barfield, 2007:1). According to IOR (2012:5), regulators take a specific interest in risk appetite because of its importance to corporate behaviour, internal risk culture and governance. Many international and local regulators, supervisory bodies and institutes indicate the importance of risk appetite, for example:

- The UK Prudential Regulation Authority (PRA) developed a supervisory statement (SS5/16), which indicates that the business strategy should be supported by a well-articulated and measurable statement of risk appetite, which is owned by the board. The board needs to sign off on the statement and needs to use it as part of their business strategy to monitor and control actual and prospective risks and to inform critical business decisions (PRA, 2016:6). Section C of the UK Corporate Governance Code (IRM, 2011:11) also states that the board is explicitly tasked with being responsible for "determining the nature and extent of the significant risks it is willing to take in achieving its strategic objectives".
- The National Association of Corporate Directors (NACD) published a report that stated, "a risk appetite statement resides at the heart of an effective risk management program and is linked to the organisation's overall risk management philosophy and strategic ambition" (Quail, 2012:25).
- The FSB (2013:1) conducted a cross-sectoral peer review of risk governance and the benefits that can be drawn from a wholly operational and firm-wide embedded RAF. The findings from this review contributed to the publication of the FSB's "Principles for an effective risk appetite framework" in November 2013 (FSB, 2013). The FSB principles set out vital elements for an effective RAF and RAS, risk limits and defining the roles and responsibilities of the board of directors and senior management.
- The Basel Committee on Banking Supervision (BCBS) advises that boards "should approve and review a risk appetite and tolerance statement for the

operational risk that articulates the nature, type and level of operational risk that the bank is willing to assume" (Quail, 2012:25).

- The Office of the Superintendent of Financial Institutions of Canada (OSFI) issued a guideline that says, "senior management should be able to identify and clearly articulate the institutions risk appetite and understand the impact of stress events on the risk profile of the institution" (Quail, 2012:25).
- The Institute of International Finance (IIF) developed a report on "Implementing robust risk appetite frameworks to strengthen financial institutions" and states (IIF, 2012:19):

> "[T]he board of directors should set the framework for risk appetite and put into place mechanisms to ensure the decision making will be consistently and transparently guided by it. A clearly articulated statement of risk appetite and the use of a well-designed risk appetite framework to underpin decision making are essential to the successful management of risk."

- The Committee of Sponsoring Organisations of the Treadway Commission (COSO) developed the COSO framework (COSO, 2004), which highlights the importance of aligning risk appetite and strategy. The board and senior management should consider the risk appetite of the organisation by evaluating strategic alternatives, developing mechanisms to manage related risks and setting objectives, which are aligned with its risk appetite (COSO, 2004:1).
- The Institute of Directors in Southern Africa (IoDSA) developed the King II Report, which indicates that the "board should determine the levels of risk tolerance, set limits for the risk appetite and monitor that risks taken are within the tolerance and appetite levels" (IoDSA, 2009:36).
- The Australian Prudential Regulation Authority (APRA) developed a prudential practice guide for risk management (CPG 220), which indicates the board should establish the risk appetite of an organisation, and an organisation should maintain an appropriate, clear and concise RAS that addresses its material risks. The board should also approve the RAS (APRA, 2015:10).

- The Senior Supervisors Group (SSG) indicates that healthy and active engagement by an organisation's board of directors and senior management plays a central role in ensuring that the RAF has a meaningful influence on the organisation (SSG, 2010:2).

As seen above, regulators are now focusing on the role of the board for setting a financial institution's risk appetite and monitoring its effective implementation by senior management (Deloitte, 2014a:15). Imeson (2014:1) remarks that the "emphasis on managing the non-financial operational risks, in particular, 'conduct risk' (the risk of acting unethically or illegally) and 'reputational risk' (the risk of damaged or destroyed reputations resulting from poor conduct) by a bank has increased". He also states that the change of attitudes by banks has been driven by the regulatory response as well as the board and senior management comprehending that they need to take responsibility for risk, with proper interaction, cross-checking and transparency between all parties. The banks now realise that operational risk includes poor conduct and lack of control (Imeson, 2014:1–2). The IIF and EY conducted a bank risk management survey in 2016, which indicated that regulators are increasingly demanding more effective RAFs for non-financial risks, such as operational and conduct risks. In the light of the high fines and threats of the removal of operating licences, banks are indicating money laundering and sanctions as two of their highest non-financial operational risks (IIF & EY, 2016:20–21).

According to Girling (2013:25), the regulation of operational risk is internationally established on Basel II. As previously discussed, Basel II introduced the importance of operational risk and was fully implemented into the regulatory framework for South African banks by the SARB. In 2011, Basel released a guidance paper called the "Principles for the sound management of operational risk" (BCBS, 2011:1). This guidance paper increased the emphasis on risk appetite and gave direction to the board on how to approve and review the operational risk appetite statement (ORAS) (Girling, 2013:167). Refer to Table 3.3 below, which indicates principle 4 in the guidance paper by the BCBS (2011:9), highlighting the sound practices of operational risk appetite:

Table 3.3: Basel II principle 4 for risk appetite

"Principle 4: The board of directors should approve and review a risk appetite and tolerance statement for operational risk that articulates the nature, types and levels of operational risk that the bank is willing to assume.
When approving and reviewing the risk appetite and tolerance statement, the board of directors should consider all relevant risks, the bank's level of risk aversion, its current financial condition and the bank's strategic direction. The risk appetite and tolerance statement should encapsulate the various operational risk appetites within a bank and ensure that they are consistent. The board of directors should approve appropriate thresholds or limits for specific operational risks, and overall operational risk appetite and tolerance.
The board of directors should regularly review the appropriateness of limits and the overall operational risk appetite and tolerance statements. This review should consider changes in the external environment, material increases in business or activity volumes, the quality of the control environment, the effectiveness of risk management or mitigation strategies, loss experience, and the frequency, volume or nature of limit breaches. The board should monitor management adherence to the risk appetite and tolerance statement and provide timely detection and remediation of breaches."

Source: BCBS (2011:9)

Basel II also requires the board and senior management to ensure that the operational risk framework is consistent with the bank's risk appetite and that it describes the bank's accepted operational risk appetite and tolerance, as well as thresholds or limits for residual and inherent risk, and the approved risk mitigation instruments and strategies (BCBS, 2011:8). Even with this extra guidance, implementing the operational risk appetite principles have been a challenge for banks, due to the fact that they must attempt to articulate a risk appetite for errors occurring due to inadequate or failed processes, people, systems or external events, which is a fairly complex process due to the nature and pervasiveness of operational risk (Girling, 2013:168). These challenges have resulted in banks still lacking a robust operational RAF, which does not reflect the best practices highlighted by the various regulators, supervisory bodies and institutes above. Based on a study conducted in 2009 by the SSG, which comprises the senior financial supervisors and regulators from seven countries[2], it was reported that one of the critical areas that required further improvement and work by financial institutions is to ensure that the board and senior management establish, measure and adhere to a level of risk appetite acceptable by the organisation (Deloitte, 2014b:2). The importance of

[2] United States, Canada, France, Germany, Japan, Switzerland and United Kingdom

implementing a board-approved risk appetite and framework is becoming a regulatory requirement (Deloitte, 2014b:1).

This issue became more apparent due to the increased number of recent operational risk-related losses incurred by banks. That is why the Basel Committee conducted a review on the implementation of its Operational Risk Principles in 2014. These were discussed in Chapter 2 (see 2.4.2.1).

The next section focuses on the key findings and observations of the BCBS review in 2014 regarding operational risk appetite and tolerance:

- "Many banks generally indicated that establishing a risk appetite and tolerance statement was more challenging for operational risk than for other risk categories, such as credit risk and market risk, and attributed this to the nature and pervasiveness of operational risk" (BCBS, 2014:4).
- "For those banks that have established an operational risk appetite and tolerance statement, a commonly observed practice was the inclusion of a metric such as operational losses as a percentage of gross revenue (BCBS, 2014:4). However, these metrics tended to be backwards-rather than forward-looking. Noteworthy practices include defining operational risk appetite and tolerance at both a divisional and a taxonomy level (BCBS, 2014:13), utilising both quantitative and qualitative components (BCBS, 2014:13), and setting limits based on established key risk indicators such as loss metrics, deficiencies, events and residual risk assessments from operational risk identification and assessment (BCBS, 2014:13). As a result, many banks indicated that work is underway to enhance the existing operational risk appetite and tolerance statement".
- "Not many banks indicated that work is underway to align the compensation policies better with the statement of risk appetite and tolerance. Noteworthy practices include remuneration linked to risk-adjusted indicators" (BCBS, 2014:7).
- "Some banks indicated that they had established an operational risk appetite and tolerance statement that is reviewed regularly and approved by the board of

directors or a delegated authority, while others noted that this was under development" (BCBS, 2014:12).

The BCBS review identified the following emerging and noteworthy practices by banks regarding operational risk appetite and tolerances:

- "Banks are defining operational risk appetite and tolerance at both a divisional and taxonomy level.
- Banks are utilising both quantitative and qualitative components within their operational risk appetite and tolerance statements.
- Banks are setting limits based on established key risk indicators, such as loss metrics, deficiencies, events and residual risk assessments using operational risk identification and assessment tools that have been implemented.
- Banks are reporting on established operational risk appetites and tolerances, and the use of an operational risk profile, or other items such as risk maps, trends and a listing of top operational risks.
- Banks' risk-taking incentives are appropriately aligned with risk appetite and tolerance.
- Banks are indicating changes made to their operational risk profile and appetite and tolerance, including the risk of existing products or activities.
- Banks' operational risk reports are including breaches of the banks' risk appetite and tolerance statement, as well as thresholds or limits.
- Banks have established a risk appetite and tolerance statement as well as performance expectations to assist in controlling and managing risk.
- Banks have allocated roles and responsibilities for both the first and second lines of defence in order to assess the risk exposure relating to change initiatives in line with the accepted risk appetite of the bank.
- A bank's first line of defence responsibilities includes –
    - using operational risk management tools to identify and manage risks;
    - assessing and enhancing controls;
    - monitoring and reporting the operational risk profile;

- ensuring that the operational risk profile is consistent with the established risk appetite and tolerance;
- adhering to policies, standards and guidelines; and
- promoting a strong risk culture" (BCBS, 2014:52–61).

Based on the above findings, practices and observations, the BCBS encourages banks in its report to:

- "Continue to make progress in aligning compensation policies with the operational risk appetite and tolerance statement.
- Develop their operational risk training and awareness programmes further and implement these programmes.
- Improve board and senior management oversight; articulation of operational risk appetite and tolerance statements, as well as risk disclosures.
- Continue their work to articulate and implement enhanced and forward-looking operational risk appetite and tolerance statements.
- Develop the consideration of IT risk within the operational risk appetite and tolerance statement" (BCBS, 2014:5, 8, 13, 42).

To conclude, it is evident from the above discussion that the statement made by Deloitte (2014b:15), namely "that risk appetite may well become the primary lens through which the quality of an organisation's risk management, governance and culture are assessed" may become true. The BCBS, FSB and SSG have each woven the concept of risk appetite into their rationale on supervision and regulation. Various national and international regulators are following in the same direction by implementing the recommendations made by these authorities. In the near future, South African banks can expect to be judged on the strength of their RAFs. The next section presents a discussion of the principles for an operational RAF.

3.3.2 The operational risk appetite framework

According to Deloitte (2014a:5), regulators, supervisors and the financial services industry agree on the fact that when an organisation wants to implement an effective risk appetite framework (RAF), such organisation needs –

- a strong risk culture and tone at the top;
- collaboration between financer, strategy, risk management and business units;
- the linkage between the strategy, business activities and risk appetite; and
- the regular evaluation of the organisation's risk profile against risk appetite.

If an RAF is implemented successfully, it can shape the organisation's risk culture and provide the means to assess the level of risk taken relative to the targeted amount of risk (Deloitte, 2014a:5). In order to achieve this, an organisation needs to understand the term 'risk appetite framework'. Various institutions and authors have developed RAF definitions in Table 3.4.

Table 3.4: Various risk appetite framework definitions

Author or institution	Risk appetite framework definition
SSG	An RAF is an "explicit effort to describe the boundaries within which management is expected to operate when pursuing the firm's strategy" (SSG, 2010:6).
IIF	An RAF "provides a context for such traditional risk management tools as risk policies, limits, and management information based on clear risk metrics" (IIF, 2012:19).
FSB	"The overall approach, including policies, processes, controls and systems through which risk appetite is established, communicated and monitored. It includes a RAS, risk limits and an outline of the roles and responsibilities of those overseeing the implementation and monitoring of the RAF. The RAF should consider material risks to the financial institution, as well as to the reputation of the institution, namely policyholders, depositors, investors and customers. The RAF aligns with the strategy of the institution" (FSB, 2013:2).
The CRO Forum and CRO Council (North America)	"The framework of policies and processes that establish and monitor adherence to the company's risk appetite. A company's RAF serves as a tool for the board and senior management to establish boundaries around risk-taking to achieve company objectives. As a critical element of a company's more comprehensive system of governance, RAFs have both strategic and operational dimensions" (CRO Forum & CRO Council, 2013:5).
Deloitte	A framework for "a structured approach to governance, management, measurement, monitoring and control of risks" (Deloitte, 2014a:5).

PwC	"An overall approach for establishing, communicating and monitoring all material risks of the firm through organisational roles and responsibilities, risk appetite, statements, policies, risk limits, processes, controls and systems" (PwC & IACPM, 2014:1).
Girling	An operational RAF covers "the bank's appetite and tolerance for operational risks, as specified in the policies for managing these risks" (Girling, 2013:168).
Taylor	A framework that contains a "RAS, risk limits, and an outline of the roles and responsibilities of those overseeing the implementation of the framework. The RAF must be an integral part of the organisation's overall enterprise risk management framework" (Taylor, 2014:88).

Based on the above definitions, it can be said that an operational risk appetite framework (ORAF) could be seen as a framework of policies, statements and processes, which oversees an organisation's appetite for operational risks. According to the FSB (2013:3), the RAF sets the financial institution's risk profile and forms part of the development and implementation process of the organisation's strategy and determination of the risks undertaken in line with the organisation's risk capacity. The RAF should be aligned with the strategy and objectives, capital planning, compensation scheme and business plan of a financial institution. The RAF should further provide a common framework and comparable measures across the financial institution for the board and senior management to understand, assess and communicate the level and types of risk that they are willing to tolerate or accept (FSB, 2013:3).

Based on a study conducted by PwC and IACPM (2014:6–7) on the insights into evolving global practice for RAFs by various financial institutions, the following values could be gained by implementing an RAF:

- Leads to better risk awareness at all organisational levels and enhances understanding of risk profiles.
- Strengthens risk governance by integrating and leveraging separate risk management elements holistically, for example, risk profiles and risk limits.
- Aligns the organisation's risk appetite with strategic goals by explicitly incorporating both risks and returns considerations to strategy formulation and business decision-making.

- Increases the importance of business line units in an organisation's risk ownership process due to them being able to provide input to risk targets in a manner that is consistent with the organisation's overall risk appetite.
- Enables all relevant stakeholders to evaluate their decisions. An RAF leads to a more proactive, firm-wide involvement in risk assessment because an RAF requires stakeholders to consider risk in their daily business decisions and activities.
- Satisfies regulatory and supervisory requirements.
- Establishes a unified framework to assess different risk types across an organisation.
- Enables and promotes inter-departmental or cross-functional collaboration concerning the analysis and decision-making of organisational objectives, risk appetite, risk profile, risk management and risk-return optimisation.
- Fosters collaboration and sharing of management information across functional units of an organisation.
- Serves as a platform where a complete range of quantifiable and non-quantifiable risk types are stated in unified terms against the same strategic plan and measured with a reliable set of tools.
- Integrates risk appetite into day-to-day management decision-making and long-term business planning.

Deloitte (2014b:2–3) also indicates the following organisational-wide benefits for embedding an RAF in an organisation:

- An RAF allows information to flow to the board and presents the information in a timely manner to enhance decision-making. The individuals responsible for the day-to-day running of a bank needs to have a firm understanding of the risks the bank is taking.

- An RAF places the board in the driving seat, giving the board the duty and the techniques for cascading down, setting and communicating the banks specified objectives and strategic plan, and its appetite for certain risks.
- A fully functioning RAF institutes internal communication that is across the board and enables risk communications to cascade up the organisation from the individuals who manage or take on risk.
- An RAF establishes business strategies that are clear, risk implications that are understood, common risk culture and employees working towards shared goals.
- An RAF identifies and quantifies risks in a structured way that relates these risks to the business objectives and strategy of the organisation.
- An RAF will inspire the business, risk managers and the board to ask challenging questions and find ways to evaluate the expected risk position.
- An RAF provides depth to risk management activities within the organisation.
- An RAF facilitates top-down direction from the board by means of cascading the RASs and their continue control and monitoring in a risk appetite language that is meaningful to everybody.

According to Girling (2013:172, 175), the following benefits can be achieved when an effective RAF is in place:

- Business decisions can be considered in terms of the risks taken and the appetite for risks of the board or senior management.
- Deliberations on risk appetite can lead to essential discussions on the strategic direction of the organisation and its primary competencies.
- A robust risk appetite which is resilient enough to assist the organisation in staying within its strategic plans and not going in another direction. However, it should be able to adjust to new strategic decisions and changing business environments.
- An RAF offers opportunities for monitoring and articulating the operational risk appetite.

According to the above, there are various benefits to implementing an RAF, but there are also challenges faced by organisations when implementing an RAF, which will be discussed next.

The PwC and IACPM study also identified the following challenges experienced when implementing an RAF:

- Integrating risk appetite into the decision-making procedure of the organisation.
- Embedding the RAF into an organisation and identifying the best approach to allocate risk below the business-level into the wider organisational-level.
- Successfully assigning risk appetite throughout the organisation.
- Articulating risk appetite through metrics and limits.
- Instituting a RAS that is well-written and known by all stakeholders in an organisation.
- Supervisory requirements. Granular supervisory perspectives are seen as prescriptive, restricting the flexibility to implement an RAF successfully.
- Industry practices are distinctly different in order to operationalise elements of an RAF and to link it with other business processes, management and governance structures (PwC & IACPM, 2014:2, 8–9).

A study conducted by the IIF (2011:20-22) identifies the following challenges faced by financial institutions when implementing an RAF:

- “Effectively cascading the risk appetite statement through the operational levels of the organisation and embedding it into operational decision-making processes.
- How best to express risk appetite for different risk types, some of which can be quantified in generally accepted ways, and some of which cannot be easily quantified.
- Using the RAF as a dynamic tool for managing risk, rather than another way of setting limits or strengthening compliance.
- Using the RAF as a driver of strategy and business decisions.
- Achieving sufficient clarity around the concept of risk appetite and some of the terminology used (for example the difference between risk appetite and risk limits).
- How effectively to relate risk appetite to risk culture.
- How to make the best use of stress testing in the risk appetite process.
- How most effectively to aggregate risks from different business units and different risk types, for risk appetite purposes”.

Girling (2013:176) also stresses the challenge experienced by organisations to articulate risk appetite, especially operational risk appetite within the RAF. As seen in previous discussions, regulatory expectations have been established and indicate that risk appetite should be articulated, and operational risk needs to be part of that articulation (Girling, 2013:176).

From the discussion above, it can be concluded that there are various benefits for and challenges faced by financial institutions when implementing an RAF. If a bank wants to diagnose the quality of risk management, governance and culture within the bank, there is no better place to start than with the RAF (Deloitte, 2014b:4). The next discussion will focus on how an operational RAF can support a bank in the articulation of its risk appetite and what principles need to be incorporated by a bank effectively to implement an operational RAF.

3.3.2.1 Implementation of an operational risk appetite framework

According to Deloitte (2014b:13), once an RAF is appropriately integrated into the business function of an organisation, the framework will both support and be supported by its risk governance, risk management tools, risk infrastructure and risk culture. The linkages are explained in detail in Table 3.5.

Table 3.5: Linkages of the RAF with the risk governance, risk management tools, risk infrastructure and risk culture of an organisation

RAF linkages	How the RAF of an organisation provides support for:	How the RAF of an organisation is supported by:
Risk governance	"The RAF and language support risk governance by providing the board and senior management with the information and tools needed to understand and communicate the risks the organisation is and should be taking in line with its risk appetite and its business and risk strategy.	"The risk governance of an organisation is essential in clarifying lines of accountability and describing how staff should adhere to the RAF of the organisation. Implementation and running of the RAF depend crucially upon the full buy-in of the board and senior management and the tone at the top.
Risk management tools	The RAF provides information to support the efficient use and development of the more comprehensive risk management tools of the organisation."	The more extensive risk management tools of the organisation support the RAF. For example, running stress tests aligned with the targeted future risk profile of the organisation and its business and risk strategy supports the calibration of the risk appetite and limits of an organisation.

Risk infrastructure	The risk infrastructure of an organisation (including timely aggregation and reporting of risk data, related systems and processes, and employee skillset) must respond to and support its current and targeted future risk profile and its business and risk strategy. The RAF identifies comprehensive, firm-wide information necessary to shape the risk infrastructure of the organisation.	A robust and well-developed risk infrastructure responding to the current and targeted future risk profile of the organisation and its business and risk strategy is essential for its RAF. It is a prerequisite for effective monitoring, reporting and control of risk appetite, profile and capacity.
Risk culture	The RAF and language inform a strengthened risk culture grounded in the shared values and the common practice of understanding, openly communicating and controlling how each employee's activities contribute to the risk profile of the organisation and the successful implementation of its strategy."	The risk culture of an organisation is in its language and the style and quality of its internal communication. It is instrumental in the full operational embedding of the RAF, since only the risk culture of the organisation, helped by the tone at the top and appropriate compensation, can turn risk appetite statements and limits into a risk appetite language that is spoken and understood throughout the firm."

Source: Deloitte (2014b:13)

Based on the table above, the importance of an operational risk appetite framework (ORAF) to be supported by and support the risk governance, risk management tools, risk infrastructure and risk culture within the bank was highlighted. In order for an ORAF to achieve this type of support, it should be implemented effectively. The following table will discuss important principles for an organisation to implement an effective RAF, as stipulated by various authors and institutions.

Table 3.6: Principles for an effective RAF

	Principles of RAF's
The CRO Forum and CRO Council (2013:4)	• "The RAF should identify and quantify risk preferences for risks. • The RAF should be cascaded down to business segments to ensure that decisions are consistent with business objectives, tolerances and limits. • The diverse interests of parties relevant in achieving business objectives should be considered. • Risk appetites should be reassessed after significant events and reviewed by the board and senior management at least annually. • For risks that are not quantifiable, qualitative boundaries should be developed and assessed. • Staying within risk appetites should be realistically achievable. • Measurements should be used to provide evidence of risk appetite and strategy alignment at the organisational and business segment levels.

	• Establishing a comprehensive RAF is a complex process, and should be crafted via an iterative process, which requires patience, diligence, flexibility and collaboration."
SSG (2010:2–9)	• "The implementation of an RAF necessitates strong internal relationships within the organisation, for example, active cooperation between the board and senior management, between the senior management and business line leaders and between the Chief Risk Officer (CRO) and the board, other senior managers and business line leaders. A strong alliance between the CRO and the Chief Financial Officer (CFO) helps to increase the transparency and dissemination of the framework. • An RAF establishes an explicit, forward-looking view of the desired risk profile of an organisation in a variety of scenarios, and sets out a process for achieving that risk profile. • Risk appetite statements (RASs) should be operationalised with the right level and type of information, fostering strong internal relationships, and establishing risk limits with actionable input for risk/business managers. • The board should ensure that senior management establishes strong accountability structures to translate the RAF into clear incentives and constraints for business lines. • A common risk appetite language across the organisation, expressed through qualitative statements and appropriately selected risk metrics, facilitating the acceptance and effective monitoring of the RAF. • The RAF typically begins with a RAS that establishes boundaries for the desired business focus and articulates the desired approach of the board to a variety of businesses, risk areas and in some cases product types. • RAFs help organisations prepare for the unexpected. Organisations with a well-developed and mature RAF set an expectation for business line strategy reviews and conduct regular discussions about how to manage unexpected economic or market events. • Boards are accountable for the RAF and use it to frame strategic decisions. Strong support from the board is crucial for the successful implementation of the RAF throughout the organisation. • To drive an effective RAF, the board needs to employ an active, iterative process of review. The board shapes the RAS of the organisation, and work regularly with senior management to align the framework with the RAS. • The RAF is a useful tool to ensure that the strategy of each business line aligns with the desired risk profile of the organisation. • RAFs should not merely be a set of loss tolerances or limits; they should include a wide array of measures to monitor the risk profile of the organisation. • RAFs should combine multiple risk metrics that help in managing or mitigating downside risk in a thoughtful, deliberate way."
FSB (2013:4–5)	• "Evaluate opportunities for appropriate risk-taking and act as a defence against excessive risk-taking. • Be adaptable to changing business and market conditions so that, subject to approval by the board and senior management, opportunities that require an increase in the risk limit of a business activity could be met while remaining within the agreed risk appetite.

	• Be driven by both top-down board and senior management leadership and bottom-up involvement of management at all levels and embedded and understood across the financial institution. • Cover activities, operations and systems of the financial institution that fall within its risk landscape, but are outside its direct control, including subsidiaries and third-party outsourced suppliers. • Establish a process for communicating the RAF across and within the financial institutions as well as sharing non-confidential information to external stakeholders (for example shareholders, depositors and fixed-income investors). • Facilitate embedding risk appetite into the risk culture of the financial institution. • Allow the risk appetite statement to be used as a tool to promote robust discussions on risk, and as a basis upon which the board, risk management and internal audit functions can effectively and credibly debate and challenge management recommendations and decisions."
Deloitte (2014a:1; 2014b:14)	• "A means to engage the board and senior management in improving risk governance and discussions of risk from a strategic point of view. • A foundation for communication among internal and external stakeholders, by using a common language, which promotes a shared understanding of terminology and enhances risk culture. • An understanding of all material risks taken by the organisation, both at the business unit level and in aggregate. • Ability to measure, adjust and monitor the actual risk positions against expressed risk appetite and facilitate communication to key stakeholders. • A clear articulation of the business activities an organisation is willing to engage in, and the levels of risk it is willing to assume. • A framework for formulating strategic and tactical business decisions. • The RAF needs to cover financial and non-financial risks. • The risk appetite statement of the board needs to be cascaded down the organisation and needs to be translated into further risk statements around the risk drivers in order to relate the overall appetite to the day jobs of people lower down the organisation. • The chief executive officer (CEO), CRO and CFO need to be risk champions of risk appetite. • Boards need to be able to give examples of decisions that have been influenced by risk appetite, and senior management should be able to explain how and why they have gone about trying to embed risk appetite. • Risk appetite can be used within the reward and remuneration plan of an organisation. Employees will be incentivised to help deliver a healthy risk appetite culture and to remain within agreed risk appetite limits. • The RAF should be dynamic and underpin proactive ways of managing risk and setting and adjusting the business and risk strategy of the organisation and its articulated risk appetite. • The RAF should be straightforward to marshal compelling evidence of the progression from strategy and objective setting to the articulation and cascading

	down of risk appetite, the monitoring and reporting against appetite and control and control steps, which lead back to the setting of strategy and objectives."
PwC and IACPM (2014:2, 6–7, 14, 21–22)	• "RAFs create a unifying platform to facilitate a common understanding of different risk types across the organisation. • RAFs strengthen risk governance by integrating and leveraging separate risk management elements in a holistic manner. • The RAF adds both risks and returns considerations to strategy formulation and business decision-making. • The RAF enables all relevant stakeholders to evaluate their decisions. • The RAF needs to be aligned with the business plan, strategy development, capital planning and compensation schemes. The RAF should be as broad as possible, with risk appetite considerations woven into all relevant aspects of the firm. These broad linkages will assist in embedding the RAF into the organisation at all levels, improve risk culture, sustain the enterprise over the long term, and strengthen institutional resilience in times of crisis. • The RAF needs to be integrated and coordinated across various departments relevant to the RAF, for example with business line management, strategy and business planning departments. • The successful implementation of the RAF is enabled by a strong risk culture, effective risk policies, appropriate analytics and reliable data. Firms need to continue making investments to enhance both the analytics and data required for calibrating risk appetite metrics for different organisational and risk dimensions."
IIF (2012:55, 77–78)	• "Strong risk culture is a prerequisite to eventually putting in place an effective RAF. The culture benefit is to align all levels of the organisation to approach decision-making with the RAF in mind. • An RAF provides a framework within which conventional controls can operate and can promote understanding and acceptance of risk policies, limits and risk metrics. • The risk management function should own the overall RAF, serve in an advisory capacity and lead the interface with the board on risk appetite. • Communication is a crucial enabler, both in the development of an effective RAF and in its practical operation. The dialogue needs to encompass the development and evolution of the framework itself, as well as the risks that are being taken throughout the business and the extent to which these risks (individually and collectively) conform to the overall risk appetite. • Active collaboration between the risk management, finance and strategy functions is fundamental when designing an RAF and is equally essential in the day-to-day operation of an RAF. • Scenario testing is also an essential component of an RAF. Scenario testing is at the heart of setting risk appetite appropriately. As indicated in Chapter 2 (see 2.6.1.1), scenario analysis is the analysis of potential risk exposures, which are identified through the use of scenarios by critical employees in a bank. • The board should set the framework for risk appetite and put into place mechanisms to ensure that decision-making will be consistently and transparently be guided by it. • Effective RAFs involve an iterative approach, with ongoing discussions on risks involving senior management and the business, and must be rooted in a strong risk culture. Engagement and challenges by the board are vital processes to achieve the

	right balance between rigidity and flexibility in the RAF. This is necessary if the framework is to be both workable and a meaningful source of discipline. • Senior management should provide visible support and own the development of the RAF. • The risk management function needs to be actively involved at all levels of the development of the RAF and its operation. It is also vital that the risk management function also develop supporting risk frameworks, policies and reporting capabilities that enable business leaders to own and enhance their RAFs. • Supervisors are encouraged to take a broad perspective when forming views regarding the commitment to and progress in the implementation of the RAFs of the firm."
PwC and Strategy (2009:10)	• "An RAF at the corporate level should develop a comprehensive set of KPIs and high-level tolerance for all risk categories. • An RAF at the business unit and product level should develop risk tolerances for all relevant risk categories. • An RAF should ensure that all data for defined KPIs is readily available as needed. • An RAF should include a high-level corporate risk appetite and tolerance dashboard for senior management and the board, as well as individual dashboards for major business units with detailed appendices, covering all relevant risk categories. • An RAF should define monitoring responsibilities and frequencies within business units and the risk management function. • Risk appetite and tolerance adherence need to be embedded consistently in all risk-related policies, guidelines and frameworks. • An RAF should ensure that the risk appetite statement is aligned with the overall corporate risk philosophy and culture. • An RAF should define clear responsibilities for setting, approving and reviewing risk appetite and tolerances. • An RAF should establish and communicate escalation mechanisms and consequences for breaches of limits and tolerances. • An RAF should put in place good communication, understanding and agreement across all organisational levels."
Young (2010,182–183)	• "Assist strategic planning by aligning strategic objectives and operational activities. • Ensure a balanced approach between being risk-seeking and risk-averse. • Enhance the view of risk expenditure, which will ensure that the cost of risk does not exceed the benefits. • Ensure sound decision-making by top management. • Enhance the corporate governance of the organisation. • Ensure the involvement of all role players by providing risk information and making sound decisions. • Ensure realistic premiums for third party insurance for loss incidents. • Enhance the improved reputation of the organisation. • Enhance a culture of risk awareness throughout the organisation."

Based on the discussions and the table above, the following principles of an ORAF for a bank can be determined:

- An ORAF should define clear responsibilities for setting, approving and reviewing operational risk appetite and tolerances.
- An ORAF should be driven by both top-down board and senior management leadership, and bottom-up involvement of management at all business levels and embedded and understood across the bank.
- The board of a bank needs to be accountable for the ORAF and use it to frame strategic decisions. The board should support the ORAF for it to be successfully implemented throughout the bank.
- Senior management should provide visible support and own the development of the ORAF.
- A common operational risk appetite language needs to be established across the bank, expressed through qualitative statements and appropriately selected risk metrics. It will then facilitate the acceptance and effective monitoring of the ORAF. By using a common operational risk appetite language, it will assist a bank to promote a shared understanding of terminology and will enhance the risk culture in a bank.
- The ORAF should ensure that each business line strategy aligns with the desired operational risk profile of the bank. An ORAF needs to establish an explicit, forward-looking view of the desired operational risk profile of a bank in a variety of scenarios and needs to set out a process for achieving that profile.
- An ORAF needs to assist in the facilitation of embedding operational risk appetite into the risk culture of the bank.
- An ORAF needs to begin with an ORAS, which establishes boundaries for the desired business focus of a bank and articulates the desired approach of the board to a variety of business and operational risk areas in a bank. The board needs to determine the ORAS of the bank.

- An ORAF needs to evaluate opportunities for appropriate risk-taking and act as a defence against excessive risk-taking by a bank. It needs to consider both financial and non-financial operational risks.
- An ORAF needs to assist in the formulation of strategic and tactical business decisions to achieve business objectives in a bank.
- An ORAF needs to be aligned with the risk policies and governance processes of a bank. Operational risk appetite and tolerance adherences need to be consistently embedded in all risk-related policies, guidelines and frameworks.
- An ORAF needs to be communicated throughout the bank. A process for communicating the ORAF across the bank needs to be established. ORAFs create a unifying platform to facilitate a common understanding of different operational risk types across the bank.
- An ORAF should be dynamic and underpin proactive ways of managing operational risk and setting and adjusting the articulated operational risk appetite of the bank.
- An ORAF should be straightforward in indicating the progression from strategy and objective setting to the articulation and cascading down of operational risk appetite, as well as the monitoring and reporting against operational risk appetite and control.
- An ORAF should establish and communicate escalation mechanisms and consequences for breaches of operational risk limits and tolerances.
- An ORAF should enhance the view of the risk expenditure on operational risks, which will ensure that the cost of risk does not exceed the benefits.
- An ORAF should assist in establishing realistic operational risk appetites, which in return can ensure that realistic premiums are determined for third party insurance for loss incidents.

To conclude, a bank needs to consider seriously the adoption of the principles for an effective ORAF identified above. The board of a bank needs to establish the institution-

wide ORAF and approve the ORAS, which is developed in collaboration with senior management (the CEO, CRO and CFO) (FSB, 2013:7). Senior management needs to interpret those expectations of the board into targets and constraints for business lines and legal entities to follow (FSB, 2013:7). According to the FSB (2013:7), the power of the relationships between the board, senior management, internal audit and business lines plays an instrumental role in the effectiveness of the ORAF.

One of the challenges identified in the discussion above is the challenge faced by banks to cascade the Risk Appetite Statement (RAS) effectively through the operational levels of the organisation, and embed it into operational decision-making processes. It is crucial for an organisation to establish a well-structured risk appetite statement at the board, executive and operational levels (Rittenberg & Martens, 2012:23). The next section will discuss the principles required by a bank to implement an Operational Risk Appetite Statement (ORAS) effectively.

3.3.3 The operational risk appetite statement

According to the SSG (2010:5), the RAS is essentially a risk philosophy or a mission statement for risk, which is driven by the board, and implemented and supported by senior management. When issued by the board, a RAS provides senior management with both guidance and constraints as they pursue the strategy of the organisation (SSG, 2010:5). The FSB (2013:5), SSG (2010:5) and Goldstein and McElligott (2014:13) state that a useful RAS should be relatively simple, understandable, easily communicated and needs to resonate with multiple stakeholders. It usually is unhelpful if a RAS is very long or requires in-depth specialist expertise in order to comprehend the concepts contained within the statement (Goldstein & McElligott, 2014:13).

RIMS (2012:9) on the other hand, explains that a RAS needs to provide a standard against which the risk profile of the organisation is reported, managed and monitored by the board, finance and risk assurance, audit and risk committees. A RAS expresses the risk-taking approach of the organisation to its internal and external stakeholders. It also paints a portfolio view of the willingness of the organisation to bear and pursue risk for an expected return (RIMS, 2012:9). A RAS furthermore describes the level of risk that is both desirable and undesirable (Goldstein & McElligott, 2014:14). It represents a collection of,

not only the risk types related to the business portfolio (qualitative statements) but also its overall risk appetite (quantitative statements) (RIMS, 2012:9).

The European Central Bank (2016:18) concurs and indicates that in order to roll out the business plan and achieve strategic objectives; a RAS should outline all types and levels of risks that the bank is willing to assume within its risk capacity. Therefore, the RAS should govern the annual limit setting, taking into consideration financial volatility and economic cycles, to ensure that there is sufficient capacity for risk appetite thresholds if a limit is breached and that the thresholds are in line with the overall risk appetite of the bank (European Central Bank, 2016:18). According to Goldstein and McElligott (2014:14), the RAS is not a list of risk limits, but instead, it is supported by the risk limits. The RAS should facilitate corrective steps to remain within the overall risk appetite. The RAS must also be definitive and consistent enough to avoid moving away from the business strategy (European Central Bank, 2016:18). The RAS is expected to reflect changes in the internal and external environment and should be a dynamic and forward-looking document (Goldstein & McElligott, 2014:14).

The practice of monitoring adherence to the ORAS and defining risk appetite can enhance informed decisions about capital allocation and confirm that strategic business decisions are made with a thorough understanding of the risks and the capacity to manage those risks (PwC, 2014:4). A well-defined and communicated ORAS at the top can ensure that the board and senior management have aligned attitudes towards operational risk and that the level of operational risk an organisation is willing to accept can be clearly communicated to internal and external stakeholders (e.g. regulators, investors and rating agencies) (PwC, 2014:4). It is becoming crucial for a bank to define its ORAS in a common risk language, which can be understood and communicated by and to all stakeholders involved. The table below indicates different definitions for a RAS from various authors and institutions.

Table 3.7: Various definitions for a risk appetite statement

Author or institution	Risk appetite statement definition
Towers Watson	A RAS "should be taken as the combination of risk strategy, tolerances and preferences, bringing together qualitative and quantitative enterprise perspectives on risk as both opportunity and threat" (Towers Watson, 2013:7)
IOR	An ORAS can consist of qualitative and quantitative operational risk appetite statements. "Qualitative expressions can emphasise the relationship between risk and business management, as well as describing the attitudes and behaviours of the organisation as a whole, in other words, its risk culture. Quantitative expressions involve hard data, usually having roots in business management information, which could be any combination of KPIs, KRIs or KCIs (key control indicators)" (IOR, 2009:6).
FSB	A RAS is an "articulation in written form of the aggregate level and types of risk that a financial institution is willing to accept, or to avoid, in order to achieve business objectives. It includes qualitative statements as well as quantitative measures expressed relative to earnings, capital, risk measures, liquidity and other relevant measures as appropriate. It should also address difficult to quantify risks such as reputation and conduct risk, as well as money laundering and unethical practices" (FSB, 2013:2).
The CRO Forum and CRO Council (North America)	A RAS reflects "the combination of risk acknowledgement, including preferences for and unacceptability of specific risks, and organisation-wide tolerances for those risks" (CRO forum & CRO Council, 2013:5).
Deloitte	A RAS is the "articulation of risk appetite in written form" (Deloitte, 2014b:7).
PwC	A RAS provides "parameters for risk consideration and intersect with strategic objectives and corporate value statements" (PwC, 2011:10).
Protiviti	A RAS "explicitly describes the boundaries within which management is expected to operate within the organisation when executing the business strategy" (Protiviti, 2012:18).
RIMS	A RAS "addresses aspects relating to the financial tolerances of the organisation, which are measured in quantitative statements, as well as aspects relating to the values and culture of the organisation, which are represented in qualitative terms" (RIMS, 2016:6).
COSO	A RAS "effectively sets the tone for risk management. It assists in expressing how much risk is acceptable and communicates management's appetite for risk" (COSO, 2012:6).
Govindaranjan	A RAS "provide strong boundaries within which management executes business strategies in line with the risk appetite of the board" (Govindaranjan, 2011:3).
SSG	A RAS "establishes boundaries for the desired business focus and articulates the desired approach to a variety of businesses, risk areas, and, in some cases, product types of the board" (SSG, 2010:5)

Based on the definitions above, it is clear that an ORAS should indicate the types of operational risks a bank is willing to accept or avoid, in order to achieve business objectives. It should also consist of qualitative and quantitative operational risk appetite measures. For this study, the study will highlight the qualitative and quantitative measures needed for the ORAS of a bank by considering general RAS and ORAS. According to RIMS (2012:9), the quantitative RAS should address:

- "the maximum tolerance for market, credit and operational losses;
- the maintenance of a minimum credit rating level;
- the minimum economic and regulatory surpluses;
- the maximum earnings volatility; and
- the minimum excess liquidity resources to meet peak stressed liquidity requirements, without the need to liquidate assets or raise capital."

The qualitative RAS should address:

- "regulatory risk;
- reputational risk;
- business mandate;
- operational risks in the execution of business plans; and
- risk-related decision-making, especially about new business opportunities" (RIMS 2012:9).

As discussed above, a RAS will normally include qualitative factors such as operational risk tolerance levels and minimum regulatory compliance standards; and quantitative elements, for example, exposure concentration and cash flow limits, a target debt rating and minimum leverage ratios (Wyman, 2007:4). It should also give distinction to 'acceptable' and 'unacceptable' risks (Wyman, 2007:4). The acceptability of risks is defined by the business strategy or objectives and stakeholder expectations. The unacceptable risks are those risks that do not contribute to the realisation of the strategic vision and objectives (Wyman, 2007:4).

The FSB (2013:5) also indicates that a RAS should classify quantitative measures of loss or adverse outcomes into aggregated and disaggregated consequences. According to the FSB (2013:5), these "quantitative measures may be expressed in terms of earnings,

capital, liquidity-at-risk, or other appropriate metrics (e.g. growth, volatility). Also, qualitative statements should complement quantitative measures; set the overall tone for the approach of the financial institution to risk-taking, articulate the motivations for taking on or avoiding certain types of risks, products, country or regional exposures, or other categories" (FSB, 2013:5).

According to the IOR (2009:6), qualitative ORAS can include communications from the CEO and board (aimed at internal and external audiences), business strategy and policies. Examples of qualitative ORAS can be the following:

- "Recognising that certain operational risks, however unwelcome, are unavoidable (e.g. terrorism, natural disasters, consequences of an economic downturn). It is therefore accepted that a certain level of such risks has to be tolerated to avoid stifling or limiting business operations.
- It is sensible to accept operational risks where the cost of mitigation/avoidance exceeds the expected loss, provided the residual risk is not too high.
- Operational risk will be accepted when the estimated losses are within prescribed tolerance levels.
- Unacceptable behaviours might include, knowingly breaking the law, knowingly breaching regulatory requirements and organisational policy, damaging the environment, disrupting service to customers.
- Unacceptable operational risks could include operating within specific countries or selling particular products.
- As difficult as it is to define damage to the reputation of an organisation, it can be useful to use qualitative measures to describe events that may lead to unacceptable damage to reputation or loss of trust with stakeholders."

According to the IOR (2009:6), quantitative ORAS should include:

- "the amount of economic and regulatory capital allocated to operational risk;
- delegated limits of authority beyond which managers have to escalate for approval;

- performance levels, for example, no more than a certain percentage of a critical business system is unavailable for more than one day in any one year;
- each component of the ORAF:
    - Losses, based on budgeting, aggregated annual amount by business area or loss type and sensitivity, for example, an adverse trend of a certain percentage may be acceptable, tolerable or unacceptable. It is essential that minimum reporting thresholds imply single loss limits, but there may also be aggregate limits as in the case of an annual budget. The aim is to cover both high volume or low value, and low volume or high-value types of events. Reporting and escalation thresholds imply explicit expressions of appetite, for example below the threshold is acceptable, above that level is tolerable or unacceptable.
    - Risk or control assessment. By establishing boundaries on a matrix of likelihood and impact to distinguish acceptable or tolerable or unacceptable levels of residual risk.
    - KRIs, where thresholds would be set in units relevant to the KRI metrics, for example, the number, financial value, percentage and variance, linked to measurements."

From the above discussion, it is evident that a qualitative ORAS needs to include acceptable and unacceptable risk types (risks that are not easily measured), and indicators for risk monitoring. The quantitative ORAS needs to include risk limits, targets and tolerances, as well as risk measures (KRIs and risk assessments). It is also crucial for a bank to articulate its ORAS in a top-down and bottom-up approach, as well as across various business lines, which could lead to ownership of risk appetite throughout the bank (IIF, 2013:8).

According to Deloitte (2014a:14), if a RAS is placed at the centre of the RAF, the business decision-making process and the governance framework of an organisation, it can add tremendous value. The RAS will be a central driver in governance and risk discussions, a vital element of capital allocation and strategic planning, a reassurance to regulators, rating agencies, and shareholders and an indicator for how much risk the organisation is

willing to take (Deloitte, 2014a:14). The Risk and Insurance Management Society (RIMS) (2016:10) agrees, and states that the benefits of a RAS:

- can assist an organisation to make better strategic and tactical decisions by emphasising the risk perspective in decision-making and providing more significant information about risk-reward balances; and
- can foster risk transparency by establishing logical thinking, processes and actions throughout the organisation.

A study conducted by Marsh et al. (2009:21–23), indicates that the benefits of implementing a RAS will lead to the following:

- improvement in board risk oversight and risk governance;
- communication of expectations for risk-taking to managers;
- communication of risk to the board;
- management consensus around risk;
- improvement in the setting of limits for risk/reward trade-offs;
- an increase in accountability for management decision-making;
- input into strategic decision-making and strategy development;
- established boundaries for risk-taking; and
- informed risk financing and insurance decisions.

According to Govindaranjan (2011:8–9), the following are benefits for having a robust RAS:

- A RAS serves as a clear, concrete, overarching and proactive articulation of the views of the board on risks that they are willing to tolerate in the pursuit of strategic objectives.
- A RAS serves as a robust instrument for ensuring that stakeholder's interest is adequately reflected in board decision-making. It enables the board to explain the preference and hierarchy for risks that may influence different stakeholders.
- A RAS can be used as a benchmark for translating the overall strategy practically into measurable and achievable objectives while considering the risk commitments. It sets the context for incongruent policies, tolerances and limits within various risk categories, business units or lines.

- A RAS assists the organisation in setting an overall risk appetite, which allows the board to articulate the nature and quantity of risks that it allows its staff to take on for the organisation.
- A RAS sets the tone when making risk decisions, and links to risk culture.
- A RAS creates an instrument to ensure that risk management practices are adequately robust for the intricacy and scale of the activities of the organisation.
- A RAS provides clarity regarding short- and long-term risk trajectories. This allows stakeholders to evaluate performance and remuneration objectively and systematically.
- A RAS assists the organisation to assess the suitability of capital and winding-down plans within stress tests and reverse stress tests required by regulators. Regulators will clearly understand the risk appetite of the organisation based on the control effectiveness, mainly when they are evaluating the stress testing and capital planning of the organisation regarding the risks that the board feels are within their appetite.

RIMS (2012:11) alternatively indicates that a RAS should ideally provide:

- Measures which disclose when deviations from anticipated outcomes are reached or when the risk tolerance limits for each risk type are breached. Awareness and monitoring of established thresholds would assist an organisation to detect changes in risks and avoid unforeseen consequences.
- Risk targets that are the perfect goal for risk-taking, based on the objectives, risk appetite and measures of the organisation for each risk type.
- Risk tolerance or a range where risks would be allowed to deviate around the defined risk target. This ensures that defined risk tolerances are in line with the risk capacity of the organisation. The board and senior management may establish high-risk appetites, but the organisation may not have enough capacity to handle the potential volatility or effect of risk over the extent of its business operations.

From the discussion above, it is evident that the most critical benefit for implementing an ORAS is to assist a bank in indicating how much operational risk it is willing to tolerate in

order to achieve business objectives. Another significant benefit of an ORAS is that it will enable a bank to make business decisions and foster risk transparency, as well as improved board risk oversight and risk governance. It is the responsibility of the board to express the risk appetite of the organisation and understand how it relates to the strategy of the organisation (Goldstein & McElligott, 2014:13).

Even though there are numerous benefits for a bank to implement an ORAS, there are also challenges when implementing an ORAS. According to Jill Douglas, Head of Risk, Charterhouse Risk Management, “The risk appetite statement is generally considered the difficult part of any enterprise risk management implementation” (IRM, 2011:9). A bank should ensure that the RAS is stable across time and is used as a driver of the strategy of the bank, rather than the strategy dictating the risk appetite (European Central Bank, 2016:18). The section below will discuss the different challenges faced by organisations concerning RASs.

Govindaranjan (2011:10–11) identifies the following challenges faced by organisations when articulating the RAS:

- Boards are delegating the creation of a RAS to senior management or the risk management function. This can lead to stakeholder objectives not being taken into consideration, or broad strategic perspectives on risk appetite are overlooked.
- Many organisations are struggling to create a realistic, yet high-level RAS due to the absence of formalised terminology and regulatory guidance. This could lead to poorly constructed and poorly used RAS, which cannot be turned into practical policies, limits or processes within the RAF.
- Certain organisations are focusing their RAS on a financial risk-return trade-off for familiar risks, for example, market or credit risk positions rather than considering the acknowledgement or articulation of trade-offs amongst stakeholder demands.
- Organisations are finding it challenging to create a wide-ranging, all-encompassing, yet realistic statement that is a counterpart of the business strategy. Often the RAS seems to focus exclusively on “what tools we will use to

manage risk" or "how we will do business", rather than "what are the risks we are or are not prepared to take?".

- Sometimes, boards are hesitant to formalise their risk appetite, as they may not want the market to view them as a risk-taking or unsafe organisation if they do anticipate to take on risks.
- The RAS of certain organisations are not sophisticated enough to match the strategic plans the organisation envisions. The organisation may have ignored important risk types, for example strategic, reputational and regulatory risk.
- Increased scrutiny has been given to areas such as shareholder returns or capital allocation when creating a RAS. Only risks that may cause share price erosion to get attention, rather than all the risk types, for example, operational risk, or what risks the organisation is willing to take.
- Organisations also have found it challenging to link their risk appetite to their existing risk management processes and mechanisms.
- Organisations are also experiencing challenges in communicating the RAS, establishing a specific risk appetite and managing the organisation within that risk appetite level.

A study conducted by Marsh et al. (2009:21–23) identified the following challenges faced when developing and implementing a RAS:

- Demonstrating the value of having a RAS.
- Insufficient in-house expertise to define risk appetite.
- Achieving management understanding of the concept of risk appetite.
- Gaining management interest in defining risk appetite.
- Inability to integrate risk appetite within business activities.
- Developing suitable quantitative risk measurements.
- Difficulty in measuring risk exposure to compare with risk appetite.
- Limited availability of relevant supporting data.

- Communication of the RAS to all employees of the organisation. The RAS tend to be confined to the board and senior management and is not cascaded down to other stakeholder groups, including employees.

From the discussion above, it can be seen that there are various challenges faced by organisations when implementing a RAS. A study conducted by PwC and IACPM (2014:17), indicates that there is a broad agreement on the principle of developing a RAS to articulate the risk appetite of an organisation, but in practice, the content of a RAS can be widely diverse concerning:

- risk types included in the RAS;
- balancing quantitative and qualitative components; and
- suitable criteria that define the risk appetite at both the business-level and other business operations.

This study aims to determine guiding principles to assist a bank to implement an ORAS effectively and to narrow down the ORAS into qualitative and quantitative components, appropriate operational risk types and metrics. According to Goldstein and McElligott (2014:14), a "good practice is to establish a RAS consisting of an overall risk appetite supported by a number of narrower risk limits, which are contextualised by the nature of the risk category to which they relate and that practical risk tolerances are then built around these limits". Table 3.8 will highlight important principles from various authors and institutions, for an organisation to implement an effective RAS.

Table 3.8: Principles for an effective RAS

	Principles of RASs
COSO (2012:6)	• "Directly links to the objectives of the organisation. • The ORAS is stated precisely clearly enough that it can be communicated throughout the organisation, effectively monitored and adjusted over time. • Helps with setting acceptable tolerances for risk, thereby identifying the parameters of acceptable risks. • Facilitates alignment of people, processes and infrastructure in pursuing organisational objectives within acceptable ranges of risk. • Facilitates monitoring of the competitive environment and considers shareholders' views in identifying the need to reassess or fully communicate the risk appetite. • Recognises that risk is time-based and relates to the period of the objectives being pursued.

	• Recognises that the organisation has a portfolio of projects and objectives, as well as a portfolio of risks to manage, implying that risk appetite has meaning at the individual and the portfolio level."
RIMS (2016:9)	• "Acknowledgement of the willingness and capacity to take on risk by an organisation. • Documented clearly and concisely. • Communicated at all appropriate levels of the organisation. • A representative of critical aspects of the business. • Reflective of the business strategy, organisational objectives, business plans and stakeholder expectations. • Inclusive of tolerance for quantifiable loss. • Understood and backed by the board. • Periodically reviewed and revised, based on evolving industry trends and market conditions."
FSB (2013:6)	• "Include essential background information and assumptions that informed the strategic and business plans of the financial institution at the time they were approved. • Be linked to the short- and long-term strategic, capital and financial plans, as well as compensation programs at the institution. • Establish the amount of risk the financial institution is prepared to accept in pursuit of its strategic objectives and business plan, considering the interests of its customers (for example depositors and policyholders) and the fiduciary duty to shareholders, as well as capital and other regulatory requirements. • Determine for each material risk and overall, the maximum level of risk that the financial institution is willing to operate within, based on its overall risk appetite, risk capacity and risk profile. • Include quantitative measures that can be translated into risk limits applicable to business lines and legal entities as relevant, and at the group level, which in turn can be aggregated and disaggregated to enable measurement of the risk profile against risk appetite and risk capacity. • Include qualitative statements that articulate clearly the motivations for taking on or avoiding certain types of risk, including for reputational and other conduct risks across retail and wholesale markets, and establish some form of boundaries or indicators (for example non-quantitative measures) to enable monitoring these risks. • Ensure that the strategy and risk limits of each business line and legal entity, as relevant, align with the institution-wide risk appetite statement as appropriate. • Be forward-looking, and where applicable, subject to scenario testing to ensure that the financial institution understands what events might push the financial institution outside its risk appetite and risk capacity."
CRO Forum and CRO Council (2013:8)	• "Comprehensive: it should have the appropriate breadth, reflecting coverage of the risk landscape, and depth within the organisational structure. • Concrete and practical: all material risks should be identified and quantified via risk tolerances. For risks that are inappropriate to quantify, qualitative boundaries should be established.

	• Consistent and coherent: tolerance throughout the organisation need to form a balanced system of appropriate boundaries, avoiding excessive allowance in some areas and excessive restrictions in others, and should align with the business model of the organisation."
PwC (2014:7)	• "The ORAS utilises both quantitative and qualitative components. This helps to ensure that the shortfalls of each (in isolation) are mitigated, at least to some extent. • Provide a clear linkage to the strategy of the organisation. As with market and credit risk, senior management must be able to tell the story of where they are headed with operational risk and what is expected of each business unit and individual in the organisation. • Specific indicators within the operational risk management tools need to support high-level ORASs. The linkage between business level indicators (if they are appropriate), can help enable the risk appetite to be understood by the organisation. • An ORAS should be easily embedded in the day-to-day operations of the organisation. There must be a clear linkage from the ORAS to key risk indicators. The ORAS should also be linked with (or be part of it) the ORAF. • The ORAS needs to be monitored by senior management on a regular basis. Besides, unlike market and credit risks, there is not a desire for senior management to 'meet' or 'reach' the operational risk limits. They are merely maximum limits that should not be exceeded. For market risk, some organisations will expect traders to operate at levels 'close' to limits, because they should be taking the risk for profit-making reasons."
Goldstein and McElligott (2014:13)	• "Risk capacities: The RAS should indicate the current limits to its risk appetite. • Desirable risks: The RAS needs to indicate which risks the organisation actively wants to take on and how the organisation will optimise these risks in order to generate a return. • Undesirable risks: The RAS should also indicate which risks it wants to avoid. • Interlinkages: The RAS needs to consider that certain identified risks can also influence other risks. • Risk timelines: The RAS should consider the risks that may materialise over short-, medium- and longer-term horizons. • The RAS needs to indicate what type of information, controls and systems the board, executive management, line management and employees require in assessing the nature of risks and how they relate to ongoing strategic objectives. • Incentive and compensation: The RAS needs to describe the strategic choices and associated risks linked to incentives and compensation. • Escalation and mitigation: The RAS needs to indicate how the risks that are outside of the risk appetite are identified, communicated and mitigated. • Brevity and clarity: The RAS needs to communicate the risk appetite concisely in an understandable format and language."
Deloitte (2014a:4–5)	• "The RAS should be closely aligned with the business strategy and objectives (mission, vision, risk philosophy). If the strategy changes, its risk appetite should also be revised. • Operating plans should be established within the defined risk appetite.

	• The assumptions underlying the operating plans and related scenario planning, as well as the types of risk that the organisation is willing to tolerate, should be specified. • The organisation should engage with the stakeholders in the organisation, regarding the strategic planning, risk management, finance departments and business units when developing a RAS. • The board needs to play a critical role in the development, review and approval of a RAS. • The RAS should include the organisational risk capacity, for example, quantitative constraints (available capital, liquidity or borrowing capacity) and qualitative constraints (regulatory standing, risk management capability or reputation/brand capacity). Risk appetite should be less than the risk capacity and include a buffer, based upon the overall risk profile. • The RAS should be communicated to lower levels of the organisation (such as business units or legal entities) regarding specific limits. • Quantitative and qualitative measures must support the RAS. • The quantitative RAS should have thresholds and be measurable, and the qualitative RAS should be observable. • The RAS should articulate the desired balance between the critical risk objectives (for example target debt ratings, earnings volatility and capital adequacy) and profitability objectives (return-on-equity and risk-adjusted return-on-capital). • The RAS should cover a multiple dimension of risks.”

Based on the discussions and the table above, the following principles of an Operational Risk Appetite Statement (ORAS) for a bank can be determined.

- An ORAS should determine the amount of risk the bank is willing to accept in pursuit of its business plan and strategic objectives, considering the interests of its customers (for example policyholders and depositors) and the fiducial duty to shareholders, as well as capital and other regulatory requirements.
- An ORAS needs to determine the maximum level of operational risk that the bank is willing to operate within, based on its overall risk appetite, profile and capacity.
- The ORAS should be closely aligned with the business strategy and objectives (mission, vision, risk philosophy). If the strategy changes, its operational risk appetite should also be revised.
- An ORAS needs to be effortlessly embedded into the everyday operations of the bank. There must be a perfect linkage from the ORAS to key risk indicators.
- The ORAS should be linked with the ORAF of the bank.

- The ORAS needs to be communicated within all of the business units of the bank and relevant stakeholders (internal and external).
- The ORAS needs to utilise both quantitative and qualitative components.
    - The ORAS needs to comprise of quantitative measures that can be interpreted into risk limits related to business units, which in turn can be aggregated and disaggregated to assist with the assessment of the risk profile against risk appetite and risk capacity.
    - The ORAS needs to contain qualitative statements that articulate undoubtedly the incentives for taking on or avoiding certain types of operational risks.
    - An ORAS needs to include all the types of operational risks, which should be identified and quantified via risk tolerances. For operational risks that are unsuitable for quantifying, qualitative boundaries should be determined.
- An ORAS should be documented clearly and concisely.
- The ORAS should be periodically reviewed and revised based on evolving industry trends and market conditions.
- The ORAS should assist with setting acceptable tolerances for risk, thereby identifying the parameters of acceptable and unacceptable risks.
- An ORAS needs to be forward-looking and where applicable, subject to scenario testing, ensuring that the bank understands which events might lead the bank to go beyond its risk appetite and risk capacity.
- An ORAS should be approved and supported by the board.
- The ORAS needs to ensure that the strategy and risk limits of each business unit align with the overall ORAS of the bank.

The principles as mentioned above will assist a bank effectively to formulate an ORAS. However, it is also crucial for the board continuously to review the ORAS of the bank due to an ever-changing environment. According to the IRM (2011:9), there are five tests, which the board can apply when reviewing the ORAS of their organisation:

- “Do the senior managers making decisions understand the degree to which they (individually) are permitted to expose the organisation to the consequences of an event or situation? Any ORAS needs to be practical, guiding managers to make risk-intelligent decisions.
- Does senior management understand their aggregated and interlinked level of operational risk, so that they can determine whether it is acceptable or not?
- Do the board and senior management understand the aggregated and interlinked level of operational risk for the organisation as a whole?
- Are both the board and senior managers clear on the fact that risk appetite is not constant? It changes as the environment and business conditions change. Anything approved by the board must have some flexibility built-in.
- Are risk decisions made with full consideration of reward? The ORAF needs to help the board and senior management determine an appropriate level of risk for the organisation, given the potential for reward.”

In conclusion, it can be deduced that an ORAS can provide management with clarity on the type and quantity of operational risk that the bank is willing to accept, and give an enhanced view on the trade-offs between risk and return (PwC, 2014:4). Protiviti (2012) states that: “a risk appetite statement is not an ornament to hang on a wall. It is a reminder to management and the board of the original core risk strategy arising from the strategy-setting process”. This means that the ORAS should provide a link between the strategy and the daily operations of the bank, and guide more effective business decisions (PwC, 2014:4). According to Wyman (2012:5), the value of a RAS is more than just established standards. It is also a source of communication and can link the performance of the organisation and its business operations in a single statement. It also activates discussion about significant financial drivers and associated risks (Wyman, 2012:5). A high-level ORAS needs to provide the context for the ORAF, operational risk appetite policies and operational limits that may well be established and managed in isolation (PwC, 2014:4).

For the purpose of this study, it is crucial for a bank to consider the adoption of the above-mentioned identified principles in order to implement an effective ORAS.

3.4 CONCLUSION

This chapter provided an overview of the literature regarding operational risk appetite in the financial and banking industry. The chapter aimed to focus on the definition of operational risk appetite, operational risk appetite practices and the implementation of an ORAF and statement in a bank. The chapter also provided an overview of the various principles needed to formulate an ORAF and statement. All the concepts are essential for a bank effectively to articulate operational risk appetite throughout its activities to achieve business objectives.

Based on the relevant literature, the definition of operational risk appetite was derived as the amount of operational risk a bank is willing to accept or tolerate to achieve strategic objectives. Literature also suggests that there is an interconnected link between risk appetite, tolerance, capacity, profile, culture and limits. An appropriate ORAF should enable an organisation to determine its risk capacity, appetite, limits, profile and tolerance in all business activities to assist a bank in determining its overall operational risk appetite.

The literature review revealed that it is essential for a bank to implement an ORAF and ORAS throughout its business processes and activities. Due to the challenges faced by organisations in setting risk appetite, regulators are forming new expectations for risk appetite with the focus on RAFs and statements. The importance of implementing a board-approved operational risk appetite and framework is becoming a regulatory requirement. The board of a bank needs to establish an institution-wide ORAF and approve the ORAS.

From the literature in the chapter, the following conclusions can be made:

- It is crucial for a bank to define its operational risk appetite because it will enable a bank to identify the operational risks it wishes to accept and tolerate, achieve business objectives and express the operational risk appetite of the board and senior management, throughout the bank.
- The operational risk appetite and risk tolerance level of a bank should be interrelated. A bank ought to operate within its risk tolerance levels to ensure that

it remains within its operational risk appetite and, in turn, achieves business objectives.

- A bank needs to understand its risk capacity to enable the bank to determine its operational risk appetite. There is no benefit for a bank to determine its operational risk appetite unless there is the capacity to manage operational risk.
- It is essential for a bank to determine its risk limit by also considering the upper and lower operational risk appetite limits.
- A bank needs to understand its risk profile in order for the bank to determine its operational risk appetite.
- It is crucial for a bank to understand the link between risk appetite, capacity, profile, tolerance, culture and limits.
- The ORAF of a bank needs to be supported and support the risk governance, risk management tools, risk infrastructure and risk culture within the bank.
- A bank needs to implement an effective ORAF and ORAS. Various principles were identified in the literature to assist a bank to articulate an ORAF and ORAS throughout its business activities.
- The ORAS of a bank should provide clarity on the quantity and type of operational risks the bank is willing to accept.

To conclude, the literature review found that it is imperative for the board and senior management to determine the operational risk appetite of a bank and implement an ORAF in order to achieve strategic objectives. The literature suggests that there is a link between operational risk appetite and the strategy of a bank, based on its acceptable and unacceptable risk exposures. The operational risk appetite needs to be articulated throughout all the business units in a bank and is understood by all employees. The board and senior management should have a clear view of how much risk the bank is exposed to and how much risk it is willing to accept or have an appetite for.

The literature review of Chapter 3 verifies the purpose of this study, which was to confirm management principles for an ORAF in a bank. Chapters 2 and 3 provided the literature

review of the study, which will serve as the basis for the empirical part of this study. The next chapter will give a detailed overview of the research methodology to be followed.

CHAPTER 4: RESEARCH DESIGN AND METHODOLOGY

4.1 INTRODUCTION

In the previous chapters, the literature review was presented. This chapter deals with the research design for the study in order to provide a blueprint of how the study will be carried out in pursuit of achieving the objectives, which sequentially will answer the research questions. The research approach, methodology and strategy adopted to achieve the objectives of the study are also explained. The chapter also discusses the population for the study and sampling method used. Also, the type of data and the data collection techniques used in the study are described. This is followed by a discussion of the data analysis procedures used. Finally, the manner in which ethical issues were considered in this study is discussed. The chapter starts with a discussion of the research design.

4.2 RESEARCH DESIGN

Research design refers to a structure and framework used for the collection and analysis of data (Bryman et al., 2015:100). According to Creswell (2014:12), “research designs are types of inquiry within qualitative, quantitative and mixed method approaches that provide specific direction for procedures in research design”. Saunders et al. (2012:159), on the other hand, state that a research design is the general plan of how the research questions of the study will be answered, specifying the sources from which the study will collect data, how the data will be collected and analysed, as well as ethical considerations and limitations. It can be concluded that research design is a strategy for the collection, measurement and analysis of data, centred on the study’s research questions (Sekaran & Bougie, 2013:95).

According to Saunders et al. (2012:170), it is crucial for a researcher to understand the nature and the objective of the research design. Research design can be exploratory, descriptive or explanatory.

- **Exploratory research**

Exploratory research is carried out with the objective to examine the possibilities of undertaking a specific research study or probe a topic where little is known (Kumar,

2011:11). Exploratory research looks for patterns and ideas to develop a hypothesis, rather than to test a hypothesis (Collis & Hussey, 2014:4). According to Struwig and Stead (2013:6), the researcher develops and classifies ideas, formulates questions and hypotheses which can lead to a precise investigation later. Exploratory research is necessary when specific facts are well-known, but more information is required for developing a feasible theoretical framework (Sekaran & Bougie, 2013:96). Exploratory research frequently depends on secondary research (such as a review of literature), and qualitative approaches to data gathering, such as informal discussions or formal approaches, for example, case studies or interviews (Sekaran & Bougie, 2013:96).

- **Descriptive research**

Descriptive research is conducted to depict occurrences as they happen. It is used to acquire and find information on the characteristics of a specific subject or problem (Collis & Hussey, 2014:4). According to Kumar (2011:10), descriptive research "attempts to describe a situation, problem, phenomenon, service or programme systematically". By contrast with exploratory research where flexibility is the key, descriptive research is an endeavour to offer a precise and comprehensive description of an issue or situation (Struwig & Stead, 2013:6). Descriptive research can be quantitative, qualitative or mixed method in nature (Sekaran & Bougie, 2013:96).

- **Explanatory research**

Explanatory research is a study that establishes causal relationships between variables (Saunders et al., 2012:172). It endeavours to explain how and why there is a relationship between two features of a phenomenon or issue (Kumar, 2011:11). Explanatory research is a continuance of descriptive research because it goes past simply describing the characteristics of the problem, but analyses and explains how or why the phenomenon exists (Collis & Hussey, 2014:4). Explanatory research is usually associated with experimental research (Sekaran & Bougie, 2013:96).

The type of research that was followed for this study is descriptive research. The study aims to identify guiding principles for an operational risk appetite framework for a bank. For the purpose of this descriptive study, the research onion approach, suggested by

Saunders et al. (2012:160), was followed (refer to Figure 4.1). The research onion approach highlights the research design of the study.

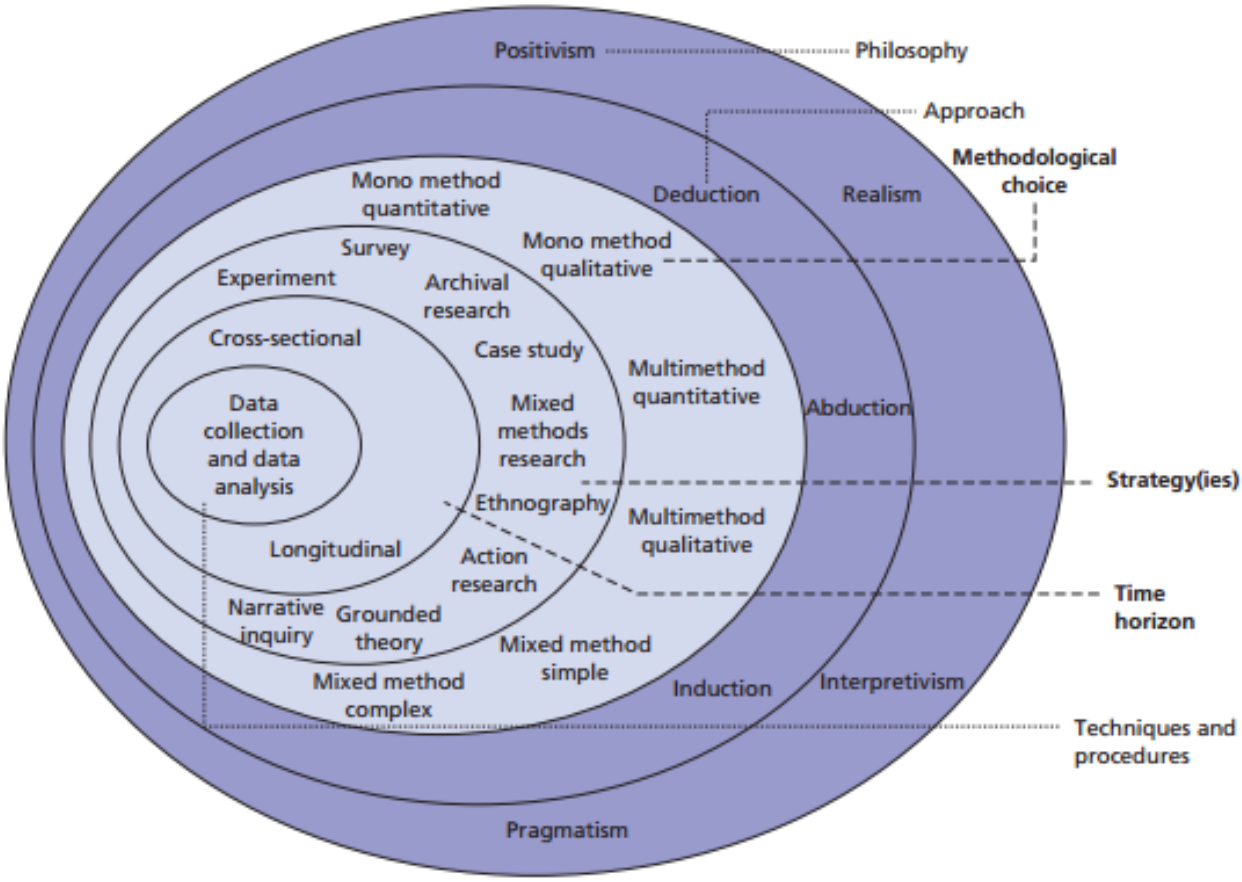


Figure 4.1: The research 'onion'
Source: Saunders et al. (2012:128)

The research onion illustrates the stages that must be covered when developing a research design. Each layer of the onion, in chronological order, describes in more detail the research philosophy, research approach, methodological choice, research strategy, time horizon, population and sample size, data collection and analysis techniques that are chosen for the study. These stages of the research design will be discussed further in the following sections.

4.2.1 Research philosophy

Research philosophy is seen as a basic set of beliefs that guide action, which is also known as paradigms (Creswell, 2014:35). Creswell states that there are four worldviews on research philosophy, namely postpositivism, constructivism (linked with interpretivism), transformatism and pragmatism. Strang (2015:22–25) explains that the commonly accepted philosophical positions are positivism, postpositivism, pragmatism and constructivism. Bryman et al. (2015:12), on the other hand, explains that a research philosophy "is concerned with the question of what is (or should be) regarded as adequate knowledge in a discipline". There are three primary positions namely positivism, interpretivism and realism (Bryman et al., 2015:12). Saunders et al. (2012:127) concur and explain that a research philosophy is the improvement and nature of knowledge.

Considering the first layer of the onion as proposed by Saunders et al. (2012:128), the philosophical positions or worldviews that may be adopted for this study are namely positivism, postpositivism, interpretivism, realism and pragmatism. These views will be considered to shape the study and give direction to which methodologies and approaches should be followed.

- **Positivism**

Positivism is the oldest and the most recognised research philosophy, which refers to the evidence- and theory-driven approach (Strang, 2015:22). Positivism is an approach that advocates applying natural science methods to study and understand social reality (Bryman et al., 2015:12). According to Strang (2015:23), "positivists apply the 'scientific method', develop a rigorous protocol, collect qualitative or mixed data and apply descriptive, as well as statistical techniques, to test a priori (theory-driven) hypothesis, formed by reviewing theories". In this philosophy, the world is regarded as being logical and methodical, depending on theories to explain most behaviours and processes. Positivistic researchers first consider a priori theory (facts and laws) and then identify a hypothesis to be tested (Strang, 2015:22). Positivism research is quantitative, which is highly structured with large samples and measurements, but can also be qualitative (Saunders et al., 2012:140). Pure positivism is seldom used, with the exception of highly controlled circumstances (such as behavioural experiments or process testing). Due to

various critiques against positivism, a revised positivist worldview emerged, called postpositivism (Strang, 2015:22). Fact-driven researchers frequently use postpositivism research, because the constraints imposed by positivist research are seen to limit the contributions to the literature severely (Strang, 2015:22). Postpositivism will be discussed next.

- **Postpositivism**

Postpositivism began from the realisation that it is problematic to have one 'factual truth' as a theory (in contrast to positivism) and because it is practically impossible to know what exists in a human brain schema (Phillips & Burbules, 2000). Postpositivism holds a deterministic philosophy, which realises that causes determine effects or outcomes (Creswell, 2014:36). Thus, the problems studied by postpositivists reveal the need to find and evaluate the causes that have an impact on outcomes, for example, experiments. It is also reductionistic because the intent is to reduce the ideas into smaller and discrete variables that are comprised of hypotheses and research questions (Creswell, 2014:36). According to Phillips and Burbules (2000:29), postpositivists see knowledge as conjectural (and antifoundational), which means the absolute truth can never be found. These conjectures are reinforced by the strongest (if possibly imperfect) warrants we can gather at the time and are continuously subject to reconsideration (Phillips & Burbules, 2000:30). Postpositive assumptions are more accurate for quantitative than qualitative research (Creswell, 2014:37).

- **Interpretivism**

Interpretivism refers to an alternative to the positivist paradigm. It assumes that any research approach needs to respect the difference between people and the objects of natural sciences. Therefore, this approach requires the social scientist to grasp the subjective meaning of the social action of a person (Bryman et al., 2015:14). According to Saunders and Tosey (2012/2013:58), this philosophy focuses on conducting research amongst individuals rather than objects, adopting a compassionate stance to understand an individual's social domain and their point of view. Interpretivism is usually qualitative research, which focuses on small samples and in-depth investigations (Saunders et al., 2012:140).

- **Realism**

According to Saunders and Tosey (2012/2013:58), like “positivism, realism is a philosophical position associated with scientific enquiry. Realism states that reality exists, independent of the mind and that what a researcher’s senses shows him or her to be the truth, although the researcher is influenced by worldviews and own experiences”. There are two types of realism. The first type is empirical or direct realism. Direct realism states that “what you see is what you get (what we experience through our senses, portrays the world accurately)” (Saunders et al., 2012:136). The second type is critical realism. Critical realism maintains that what we experience are your emotions and sensations, the images of things in everyday life, not the actual things (Saunders et al., 2012:136). The realism approach can be quantitative or qualitative, but the method chosen must fit the topic (Saunders et al., 2012:140).

- **Pragmatism**

Creswell (2014:39) explains that pragmatism arises out of actions, situations and consequences, rather than antecedent conditions (as is the case in postpositivism). Instead of focusing on methods, researchers emphasise the research problem and use all approaches available to understand the problem (Creswell, 2014:39). According to Saunders et al. (2012:130), pragmatists “recognise that there are many different ways of interpreting the world and undertaking research, that no single point of view can ever give the entire picture, and that there may be multiple realities”. Pragmatism can be seen as a philosophical underpinning for mixed method studies (quantitative and qualitative) (Creswell, 2014:40). This does not mean that pragmatists always use multiple methods. They instead use the method or methods that enable credible, well-founded, reliable and relevant data to be collected that support the research (Saunders et al., 2012:130).

This study focused on the postpositive paradigm, as the assumptions made in this paradigm is for quantitative research, which seeks to develop relevant, true statements that can assist in explaining the defined causal relationship of interest for the study. In quantitative studies, a researcher determines the relationship between different variables and pose this in terms of research questions or hypotheses (Creswell, 2014:47–48). This study poses the following research question: What are the principles needed to formulate

a realistic operational risk appetite framework for a bank? The next section discusses the research approach.

4.2.2 Research approach

The second layer of the research onion comprises the research approach. According to Collis and Hussey (2014:3), a research approach is used to determine whether the research reasoning moves from the general to the specific or vice versa. Saunders et al. (2012:143) explain that the extent to which a study is clear about the theory at the beginning of the research raises an important question about the reasoning of the study. It is crucial for a research study to consider what type of reasoning to adopt, namely deductive, inductive or abductive.

- **Deductive approach**

Deductive reasoning symbolises the popular beliefs with regards to the nature of the relationship between research and theory (Bryman & Bell, 2011:9). Deductive refers to testing a priori theories, concepts, constructs or instruments to replicate findings or to discover differences when the context changes (Strang, 2015:39). According to Collis and Hussey (2014:7), the deductive approach is where a conceptual and theoretical structure is developed and then tested by empirical observation, for example, where particular instances are deducted from general inferences. Sekaran and Bougie (2013:26), on the other hand, state that a deductive approach consists of the identification of a broad problem area, defining the problem statement, hypothesising, determining measures, data collection, data analysis and the interpretation of the results. Saunders et al. (2012:150) explain that with deduction, theory and hypothesis (or hypotheses) are developed, and a research strategy is designed to test or verify the hypothesis. A deductive approach is commonly used in quantitative research (Bryman & Bell, 2011:11).

- **Inductive approach**

Inductive refers to building theories, concepts, constructs, or instruments from the sample data (Strang, 2015:39). Inductive research is a study in which a theory is developed from the observation of empirical reality, for example, where general inferences are induced from particular instances, which is the opposite of the deductive method (Collis & Hussey,

2014:7). According to Sekaran and Bougie (2013:26), the inductive approach is a process where a specific phenomenon is observed to reach a general conclusion or create a framework. Saunders et al. (2012:150) explain that with an inductive approach, data is collected and a theory is developed as a result of the data analysis. An inductive approach is frequently used in qualitative research (Bryman & Bell, 2011:11).

- **Abductive approach**

An abductive approach is seen as a combination of a deductive and inductive approach (Saunders et al., 2012:147). According to Bryman and Bell (2011:26), induction and deduction are often used sequentially in a research study, which can be described as "the double movement of reflective thought". Saunders et al. (2012:150) describe that the abductive approach is used to examine a phenomenon, identify themes and explain patterns, to create a new or modify an existing theory, which is subsequently tested through further data collection. An abductive approach can be used in both a quantitative and qualitative study.

For the purpose of this study, a deductive approach was followed, based on the nature of the study, which aimed to determine guiding principles for the development and implementation of an operational risk appetite framework for South African banks. An empirical study was conducted to evaluate existing literature relevant to operational risk appetite in order to explore various principles required to implement an operational risk appetite framework. The study collected and analysed data from various South African banks, based on these identified principles in order to link the empirical research with the findings (deductive approach). The next section will discuss the methodological choice.

4.2.3 Methodological choice

The third layer of the research onion is called methodological choice, which means choosing between different research methods for the study. When conducting research, the research design usually includes quantitative or qualitative methods, or a combination of the two, known as mixed methods (Struwig & Stead, 2015:3). These research methods indicate the different forms of data collection, analysis and interpretations that a research study can have (Creswell, 2014:45). In order to determine which research method to use for this study, the different methods will be discussed briefly in the section below.

- **Quantitative research methods**

Quantitative research is a data analysis procedure (such as graphs or statistics) or a data collection technique (such as a questionnaire) that generates or uses statistical data for analysis in a research study (Saunders et al., 2012:161). According to Kumar (2011:104), "quantitative research is the measurement and classification of information, which is structured, rigid, fixed and predetermined in order to ensure accuracy in the measurement and classification of the data". The objective of quantitative research is to verify or test a theory instead of developing one, the researcher improves the theory, collects data to test it, and reflects on the confirmation or disconfirmation of the results (Creswell, 2014:93).

When a study must focus on the factors that may influence an outcome, which needs to be identified or to gain an understanding of the best predictors of outcomes, it is recommended by Creswell (2009) to use the quantitative approach. According to Creswell (2009), "quantitative studies use theory deductively and place the literature review towards the beginning of the study with the objective of testing or verifying a theory, rather than developing it. The theory will then become the framework for the study that organises the research questions and the data collection procedure."

Quantitative research is objective and generates reliable population-based and generalisable data, which is well suited to establish cause-and-effect relationships (Strang, 2015:515). According to Bryman and Bell (2011:31), quantitative research approaches tend to:

- "emphasise quantification in the collection and analysis of data;
- adopt a deductive approach to the relationship between theory and research, in which the emphasis is placed on the testing of theories;
- incorporate the practices and norms of the model of the natural sciences and positivism in particular; and
- embody a view of social reality as an external, objective reality."

As seen above, quantitative research is generally associated with positivism, where stipulated and highly structured data collection techniques are used, and a deductive approach, where the focus is on using data to test theory (Saunders et al., 2012:162). However, a quantitative approach may also be used within realist and pragmatist

philosophies and incorporate an inductive approach where data is used to develop a theory (Saunders et al., 2012:162).

- **Qualitative research methods**

In contrast to quantitative research, qualitative research aims to gain an understanding of a specific organisation or event, rather than a description of a large sample of a population. Qualitative research also aims to provide a clear interpretation of the structure, order and broad patterns found amongst a group of participants (Strang, 2015:515). The focus of qualitative research is to explore, understand, discover, explain and clarify values, situations, perceptions, feelings, experiences, attitudes and beliefs of a group of participants (Kumar, 2011:104). According to Saunders et al. (2012:161), qualitative research is a data collection technique (such as an interview) or data analysis procedure (such as categorising data) that generates or uses non-numerical data.

When analysing qualitative data, a researcher seeks to discover patterns, such as changes over time or possible causal links between variables (Strang, 2015:515). Qualitative research selects participants purposively and integrates a small number of cases according to their relevance, and researchers tend to use open-ended questions (Flick, 2015). According to Bryman and Bell. (2011:31), qualitative research approaches:

- usually emphasise words in the collection and analysis of data, rather than quantifying the data;
- mostly use an inductive approach, which is the relationship between theory and research and place the focus on generating rather than proving theories;
- discard the norms and practices of the natural scientific model and positivism, focusing on how individuals understand their reality; and
- view social existence as both constantly shifting and emerging.

Qualitative research is generally associated with interpretivism (subjective and socially constructed meanings expressed about the phenomenon being studied) and an inductive approach (a new research design is used to develop a rich theoretical perspective that already exists in literature) (Saunders et al., 2012:163). However, a qualitative approach may also be used within realist and pragmatist philosophies and incorporate a deductive

approach (to test an existing theoretical perspective using qualitative procedures) or an abductive approach (where inductive interpretations are developed, and deductive ones are tested iteratively throughout the research study) (Saunders et al., 2012:163).

- **Mixed methods**

Mixed methods research is used to describe research that combines or integrates qualitative and quantitative research methods within a single project or method (Bryman & Bell, 2011:62). Creswell and Plano Clark (2017) define mixed methods as a research approach that includes at the very least one quantitative method (designed to collect numbers) and one qualitative method (designed to collect words), where none of the two methods is linked to a specific research paradigm. According to Saunders and Tosey (2012/2013:59), a mixed method approach can start with a qualitative research technique (for example, a series of focus groups to identify a range of possible factors) and follow this with a quantitative research technique (for example, a questionnaire to determine the relative frequency of these different factors). On the other hand, a researcher could also choose to use a quantitative analysis technique to examine qualitative data (for example, comparing the frequency of occurrences of different notions in interview transcripts between a diverse group of individuals statistically) (Saunders & Tosey, 2012/2013:59).

In the mixed methods approach, the researcher:

- collects and analyses both quantitative and qualitative data thoroughly in terms of the research hypotheses and questions;
- integrates the two forms of data and their results;
- organises these processes into detailed research designs that provide the logical reasoning for conducting the study; and
- highlights these procedures within philosophy and theory (Creswell & Plano Clark, 2017).

Mixed methods research is generally associated with realism (quantitative analysis of published data followed by qualitative research methods to explore perceptions) and pragmatism (a pragmatist values both qualitative and quantitative research and the exact choice will depend on the particular nature of the research) (Saunders et al., 2012:164). The mixed methods approach may either use a deductive or abductive approach and will

probably combine them both, for example, qualitative or quantitative research may be used to test a theoretical proposition or propositions, followed by further qualitative or quantitative research to develop a rich theoretical viewpoint (Saunders et al., 2012:164).

For this descriptive study, the quantitative approach was seen as the most appropriate research methodology to follow in order to achieve the aim of the study. The literature relevant to operational risk management and operational risk appetite was reviewed in Chapters 2 and 3 to identify the appropriate research questions for the questionnaire in order to collect the data for the study. The study examined relationships between different variables, which were measured numerically and analysed using a range of statistical techniques. The next section will discuss the research strategy.

4.2.4 Research strategy

The fourth layer of the research onion is the research strategy. A research strategy is defined as a plan for how a researcher will go about answering the research question(s) in order to meet the research objective(s) (Saunders et al., 2012:173). The research strategy is seen as the methodological link between the philosophy of the study and the method chosen to collect and analyse the data (Saunders et al., 2012:173). There are various research strategies to consider when conducting qualitative, quantitative or mixed methods research. Saunders et al. (2012:173), Sekaran and Bougie (2013:102–103) and Creswell (2014:41–44) have identified some research strategies that can be used in these research methods:

- experiments (quantitative)
- surveys (quantitative)
- case studies (mixed method)
- archival research (mixed method)
- ethnography (qualitative)
- grounded theory (qualitative)
- phenomenology (qualitative)
- action research (qualitative)
- narrative inquiry (qualitative).

The strategies used for quantitative research will be discussed below to determine the research strategy that was followed for this study:

- **Experiments**

Experiments are usually associated with a deductive approach and identify causal relationships or causalities (to what extent do a set of variables that influence other variables) (Sekaran & Bougie, 2013:102). According to Hakim (2000, cited in Saunders et al., 2012:174), an experiment is a form of research that is grounded in the natural sciences and studies the probability of a change in an independent variable, which causes a change in another dependent variable. Collis and Hussey (2014:60) state that an experimental study is a methodology used to investigate the relationship between variables, where the independent variable (for example noise levels) is deliberately manipulated to observe the effect on the depended variable (for example the productivity of factory workers). There are two types of experiments, namely a laboratory experiment (takes place in a laboratory in a controlled environment) and a field experiment (which occurs in a real-life setting, for example, a workplace or a retail space) (Bryman et al., 2015:101).

According to Saunders et al. (2012:174), an experiment uses predictions, known as hypotheses, in order to anticipate whether a relationship will exist between variables. There are two types of hypotheses in an experiment, namely the null hypothesis and the alternative hypothesis (often referred to as the hypothesis) (Saunders et al., 2012:174). The null hypothesis predicts that there will not be a significant difference or a relationship between the variables. Experimental designs can consist of the following:

- Classical/true experiments: Individuals are randomly assigned to groups; either an experimental or control group, which leads to a stronger argument for a cause-and-effect relationship. This experimental design has a random selection of participants, random assignment of treatments and random assignment of groups.
- Quasi-experiments: Individuals are not randomly assigned to groups; they are preassigned (beforehand) to groups, based on specific characteristics or experiences of the group, for example, an individual's age, gender, race or illness. This type of study is also called post hoc (or after the fact) research. The quasi-

experiment allows for the examination of topics that otherwise could not be explored, because of moral, practical and ethical concerns.

- Pre- or within-group design experiments: There is no random selection of participants or a control group, only an experimental group. The influence of the research to discover the causal nature of the relationship between dependent and independent variables are significantly reduced, if not removed. This experiment allows little or no control over minor variables that might be responsible for outcomes other than what the researcher anticipated (Salkind, 2012:230; Saunders et al., 2012:175–246).

Based on the above information, it is evident that the primary intent of experiments is to test the impact of a treatment (or an intervention) on an outcome (Creswell, 2014:42). As one form of control, researchers randomly assign individuals to groups. When one group receives treatment, and the other group does not, the experimenter can distinguish if it is the treatment and no other factors that influence the outcome (Creswell, 2014:214).

- **Surveys**

According to Creswell (2014:201), “a survey provides a quantitative or numeric description of trends, attitudes or opinions of a population by studying a sample of that population.” A population is a defined body of people or objects under consideration for statistical purposes, and a sample is a subcategory of a population (Collis & Hussey, 2014:62). A survey is defined as a methodology designed to collect primary or secondary data from a sample, with the view to analyse the data statistically and generalising the results to a population (Colllis & Hussey, 2014:62).

A survey strategy is commonly associated with a deductive research approach and can be used for quantitative research (Saunders et al., 2012:176). According to Sekaran and Bougie (2013:102), “a survey is a system for collecting information from or about people to describe, compare or explain their knowledge, attitudes and behaviour.” Salkind (2012:198) agrees and states that survey research scrutinises the frequency and relationships between sociological and psychological variables and considers constructs such as attitudes, beliefs, prejudices, preferences and opinions. A survey process consists of designing the study, setting objectives for data collection, preparing a reliable

and valid survey instrument, administering the survey, collecting and analysing survey data, and reporting the results (Fink, 2003, cited in Sekaran & Bougie, 2013:102).

A survey is a popular strategy to follow when conducting quantitative research because it permits the researcher to collect quantitative data on numerous types of research questions (Sekaran & Bougie, 2013:102). The questions in survey instruments are typically arranged into self-administered questionnaires that a respondent complete on his/her own, either on paper or with a computer (Sekaran & Bougie, 2013:102). According to Saunders et al. (2012:177), using questionnaires will allow a researcher to collect standardised data from a sizeable population in a very economical way, allowing for easy comparison. The data collected can be used to propose possible reasons for specific relationships between variables and contribute to developing models for these relationships (Saunders et al., 2012:177).

As indicated in the sections above, this descriptive study focused on the postpositive paradigm and followed the deductive and quantitative research approach. Based on these conclusions and the discussion of what type of research strategies there are in quantitative research, this study followed a survey research strategy. The survey research strategy was chosen to fit in with the aim and objective of this study, which is to determine the principles required to develop a realistic operational risk appetite framework and statement in a South African bank. The reason for using this strategy is that a representative population sample to gather primary quantitative data to analyse empirically through self-administered questionnaires was used. The next section will discuss the time horizon of the study.

4.2.5 Time horizon

The final layer of the onion, before reaching the core, highlights the time horizon over which the researcher will conduct the research (Saunders & Tosey, 2012/2013:59). The time horizon over which a study is conducted can be either cross-sectional or longitudinal (Sekaran & Bougie, 2013:106). The cross-sectional design examines several groups of people at one point in time, and the longitudinal design assesses changes in behaviour in one group of subjects at more than one point in time (Salkind, 2012:252–253). Cross-sectional designs are associated with surveys in which data are collected through

questionnaires or structured interviews on more than one case and at a single point in time (Bryman et al., 2015:107). The longitudinal design, on the other hand, allows a researcher to measure the pattern of change and obtain information, requiring collection on a regular or continuing basis, thus enhancing its accuracy (Kumar, 2011:110). For this study, the time horizon was cross-sectional, as data were collected at a single point in time, due to limited time and resources. The next section describes the techniques and procedures of the study.

4.2.6 Techniques and procedures of the study

Finally, the core of the research onion is reached, which is the techniques and procedures that will be followed in order to collect and analyse data for the study (Saunders et al., 2012:128). The impending discussion will focus on the population, sampling, data collection and data analysis techniques that were used.

4.2.6.1 The population of the study

Sekaran and Bougie (2013:240) explain that a population refers to an entire group of people, events or things of interest that the researcher wants to investigate, based on sample statistics. As mentioned in 1.6.2, the target population of the study was the participants in the South African banking industry. The population consisted of the six main banks in South Africa, namely Absa Group Limited, First National Bank, Nedbank Group, the Standard Bank of South Africa Limited, Capitec Bank and Investec South Africa. The six banks have been identified based on their market share and asset value in the South African banking industry. These banks are also the leading practice based on the regulatory requirements of the South African Reserve Bank and are instrumental in managing the operational risk exposures of a bank (SARB, 2018).

The following section explains the sampling technique that was used for this study.

4.2.6.2 Sampling technique

Sampling is a depiction of all the components in the population from which the sample is collected (Sekaran & Bougie, 2013:240). In other words, a sample is a subset of a population (Salkind, 2012:95). In quantitative research, a sample is selected in such a way that it is unbiased and represents the population from which it is selected, whereas

in qualitative research some considerations may impact the selection of a sample (Kumar. 2011:192). This study focused on the quantitative data collection method which is steered by a predetermined sample size that is based upon many considerations and available resources (Kumar, 2011:192). According to Kumar (2011:197–198), various sampling techniques can be used in quantitative research.

- **Random or probability sampling**

According to Salkind (2012:96), the most common sampling technique is probability sampling, because the selection of participants is determined by chance. The determination of who will end up in the sample is based on non-systematic and arbitrary rules, where the chance of the sample representing the population is amplified (Salkind, 2012:96). Probability sampling is linked with survey research strategies where a researcher needs to make inferences from the sample about a population to meet the research objectives and answer the research questions (Saunders et al., 2012:262). Various authors, namely Saunders et al. (2012:270), Kumar (2011:203–204), Salkind (2012:96–102), and Sekaran and Bougie (2013:247–248) identify the main techniques in selecting a probability sample as simple random, systematic random, stratified random, cluster and multi-stage sampling.

- **Non-random or non-probability sampling**

In non-probability sampling, the probability of any individual member of the population being selected is unknown, and the variety of sampling units is random as researchers depend on individual judgement (Struwig & Stead, 2013:116). According to Kumar (2011:206), non-probability sampling can be used in quantitative or qualitative research. In quantitative research, the researcher selects a predetermined number of cases or the sample size, whereas in qualitative research the researcher does not decide on the number of respondents in advance, but continue to select additional cases until the researcher reaches the data saturation point (Kumar, 2011:206). There are various techniques that can be considered when using non-probability sampling, namely quota, convenience/haphazard/accidental, purposive/judgmental, snowball/volunteer or expert sampling (Kumar, 2011:206; Saunders et al., 2012:284; Sekaran & Bougie, 2013:252–253; Struwig & Stead, 2013:116–118).

After considering the abovementioned sampling methods, it was decided that the non-probability sampling method, in the form of purposive or judgmental sampling would be employed for the purpose of this study. According to Daniel (2012:90–91), the following are the strengths and weaknesses of purposive sampling (see Table 4.1).

Table 4.1: Purposive sampling strengths and weaknesses

Strengths	**Weaknesses**
Provides control over who is selected to be included in a sample.	Needs resources concerning time and money.
Provides for research focused on particular segments of a target population.	Needs current information and knowledge about the population.
Findings are generalisable.	Requires effort.
There is not as much of selection bias in this method.	If expert or judgement sampling is used, there may be bias because of that specific person's beliefs.
There is a smaller amount of bias which may come from underrepresentation and overrepresentation.	The researcher must know the population, and their locations, as well as the requirements of the research.

Source: Daniel (2012:90–91)

As seen from the advantages above, the primary consideration in purposive sampling is the researcher's judgement as to who can provide the most substantial information to realise the study's objectives (Kumar, 2011:207). According to Battaglia (2011:646), the primary purpose of a purposive sample is to yield a sample that is representative of the population and is often achieved by applying expert knowledge of the population in order to select in a non-random manner a sample of elements that signify a cross-section of the population. This technique is often used when working with a tiny sample or a limited number of people who have the information that is sought by the researcher (Sekaran & Bougie, 2013:252). For the current study, only experts in operational risk management within a bank were used as the target sample of the study. The next section will discuss the sample of the study.

4.2.6.2.1 Overview of the sample of the study

The sample was drawn from the participants across a variety of appropriate roles within the top (senior or executive) management, board directors, chief risk officers, chief financial officers, risk managers or specialists, internal auditors, compliance officers,

finance managers and business managers of a bank, who are involved in operational risk management within the bank.

4.2.6.3 Data collection

There are two types of methods that can be used when gathering data in a quantitative research study, namely primary and secondary data. According to Sekaran and Bougie (2013:36), these two methods can be distinguished as follows:

- Secondary data are data that already exist and do not have to be collected by the researcher, for example, online data, case study records, statistical bulletins, published or unpublished documents, government publications, library records, company websites and previous research studies.
- Primary data refer to information that the researcher collects through instruments such as surveys, interviews, focus groups or observations.

Primary data collection in the form of a questionnaire was used in this study to support the research case. A questionnaire is the most widely used instrument for collecting primary data through a survey strategy (Saunders et al., 2012:417). According to Kumar (2011:148–149), the following are the advantages and disadvantages when using a questionnaire (see Table 4.2).

Table 4.2: Questionnaire: advantages and disadvantages

Advantages of a questionnaire	**Disadvantages of a questionnaire**
This method is relatively low-cost.	The application of this method is limited.
Saves time.	The response rate is low.
Convenience for participants.	There is a self-selecting bias.
Provides for a reasonable degree of anonymity.	Opportunity to clarify issues is lacking.
	No allowance for spontaneous responses.
	The response to a question may be subjective to the response to other questions.
	Consulting others is possible.
	A response cannot be supplemented with other information.

Source: Kumar (2011:148–149)

One of the main advantages of a questionnaire is that each person is asked to respond to the same set of questions, which will provide for an efficient way of collecting responses from a big sample (Saunders et al., 2012:417). The questionnaire structure consisted of the following:

- **The cover letter**

The cover letter contained a brief introduction to the study and explained the main objectives and relevance of the study. It explained that the completion of the questionnaire is voluntary, that all information obtained will be confidential, and that anonymity will be maintained. The cover letter also explained that if the participant completes the questionnaire, the participant gives informed consent to partake in the study.

- **The instructions**

With a self-administered questionnaire, the instructions are essential. The questionnaire contained an instruction section indicating how the participant needs to complete the questionnaire, and the definitions of the main terms used in the questionnaire were listed.

- **The main body**

The main body is the actual questions. The questionnaire consisted of twenty close-ended questions, which included the biographical information of the participant and the identified principles for an operational risk appetite framework for a bank. Each question was indicated as a scaled-response question to gather data on the attitude or perception of a participant (Struwig & Stead, 2013:98). A 5-point Likert-type scale was used namely: 1 = Strongly Disagree (SD), 2 = Disagree (D), 3 = Neutral (N), 4 = Agree (A) and 5 = Strongly Agree (SA).

According to Struwig and Stead (2013:98), “a 5-point Likert-type scale is usually linked to a number of statements to measure attitudes or perceptions, and 5-point or 7-point scales are often used.” The participant had to indicate to what extent he or she agreed or disagreed that the listed principles are principles to manage an operational risk appetite framework and indicate to what extent the principles are applied in the bank to which he or she is affiliated.

The questionnaire (refer to Appendix A) was sent via e-mail to prospective participants from a predetermined database, with the covering letter (refer to Appendix B).

The next section explains the pilot testing of the questionnaire.

4.2.6.3.1 Pilot testing

A researcher pilot tests a questionnaire to ensure that the survey questions and the research instrument as a whole function well, to determine which questions are not understood by participants and the adequacy of the instructions to the participants (Bryman & Bell, 2011:209). A group of experts from the banking industry and academia was asked to comment on the representativeness, structure, content and suitability of the questions. The questionnaire and a diagnostic questionnaire (Refer to Appendix C) was sent out to the group of experts to complete and on which to comment. The relevant suggestions and comments were incorporated into the questionnaire after the pilot testing took place. Duplicate questions were removed, ambiguous questions were clarified, and additional questions were included to cater for omitted topics to create the final version of the questionnaire that was used for the study.

The following section explains the data analysis methods used in the study.

4.2.6.4 Data analysis

The research purpose, questions, method and design used in a research study affects the nature of the conclusions drawn from a data analysis, the type of analyses that may be appropriate, the amount of data that is required and the likelihood that the assumptions of a particular data analyses will be met (Scherbaum & Shockley, 2015). This study used the quantitative research approach, and from this, the data analysis method was determined. Quantitative research can be done through descriptive and inferential statistics. With descriptive analysis, the data are described using a set of descriptive statistics, in order to define the overall characteristics of a set or distribution of scores and is used for a small number of participants (Salkind, 2012:162). From the descriptive statistics, inferential analysis can then further analyse the variables or compare groups in terms of the variables so that conclusions can be drawn from the sample to a population and can be used to evaluate research questions and hypotheses to support

generalisations (Creswell, 2014:209). In light of the purpose of the study, which is to determine guiding principles for an operational risk appetite framework and the small population, the descriptive and inferential method for data analysis was used.

The goal of descriptive analysis, using quantitative data, is to describe quantitatively or summarise data (Scherbaum & Shockley, 2015). The descriptive statistics of the study consisted of frequencies and percentages, which provide descriptive information about a set of data (Sekaran and Bougie, 2013:393). The central tendency and variability or dispersion of the descriptive data was then determined. The descriptive information gained from the data analysis was further used to infer from the smaller sample from which the data were collected to the larger population from which the data were initially selected (Salkind, 2012:162). The inferential statistics of the study was obtained through non-parametric tests in the form of the Spearman's rank order correlation (rho) (Pallant, 2011:128). The Spearman's correlation coefficient does not make any assumption about the distributions of the two variables; it assumes that the sample is being selected at random and that the data are ranked in a scale that is ordinal, showing the relationship or association between the two variables (Maree, 2016:267). For this study, the association between the identified principles for an operational risk appetite framework and the implementation of these principles in a South African bank were tested and ranked accordingly.

This study used a survey research strategy in the form of a questionnaire. The primary quantitative data obtained from the questionnaire were statistically analysed with Microsoft Office Excel 2010 and IBM SPSS statistics, using descriptive and inferential statistics. The descriptive data of the study were reported by making use of tables and bar charts.

The next section discusses the process of determining the validity and reliability of the research instrument for the study, namely the questionnaire.

4.3 ENSURING VALIDITY AND RELIABILITY

It is crucial for a researcher to determine the quality of the results of a study (Kumar, 2011:177). According to Kumar (2011:177), it is vital to establish the accuracy, quality and appropriateness of the procedures the study adopted for finding answers to the

research questions. According to Salkind (2012:115), respected levels of reliability and validity are the hallmarks of good measurement practices.

4.3.1 Validity

According to Kumar (2011:178), validity is seen as the ability of a questionnaire to measure what it is designed to measure. Validity is concerned with what the researcher finds with the questionnaire so that it represents the reality of what the study is measuring (Saunders et al., 2012:429). Three methods can be used when determining the validity of a quantitative questionnaire.

- **Face and content validity**

According to Kumar (2011:179), the judgement that a questionnaire is measuring what it is supposed to measure is primarily based upon the rational link between the questions and the objectives of the study, and this can be achieved through the face and content validity. With face validity, each question in the questionnaire is tested to see if it has a logical link with the objectives of the study (Kumar, 2011:180). Content validity, on the other hand, determines whether the questionnaire measures the content it was intended to measure (Creswell, 2014:206). Expert opinions are often used to establish the content validity of a questionnaire (Salkind, 2012:124).

- **Criterion validity**

Criterion validity is concerned with either how well a test determines present performance, called concurrent validity, or how well it predicts performance, called predictive validity (Salkind, 2012:124). Predictive validity is judged by the degree to which a question can forecast an outcome, and concurrent validity is judged by how well a question compares with a second assessment, which is completed concurrently (Kumar, 2011:180). This method indicates that a question is unrelated or related to some degree to another question (Struwig & Stead, 2013:140). This method uses statistical analysis, for example, correlation, to determine validity (Saunders et al., 2012:430).

- **Construct validity**

According to Saunders et al. (2012:430), construct validity refers to the extent to which the questions measure the presence of the constructs that the questionnaire planned to

measure. Construct validity determines whether a question measured hypothetical constructs or concepts (Creswell, 2014:206). After the data analysis, statistical procedures need to establish the contribution of each construct to the total variance (Kumar, 2011:181). The contribution of these factors to the total variance is an indication of the degree of validity of the questionnaire (Kumar, 2011:181).

For the purpose of this study, the face and content validity methods were used to test for validity of the questionnaire. The questionnaire was pretested in the pilot study by a small number of experts to ensure content and face validity. In order to test the content validity of the questionnaire, experts in the field were required to complete the diagnostic questionnaire after evaluating the actual questionnaire. The feedback from the pre-testing of the questionnaire relating to the content validity of the actual questionnaire (refer to Appendix A) is presented in Table 4.3 below.

Table 4.3: Results from the diagnostic survey

1. The objective of the survey is clear.								
Option	Strongly disagree	Disagree	No option	Agree	Strongly agree		Median	Average
	0%	0%	0%	60%	40%		4	4.4
2. The survey is comprehensive in terms of the principles for an operational risk appetite framework within a bank.								
Option	Strongly disagree	Disagree	No opinion	Agree	Strongly agree		Median	Average
	0%	0%	20%	20%	60%		5	4.4
3. The instructions to complete the survey are clear.								
Option	Strongly disagree	Disagree	No opinion	Agree	Strongly agree		Median	Average
	0%	0%	0%	40%	60%		5	4.6
4. The survey is structured in a logical manner								
Option	Strongly disagree	Disagree	No opinion	Agree	Strongly agree		Median	Average
	0%	0%	0%	40%	60%		5	4.6
5. The statements are easy to understand.								
Option	Strongly disagree	Disagree	No opinion	Agree	Strongly agree		Median	Average
	0%	20%	0%	20%	60%		5	4.2
6. The scale of the survey is appropriate.								

Option	Strongly disagree	Disagree	No opinion	Agree	Strongly agree		Median	Average
	0%	0%	0%	80%	20%		4	4.2
7. Questions 4 to 18 cover the principles needed for an operational risk appetite framework.								
Option	Strongly disagree	Disagree	No opinion	Agree	Strongly agree		Median	Average
	0%	0%	0%	40%	60%		5	4.6
8. The time, in minutes, required to complete the questionnaire was …								
Option								Response percentage
0–5 minutes								0%
6–10 minutes								40%
11–15 minutes								60%
16–20 minutes								0%
More than 20 minutes								0%
9. Are there any questions you would like to add to the questionnaire?								
Options								Response percentage
Yes								60%
No								40%
10. Additional comments								
Some structural and editorial changes were suggested. A few questions to the questionnaire was added (the final questionnaire had 20 questions).								

The feedback from Table 4.3 can be summarised as follows:

- The objectives of the survey were clear with a median score of 4 and an average of 4.4, where 60% of the participants agreed, and 40% strongly agreed with the statement.
- The survey is comprehensive in terms of the principles for an operational risk appetite framework within a bank, with a median score of 5 and an average of 4.4, where 20% of the participants agreed, 60% strongly agreed, and 20% had no opinion.

- The instructions to complete the survey were clear, according to 40% who agreed and 60% who strongly agreed. All participants answered the questions with a median score of 5 and an average of 4.6.
- All the participants answered the question relating to the logical structure of the survey with a median score of 5 and an average of 4.6, where 40% of the participants agreed and 60% strongly agreed.
- The questions were easy to understand, according to 20% of the participants who disagreed, 20% who agreed and 60% who strongly agreed. All participants answered the question with a median score of 5 and an average of 4.2.
- All the participants answered the question relating to the appropriateness of the scale of the survey with a median score of 4 and an average of 4.2, with 80% of the participants agreeing and 20% strongly agreeing with the statement.
- 40% of the participants agreed, and 60% strongly agreed that questions 4 to 18 covered the principles needed for an operational risk appetite framework. The median score was 5 and the average 4.6.
- It took the participants approximately five to fifteen minutes to complete the questionnaire.
- There were no questions that they think could be added to the questionnaire, according to 40% of the participants, with 60% indicating that they would like to add questions that might add value to the research study. Two questions were added to the final questionnaire.
- The participants suggested specific structural and editorial changes.

The feedback received from the participants was incorporated into the questionnaire to ensure that the content is correct regarding the objectives of the study. The results indicated that the questionnaire is valid for this study.

4.3.2 Reliability

Reliability occurs when a test measures the same thing more than once and results in the same outcomes (Salkind, 2012:115). For a questionnaire to be valid, it must be reliable.

This means that reliability does not automatically imply validity, however, if a measure is valid, it will be reliable (Saunders et al., 2012:430). There are four types of reliability techniques that can be used to test for the reliability of the findings of a study.

- **Test-retest reliability**

With this technique, a questionnaire is administered once, and then again, under similar or the same conditions (Kumar, 2011:182). The ratio between the test and retest marks is an indication of the reliability of the questionnaire. The greater the value of the ratio, the higher the reliability (Kumar, 2011:182–183). According to Struwig and Stead (2015:140), test-retest reliability is calculated by pairing the scores from the first and second testing sessions for each participant and then using an appropriate correlation coefficient on the scores from the measure.

- **Parallel forms reliability**

Parallel forms reliability examines consistency between two questionnaires for the same group of participants (Salkind, 2012:120). Both questionnaires have indistinguishable items and the same response format, the only changes being the wording and the sequence or order of the questions (Sekaran & Bougie, 2013:229). The results obtained from one test are compared with the second test results. If the results are similar, it is assumed that the questionnaire is reliable (Kumar, 2011:183).

- **Internal consistency reliability**

Internal consistency is evaluated by correlating performance on each of the questions on a scale format with the total performance on the scale and takes the form of a correlation coefficient (Salkind, 2012:122). The most common statistical tools used in this technique are Cronbach's alpha and Kuder–Richardson correlation coefficient (Salkind, 2012:122). Reliability can be tested with Cronbach's alpha coefficient for Likert-type scales, which is regarded as a mature measure of internal reliability and consistency (Saunders et al., 2012:430). According to Saunders et al. (2012:430), "this statistic is used to measure the consistency of responses to a set of questions that are combined as a scale to measure a particular concept."

- **Split-half reliability**

The split-half reliability technique reflects the correlations between two halves of a questionnaire (Sekaran & Bougie, 2013:229). The questions are divided in half, in such a way that any two questions intended to measure the same aspect in a questionnaire fall into different halves (Kumar, 2011:184). Cronbach's alpha is the average of all split-half correlations and measures how one half of a test corresponds with the other half, but averages out the variation in the split-half method (DeVillis, 2011:109).

For the purpose of this study, the internal consistency technique in the form of Cronbach's alpha was used to test for the reliability of the questionnaire. A questionnaire was developed to measure the participants' perception of the principles needed for an operational risk appetite framework in a South African bank. The participants were required to evaluate the statements on a 5-point Likert-type scale, and the biographical information obtained from the questionnaire was not used to test for reliability. Only the Likert-type scale items in the questionnaire (Questions 4 to 20) were tested for reliability. The scale items consisted of strongly disagree, disagree, neutral, agree and strongly agree. The Cronbach's alpha for the participants' questionnaires was 0.9564, which indicates a relatively high standard of internal consistency (refer to Appendix D). The results of the internal consistency analysis indicated that there is consistency in the responses to the research questions, which means the questionnaire was reliable. The next section will discuss the ethical considerations for the study.

4.4 ETHICAL CONSIDERATIONS

As discussed in Chapter 1, ethical considerations are important to consider, especially if the research study involves human participants. According to Israel and Hay (2006, cited in Creswell, 2014:132), it is vital for researchers to protect their research participants, develop a trusting relationship with them, promote the integrity of the research and guard against impropriety and misconduct that might reflect on their organisations or institutions. That is why ethical considerations are so important when conducting a research study because these individuals must be treated in such a way that their dignity is maintained despite the research or the outcome (Salkind, 2012:85).

Ethics in business research is defined as a code of conduct or expected societal norms of behaviour while conducting research (Sekaran & Bougie, 2013:13). Over the years ethical principles in research have been identified, developed and mentioned by various authors, such as Creswell (2014), Saunders et al. (2012), Salkind (2012), Kumar (2011), Bryman and Bell (2011), Babbie (2008), Cooper and Schindler (2008) and Sarafino (2005), in order to assist a researcher to conduct research in an ethical manner. Based on these authors, the following ethical principles were applied in this study.

4.4.1 Informed consent

The principle of informed consent requires that participants should be fully informed about the research process (Bryman et al., 2015:124). The participants were informed regarding how they were expected to participate in the study using emails, which included the cover letter where the participants could give consent to take part in the study (refer to Appendix B for the cover letter). The participants were made aware of the type of information required from them, the purpose of the study and why the information was needed and how the study will affect them (Kumar, 2011:244). The form is definitive in stating that participation is voluntary and that they can withdraw at any point without penalty. Each participant was required to read the informed consent form and complete the questionnaire. The form guaranteed confidentiality and further informed participants of the possible outcomes of the research. For this study, ethical clearance was granted by the Finance, Risk Management and Banking Research Ethics Review Committee (refer to Appendix E for the ethical clearance certificate) before the data were collected from the participants.

4.4.2 Avoidance of harm

According to Diener and Crandall (1978, cited in Bryman et al., 2015:121), “harm can be physical harm, harm to participants’ development or self-esteem, stress, harm to career prospects or future employment, and inducing subjects to perform reprehensible acts.” The researcher protected all information at all stages of the research to prohibit harm to participants. Data collected from participants will be provided on request of the participants, except if the data can be used to acquire a potential advantage against direct market competition.

4.4.3 Deception

Sarafino (2005:70) stated: “deception refers to the act of misleading or withholding information to give a false impression, to create or hide a variable.” Whereas Struwig and Stead (2015) explain that deception means that participants were misled or misinformed about the nature of a study and, had they known the true nature of the study, they may have refused to participate. Cooper and Schindler (2008:36), on the other hand, suggest that some researchers do deceive participants to yield results that are accurate or to protect confidential information. Any deception by the researcher or the study was avoided by declaring the objective and intention of the study to the participants.

4.4.4 Privacy, confidentiality and anonymity

According to Salkind (2012:88), anonymity is where the names of participants are not linked to the questionnaire records, whereas confidentiality is when anything that is learned about the participants is held in the strictest of confidence. All of the information that participants provided in the survey were private at all times, and the identity of the participants in the study was unknown (anonymity). Babbie (2008:70) acknowledges that confidentiality should be assured when a researcher can still identify the participant who contributed to the study. The researcher divulged no information obtained from participants to others. Refer to Appendix F for the confidentiality agreement with the statistician.

4.4.5 Coercion, incentives and sensitive information

Participants should not be forced, for whatever reason, to participate in a study (Salkind, 2012:86). The participants were not coerced or forced to participate in the study. The researcher refrained from using any manoeuvres to influence participants to participate in the study. No incentives were provided to participants to share information in the questionnaire. The researcher understands that specific information can be regarded as sensitive or confidential by some participants and was dealt with accordingly.

4.5 CONCLUSION

This chapter outlined the theory underlying the research design and methodology of the study. The research philosophy, approach, methodological choice, strategy, time horizon,

techniques and procedures of the study were explained. Descriptive research in the form of a deductive approach was adopted for the study, as the aim of the study was to determine guiding principles for the development and implementation of an operational risk appetite framework for a South African bank. Therefore, a quantitative research methodology was followed. A survey strategy in the form of a questionnaire was selected for this study. The questionnaire tested as reliable and valid for this study. Data were collected from the purposively selected sample, which consisted of experts working in operational risk management within the top banks in South Africa. The data analysis methods used were also clarified in this chapter. Lastly, ethical considerations were discussed. The next section will discuss the analysis of the survey which includes a summary of the respondents.

CHAPTER 5: ANALYSIS OF SURVEY

5.1 INTRODUCTION

The previous chapter explained the research design and methodology that was used to answer the research questions of the study. This chapter will present the analysis and findings of the survey in order to achieve the following primary and secondary objectives of the study:

- determine guiding principles to formulate an operational risk appetite framework (ORAF) for a South African bank;
- research the current theoretical knowledgebase for operational risk appetite in order to identify relevant principles for an ORAF;
- highlight the importance of an ORAF in terms of the identified principles; and
- determine the current status of the implementation of the identified principles for an ORAF by South African banks.

The descriptive study involved the collection of primary data through the distribution of a questionnaire to experts working in operational risk management within a South African bank as indicated in Chapter 4. This chapter will explain the analysis of the questionnaire which consisted of section A, where the biographical information of the participants was obtained, and section B, consisting of 17 Likert-type questions regarding the principles needed for an ORAF for a bank (refer to Appendix G for the descriptive statistics).

5.2 BIOGRAPHICAL INFORMATION OF THE PARTICIPANTS

This section indicates the participants' biographical information extracted from section A of the questionnaire. Thirty participants answered the questionnaire. In order to preserve the anonymity of the banks as well as the participants, and to comply with the ethical requirements of the study, each participant was assigned a number, which was used instead of their names. The next section will describe the biographical data in the form of tables and percentages, created in Microsoft Excel spreadsheets.

5.2.1 Participant's position at a bank

The participants had to indicate their position within a bank. The positions were classified into eight categories, namely top management (chief executive officer [CEO], board director, senior management), risk manager or officer, financial manager or officer, internal auditor, business manager, compliance officer and other. Table 5.1 illustrates the various positions held by the participants within a bank who completed the questionnaire.

Table 5.1: Positions of participants with a bank

Designation	Participants	Percentage (%)
Top management (CEO, board director, senior management)	5	16.7%
Risk manager or officer	13	43.3%
Internal auditor	2	6.7%
Business manager	2	6.7%
Risk consultant	5	16.7%
Risk analyst	3	10.0%
Total	30	100%

The participants' designations covered a broad spectrum of positions within a bank; most of them were risk managers or officers, top management and risk consultants. The focus of the study was to engage with top management members, risk managers or officers and risk consultants, concerning the strategic management of operational risk in a bank. The study also found it essential to obtain information from the business managers, risk analysts and internal auditors at the operational level within a bank.

5.2.2 Experience of participants within a banking environment

The experience of participants relates to the number of years that they had been working in a banking environment. The participants' duration of service within a bank was categorised as follows: 0–1 year, 2–3 years, 4–5 years, 6–10 years, and more than ten years. Table 5.2 shows the experience of the participants within a banking environment.

Table 5.2: Experience of participants within a banking environment

Experience in years	Participants	Percentage (%)
0–1 year	2	6.7%
2–3 years	1	3.3%
4–5 years	3	10.0%
6–10 years	5	16.7%
More than ten years	19	63.3%
Total	30	100%

More than half of the participants had more than ten years of experience within a banking environment (63.3%). Of the participants, 16% were on the scale of 6–10 years, while 19% of the participants had 1–5 years of experience. The participants' years of experience within a bank strengthens the perceptions and input gained from the questionnaire to determine the principles required for an ORAF for a bank. The years of experience will also indicate their knowledge and understanding of the implementation of an ORAF within their bank.

5.2.3 Experience of participants within operational risk management

This question requested information regarding the years of experience of the participants in operational risk management. The aim was to ensure that the feedback from the respondents was based on experienced employees regarding risk management. Their years of experience in operational risk management was categorised as within 0–1 year, 2–3 years, 4–5 years, 6–10 years, and more than ten years. Table 5.3 depicts the results of this question.

Table 5.3 Experience of participants in terms of operational risk management in a bank

Experience in years	Participants	Percentage (%)
0–1 year	3	10.0%
2–3 years	3	10.0%
4–5 years	8	26.7%
6–10 years	7	23.3%
More than ten years	9	30.0%
Total	30	100%

The response indicated that 30% had more than ten years' experience in risk management, 23.3% had 6–10 years, 26.7% had 4–5 years and 20% had 0–3 years. Because 53.3% had more than five years' experience in risk management, it can be concluded that the responses to the questionnaire are valid regarding experience in operational risk management. The input and perceptions gained from the participants, based on their experience, should be beneficial in understanding the principles required for an ORAF for a bank, and an indication of the status of implementation. The next section will analyse the principles for, and the implementation of, an ORAF in the form of tables, charts and percentages created in Microsoft Excel spreadsheets.

5.3 ANALYSIS OF THE QUESTIONS

This section deals with the findings of section B of the questionnaire, which was comprised of 17 Likert-type questions (questions 4 to 20), which was divided into a and b questions. The first part of each question requests the participant to indicate to what extent he or she agrees or disagrees that the statement made can be seen as a principle to manage an ORAF. The second part of the question requires the respondents to indicate to what extent the principle is applied in the bank to which he or she is affiliated. The questions were derived from the literature review conducted in Chapters 2 and 3, which aimed to identify the principles needed for an ORAF. The next section provides an analysis of the data received.

5.3.1 Question 4

The question concerns the principle regarding an ORAF that should assist a bank with its strategic planning process and the achievement of objectives.

The response is reflected in Figure 5.1 below, and represents the opinions of the participants regarding this principle and the current implementation status thereof.

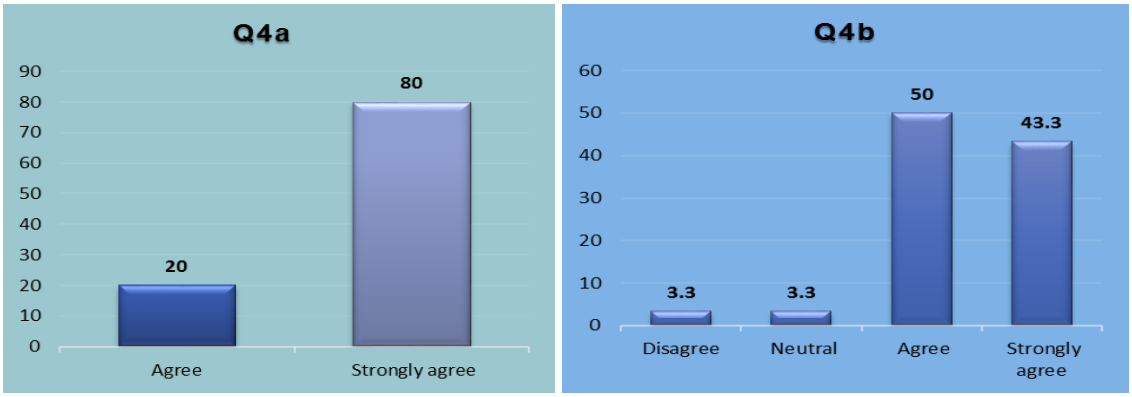


Figure 5.1: An operational risk appetite framework should assist a bank with its strategic planning process to achieve business objectives

According to the responses, 100% of the participants agreed that it is necessary for an ORAF to assist a bank with its strategic planning process to achieve business objectives, and 94% implied that it is currently implemented within the bank. Based on the responses, it can be concluded that an ORAF is a crucial principle, and should be incorporated into the strategic planning process of a bank to achieve business objectives. This finding also supports a previous finding by Young (2010), that an RAF should assist strategic planning by aligning strategic objectives and operational activities to achieve business objectives (refer to Table 3.6 of the literature review).

5.3.2 Question 5

This question presents the principle of an ORAF that should inform decision-making throughout the bank.

The responses received are portrayed in Figure 5.2 below and indicate the opinions of the participants regarding this principle and the current implementation status thereof.

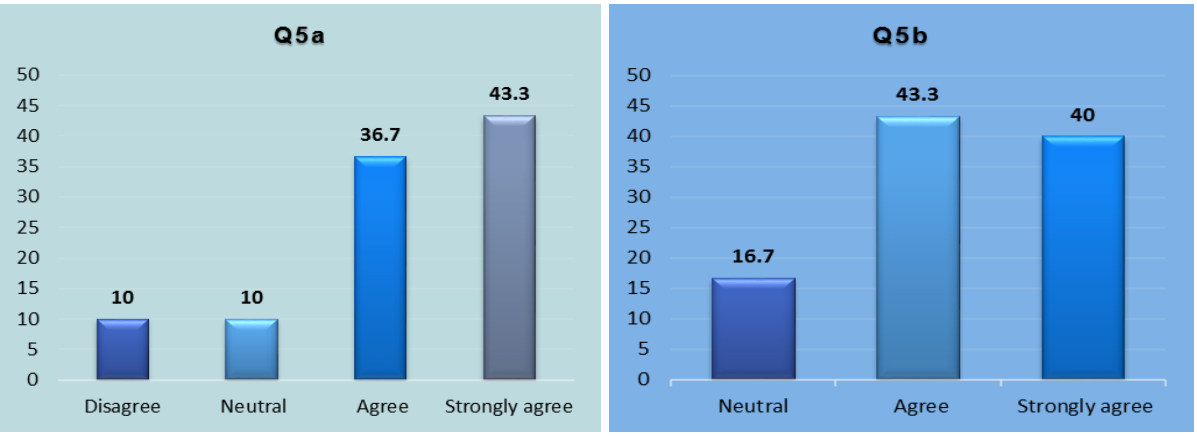


Figure 5.2: The operational risk appetite framework informs decision-making throughout the bank

According to the responses, 80% agreed that the ORAF should inform and support decision-making, indicating that it is an important principle. The current status of implementation is also about 80%, confirming that banks are using an ORAF to assist in decision-making. However, 16.7% of the respondents gave a neutral response, which could indicate that there is possibly still a lack of knowledge regarding the use of an ORAF. This finding is in support of the literature where Deloitte (2014a) indicates that an RAF should be used for formulating strategic and tactical business decisions (refer to Table 3.6). The SSG (2010) also stresses the need for the board to be accountable for the RAF and to use it to formulate strategic decisions (refer to Table 3.6).

5.3.3 Question 6

The question revolves around the principle that a bank should have a common risk language that should include the understanding of operational risk appetite.

The responses in Figure 5.3 below show the opinions of the participants regarding this principle and the current implementation status thereof.

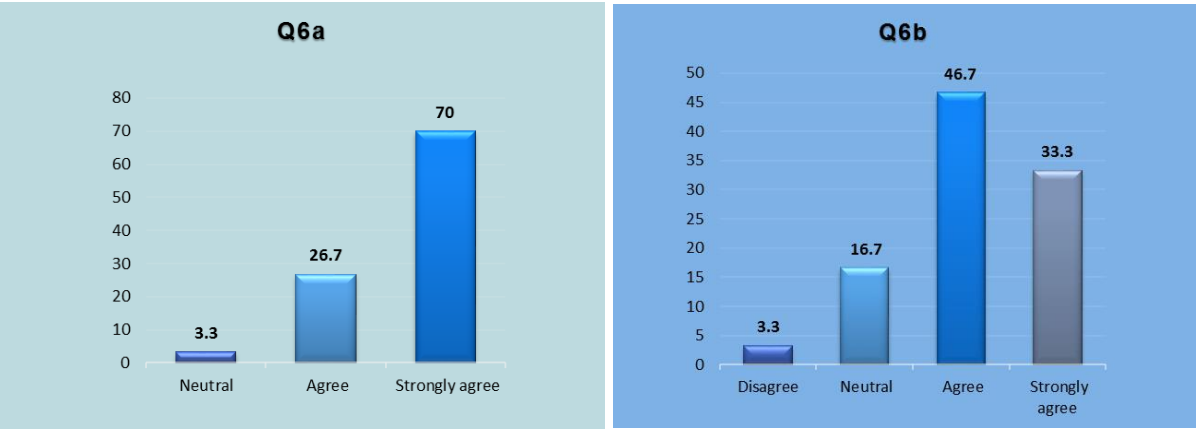


Figure 5.3: The bank should have a common risk language including the understanding of operational risk appetite

Seventy per cent of the respondents strongly agreed that a common risk language, including a definition of operational risk appetite, should be a risk management principle. However, only 33.3% strongly agreed that it is currently the case, 46% agreed, while 20% was uncertain or disagreed that operational risk appetite forms part of a common risk language. As such, it can be concluded that, although the majority agreed that a common risk language for operational risk appetite is an important principle, the current status of implementation indicates that it must still be refined in terms of a unifying platform to facilitate a common understanding of operational risk (refer to Table 3.6 in the literature review).

5.3.4 Question 7

In addition to the previous question, this question concerns the principle that operational risk appetite should be clearly defined.

The responses in Figure 5.4 below illustrate the opinions of the participants regarding this principle and the current implementation status thereof.

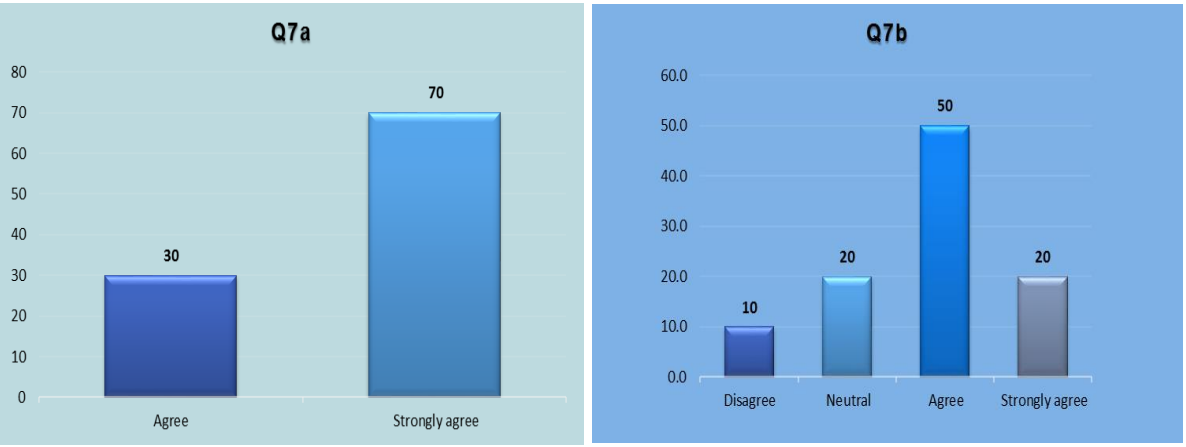


Figure 5.4: Operational risk appetite should be clearly defined

According to the responses, 70% of the respondents strongly agreed, and 30% agreed that operational risk appetite should be clearly defined. This indicates that operational risk appetite is an essential principle for an ORAF since 70% of the respondents agreed that operational risk appetite is clearly defined in their bank, while 30% were uncertain or disagreed that it is defined correctly. Lastly, it is crucial for a bank to define operational risk appetite clearly. This is supported by a previous finding by PwC (2014) that it is imperative that senior management of an organisation defines operational risk appetite in a way that is understood and accepted throughout the organisation. By achieving this, an organisation will reach its objectives through informed decision-making (refer to section 3.2 in the literature review).

5.3.5 Question 8

The question concerns the principle of an ORAF that should include a definition of operational risk appetite.

Figure 5.5 below presents the opinions of the participants regarding this principle and the current implementation status thereof.

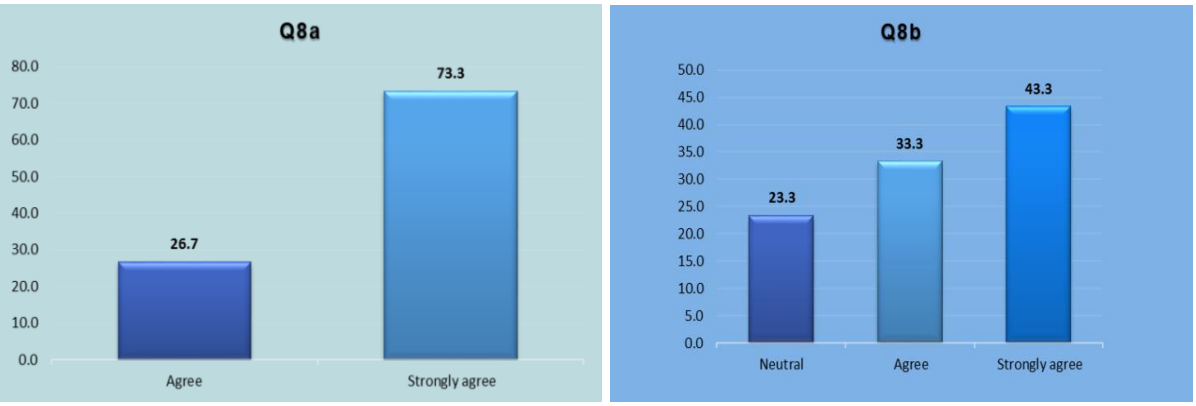


Figure 5.5: An operational risk appetite definition should be included in an operational risk appetite framework

All of the respondents agreed that an ORAF should include an operational risk appetite definition, which confirms it as a crucial principle. However, only 76.6% confirmed that this is currently the case, while 23.3% were uncertain. This may indicate that a bank needs to communicate or define operational risk appetite in a holistic way. If a bank defines its operational risk appetite clearly in its ORAF, it can be communicated throughout the bank to create a risk-aware culture (refer to 3.2 in the literature review). An operational risk appetite definition should be included as an essential principle for an ORAF.

5.3.6 Question 9

The question revolves around the principle of an ORAF, which should include an operational risk appetite statement (ORAS).

The response is illustrated in Figure 5.6 below and gives the opinions of the participants regarding this principle and the current implementation status thereof.

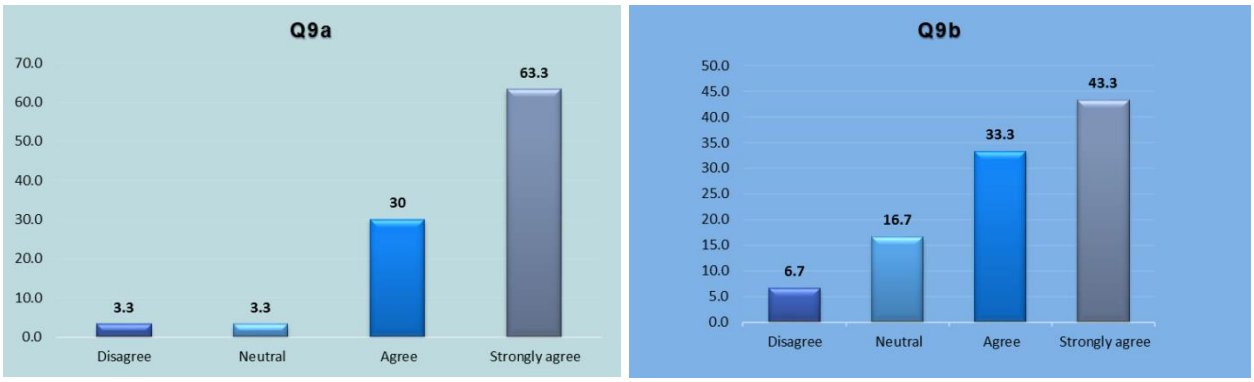


Figure 5.6: An operational risk appetite framework should include an operational appetite statement

It is evident from the responses that 93.3% of the respondents were of the opinion that an ORAF should include an ORAS, confirming it as an important principle. The status of implementation is at 76.6%, indicating that banks are including an ORAS in their ORAF. However, 23.4% of the respondents disagreed or gave a neutral response. This could indicate that there might still be a challenge for some banks to establish an ORAS compared to other risks, as found in the review conducted by the Basel Committee on the implementation of its operational risk principles in 2014 (refer to 3.3.1.1 in the literature review). An ORAF needs to begin with an ORAS, which establishes boundaries for the desired business focus of a bank and articulates the desired approach of the board to a variety of operational risk areas in a bank (SSG, 2010:2–9).

5.3.7 Question 10

This question refers to the principle that the board should approve the ORAS.

The response is reflected in Figure 5.7 below, and represents the opinions of the participants regarding this principle and the current implementation status thereof.

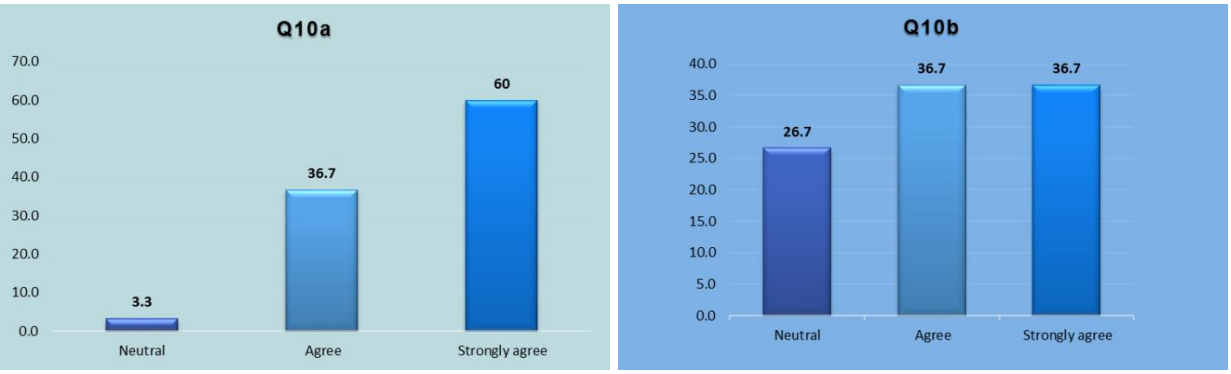


Figure 5.7: The board should approve the operational risk appetite statement

According to the responses, 96.7% of the respondents agreed that the board should approve the ORAS, confirming it as an important principle for an ORAF. However, only 73.4% of the respondents indicated that the board had approved the ORAS, whereas 26.7% of the respondents were neutral. This might indicate a lack of certainty from the respondents as to whether the board is approving the ORAS. This finding is in support of the literature where the Basel Committee (BCBS, 2014:4, 7 - 8) recommends that the board should approve and review a risk appetite and tolerance statement for operational risk that articulates the nature, types and levels of operational risk that the bank is willing to assume (refer to 3.3.1.1 of the literature review). To conclude, the approval the ORAS by the board should be included as a principle for an ORAF.

5.3.8 Question 11

In addition to the previous question, this question concerns the principle that the top management of a bank should submit the ORAS to the risk or audit committee for recommendation to the board.

The responses are portrayed in Figure 5.8 below and indicate the opinions of the participants regarding this principle and the current implementation status thereof.

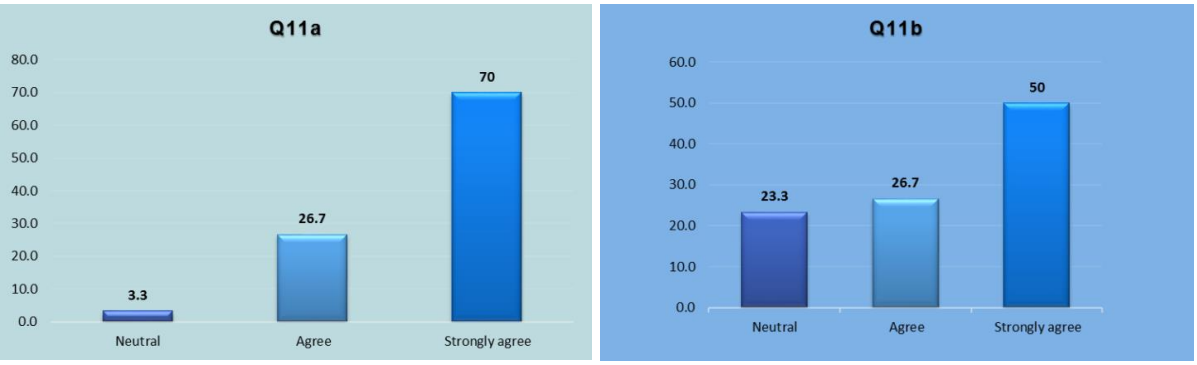


Figure 5.8: Top management should submit the operational risk appetite statement to the risk/audit committee for recommendation to the board

Of the respondents, 70% strongly agreed, and 26.7% agreed that top management should submit the ORAS to the risk or audit committee for recommendation to the board. This indicates that this is an important principle. About 76.7% of the respondents agreed that this process is currently being implemented in their bank, whereas 23.3% of them were uncertain. According to literature, the strength of the relationships between the board, senior management, business lines, risk manager and internal audit all play an instrumental role in the effectiveness of the ORAF and ORAS. The board needs to establish the ORAF and approve the ORAS, which should be developed in collaboration with top management (refer to 3.2 of the literature review).

5.3.9 Question 12

This question implies that an ORAS should include quantitative expressions.

The responses in Figure 5.9 below indicate the opinions of the participants regarding this principle and the current implementation status thereof.

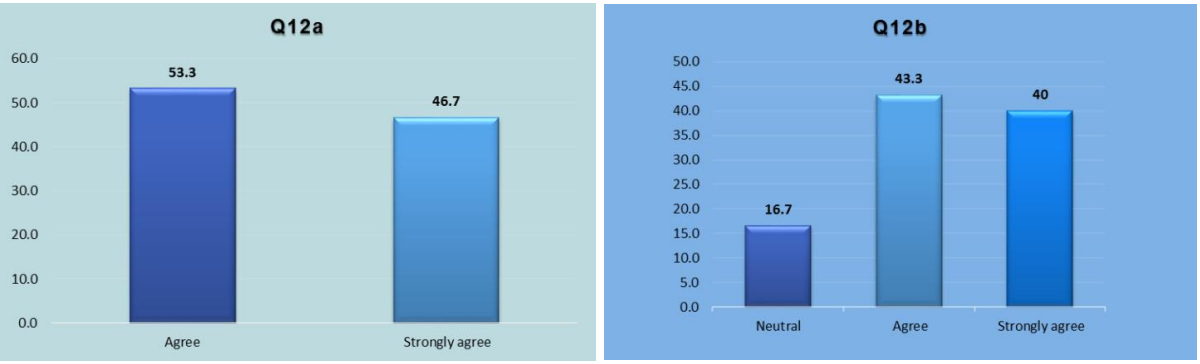


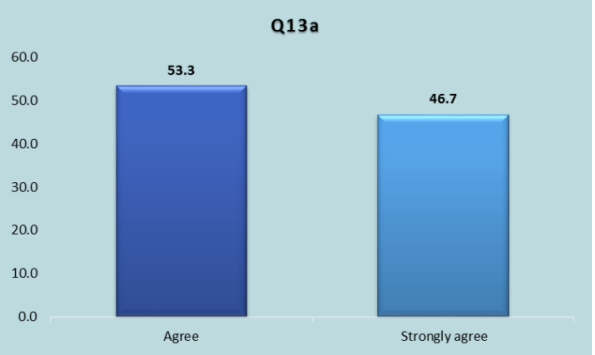
Figure 5.9: The operational risk appetite statement should include quantitative expressions

It is evident from the responses that all (100%) the respondents were of the opinion that the ORAS should include quantitative expressions, which makes it a crucial principle. However, only 83.3% indicated that the ORASs of their banks include quantitative expressions, whereas 16.7% were neutral. This might indicate a lack of knowledge of how an ORAS should be expressed in quantitative terms. This finding is in support of the literature, where Deloitte (2014a) states that the ORAS needs to include quantitative measures that can be translated into risk limits or thresholds applicable to business units within a bank (refer to Table 3.8 in the literature review). Therefore, it can be concluded that an ORAS should be expressed in quantitative terms and can be regarded as an essential principle.

5.3.10 Question 13

This question suggests that an ORAS should include qualitative expressions.

Figure 5.10 below shows the opinions of the participants regarding this principle and the current implementation status thereof.



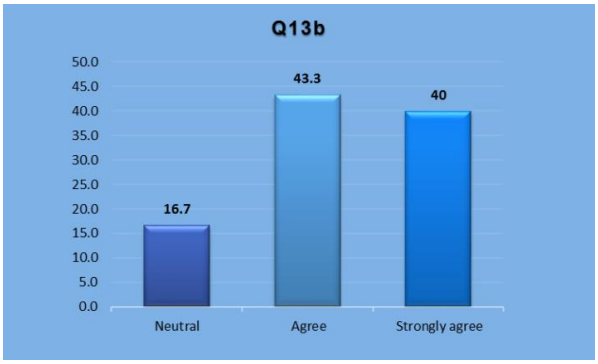


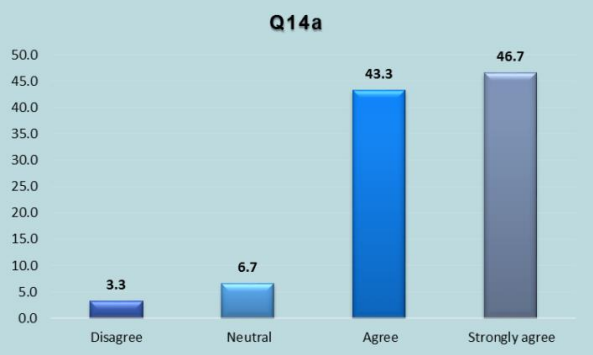
Figure 5.10: The operational risk appetite statement should include quantitative expressions

All of the respondents agreed that the ORAS should include qualitative expressions, which makes it a crucial principle. As with the previous question, only 83.3% of them agreed that their bank is expressing the ORAS in terms of qualitative measures. According to the IOR (2009), qualitative expressions can emphasise the relationship between risk and business management, as well as describing the attitudes and behaviours of the organisation as a whole, in other words, its risk culture (refer to Table 3.7 in the literature review). To conclude, it is imperative for banks to utilise both quantitative and qualitative components within their ORAS.

5.3.11 Question 14

The question concerns the principle that an ORAS should be defined through a bottom-up process, which includes the level where the risk exposure originated.

The responses are shown in Figure 5.11 below and are the opinions of the participants regarding this principle and the current implementation status thereof.



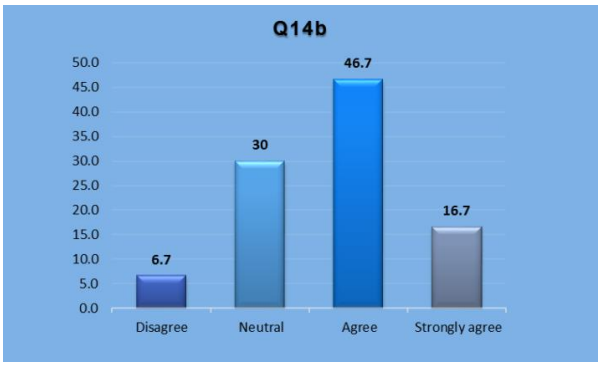


Figure 5.11: To define an operational risk appetite statement should be a bottom-up process including the level where the risk exposure originated

According to the responses, 90% of the respondents agreed that in order to define an ORAS, it should be a bottom-up process, including the level where the risk exposure originated, indicating that it is an important principle. However, only 63.4% of the respondents were of the opinion that their bank is implementing this process. Of the respondents, 30% were neutral, and 6.7% disagreed, which might indicate that the ORAS is not effectively communicated throughout the operational levels of the bank, and not embedded into the operational decision-making processes from where the risk is emanating (refer to 3.3.2 in the literature review). This also supports the finding of the IIF (2013), which highlights the importance for a bank to articulate its ORAS in a top-down and bottom-up approach, as well as across various business lines, which could lead to ownership of risk appetite throughout the bank (refer to 3.3.3 of the literature review).

5.3.12 Question 15

This question revolves around the principle concerning the different operational risk methodologies used to determine the operational risk appetite of a bank. The following four methodologies were identified and will be analysed in the following sub-sections: key risk indicator (KRI), loss data analysis or incident management, risk control self-assessment (RCSA), and scenarios.

5.3.12.1 Question 15.1

This question represents the principle that key risk indicators are used as an input to determine the operational risk appetite of a bank.

Figure 5.12 below indicates the opinions of the participants regarding this principle and the current implementation status thereof.

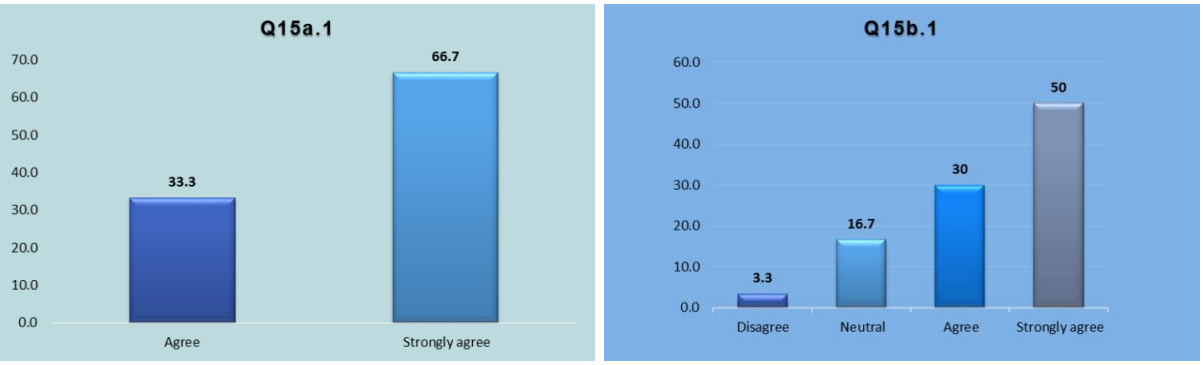


Figure 5.12: Key risk indicators are used as an input to determine a banks operational risk appetite

All of the respondents indicated that key risk indicators should be used as an input in determining the operational risk appetite of a bank, which makes it an operational risk methodology for an ORAF. Of the respondents, 80% indicated that the implementation is happening, while 20% were neutral or disagreed. This might show that there are still banks which are not using key risk indicators to determine their operational risk appetite. Lastly, key risk indicators are essential for a bank to understand significant risk exposures that might influence the operational risk appetite of a bank (refer to 2.6.1.1 in the literature review). Therefore, it can be concluded that key risk indicators should be seen as an essential principle for an ORAF.

5.3.12.2 Question 15.2

This question suggests that the loss data analysis or incident management method should be used as an input to determine the operational risk appetite of a bank.

The responses are reflected in Figure 5.13 below and represent the opinions of the participants regarding this principle, and the current implementation status thereof.

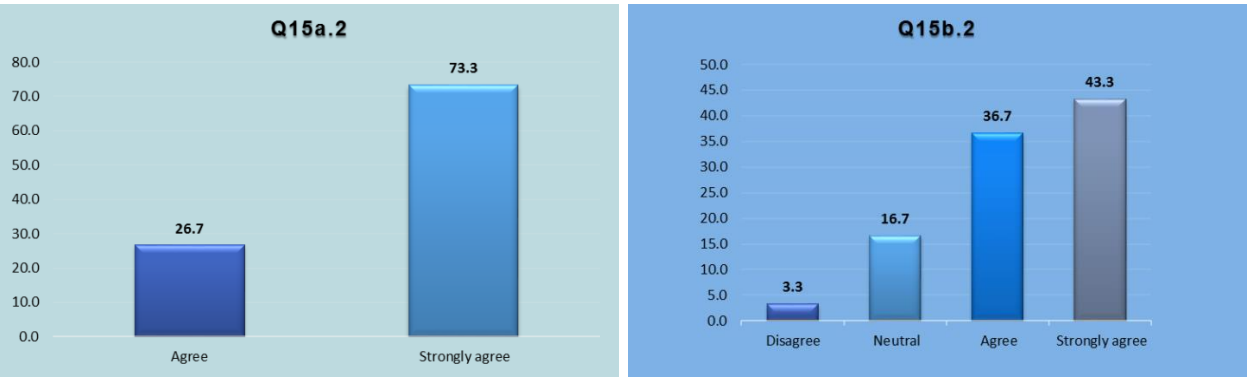


Figure 5.13 The loss data analysis/incident management method is used as an input to determine a banks operational risk appetite

It is evident from the responses that 100% of the respondents were of the opinion that the loss data analysis, or incident management method, should be used as an input to determine the operational risk appetite of a bank, confirming it as a crucial operational risk methodology principle in an ORAF. As with the previous question, only 80% of the respondents indicated that this method is currently being implemented in their bank, while 20% were uncertain, or disagreed that this method was or is used. According to the BCBS (2011), it is essential for a bank to analyse internal loss data which provides information regarding its operational risk exposures, and external loss data that gives relevant information regarding operational loss events occurring at other organisations, in order for a bank to determine its operational risk appetite (refer to 2.6.1.1).

5.3.12.3 Question 15.3

The question concerns the principle that risk control self-assessments are used as an input to determine the operational risk appetite of a bank.

The responses are shown in Figure 5.14 below and give the opinions of the participants regarding this principle and the current implementation status thereof.

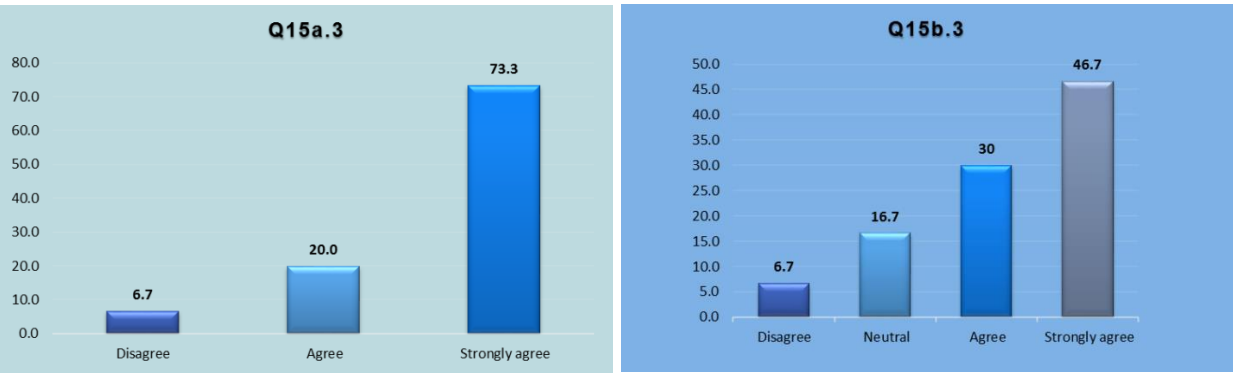


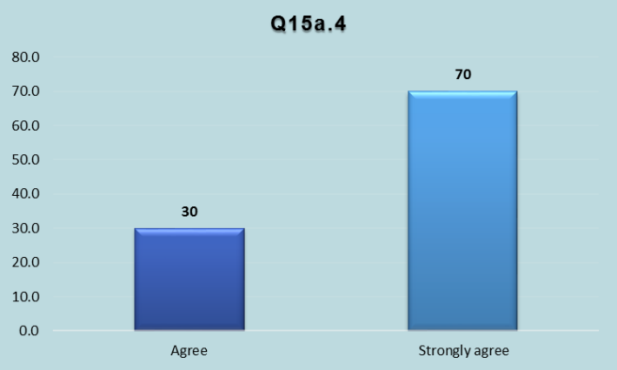
Figure 5.14: Risk control self-assessments are used as an input to determine a banks operational risk appetite

According to the responses, 93.3% of the respondents indicated that they agree that risk control self-assessments should be used as an input to determine the operational risk appetite of a bank, indicating that it is an important operational risk methodology principle in an ORAF. Only 76.7% of the respondents indicated that this method is currently being used to determine the operational risk appetite of a bank, while 23.4% indicated they are uncertain or disagree that it is being used. To conclude, it is crucial for a bank to use risk control self-assessments to assess the processes underlying its operations against a vast majority of potential threats and vulnerabilities and consider their potential impact in order for the bank to determine its operational risk appetite (refer to 2.6.1.1 in the literature review).

5.3.12.4 Question 15.4

The question represents the principle that scenario analysis is used as an input to determine the operational risk appetite of a bank.

Figure 5.15 below illustrates the opinions of the participants regarding this principle and the current implementation status thereof.



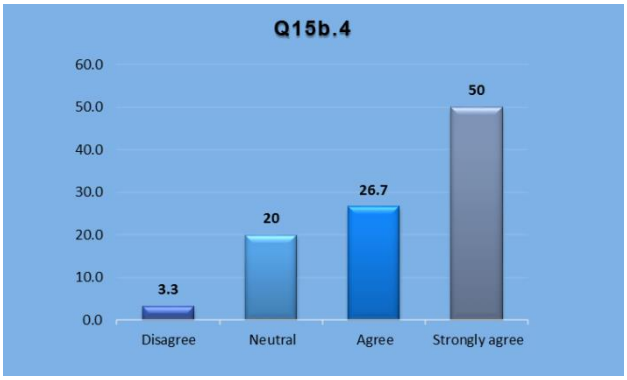


Figure 5.15: Scenarios are used as an input to determine a banks operational risk appetite

All of the respondents indicated that scenarios should be used as an input in determining the operational risk appetite of a bank, which makes it a crucial operational risk methodology principle in an ORAF. However, only 76.6% of respondents agreed that this method is being implemented in their bank, while 23.3% were neutral or disagreed that this is being done within their bank. This finding supports a previous finding by the IIF (2012), where scenario testing is indicated as an essential component of an ORAF because it analyses potential risk exposures which are identified through the use of scenarios by key employees in a bank (refer to Table 3.6 in the literature review).

To conclude, based on the above analysis of the responses, the four identified methods can all be seen as important risk methodologies and should form an integrated part of an ORAF.

5.3.13 Question 16

In addition to the previous question, this question concerns the principle that the operational risks should be managed within the approved limits of the operational risk appetite of a bank.

Figure 5.16 below represents the opinions of the participants regarding this principle and the current implementation status thereof.

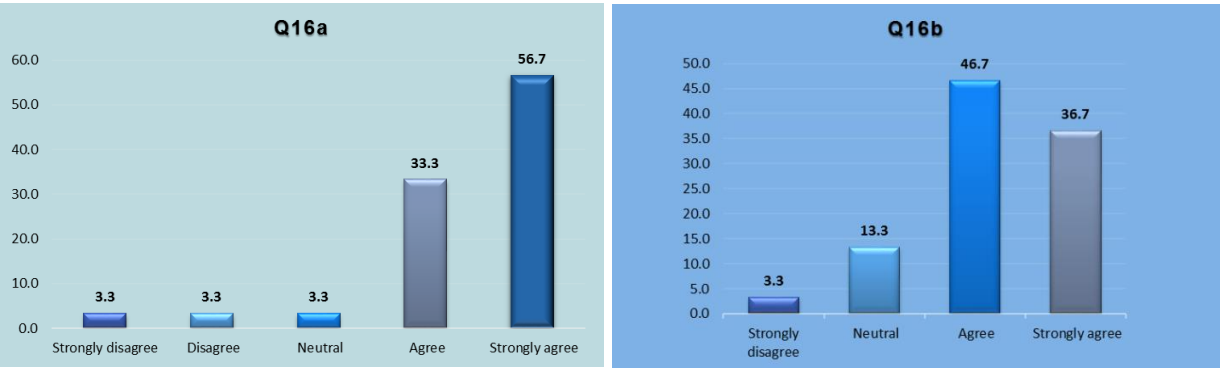


Figure 5.16: The operational risks should be managed within the approved limits of the operational risk appetite of a bank

It is evident from the responses that 90% of the respondents were of the opinion that operational risks should be managed within the approved limits of the operational risk appetite of a bank, confirming it as an important principle. The current status of implementation is also about 83.4%, confirming that banks are managing their operational risks within the approved limits of the operational risk appetite of a bank. However, 13.3% were neutral, and 3.3% strongly disagreed with the implementation status thereof, which might indicate that there might be instances where operational risks are not managed within the approved limits of the operational risk appetite of the bank. This supports the findings of the RIMS executive report: The risk perspective (RIMS, 2012), that many organisations involved in the financial crisis of 2008 did not define their risk appetite and did not communicate or enforce their risk limits across the organisation (refer to 3.2 of the literature review). It is also crucial for a bank to manage its upper and lower risk limits within its operational risk appetite in order to achieve good risk governance within its ORAF.

5.3.14 Question 17

This question revolves around the principle that operational risks should continuously be monitored against the ORAS of a bank.

Figure 5.17 below gives the opinions of the participants regarding this principle and the current implementation status thereof.

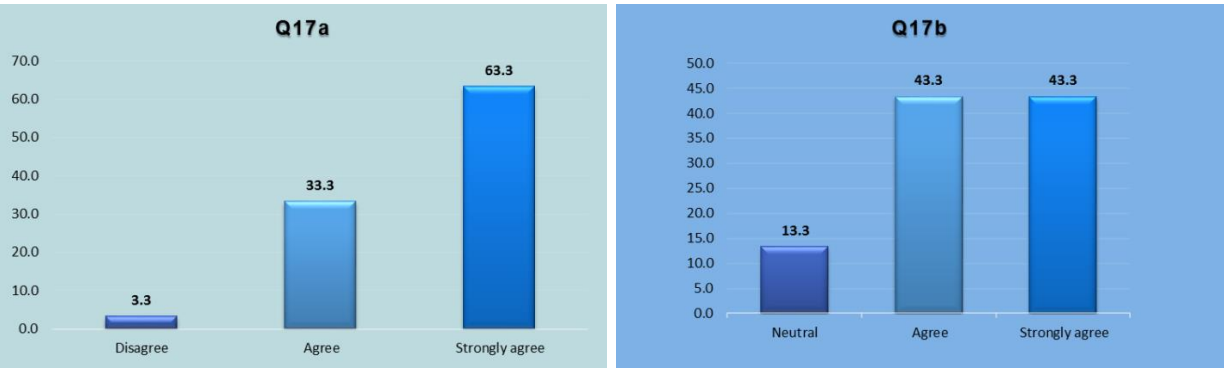


Figure 5.17: Operational risks should continuously be monitored against the operational risk appetite statement of a bank

According to the responses, 96.6% of the respondents agreed that operational risks should continuously be monitored against the ORAS of a bank, which confirms it as an important principle. Almost 87% of the respondents indicated that this process is being implemented in their bank, while 13.3% were uncertain. This might indicate that there are cases where operational risks are not continuously monitored against the ORAS. According to PwC (2014), the process of defining risk appetite and monitoring adherence to the ORAS can enhance informed decisions about capital allocation and ensure that decisions are made within the capacity to manage those risks in a bank (refer to 3.3.3 in the literature review).

5.3.15 Question 18

This question suggests that operational risks should be monitored to ensure that those are managed according to the approved ORAS of the bank.

The responses are reflected in Figure 5.18 below and represent the opinions of the participants regarding this principle and the current implementation status thereof.

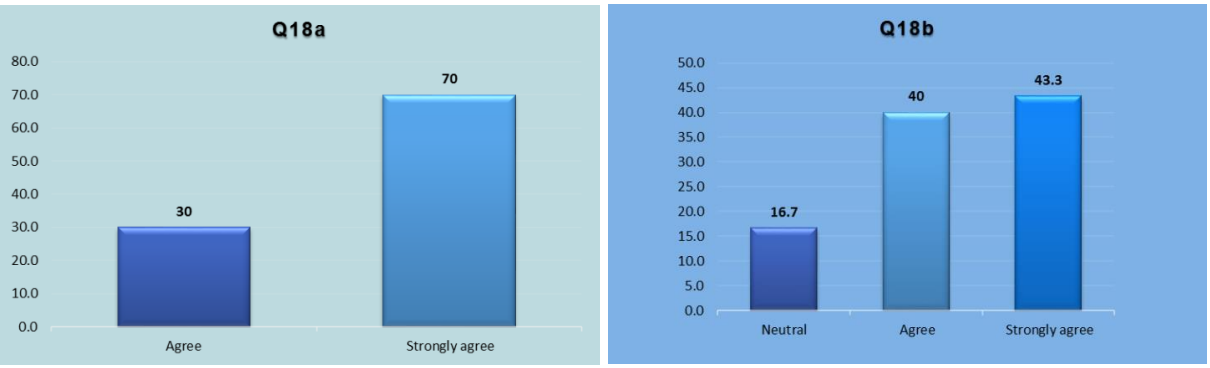


Figure 5.18: Operational risks should be monitored to ensure that it is managed according to the bank's approved operational risk appetite statement

All of the respondents indicated that operational risks should be monitored to ensure that it is managed according to the approved ORAS of the bank, which makes it a crucial ORAF principle. About 83.3% of the respondents indicated that this process is currently being implemented within their bank, while 16.7% indicated that they were uncertain whether it is monitored correctly. To conclude, it is vital for an ORAS to create awareness and monitor the risk thresholds to detect any changes in the operational risks in a bank to avoid unexpected losses (refer to 3.3.3 of the literature review).

5.3.16 Question 19

The question concerns the principle that regular operational risk reporting should include the performance of the business, compared to the tolerance levels of the ORAS.

Figure 5.19 below indicates the opinions of the participants regarding this principle and the current implementation status thereof.

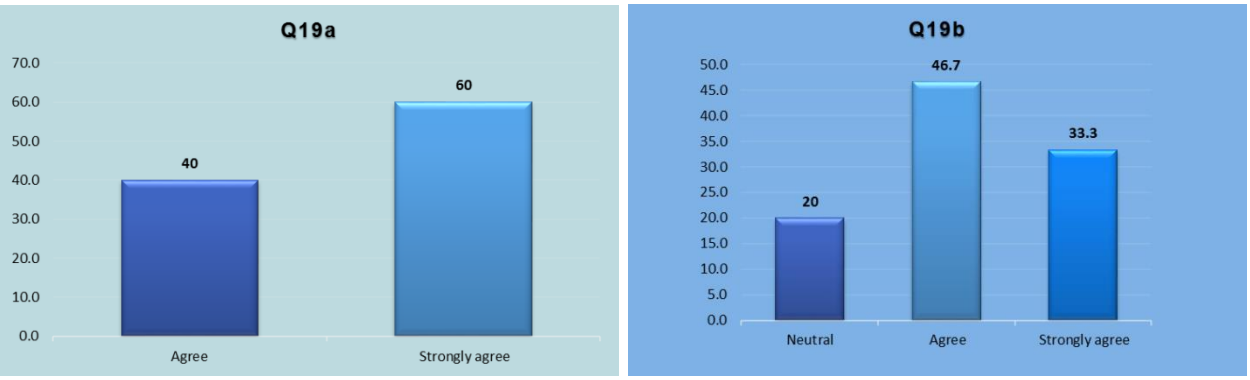


Figure 5.19: Regular operational risk reporting should include the performance of the business compared to the tolerance levels of the operational risk appetite statement

It is evident from the responses that 100% of the respondents were of the opinion that regular operational risk reporting should include the performance of the business compared to the tolerance levels of the ORAS, confirming it as a crucial principle. The current status of implementation is at 80%, confirming that banks are reporting on the performance of the business, compared to the tolerance levels of the ORAS. Of the respondents, 20% indicated that they were uncertain how this operational risk reporting process is conducted within their bank. This supports the findings of the BCBC (2014), that the operational risk reports of a bank should include the breaches of the risk appetite and tolerance statement, as well as thresholds or limits of a bank. Banks should report on established operational risk appetites and tolerances, its operational risk profile, or other items such as risk maps, trends and top operational risks that might have an impact on business performance (refer to 2.6.1.1)

5.3.17 Question 20

This question implies that operational risk reporting should indicate how changes in the ORAS are managed within the bank.

Figure 5.20 below shows the opinions of the participants regarding this principle and the current implementation status thereof.

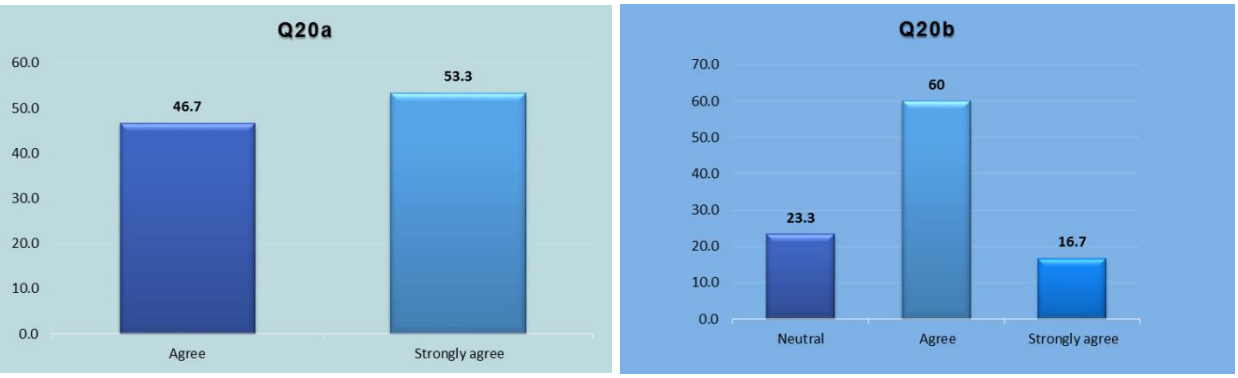


Figure 5.20: Operational risk reporting should include how changes in the operational risk appetite statement are managed within the bank

According to the responses, 100% of the respondents agreed that operational risk reporting should include how changes in the ORAS are managed within the bank, which makes it a crucial ORAF principle. However, only 76.7% of the respondents indicated that this operational risk reporting is being implemented within their bank, while 23.3% were uncertain whether this is the case in their bank. This could indicate that there might still be a challenge for certain banks to establish an ORAS that is reported and reviewed regularly and approved by the board, as found in the review conducted by the Basel Committee on the implementation of its operational risk principles in 2014 (refer to 3.3.1.1 in the literature review).

Based on the analysis above, it can finally be concluded that most of the identified principles in the survey were seen as important and crucial elements for the ORAF for a South African bank. However, not all of these principles have been fully implemented by some banks and should be addressed to ensure the development and implementation of a sound ORAF. The next section deals with the inferential data analysis conducted for this study.

5.4 INFERENTIAL ANALYSIS OF THE RESEARCH FINDINGS

The objective of this analysis is to determine the association between the identified principles for an ORAF and the implementation of these principles in a South African bank. The inferential statistics of the study were obtained through non-paramedic tests in the form of the Spearman's Rank Order Correlation (rho) (Pallant, 2011:128). The association between the identified principles for an ORAF and the implementation of

these principles in a South African bank are illustrated and ranked in Table 5.4 below (also refer to Appendix H for the correlation results).

Table 5.4: The strength of the association between question A (opinion) and B (implementation)

QUESTION	CORRELATION (rho)	SIGNIFICANCE (p-value)
5	0.836**	0.000
13	0.770**	0.000
16	0.744**	0.000
9	0.684**	0.000
12	0.665**	0.000
11	0.611**	0.000
10	0.561**	0.0001
8	0.542**	0.002
18	0.483**	0.007
19	0.459*	0.011
4	0.454*	0.012
15	0.446*	0.013
17	0.421*	0.020
6	0.249	0.184
7	0.245	0.192
20	0.106	0.578
14	0.053	0.780

The measure of association is the statistical evidence that confirms the conclusions made in 5.3. The coefficients are ranked from the strongest association to the weakest association, indicating that question 5 had the strongest association, and question 14 had the weakest association between the participants' opinions and the implementation of the principle. For example, in question 5a, 80% agreed that the ORAF should inform and support decision-making in a bank, and in question 5b, 83.3% agreed that banks are using an ORAF to assist in decision-making. This indicates a very strong association (rho = 0.836** and 2-tailed p-value = 0.000) between the two variables. While in question 17a, 96.6% agreed that operational risks should continuously be monitored against the ORAS of a bank, and in question 17b, only 86.6% agreed that this process is being implemented

in their bank. It appears that there is a moderate association (rho = 0.421 and 1-tailed p-value = 0.020) between the two variables.

For question 6a, 70% of the respondents strongly agreed that a common risk language, including an understanding of operational risk appetite, should be a risk management principle. However, only 33.3% strongly agreed that it is currently the case in their bank, which indicates a weak association (rho = 0.421 and 1-tailed p-value = 0.020) between the two variables. As such, it can be seen as an important principle, but the current implementation of the principle is still low. To conclude, the last three coefficients, which are also not significant and have a weak association, seems to indicate that the principles are considered important, but are not implemented effectively. The main reasons for this gap between the principle and its implementation fall outside the scope of this research and could be a topic for further study.

Regarding question 15, which deals with the principle of the operational risk methodologies used to determine the operational risk appetite of a bank, the following ranking was obtained (refer to Table 5.5).

Table 5.5: Strength of the association between question 15a (opinion) and 15b (implementation)

QUESTION	CORRELATION	SIGNIFICANCE	Opinion %	Implementation %
15.1	0,676**	0,000	100	80
15.4	0,511**	0,004	100	76.6
15.3	0,489**	0,006	93.3	76.7
15.2	0,402*	0,027	100	80

Although all four methodologies are statistically significant, the strongest association was for the key risk indicator, followed by scenarios, risk control self-assessment and loss data analysis or incident management. According to the descriptive analysis and the Spearman's Rank Order Correlation test, identified methods can be regarded as important risk methodologies and should form an integrated part of an ORAF.

Also, the results from the descriptive analysis and the Spearman's Rank Order Correlation test indicated the following:

- The respondents were of the opinion that all of the identified principles (deduced from the literature review) could be regarded as necessary for the ORAF of a bank. The following six principles had the strongest association (in order of the strongest to the weakest), according to the response and the subsequent implementation thereof:

1. An ORAF should inform decision-making throughout the bank.
2. An ORAS should include qualitative expressions.
3. An ORAS should be defined from a bottom-up process, which includes the level where the risk exposure originated.
4. An ORAF should include an ORAS.
5. An ORAS should include quantitative expressions.
6. The top management of a bank should submit the ORAS to the risk or audit committee for recommendation to the board.

- According to the responses, not all of the principles have been fully implemented, which requires attention when developing and implementing an ORAF. The following four principles had the weakest association according to the responses:
    1. a bank should have a common risk language including the understanding of operational risk appetite;
    2. operational risk appetite should be clearly defined throughout the bank;
    3. operational risk reporting should indicate how changes in the ORAS are managed within the bank; and
    4. an ORAS should be defined from a bottom-up process, which includes the level where the risk exposure originated.

According to the literature review, it became apparent that the above principles are essential for the establishment of an ORAF. The study indicated that a common language should exist regarding the concepts even before a framework is developed. Therefore, it is necessary that the definition of risk appetite should be clear and part of the common risk language of the organisation.

Also, the changes in the ORAS should be supported by adequate risk reporting. This principle would ensure that any changes in an ORAS are substantiated and based on facts, included in the risk reports. As such, it can once again be emphasised that this principle, although indicated as a weaker principle, is still vital for an effective ORAF.

The weakest principle, according to the analysis of the responses, is the defining of the ORAS from a bottom-up approach. The literature indicated that the risk must be managed as close to the exposure as possible. Therefore, it is imperative to initiate an ORAS at the lowest level to ensure that it is realistic and accurate when top management approves it. Although this principle is rated the weakest, it is clear that it is still a crucial principle for an ORAF.

By dealing with the importance of the weakest-rated principles and concluding that even the lowest-rated are still important, it can be concluded that all the identified principles are valid and necessary to ensure an effective ORAF.

5.5 CONCLUSION

This chapter presented the analysis and results of the study. In order to evaluate the primary and secondary objectives of this study, descriptive and inferential statistical analyses were conducted.

The first section discussed the biographical information of the participants. The second section analysed the respondents' opinions on the importance and the implementation status of the principle for an ORAF within their bank in the form of descriptive statistics. The last section of this chapter consisted of the inferential statistics, which ranked the seventeen principles based on the association between the identified principle for an ORAF, and the implementation of the principle in a South African bank, using the Spearman's Rank Order Correlation test. The seventeen principles below are ranked according to their strongest to weakest association based on the findings of the inferential analysis.

- **Principle 1:** An ORAF should inform decision-making throughout the bank.
- **Principle 2:** An ORAS should include qualitative expressions.

- **Principle 3:** Operational risks should be managed within the approved limits of the operational risk appetite of a bank.
- **Principle 4:** An ORAF should include an ORAS.
- **Principle 5:** An ORAS that should include quantitative expressions.
- **Principle 6:** The top management of a bank should submit the ORAS to the risk or audit committee for recommendation to the board.
- **Principle 7:** The board should approve the ORAS.
- **Principle 8:** An ORAF should include a definition for the operational risk appetite.
- **Principle 9:** Operational risks should be monitored to ensure that it is managed according to the approved ORAS of the bank.
- **Principle 10:** Regular operational risk reporting should include the performance of the business compared to the tolerance levels of the ORAS.
- **Principle 11:** An ORAF should assist a bank with its strategic planning process and achievement of objectives.
- **Principle 12:** A key risk indicator (KRI), loss data analysis or incident management, risk control self-assessment (RCSA) and scenarios are different operational risk methodologies used to determine the operational risk appetite of a bank.
- **Principle 13:** Operational risks should continuously be monitored against the ORAS of a bank.
- **Principle 14:** A bank should have a common risk language, including the understanding of operational risk appetite.
- **Principle 15:** Operational risk appetite should be clearly defined throughout the bank.
- **Principle 16:** Operational risk reporting should indicate how changes in the ORAS are managed within the bank.
- **Principle 17:** An ORAS should be defined from a bottom-up process, which includes the level where the risk exposure originated.

It can be concluded, that the above principles can be seen as crucial for an effective ORAF. The final chapter deals with a summary of the most important conclusions, which will form the basis of the recommendations of this study.

CHAPTER 6: SUMMARY, CONCLUSION AND RECOMMENDATIONS

6.1 INTRODUCTION

The previous chapter dealt with the analysis of the survey for this study. This chapter provides detail on the findings that form the platform for recommendations regarding the principles required for an effective ORAF for a South African bank.

Firstly, the chapter will give a summary and overview of the study. Secondly, the main conclusions and recommendations regarding how a South African bank can adopt the identified principles for their ORAF will be presented. Then, the contribution of the study to the body of knowledge will be explained. The chapter will conclude with the limitations of the study, and suggestions for future research.

6.2 SUMMARY OF THE STUDY

The study consisted of six chapters and can be summarised as follows.

Chapter 1 gave a brief overview of the literature, highlighting the current banking industry in South Africa and the importance of managing operational risk within the industry. The problem statement, research objectives, research methodology, ethical considerations and limitations were set.

Chapter 2 provided a review of the relevant literature. The chapter focused on operational risk management, the different national and international frameworks, standards and reports developed to manage operational risk and operational risks in the banking industry. The chapter concluded by providing a relevant theoretical knowledge base to support the primary and secondary research objectives.

Chapter 3 highlighted the importance of determining operational risk appetite and implementing an ORAF. The chapter provided an overview of the various approaches and principles required to formulate an ORAF, as well as the challenges experienced with the implementation thereof.

Chapter 4 focused on the research design of the study and provided further details of the research methodology used to gather the data as well as the statistical techniques used.

Chapter 5 presented the interpretation of the findings of the survey results, based on the descriptive and inferential statistical analysis of the principles. Chapter 6 will conclude with the findings, summary, research contribution, conclusions and recommendations of the study. The limitations of the study and suggestions for future research are also presented.

The next section provides a brief overview of the study.

6.3 OVERVIEW OF THE STUDY

This section provides a brief overview of this study concerning the aim and research objectives.

6.3.1 The aim of the study

The study aimed to identify guiding principles for an ORAF for the banking industry in South Africa. The focus was on the establishment of the principles needed to implement an effective ORAF in a bank. A comprehensive literature review was conducted to determine the leading practices for operational risk, operational risk appetite and the principles for an ORAF. The important principles and the current implementation status of these principles by South African banks were identified and form the crux of this study. The next section will revisit the objectives of the study.

6.3.2 Objectives of the study

The primary research objective and the secondary objectives of the study are summarised as follows.

6.3.2.1 Primary objective

The primary objective was to determine guiding principles to formulate an ORAF for a South African bank. Through the literature review in Chapter 3, seventeen principles for an ORAF were identified. These principles were then tested in the questionnaire regarding the participants' opinions regarding the importance of the principle and the implementation status thereof. The overall conclusion can be made that all seventeen principles were seen as important principles to ensure the establishment of an ORAF for a bank.

6.3.2.2 Secondary objectives

The first secondary objective was to research the current theoretical knowledge base for operational risk appetite in order to identify relevant principles for an ORAF. This was done through an extensive literature review of operational risk and operational risk appetite, based on leading practices and developments in the banking industry. The literature review in Chapter 2 found that it is imperative for the board and senior management to determine the operational risk appetite of a bank and implement an ORAF in order to achieve strategic objectives.

The second secondary objective was to highlight the importance of an ORAF regarding the identified principles. This was done through an extensive literature review regarding ORAFs and statements based on national and international frameworks, standards, reports and research conducted by various authors. The various challenges, benefits and principles needed for an effective ORAF and statement were highlighted in Chapter 3 (see 3.3.2 and 3.3.3), to assist banks to implement a realistic ORAF.

The third secondary objective was to determine the current status of the implementation of the identified principles for an ORAF by South African banks. This was tested through the questionnaire, where the participants had to indicate to what extent the principle was implemented in their bank. From the responses received, the study found that not all of the principles were effectively implemented in the banks, which needs to be addressed.

The objectives of this study and the underlying literature review resulted in the identification of the guiding principles for an ORAF, which were subjected to an empirical analysis to confirm its authenticity. The main conclusions and recommendations of this study are dealt with in the ensuing section.

6.4 MAIN CONCLUSIONS AND RECOMMENDATIONS

This section deals with the main conclusions based on the empirical analysis as well as the recommendations of this study. The conclusions are incorporated into the identified principles for an ORAF for a South African bank, and also indicate the current implementation status thereof. From the survey analysis, it can be highlighted that all of the identified principles were regarded as essential principles for an effective ORAF.

However, not all of these principles have been implemented by the banks. Seventeen principles, ranked according to their strength of association, from the strongest to the weakest, were identified and expressed as follows.

- **Principle 1:** An ORAF should inform decision-making throughout the bank.

  The objective of this principle was to highlight the importance of an ORAF to support decision-making throughout a bank. This principle was indicated as the highest priority, and it is recommended that it is developed and embedded in the ORAF of a bank to ensure sound business decisions.

- **Principle 2:** An ORAS should include qualitative expressions.

  This principle indicated that an ORAS should include qualitative expressions. It is crucial for a bank to indicate the commitment of a board to the alignment of strategic objectives with the approved ORAS. As such, it is imperative that this statement should be expressed in a qualitative format, for example, a statement concerning a zero tolerance for fraud. Therefore, it is recommended that this principle is incorporated into the ORAF of a bank.

- **Principle 3:** Operational risks should be managed within the approved limits of the operational risk appetite of a bank.

  This principle was also indicated as one of the highest priority principles for an ORAF. It is vital for an ORAF to indicate the limits and targets or thresholds for specific operational risks. It is recommended that a bank manages its upper and lower limits within its operational risk appetite and that the ORAF indicate the approved limits.

- **Principle 4:** An ORAF should include an ORAS.

  The objective of this principle was to determine the importance of an ORAF to include an ORAS. One of the critical parts of an ORAF is to define the ORAS. It is recommended that an ORAF include an ORAS, which can be used as a key communication tool to strengthen the consideration of operational risks concerning their threats and opportunities in the decision-making process of a bank.

- **Principle 5:** An ORAS should include quantitative expressions.

  This principle highlighted the importance of an ORAS to include quantitative expressions. It is crucial for an ORAS to include risk limits, targets and tolerances, as well as risk measures, for example, KRIs and risk control self-assessments, and describe the performance level of a bank. This study recommends that an ORAF should have an ORAS expressed in quantitative measures.

- **Principle 6:** The top management of a bank should submit the ORAS to the risk or audit committee for recommendation to the board.

  It is imperative for a bank to establish a process where the risk or audit committee and senior management recommend the ORAS to the board for approval. It is therefore recommended that an ORAF include the practice of the top management of a bank submitting the ORAS to the risk or audit committee for recommendation to the board.

- **Principle 7:** The board should approve the ORAS.

  The objective of this principle was to indicate the importance of the board to approve the ORAS. Regarding best practices (including King IV), the ORAS should be approved by the board. This study recommends that the ORAF includes the process for the board to approve the ORAS to ensure that there is clear communication and no misalignment in the bank concerning the approved statement of the board.

- **Principle 8:** An ORAF should include a definition of operational risk appetite.

  This principle is seen as crucial because a bank needs to communicate or define operational risk appetite in a holistic way. In 3.2, the following operational risk appetite definition was accepted for this study: “The amount of operational risks an organisation is willing to accept or tolerate to achieve strategic objectives”. It is recommended that the ORAF of a bank includes a formal definition of operational risk appetite, which considers both the opportunities and threats of operational risks.

- **Principle 9:** Operational risks should be monitored to ensure that it is managed according to the approved ORAS of the bank.

  This principle highlights the importance of monitoring operational risks to ensure that it is managed according to the approved ORAS of the bank. A bank needs to monitor its operational risks in order to ensure that corrective actions against the risk exposures are taken and to check that they are still in line with the approved ORAS of the bank. This study, therefore, recommends that an ORAF includes the monitoring of operational risks to ensure that it is managed against the approved ORAS of the bank.

- **Principle 10:** Regular operational risk reporting should include the performance of the business compared to the tolerance levels of the ORAS.

  This principle indicates the importance for a bank to report on the performance of the business compared to the tolerance levels of the ORAS. A bank will be able to identify the top operational risks that are affecting performance and deterring the achievement of business objectives. It is recommended that an ORAF includes a process for the regular reporting of the performance of the business, compared to the tolerance levels of the ORAS in order to get adequate operational risk information for decision-making.

- **Principle 11:** An ORAF should assist a bank with its strategic planning process and achievement of objectives.

  This principle indicates the importance for a bank to consider its operational risk appetite when arriving at business objectives. Therefore, the study recommends that an ORAF should be utilised actively by a bank to inform decision-making during the strategic planning process to enhance the likelihood for business objectives to be met.

- **Principle 12:** KRI, loss data analysis or incident management, RCSA and scenarios can be used to determine the operational risk appetite of a bank.

  The objective of this principle was to indicate that a bank needs to set its risk appetite and tolerance limits based on data generated by established key risk indicators, risk

control self-assessments, scenarios and loss data metrics. It is recommended that an ORAF includes the different measures or metrics to determine the operational risk appetite and tolerance of a bank.

- **Principle 13:** Operational risks should continuously be monitored against the ORAS of a bank.

  Operational risks should be continuously monitored against the ORAS in order to check that new or existing operational risk exposures are managed accordingly and are within performance expectations. This study recommends that the ORAF includes a process where operational risks are continuously monitored against the ORAS to ensure that the operational risks are managed within the tolerance levels of the bank.

- **Principle 14:** A bank should have a common risk language, including the understanding of operational risk appetite.

  This principle indicates the importance for a bank to have a common risk language, including the understanding of operational risk appetite. A common risk language will create a risk-aware culture throughout the bank and give clarity to what operational risk appetite entails. If the board understands what operational risk appetite is about, the board will be in a position to make decisions concerning the operational risk appetite of the bank. It is therefore recommended that an ORAF emphasises operational risk appetite as a common risk language.

- **Principle 15:** Operational risk appetite should be clearly defined throughout the bank.

  A bank should have a formalised definition for operational risk appetite, which needs to align effectively with the broad risk appetite definition. This study recommends that the ORAF of a bank defines operational risk appetite so that it is understood and accepted throughout the bank.

- **Principle 16:** Operational risk reporting should indicate how changes in the ORAS are managed within the bank.

  This principle indicates the importance of an ORAS to be reviewed regularly and that the changes in the ORAS should be indicated in the risk reports. It is recommended

that an ORAF includes a reporting process on how changes in the ORAS are managed within the bank.

- **Principle 17:** An ORAS should be defined from a bottom-up process, which includes the level where the risk exposure originated.

  Even though this principle was indicated as the lowest priority, it is still crucial. It is crucial for a bank to determine and define its ORAS across all the operational levels in the bank, which can be done through top-down and bottom-up processes. The study recommends that an ORAF indicate how an ORAS should be defined from a bottom-up process, which includes the level where the risk exposure originated.

The abovementioned principles can be regarded as the main principles for an effective ORAF for a bank. As such, it would be to the benefit of a bank to consider the adoption of the identified principles for an effective ORAF that will ensure a sound operational risk management process to support the optimum achievement of the business objectives of a bank. It is, however, important that there is an integrated approach between strategic and risk management to ensure that business objectives are aligned within the approved parameters of the operational risk appetite of a bank. In this sense, the next section will highlight the research contribution of the study.

6.5 RESEARCH CONTRIBUTION

This study contributes to the existing body of knowledge concerning operational risk appetite and the principles for an ORAF. It contributes by adding value to the understanding and determination of an ORAF and process for a bank. It also highlights the importance for a bank to define its ORAS accurately to achieve strategic objectives. The study emphasises the importance and value of implementing and adhering to the principles for an effective ORAF and statement by a bank. Although the identified principles relate to the banking industry, it is generically defined and can be used as guiding principles for any organisation exposed to operational risks. In this regard, the identified principles can be used as a checklist to determine the status of the development and implementation of an ORAF (refer to Appendix I for such a checklist).

6.6 LIMITATIONS OF THE STUDY AND SUGGESTIONS FOR FUTURE RESEARCH

Although this study endeavoured to be as comprehensive as possible, it is not always possible accurately to address certain limitations.

6.6.1 Limitations of the study

The first limitation is that the research study was limited to participants that are actively involved in the process of operational risk in a bank in South Africa. The research is restricted specific to operational risk, and any other risk types fell outside the scope of this study.

The second limitation was the availability of data, which may be protected or may not be publically available, due to the sensitivity of the information in the banking industry. However, the data collated were regarded as sufficient to serve as a basis for the empirical analysis and conclusions.

6.6.2 Suggestions for future research

The study aimed to identify guiding principles for an ORAF for the banking industry in South Africa. As identified in the study, not all of these principles have been implemented by the banks. The main reasons for this gap between the principles and its implementation fall outside the scope of this study and could form an introduction for further research. Also, this study could form a platform for similar research, involving other private and or public institutions.

6.7 CONCLUSION

The study determined the principles needed for an ORAF for a South African bank. In order to accomplish the primary and secondary objectives, empirical research was conducted through an extensive literature review researching operational risk, operational risk appetite and related principles for an ORAF. These principles were subjected to an empirical analysis, which revealed its importance to establish an ORAF. Although the principles were confirmed as crucial for a sound ORAF, the research also indicated certain inadequacies in the current implementation thereof. As such, banks can effectively use the results of this study to determine their status and address any shortcomings in developing and implementing an ORAF. Such a framework will ensure a streamlined

approach to operational risk management as a management discipline that should be integrated with the strategic planning process of an organisation, ensuring sound business decisions.

REFERENCES

AIRMIC, Alarm & IRM. 2010. *A structured approach to enterprise risk management (ERM) on the requirements of ISO 31000.* Retrieved from https://www.theirm.org/media/886062/ISO3100_doc.pdf [Accessed 12 November 2013].

Apostolik, R., Donohue, C. & Went, P. 2009. *Foundations of banking risk: an overview of banking, banking risks, and risk-based banking regulation.* Hoboken, NJ: Wiley.

APRA (Australian Prudential Regulation Authority). 2015. *A prudential practice guide for risk management (CPG 220).* Retrieved from https://www.apra.gov.au/file/19656 [Accessed 8 March 2017].

Ashby, S. 2008. Operational risk: Lessons from nonfinancial organisations. *Journal of Risk Management in Financial Institutions*, 1(4):406–415.

Aven, T. 2013. On the meaning and use of the risk appetite concept. *Risk Analysis*, 33(3):462–468.

Babbie, E.R. 2008. *The basics of social research.* Fourth edition. Belmont, CA: Thomson Wadsworth.

Barfield, R. 2007. Risk appetite – how hungry are you? *The journal: Special risk management edition*. PricewaterhouseCoopers. Retrieved from https://www.pwc.com/gx/en/banking-capital-markets/pdf/risk_appetite.pdf [Accessed 15 October 2013].

Battaglia, M.P. 2011. Purposive sample. In *Encyclopedia of survey research methods*. Edited by Paul J. Lavrakas. Thousand Oaks, CA: Sage, 645–647.

BCBS (Basel Committee on Banking Supervision). 2002. *Sound practices for the management and supervision of operational risk*. Retrieved from https://www.bis.org/publ/bcbs96.htm [Accessed 15 October 2013].

BCBS (Basel Committee on Banking Supervision). 2004. *International convergence of capital measurement and capital standards: A revised framework.* Retrieved from https://www.bis.org/publ/bcbs128.htm [Accessed 21 June 2013].

BCBS (Basel Committee on Banking Supervision). 2010. *Consultative document: Operational risk – supervisory guidelines for the advanced measurement*

approaches. Retrieved from https://www.bis.org/publ/bcbs184.pdf [Accessed 15 October 2013].

BCBS (Basel Committee on Banking Supervision). 2011. *Principles for the sound management of operational risk.* Retrieved from http://www.bis.org/publ/bcbs195.pdf [Accessed 15 October 2013].

BCBS (Basel Committee on Banking Supervision). 2014. *Review of the principles of the sound management of operational risk.* Retrieved from https://www.bis.org/publ/bcbs292.htm [Accessed 8 March 2017].

Bessis, J. 2003. *Risk management in banking*. London: Wiley.

Bhargava, A. 2014. Examining best practices in operational risk management. *The RMA Journal*, 97(2):64–69.

Blunden, T. & Thirlwell, J. 2010. *Mastering operational risk: A practical guide to understanding operational risk and how to manage it.* Edinburg Gate: Pearson.

Blunden, T. & Thirlwell, J. 2013. *Mastering operational risk: A practical guide to understanding operational risk and how to manage it*. Second edition. Edinburg Gate: Pearson.

Bostander, D.E. 2007. Operational risk events in banks and practices for collecting internal loss data. Unpublished master's thesis. Pretoria: University of South Africa.

Breden, D. 2008. Monitoring the operational risk environment effectively. *Journal of Risk Management in Financial Institutions*, 1(2):156–164.

Bryman, A. & Bell, E. 2011. *Business research methods.* Third edition. New York, NY: Oxford University Press.

Bryman, A., Bell, E., Hirschsohn, P., Du Toit, J., Dos Santos, A., Wagner, C., Van Aardt, I. & Masenge, A. 2015. *Research methodology: Business and management contexts.* Fifth edition. Cape Town: Oxford University Press.

Business Report. 2014. Abil hit risks R4bn in state pensions, 30 September. Retrieved from http://www.iol.co.za/business/companies/abil-hit-risks-r4bn-instatepensions-1.1757918#.VCu9bU0U9zk [Accessed 1 October 2014].

Cameron, B. 2014. African Bank rescue plan. *News24,* 31 August. Retrieved from http://www.news24.com/MyNews24/African-Bank-Rescue-Plan-20140831 [Accessed 1 October 2014].

Casu, B., Molyneux, P. & Girardone, C. 2006. *Introduction to banking.* Essex: Pearson.

Chapman, R.J. 2011. *Simple tools and techniques for enterprise risk management*. Second edition. Chichester: Wiley.

Chorafas, D.N. 2000. *Reliable financial reporting and internal control: A global implementation guide*. New York, NY: Wiley.

Collis, J. & Hussey, R. 2014. *Business research: A practical guide for undergraduate and postgraduate students.* Fourth edition. New York, NY: Palgrave Macmillan.

Cooper, D.R.I. & Schindler, P.S. 2008. *Business research methods.* Tenth edition. New York, NY: McGraw-Hill.

COSO (The Committee of Sponsoring Organizations of the Treadway Commission). 2004. *Enterprise risk management. Integrated framework: Executive summary.* Retrieved from https://www.coso.org/Documents/COSO-ERM-Executive-Summary.pdf [Accessed 13 November 2013].

COSO (The Committee of Sponsoring Organizations of the Treadway Commission). 2009. *Effective enterprise risk oversight: The role of the board of directors.* Retrieved from https://www.coso.org/Documents/COSOBoardsERM4pager-FINALRELEASEVERSION82409_001.pdf [Accessed 13 November 2013].

COSO (The Committee of Sponsoring Organizations of the Treadway Commission). 2011. *Embracing enterprise risk management: Practical approaches for getting started*. Retrieved from https://www.coso.org/Documents/Embracing-ERM-Getting-Started.pdf [Accessed 5 August 2015].

COSO (The Committee of Sponsoring Organizations of the Treadway Commission). 2012. *Enterprise risk management: Understanding and communicating risk appetite*. Retrieved from https://www.coso.org/Documents/ERM-Understanding-and-Communicating-Risk-Appetite.pdf [Accessed 5 August 2015].

Creswell, J.W. 2009. *Research design*: *Qualitative, quantitative and mixed methods approaches.* Third edition. Los Angeles, LA: Sage.

Creswell, J.W. 2014. *Research design*: *Qualitative, quantitative and mixed methods approaches.* Fourth edition. Sage. Retrieved from https://www.researchgate.net/file.PostFileLoader.html?id=5901dad84048541d6c2b1fc3&assetKey=AS%3A487723636137986%401493293784496 [Accessed 20 January 2017].

Creswell, J.W. & Plano Clark, V.L.P. 2017. *Designing and conducting mixed methods research*. Third edition. Thousand Oaks, CA: Sage.

CRO Forum & CRO Council. 2013. *Establishing and embedding risk appetite: Practitioners view*. Retrieved from https://www.thecroforum.org/wp-content/uploads/2013/12/CRO-Forum-Council-Risk-Appetite-FINAL-2.pdf [Accessed 20 January 2014].

Croitoru, I. 2014. Operational risk management and monitoring. *Internal Auditing and Risk Management*, 36(1): 21-31.

Crowther, D. & Lancaster, G. 2009. *Research methods: A concise introduction to research in management and business consultancy.* Second edition. Oxford: Elsevier Butterworth-Heinemann.

Daniel, J. 2012. *Sampling essentials: Practical guidelines for making sampling choices*. Thousand Oaks, CA: Sage.

Deloitte. 2014a. *Risk appetite frameworks: How to spot the genuine article.* Retrieved from https://www2.deloitte.com/content/dam/Deloitte/au/Documents/risk/deloitte-au-risk-appetite-frameworks-financial-services-0614.pdf [Accessed 7 March 2017]

Deloitte. 2014b. *Risk appetite in the financial services industry: A requisite for risk management today*. Retrieved from https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/FinancialServices/2014_risk_appetite_deloitte_ireland.pdf [Accessed 8 March 2017]

Deloitte. 2016. *King IV bolder than ever.* Retrieved from https://www2.deloitte.com/content/dam/Deloitte/za/Documents/governance-risk-compliance/ZA_King_IV.pdf [Accessed 2 February 2017].

Deloitte. 2017. *Risk appetite frameworks for corporates: Do you know what is on your plate?* Retrieved from https://www2.deloitte.com/content/dam/Deloitte/za/Documents/financialservices/za_Risk_Appetite.pdf [Accessed 13 July 2017].

DeVillis, R. (Ed.). 2011. *Scale development: Theory and application*. Los Angeles, CA: Sage.

Du Randt, R. 2011. *Risk management for banks: Study guide for RSK1501*. Pretoria: University of South Africa.

ERM Initiative Faculty & Cox, C. 2014. *Understanding risk appetite.* Retrieved from https://erm.ncsu.edu/library/article/understanding-risk-appetite [Accessed 1 February 2016].

European Central Bank. 2016. *SSM supervisory statement on governance and risk appetite*. Retrieved from https://www.bankingsupervision.europa.eu/ecb/pub/pdf/ssm_supervisory_statement_on_governance_and_risk_appetite_201606.en.pdf [Accessed 20 January 2017].

EY (Ernst & Young). 2016. *Risk appetite: The strategic balancing act.* Retrieved from http://www.ey.com/GL/en/Services/Advisory/Risk-appetite--the-strategic-balancing-act [Accessed 20 January 2017].

Financial Regulatory Reform Steering Committee. 2013. *Implementing a twin peaks model of financial regulation in South Africa.* Retrieved from http://www.treasury.gov.za/twinpeaks/20131211%20-%20Item%203%20Roadmap.pdf [Accessed 20 January 2014].

Flick, U. 2015. *Introducing research methodology: A beginner's guide to doing a research project*. Second edition. Thousand Oaks, CA: Sage.

Fraser, J. & Simkins, B.J. 2011. *Enterprise risk management.* Hoboken, NJ: Wiley.

FSB (Financial Stability Board). 2013. *Principles for an effective risk appetite framework.* Retrieved from http://www.fsb.org/wp-content/uploads/r_131118.pdf [Accessed 20 January 2014].

FSB (Financial Stability Board). 2014. *Guidance on supervisory interaction with financial institutions on risk culture: A framework for assessing risk culture.* Retrieved from http://www.fsb.org/wp-content/uploads/140407.pdf [Accessed 1 February 2016].

Gardener, E.P.M. & Ayling, D.E. 1984. Operational approaches to risk management in financial institutions: A technique for commercial banks. *Managerial Finance*, 10(1):15–19.

Ghosh, A. 2012. *Managing risks in commercial and retail banking.* Singapore: Wiley.

Gill, J. & Johnson, P. 2010. *Research methods for managers.* Fourth edition. London: Sage.

Girling, P. 2013. *Operational risk management: A complete guide to a successful operational risk framework*. Hoboken, NJ: Wiley.

Goldstein, R. & McElligott, J. 2014. *Risk appetite: A discussion paper.* Central Bank of Ireland. Retrieved from https://www.centralbank.ie/docs/default-source/publications/discussion-paper-4/risk-appetite-paper.pdf?sfvrsn=2 [Accessed 1 February 2016].

Gorzeń-Mitka, I. & Wieczorek-Kosmala, M. 2013. *Risk appetite: Critical element of enterprise risk management process.* Retrieved from http://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.desklight-58053b7c-de88-4ab9-9276-c768a9448f90 [Accessed 20 January 2014].

Govindarajan, D. 2011. *Corporate risk appetite: Ensuring board and senior management accountability for risk*. ICMA Centre discussion papers in finance, DP2011-22. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1962126 [Accessed 8 November 2013].

Grody, A.D. & Hughes, P.J. 2008. Financial services in crisis: Operational risk management to the rescue! *Journal of Risk Management in Financial Institutions*, 2(1):47–56.

Hannoun, H. 2010. *The Basel III Capital Framework: A decisive breakthrough.* Bank for International Settlements. Retrieved from http://www.bis.org/speeches/sp101125a.pdf [Accessed 16 October 2013].

Harmantzis, F.C. 2003. *Operational risk management in financial services and the new Basel Accord*. School of Technology Management, Stevens Institute of Technology. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=579321 [Accessed 20 January 2014].

Haubenstock, M. 2001. The evolving operational risk management framework. *The RMA Journal*, December 2001 – January 2002: 26–29. Retrieved from https://cms.rmau.org/uploadedFiles/Credit_Risk/Library/RMA_Journal/Operational_Risk_Topics/The%20Evolving%20Operational%20Risk%20Management%20Framework.pdf [Accessed 20 January 2014].

Heffernan, S. 2005. *Modern banking.* Chichester: Wiley.

Hendrikse, J.W. & Hefer-Hendrikse, L. 2012. *Corporate governance handbook: Principles and practices*. Second edition. Kenwyn, South Africa: Juta.

Hillson, D. 2012. *How much risk is too much risk? Understanding risk appetite.* Originally published as part of 2012 PMI Global Congress Proceedings, Marseille. Retrieved from http://www.risk-doctor.com/docs/ISS04%20Hillson%20Risk%20appetite%20paper.pdf [Accessed 14 October 2013].

Hillson, D. & Murray-Webster, R. 2011*. Shedding light on risk appetite: Using risk appetite and risk attitude to support appropriate risk-taking.* Risk Doctor & Lucidus Consulting. Retrieved from http://www.risk-doctor.com/docs/Risk%20Doctor-Lucidus%20white%20paper%20-%20Shedding%20Light%20on%20Risk%20Appetite%20110601.pdf [Accessed 14 October 2013].

IIF (Institute of International Finance). 2011. *Implementing robust risk appetite frameworks to strengthen financial institutions.* Retrieved from http://www.academia.edu/25713624/implementing_robust_risk_appetite_frameworks_to_strengthen_financial_institutions [Accessed 20 January 2014].

IIF (Institute of International Finance). 2012. *Governance for strengthening risk management.* Retrieved from https://www.theirm.org/media/1074222/IIF_Governance_for_Strengthened_Risk_Management_2012.pdf [Accessed 20 January 2014].

IIF (Institute of International Finance). 2013. *IIF response to FSB's principles for effective risk appetite framework.* Retrieved from http://www.fsb.org/wp-content/uploads/c_131011r.pdf [Accessed 20 January 2014].

IIF & EY (Institute of International Finance & Ernst & Young). 2016. *A set of blueprints for success: Seventh annual global EY/IIF bank risk management survey*. Retrieved from https://www.ey.com/Publication/vwLUAssets/ey-a-working-set-of-blueprints-to-deliver-sustainable-returns/$FILE/ey-a-working-set-of-blueprints-to-deliver-sustainable-returns.pdf [Accessed 20 January 2017].

Imeson, M. 2014. Conduct, reputation and control. *The Banker*, 2 January: 11–12. Retrieved from https://www.ey.com/Publication/vwLUAssets/The_Banker_January_2014_Special_Report_-_Transforming_the_Bank__Regulation_and_

Strategy/$FILE/EY-Banker-Special-Report-Jan-2014-Transforming-the-Bank-Regulation-and-Strategy.pdf [Accessed 1 February 2016].

IMF (International Monetary Fund). 2014. *South Africa: Financial system stability assessment.* IMF country report no. 14/340. Retrieved from https://www.imf.org/external/pubs/ft/scr/2014/cr14340.pdf [Accessed 1 February 2016].

IoDSA (Institute of Directors Southern Africa). 2002. *King Report on Governance for South Africa 2002.* Johannesburg.

IoDSA (Institute of Directors Southern Africa). 2009. *King Report on Governance for South Africa 2009.* Johannesburg.

IoDSA (Institute of Directors Southern Africa). 2016. *The King IV Report on Corporate Governance for South Africa*. Johannesburg.

IOR (The Institute of Operational Risk). 2009. *Risk appetite.* Institute of Operational Risk sound practice guidance paper. Retrieved from https://ior-institute.org/public/RiskAppetiteSPGVersion1.pdf [Accessed 29 September 2014].

IOR (The institute of Operational Risk). 2011. *Risk categorisation.* Institute of Operational Risk sound practice guidance paper. Retrieved from https://www.ior-institute.org/sound-practice-guidance/risk-categorisation [Accessed 27 March 2015].

IOR (The Institute of Operational Risk). 2012. *Risk appetite.* Institute of Operational Risk sound practice guidance. Retrieved from https://www.ior-institute.org/sound-practice-guidance/risk-appetite [Accessed 29 September 2014].

IOR (The Institute of Operational Risk). 2016. *Embedding an operational risk management framework.* Institute of Operational Risk sound practice guidance paper. Retrieved from https://www.ior-institute.org/sound-practice-guidance/embedding-an-operational-risk-management-framework [Accessed 16 November 2016].

IRM (The Institute of Risk Management). 2011. *Risk appetite and tolerance guidance paper.* Crowe Horwath Global Risk Consulting, Charterhouse Risk Management Ltd and the Institute of Risk Management. Retrieved from

https://www.theirm.org/media/3779216/64355_Riskapp_A4_web.pdf [Accessed 12 November 2013].

ISO (International Organization for Standardization). 2009. *ISO 31000: Risk management – Principles and guidelines.* ISO 31000:2009(E). Retrieved from http://ehss.moe.gov.ir/getattachment/56171e8f-2942-4cc6-8957-359f14963d7b/ISO-31000 [Accessed 14 October 2013].

Jednak, D. & Jednak, J. 2013. Operational risk management in financial institutions. *Management: Journal of Theory and Practice Management,* 66:71–80.

Jobst, A.A. 2010. The credit crisis and operational risk – implications for practitioners and regulators. *The Journal of Operational Risk*, 5(2):43–62.

Khan, M.I. 2015. Effects of operational risk management on financial institutions. *Journal of Business Strategies*, 9(1):83–105.

Knight, K.W. 2010. AS/NZS ISO 31000:2009 - The new standard for managing risk. *Keeping good companies*, 62(2): 68–69. Retrieved from https://search.informit.com.au/fullText;dn=142580477681767;res=IELBUS [Accessed 27 March 2015].

KPMG & EIU (Economist Intelligence Unit). 2013. *Expectations of risk management outpacing capabilities – it's time for action: Top eight risk management imperatives for the C-suite in 2013.* Retrieved from https://assets.kpmg.com/content/dam/kpmg/pdf/2013/08/expectations-risk-management-survey-v3.pdf [Accessed 27 March 2015].

Kubat, M. 2014. Does Basel III bring anything new? A comparison between capital accords Basel II and Basel III. In *Proceedings of the Second Economics & Finance Conference*, Vienna, 3 June, 337–355. Retrieved from https://www.iises.net/proceedings/2nd-economics-finance-conference-vienna/table-of-content?cid=4&iid=19&rid=1713.pdf [Accessed 2 February 2016].

Kulpa, W. & Magdoń, A. 2012. Operational-risk management in a bank. *Internal Auditing & Risk Management*, 7(4):35–50.

Kumar, R. 2011. *Research methodology: A step by step guide for beginners*. Third edition. London: Sage.

Leedy, P.D. & Ormrod, J. 2010. *Practical research: Planning and design*. Ninth edition. Upper Saddle River, NJ: Pearson Education, Merrill.

Maree, K. (Ed.). 2016. *First steps in research*. Second edition. Pretoria: Van Schaik.

Marsh, Nottingham University Business School & AIRMIC. 2009. *Research into the definition and application of the concept of risk appetite*. Retrieved from http://www.financialmutuals.org/files/files/definition%20and%20application%20of%20the%20concept%20of%20risk%20appetite.pdf [Accessed 27 March 2015].

Martin, H.M. 2009. Operational risk forum: As risk management evolves, is operational risk management important? *Journal of Operational Risk*, Winter 2009/2010, 4(4):75–84.

Matiş, E.A. 2009. Operational banking risk management – research performed at the Romanian Commercial Bank. *Economic Science Series*, 18(3):593–597.

McNally, J.S. 2013. *The 2013 COSO Framework & SOX compliance: One approach to an effective transition*. COSO. Retrieved from https://www.coso.org/documents/COSO%20McNallyTransition%20Article-Final%20COSO%20Version%20Proof_5-31-13.pdf [Accessed 13 November 2013].

Moore, S., Neville, C., Murphy, M. & Connolly, C. 2010. *The ultimate study skills handbook*. New York, NY: McGraw-Hill.

Moosa, I.A. 2007. *Operational risk management*. New York, NY: Palgrave Macmillan.

Nâstase, P. & Unchiaşu, S.F. 2013. Implications of the operational risk practices applied in the banking sector on the information systems area. *Accounting and Management Information Systems*, 12(1):101–117.

Pallant, J. 2011. *SPSS survival manual: A step by step guide to data analysis using SPSS*. Fourth edition. Crows Nest, N.S.W: Australia Allen & Unwin.

Pelzer, P. 2013. *Risk, risk management and regulation in the banking industry: The risk to come*. Oxon: Routledge.

Phillips, D.C. & Burbules, N.C. 2000. *Postpositivism and educational research: Philosophy, theory, and educational research series*. Lanham, MD: Rowman & Littlefield.

PRA (Prudential Regulation Authority). 2016. *A supervisory statement (SS5/16) on corporate governance: Board responsibilities*. Prudential Regulation Authority,

Bank of England. Retrieved from https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/supervisorystatement/2016/ss516.pdf?la=en&hash=FAC29DDE01AD00BF8E45222374D55F64468D18AE [Accessed 20 January 2017].

Protiviti. 2012. *Defining risk appetite. Early mover series: Integrating corporate performance management and risk management*. Retrieved from https://www.protiviti.com/sites/default/files/united_states/pov-defining-risk-appetite-protiviti.pdf [Accessed 27 March 2015].

Purdy, G. 2010. ISO 31000:2009: Setting a new standard for risk management. *Risk Analysis*, 30(6):881–886.

PwC. 2011. *Governance of risk.* Retrieved from https://www.pwc.co.za/en/assets/pdf/governance-of-risk.pdf [Accessed 27 March 2015].

PwC. 2014. *Operational risk appetite.* Retrieved from https://www.pwc.com/gx/en/banking-capital-markets/events/assets/pwc-operation-risk-appetite.pdf [Accessed 27 March 2015].

PwC. 2016. *A summary of the King IV Report on Corporate Governance for South Africa, 2016. King IV: An outcomes-based corporate governance code fit for a changing world*. Retrieved from http://www.pwc.co.za/en/assets/pdf/king-iv-steering-point.pdf [Accessed 2 February 2017].

PwC & IACPM. 2014. *Risk appetite frameworks: Insight into evolving global practices. An IACPM/PwC study.* Retrieved from http://iacpm.org/wp-content/uploads/2017/08/IACPMPwCRiskAppetiteFrameworksWhitePaper112014.pdf [Accessed 20 January 2017].

PwC & Strategy&. 2009. *A comprehensive risk appetite framework for banks.* Retrieved from https://www.strategyand.pwc.com/report/comprehensive-risk-appetite-framework-banks-2 [Accessed 13 November 2013].

Quail, R. 2012. Defining your taste for risk – ERM Framework: A new approach for articulating and managing risk appetite in your organisation. *Corporate Risk Canada*, Spring: 25–30. Retrieved from https://erm.ncsu.edu/az/erm/i/chan/library/338_Corporate_Risk_Canada_Risk_Appetite_2012.pdf [Accessed 27 March 2015].

RIMS (Risk and Insurance Management Society). 2012. *Exploring risk appetite and risk tolerance.* RIMS executive report: The risk perspective. Retrieved from https://www.rims.org/resources/ERM/Documents/RIMS_Exploring_Risk_Appetite_Risk_Tolerance_0412.pdf [Accessed 16 November 2016].

RIMS (Risk and Insurance Management Society). 2016. *The steps to successful risk taking: Developing effective risk appetite and tolerance statements.* RIMS executive report: The risk perspective. Retrieved from https://www.rims.org/RiskKnowledge/RISKKnowledgeDocs/2016-Developing_Risk_Appetite_Statements_452016_94337.pdf [Accessed 20 January 2017].

Rittenberg, L. & Martens, F. 2012. *Thought leadership in ERM. Enterprise risk management: Understanding and communicating risk appetite*. COSO. Retrieved from https://www.coso.org/Documents/ERM-Understanding-and-Communicating-Risk-Appetite.pdf [Accessed 12 November 2013].

Rosenthal, A. 2014. Bring your operational risk framework. *The RMA Journal*, 97(2):72–75.

RSA (Republic of South Africa). 2008. *Companies Act, no. 71, 2008*. Pretoria: Government Printer.

Salkind, N.J. 2012. *Exploring research.* Eight edition. Upper Saddle River. NJ: Pearson Education.

Sarafino, E.P. 2005. *Research methods: Using process and procedures of science to understand behavior.* Upper Saddle River, NJ: Pearson Education.

SARB (South African Reserve Bank). Government Gazette, No. 35880. (2012). Banks Amendment Bill. Minister of Finance, Parliament of the Republic of South Africa. Retrieved from https://juta.co.za/media/filestore/2012/12/b_43_-_2012_-_Banks_AB.pdf [Accessed 20 January 2014].

SARB (South African Reserve Bank). 2016. *South Africa's implementation of Basel II.* Retrieved from https://www.resbank.co.za/PrudentialAuthority/Deposit-takers/Banks/Supervision/Pages/South-Africa%27s-implementation-of-Basel-II-and-Basel-III.aspx [Accessed 2 February 2016].

SARB (South African Reserve Bank). 2018. *Compliance and operational risk.* Retrieved from https://www.resbank.co.za/Markets/ForeignReserves/RiskManagement/Pages/Compliance-and-operational-risk.aspx [Accessed 15 August 2018].

Saunders, M., Lewis, P. & Thornhill, A. 2012. *Research methods for business students*. Sixth edition. New York, NY: Pearson Education.

Saunders, M. & Tosey, P. 2012/2013. The layers of research design. *Academia, Rapport*, Winter 2012/2013:58–59. Retrieved from http://www.academia.edu/4107831/The_Layers_of_Research_Design [Accessed 10 January 2018].

Scandizzo, S. 2005. Risk mapping and key risk indicators in operational risk management. *Economic Notes: Review of Banking, Finance and Monetary Economics*, 34(2):231–256.

Scherbaum, C. & Shockley, K. 2015. *Analysing quantitative data for business and management students: Mastering business research methods.* Thousand Oaks. CA: Sage.

Schwartz Gârliste, M.A. 2013a. Operational risk – definition and regulations in banking. *Review of Management and Economic Engineering*, 12(1):173–188.

Schwartz Gârliste, M.A. 2013b. The operational risk management in banking – evolution of concepts and principles, Basel II challenges. *Review of International Comparative Management*, 14(1):165–174.

Sekaran, U. & Bougie, R. 2013. *Research methods for business: A skill-building approach.* Sixth edition. Chichester, UK: Wiley.

SSG (Senior Supervisors Group). 2010. *Observations on developments in risk appetite frameworks and IT infrastructure.* Retrieved from https://www.newyorkfed.org/medialibrary/media/newsevents/news/banking/2010/an101223.pdf [Accessed 20 January 2017].

Standards Australia/New Zealand. 2009. *AS/NZS ISO 31000:2009. Risk management – principles and guidelines.* Retrieved from https://infostore.saiglobal.com/preview/as/as30000/31000/31000-2009.pdf?sku=1378670 [Accessed 14 October 2013].

Strang, K.D. 2015. *The Palgrave handbook of research design in business and management.* New York, NY: Palgrave Macmillan.

Struwig, F.W. & Stead, G.B. 2013. *Research: Planning, designing and reporting.* Second edition. Cape Town: Pearson Education South Africa.

Sweeting, P. 2011. *Financial enterprise risk management*. Cambridge: Cambridge University Press.

Taylor, L. 2014. *Practical enterprise risk management: How to optimize business strategies through managed risk taking.* London, UK: Kogan Page.

Tchankova, T. 2002. Risk identification – basic stage in risk management. *Environmental Management and Health*, 13(3):290–297.

Teplý, P., Chalupka, R. & Černohorský, J. 2009. The importance of operational risk modeling for economic capital management in banking. In *Proceedings of the 12th International Conference on Finance & Banking: Structural & Regional Impacts of Financial Crises*, 1 January: 689–712. Retrieved from https://www.researchgate.net/publication/238749746_THE_IMPORTANCE_OF_OPERATIONAL_RISK_MODELING_FOR_ECONOMIC_CAPITAL_MANAGEMENT_IN_BANKING_1 [Accessed 14 October 2013].

The Hong Kong Institute of Bankers. 2013. *Operational risk management*. Singapore: Wiley.

Towers Watson. 2013. *Another bite at the apple: Risk appetite revisited.* Retrieved from https://cas.confex.com/cas/ica14/webprogram/Handout/Paper3284/Risk%20Revisited%20-%20handout.pdf [Accessed 27 March 2015].

Valsamakis, A.C., Vivian, R.W. & Du Toit, G.S. 2010. *Risk management.* Fourth edition. Sandton: Heinemann.

Wyman, O. 2007. *What's your risk appetite? How much risk do you want to take?* Oliver Wyman Limited. Retrieved from http://www.oliverwyman.com/content/dam/oliver-wyman/global/en/files/archive/2011/Risk_Appetite_CRC_0705.pdf [Accessed 14 October 2013].

Wyman, O. 2012. *Defining your risk appetite: The importance of taking a quantitative and qualitative approach*. Oliver Wyman Limited. Retrieved from http://www.oliverwyman.com/our-expertise/insights/2012/nov/defining-your-risk-appetite.html [Accessed 14 October 2013].

Young, J. 2010. Towards developing guiding principles for managing operational risk appetite. *Corporate Ownership & Control*, 8(1):176–187.

Young, J. 2012. The use of key risk indicators by banks as an operational risk management tool: A South African perspective. *Corporate Ownership & Control*, 9(3):172–185.

Young, J. 2014. *Operational risk management.* Second edition. Pretoria: Van Schaik.

Young, J. 2015. Guiding criteria for operational risk reporting in a corporate environment. *Corporate Ownership & Control*, 13(1):881–896.

APPENDIX A: RISK APPETITE QUESTIONNAIRE

Respondent no.			

Principles for an operational risk appetite framework for a bank: A South African perspective

Dear Risk owner/manager

Thank you for your willingness to participate in this survey. The purpose of the survey is to confirm management principles for an operational risk appetite framework in a bank. The survey should not take more than 15 minutes to complete. This is an anonymous and confidential survey. You cannot be identified and the answers you provide will be used for academic research purposes only. The following definitions are applicable in answering the questionnaire:

- Operational risk appetite is the amount of operational risks the bank is willing to accept or tolerate to achieve strategic objectives.
- An operational risk appetite framework is a framework of policies, statements and processes, which oversees the bank's appetite for operational risks.
- An operational risk appetite statement is a statement that indicates the operational risks the bank is willing to accept, tolerate or avoid, in order to achieve business objectives.

Please answer all questions by an "X" in the space provided. There are no correct or incorrect answers.

SECTION A: Biographic information

1. Please indicate your position at the bank

Top management (CEO, Board Director, Senior Management)	1	
Risk manager/officer	2	
Financial manager/officer	3	
Internal auditor	4	
Business unit manager	5	
Compliance officer	6	
Other (please specify)	7	

2. How many years' experience do you have in a banking environment?

0 - 1 year	1	
2 - 3 years	2	
4 - 5 years	3	
6 - 10 years	4	
More than 10 years	5	

3. How many years' experience do you have in operational risk management?

0 - 1 year	1	
2 - 3 years	2	
4 - 5 years	3	
6 - 10 years	4	
More than 10 years	5	

SECTION B: PRINCIPLES FOR AND THE IMPLEMENTATION OF AN OPERATIONAL RISK APPETITE FRAMEWORK

To what extend do you agree or disagree that the following are principles to manage an operational risk appetite framework and indicate to what extend the principles are applied in the bank you are affiliated to.

1 = Strongly Disagree (SD), 2 = Disagree (D), 3 = Neutral (N), 4 = Agree (A) and 5 = Strongly Agree (SA)

Mark your answer with an X in the appropriate box.

Question	Principle	1 SD	2 D	3 N	4 A	5 SA
4.a	An operational risk appetite framework should assist a bank with its strategic planning process to achieve business objectives.					
4.b	The operational risk appetite framework is considered in my bank's strategic planning process.					
5.a	The operational risk appetite framework informs decision-making throughout the bank.					
5.b	My bank's operational risk appetite framework informs decision-making.					
6.a	The bank should have a common risk language including the understanding of operational risk appetite.					
6.b	My bank has a common risk language which includes operational risk appetite.					
7.a	Operational risk appetite should be clearly defined throughout the bank.					

7.b	The operational risk appetite is clearly defined throughout the bank.					
8.a	An operational risk appetite definition should be included in an operational risk appetite framework.					
8.b	The operational risk appetite definition is included in the operational risk appetite framework of my bank.					
9.a	An operational risk appetite framework should include an operational risk appetite statement.					
9.b	My bank's operational risk appetite framework includes an operational risk appetite statement.					
10.a	The Board should approve the operational risk appetite statement.					
10.b	My bank's Board approves the operational risk appetite statement.					
11.a	Top management should submit the operational risk appetite statement to the Risk/Audit Committee for recommendation to the Board.					
11.b	My bank's top management is submitting the operational risk appetite statement to the Risk/Audit Committee for recommendation to the Board.					
12.a	The operational risk appetite statement should include quantitative expressions.					
12.b	My bank's operational risk appetite statement includes quantitative expressions.					
13.a	The operational risk appetite statement should include qualitative expressions.					
13.b	My bank's operational risk appetite statement includes qualitative expressions.					

14.a	To define an operational risk appetite statement should be a bottom-up process including the level where the risk exposure originated from.					
14.b	The operational risk appetite statement has been defined by means of a bottom-up process, which includes the level where the risk exposure originated from.					
15.a	The following operational risk methodologies should be used as an input to determine operational risk appetite:					
1.	Key Risk Indicators (KRI)					
2.	Loss data analysis/Incident management					
3.	Risk control self-assessment (RCSA)					
4.	Scenarios					
15.b	The following operational risk methodologies are used as an input to determine operational risk appetite in my bank:					
1.	Key Risk Indicators (KRI)					
2.	Loss data analysis/Incident management					
3.	Risk control self-assessment (RCSA)					
4.	Scenarios					
16.a	The operational risks should be managed within the approved limits of the operational risk appetite.					
16.b	The operational risks are managed within the approved limits of the operational risk appetite of my bank.					
17.a	Operational risks should continuously be monitored against the operational risk appetite statement.					

17.b	The operational risks are continuously monitored against the operational risk appetite statement in my bank.					
18.a	Operational risks should be monitored to ensure that it is managed according to the approved operational risk appetite statement.					
18.b	The operational risks are monitored to ensure that it is managed according to the approved operational risk appetite statement of my bank.					
19.a	Regular operational risk reporting should include the performance of the business compared to the tolerance levels of the operational risk appetite statement.					
19.b	The performance of the business is compared to the tolerance levels of the operational risk appetite statement included in operational risk reporting in my bank.					
20.a	Operational risk reporting should indicate how changes in the operational risk statement are managed.					
20.b	My bank's operational risk reporting indicates how the changes in the operational risk statement are managed.					

Thank you for taking part in this survey.
If you would like to receive a report on the findings, please email a request to the researcher.

Suné Maré
(mares@unisa.ac.za or 012 429 8222)

APPENDIX B: EMAIL COVER PAGE FOR QUESTIONNAIRE

Dear Prospective Participant,

My name is Miss Suné Maré, and I am conducting research with Prof Jackie Young in the Department of Finance, Risk Management and Banking towards an M.Com degree at the University of South Africa. We are inviting you to participate in a study entitled: **"*Principles for an operational risk appetite framework for a bank: A South African perspective*"**. The aim of the study is to establish a process/framework that can be used in determining a bank's operational risk appetite. In addition, the study attempts to investigate the principles needed to formulate a realistic operational risk appetite framework for a bank.

You were selected to participate in this survey because you are involved one way or another in the managing of operational risk exposures in a bank. By completing this survey, you agree that the information you provide may be used for research purposes in a dissertation and dissemination through peer-reviewed publications and conference proceedings.

It is anticipated that the information we gain from this survey may be used to simplify the process to determine a bank's operational risk appetite through its operational risk appetite framework. You are, however, under no obligation to complete the survey and you can withdraw from the study before submitting the survey. The survey is developed to be anonymous, meaning that we will have no way of connecting the information that you provide to you personally. If you choose to participate in this survey, it will take up no more than 15 minutes of your time. You will not benefit from your participation as an individual. We do not foresee that you will experience any negative consequences by completing the survey. The researcher(s) undertake to keep any information provided herein confidential, not to let it out of our possession and to report on the findings from the perspective of the participating group and not from the perspective of an individual.

The records will be kept for five years for audit purposes after that it will be permanently deleted from the hard drive of the computers of the researchers. You will not be reimbursed or receive any incentives for your participation in the survey.

The research was reviewed and approved by the Professional Research Committee. The primary researcher, Miss Suné Maré, can be contacted during office hours at mares@unisa.ac.za or 012 429 8222. Should you have concerns about the way in which the research has been conducted, you may contact the College Research Ethics Review Committee of the University of South Africa via email at engelm1@unisa.ac.za.

If you would like to participate in the survey, please open the attached document to complete the survey. You are free to withdraw from the study at any time.

Please save the document after completion and send back to mares@unisa.ac.za.

Thank you in advance for your time and participation.
Ethical clearance #: 2017_CEMS_DFRB_013

Regards

Suné Maré
Lecturer: Banking and Risk Management
Dept: Finance, Risk Management and Banking
University of South Africa
AJHvdWalt 5-115
☎: +27 (0) 12 429 8222
: +27 (0) 86 641 4653
: mares@unisa.ac.za
UNISA

APPENDIX C: DIAGNOSTIC QUESTIONNAIRE

Introduction

Kindly complete the survey in order to evaluate the diagnostic statements below.

Diagnostic survey on the operational risk appetite framework questionnaire:

Please circle the number, which represents your opinion about the questionnaire on operational risk appetite.	**Strongly Disagree**	**Disagree**	**No opinion**	**Agree**	**Strongly Agree**
1. The objective of the survey is clear.	**1**	**2**	**3**	**4**	**5**
2. The survey is comprehensive in terms of the principles for an operational risk appetite framework within a bank.	**1**	**2**	**3**	**4**	**5**
3. The instructions to complete the survey are clear.	**1**	**2**	**3**	**4**	**5**
4. The survey is structured in a logical manner.	**1**	**2**	**3**	**4**	**5**
5. The statements are easy to understand.	**1**	**2**	**3**	**4**	**5**
6. The scale of the survey is appropriate.	**1**	**2**	**3**	**4**	**5**
7. Questions 4 to 18 cover the principles needed for an operational risk appetite framework.	**1**	**2**	**3**	**4**	**5**
8. The time in minutes required to complete the survey was …	**0-5**	**5-10**	**10-15**	**15-20**	**20>**
9. Are there any questions that you wish to add to or change in the survey?				**Yes**	**No**
If Yes, please indicate below:					

APPENDIX D: RELIABILITY CALCULATOR

Created by Del Siegle (del.siegle@uconn.edu) for EPSY 5601

Cronbach's Alpha	**0.956353531**
Split-Half (odd-even) Correlation	**0.793003678**
Spearman-Brown Prophecy	**0.88455332**
Mean for Test	**174.5333333**
Standard Deviation for Test	**17.14396557**
KR21	**3.074070929**
KR20	**3.08383244**

Questions	Participants
40	30

	Q4a	Q4b	Q5a	Q5b	Q6a	Q6b	Q7a	Q7b	Q8a	Q8b	Q9a	Q9b	Q10a	Q10b	Q11a	Q11b	Q12a	Q12b	Q13a	Q13b	Q14a	Q14b	Q15a.1	Q15a.2	Q15a.3	Q15a.4	Q15b.1	Q15.b.2	Q15b.3	Q15b.4	Q16a	Q16b	Q17a	Q17b	Q18a	Q18b	Q19a	Q19b	Q20a	Q20b
1	5	5	5	5	5	4	5	4	5	5	5	5	5	5	5	5	4	4	4	4	4	4	5	5	5	5	5	5	5	5	4	4	4	4	4	4	4	4	4	4
2	5	5	5	5	5	5	5	5	5	5	4	4	4	4	3	3	4	4	4	4	4	4	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	4	4	
3	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
4	5	4	5	5	5	4	5	4	5	4	5	4	5	4	5	4	5	4	5	4	5	4	5	5	5	5	4	4	4	4	4	4	5	4	5	4	5	4	5	4
5	5	5	5	5	5	4	5	4	5	5	5	5	5	5	5	5	5	5	5	5	4	4	5	5	5	5	5	5	5	5	5	5	5	5	5	4	4	5	5	
6	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
7	5	5	5	5	5	4	4	5	5	4	5	3	5	3	5	3	4	3	4	3	5	2	4	4	5	5	3	3	3	3	3	3	5	4	5	3	4	4	5	4
8	4	4	4	4	5	2	5	3	5	3	3	3	4	4	4	3	4	3	4	4	2	4	4	4	4	4	4	2	2	2	4	4	4	4	4	4	4	4	4	4
9	4	2	2	3	3	3	4	2	4	3	5	4	4	4	4	4	4	3	4	3	4	3	5	5	5	5	5	4	5	5	5	5	4	4	4	4	4	4	4	3
10	5	5	5	4	4	4	5	4	5	5	5	5	5	5	5	5	4	4	4	4	4	4	5	5	5	5	5	4	5	5	5	4	5	4	5	4	5	4	5	4
11	5	4	4	4	5	5	5	4	5	5	5	5	5	5	5	5	5	5	5	5	4	4	5	5	5	5	4	4	4	4	5	4	5	4	5	4	5	5	5	4

12	5	4	4	3	5	4	5	2	5	4	4	2	5	3	5	3	4	4	4	4	4	4	4	4	4	3	3	3	3	4	3	4	3	4	3	4	3	4	3
13	5	5	5	5	4	5	5	3	5	4	5	4	5	4	5	4	4	4	4	3	5	4	5	5	5	5	4	4	4	4	5	4	5	5	5	5	5	5	4
14	4	4	3	3	4	4	5	4	4	4	5	4	4	3	4	4	5	5	5	5	5	4	4	5	5	5	2	5	2	5	5	4	5	5	5	4	5	4	4
15	5	4	4	4	4	4	4	4	4	3	4	3	4	3	4	3	4	3	4	3	4	3	5	5	5	5	3	3	3	3	4	3	5	3	5	3	5	3	5	3
16	5	4	4	4	5	4	5	4	5	5	4	4	5	4	5	4	4	4	4	4	3	3	5	5	5	5	5	5	5	5	5	5	5	5	5	5	4	4	4	4
17	4	4	2	3	4	3	4	3	4	3	4	3	4	4	4	4	4	4	4	4	5	3	4	5	2	4	3	3	3	3	4	3	4	3	4	3	4	3	4	3
18	5	3	3	4	5	4	4	2	4	3	2	2	4	3	5	5	4	4	4	4	5	3	4	4	4	4	4	5	4	5	1	1	4	4	4	4	5	5	4	4
19	5	4	4	4	4	4	4	4	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	4
20	5	5	4	4	5	5	5	5	5	5	5	5	4	4	5	5	5	4	4	4	4	5	5	5	5	4	5	4	4	4	4	4	4	4	5	5	5	4	4	4
21	5	4	2	3	5	4	5	4	5	3	5	3	5	3	5	3	5	3	5	3	5	3	5	5	5	5	3	3	3	3	5	4	5	3	5	3	5	3	5	3
22	5	4	5	4	5	3	5	3	5	4	5	5	5	5	5	5	5	5	5	5	5	4	5	5	5	5	5	5	5	5	5	4	5	4	5	4	5	4	5	3
23	5	5	5	5	5	5	5	4	5	5	5	5	5	5	5	5	5	5	5	5	5	3	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	3	5	3
24	5	5	4	4	5	3	4	3	4	4	4	4	4	3	4	3	4	4	4	4	4	3	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	3	4	4
25	5	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
26	4	4	3	4	5	3	5	3	5	3	4	4	5	4	5	5	4	5	5	5	5	2	4	4	2	4	4	4	4	3	2	4	2	5	5	5	5	4	5
27	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
28	5	4	4	5	5	5	5	5	5	4	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	4	5	4	5	5	5	5	5	5	5	5	5	5
29	5	5	5	5	5	5	5	4	5	5	5	5	5	5	5	5	5	5	5	5	5	4	4	5	5	5	5	5	5	5	5	5	5	5	5	4	4	5	4
30	5	5	5	5	5	5	5	4	5	5	5	5	3	3	5	5	5	5	5	5	3	3	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	4	4

APPENDIX E: ETHICAL CLEARANCE CERTIFICATE

UNISA university of south africa

FINANCE, RISK MANAGEMENT & BANKING RESEARCH ETHICS REVIEW COMMITTEE

23 August 2017

Ref #: 2017/CEMS/DFRB/013
Name of applicant: Ms S Mare
Student #: 55516106
Supervisor: Prof Young
Staff #: 90074904

Dear Ms Mare

Decision: Ethics Approval

Name: Ms S Mare,mares@unisa.ac.za

Supervisor: Prof J Young, Youngj@unisa.ac.za, 012 429 3010

Proposal: A critical analysis of operational risk appetite for the banking industry in South Africa

Qualification: MCOM

Thank you for the application for research ethics clearance by the Department of Finance, Risk Management and Banking Research Ethics Review Committee for the above mentioned research. Final approval is granted for the duration of the project.

For full approval: The application was reviewed in compliance with the Unisa Policy on Research Ethics by the DFRB RERC 23 August 2017.

The proposed research may now commence with the proviso that:

1) The researcher/s will ensure that the research project adheres to the values and principles expressed in the UNISA Policy on Research Ethics.
2) Any adverse circumstance arising in the undertaking of the research project that is relevant to the ethicality of the study, as well as changes in the methodology, should be communicated in writing to the department of Finance, Risk Management and Banking Ethics Review Committee. An amended application could be requested if there are substantial changes from the existing proposal,

Open Rubric

University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

especially if those changes affect any of the study-related risks for the research participants.

3) The researcher will ensure that the research project adheres to any applicable national legislation, professional codes of conduct, institutional guidelines and scientific standards relevant to the specific field of study.

Note:

The reference number 2017/CEMS/DFRB/013 should be clearly indicated on all forms of communication [e.g. Webmail, E-mail messages, letters] with the intended research participants, as well as with the [DFRB] RERC.

Kind regards,

Mr Gerhard Grebe
Chairperson: DFRB Research Ethics Review Committee
0124296723/grebegpm@unisa.ac.za

Prof Thomas Mogale
Executive Dean: CEMS

University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

APPENDIX F: CONFIDENTIALITY AGREEMENT STATISTICIAN

This is to certify that I, Dion van Zyl, the statistician of the research project ***"Principles for an operational risk appetite framework for a bank: A South African perspective",*** agrees to the responsibilities of the administration, analysing and capturing of completed questionnaires from participants for data analysis (and additional tasks the researcher(s) may require in my capacity as statistician). I acknowledge that the research project is/are conducted by Suné Maré and Prof Jackie Young of the Department of Finance, Risk Management and Banking, University of South Africa.

I understand that any information (written, verbal or any other form) obtained during the performance of my duties must remain confidential and in line with the UNISA Policy on Research Ethics. This includes all information about participants, their employees/their employers/their organisation, as well as any other information.

I understand that any unauthorised release or carelessness in the handling of this confidential information is considered a breach of the duty to maintain confidentiality.

I further understand that any breach of the duty to maintain confidentiality could be grounds for immediate dismissal and possible liability in any legal action arising from such breach.

Full Name of Statistician: Dion van Zyl

Signature of Statistician: 

Address of statistician: 888 29th Avenue, Rietfontein, Pretoria

Statistical Company: Private

Any Job/reference number: N/A

Full Name of Primary Researcher: Suné Maré

Signature of Primary Researcher:  Date: 13/09/2018

APPENDIX G: DESCRIPTIVE STATISTICS

Q1 1. Position at the bank.

	Frequency	Per cent
1 Top management (CEO, Board Director, Senior Management)	5	16.7
2 Risk manager/officer	13	43.3
4 Internal auditor	2	6.7
5 Business manager	2	6.7
7 Risk consultant	5	16.7
8 Risk analyst	3	10.0
Total	30	100.0

Q2 2. How many years' experience do you have in a banking environment?

	Frequency	Per cent
1 0 - 1 year	2	6.7
2 2 - 3 years	1	3.3
3 4 - 5 years	3	10.0
4 6 - 10 years	5	16.7
5 More than ten years	19	63.3
Total	30	100.0

Q3 3. How many years' experience do you have in operational risk management?

	Frequency	Per cent
1 0 - 1 year	3	10.0
2 2 - 3 years	3	10.0
3 4 - 5 years	8	26.7
4 6 - 10 years	7	23.3
5 More than ten years	9	30.0
Total	30	100.0

Q4a An operational risk appetite framework should assist a bank with its strategic planning process to achieve business objectives.

	Frequency	Per cent
4 Agree	6	20.0
5 Strongly agree	24	80.0
Total	30	100.0

Q4b The operational risk appetite framework is considered in my bank's strategic planning process.

	Frequency	Per cent
2 Disagree	1	3.3
3 Neutral	1	3.3
4 Agree	15	50.0
5 Strongly agree	13	43.3
Total	30	100.0

Q5a The operational risk appetite framework informs decision-making throughout the bank.

	Frequency	Per cent
2 Disagree	3	10.0
3 Neutral	3	10.0
4 Agree	11	36.7
5 Strongly agree	13	43.3
Total	30	100.0

Q5b My bank's operational risk appetite framework informs decision-making.

	Frequency	Per cent
3 Neutral	5	16.7
4 Agree	13	43.3
5 Strongly agree	12	40.0
Total	30	100.0

Q6a The bank should have a common risk language including the understanding of operational risk appetite.

	Frequency	Per cent
3 Neutral	1	3.3
4 Agree	8	26.7
5 Strongly agree	21	70.0
Total	30	100.0

Q6b My bank has a common risk language which includes operational risk appetite.

	Frequency	Per cent
2 Disagree	1	3.3
3 Neutral	5	16.7
4 Agree	14	46.7
5 Strongly agree	10	33.3
Total	30	100.0

Q7a Operational risk appetite should be clearly defined throughout the bank.

	Frequency	Per cent
4 Agree	9	30.0
5 Strongly agree	21	70.0
Total	30	100.0

Q7b The operational risk appetite is clearly defined throughout the bank.

	Frequency	Per cent
2 Disagree	3	10.0
3 Neutral	6	20.0
4 Agree	15	50.0
5 Strongly agree	6	20.0
Total	30	100.0

Q8a An operational risk appetite definition should be included in an operational risk appetite framework.

	Frequency	Per cent
4 Agree	8	26.7
5 Strongly agree	22	73.3
Total	30	100.0

Q8b The operational risk appetite definition is included in the operational risk appetite framework of my bank.

	Frequency	Per cent
3 Neutral	7	23.3
4 Agree	10	33.3
5 Strongly agree	13	43.3
Total	30	100.0

Q9a An operational risk appetite framework should include an operational risk appetite statement.

	Frequency	Per cent
2 Disagree	1	3.3
3 Neutral	1	3.3
4 Agree	9	30.0
5 Strongly agree	19	63.3
Total	30	100.0

Q9b My bank's operational risk appetite framework includes an operational risk appetite statement.

	Frequency	Per cent
2 Disagree	2	6.7
3 Neutral	5	16.7
4 Agree	10	33.3
5 Strongly agree	13	43.3
Total	30	100.0

Q10a The Board should approve the operational risk appetite statement.

	Frequency	Per cent
3 Neutral	1	3.3
4 Agree	11	36.7
5 Strongly agree	18	60.0
Total	30	100.0

Q10b My bank's Board approves the operational risk appetite statement.

	Frequency	Per cent
3 Neutral	8	26.7
4 Agree	11	36.7
5 Strongly agree	11	36.7
Total	30	100.0

Q11a Top management should submit the operational risk appetite statement to the Risk/Audit Committee for recommendation to the Board.

	Frequency	Per cent
3 Neutral	1	3.3
4 Agree	8	26.7
5 Strongly agree	21	70.0
Total	30	100.0

Q11b My bank's top management submits the operational risk appetite statement to the Risk/Audit Committee for recommendation to the Board.

	Frequency	Per cent
3 Neutral	7	23.3
4 Agree	8	26.7
5 Strongly agree	15	50.0
Total	30	100.0

Q12a The operational risk appetite statement should include quantitative expressions.

	Frequency	Per cent
4 Agree	16	53.3
5 Strongly agree	14	46.7
Total	30	100.0

Q12b My bank's operational risk appetite statement includes quantitative expressions.

	Frequency	Per cent
3 Neutral	5	16.7
4 Agree	13	43.3
5 Strongly agree	12	40.0
Total	30	100.0

Q13a The operational risk appetite statement should include qualitative expressions.

	Frequency	Per cent
4 Agree	16	53.3
5 Strongly agree	14	46.7
Total	30	100.0

Q13b My bank's operational risk appetite statement includes qualitative expressions.

	Frequency	Per cent
3 Neutral	5	16.7
4 Agree	13	43.3
5 Strongly agree	12	40.0
Total	30	100.0

Q14a To define an operational risk appetite statement should be a bottom-up process including the level where the risk exposure originated from.

	Frequency	Per cent
2 Disagree	1	3.3
3 Neutral	2	6.7
4 Agree	13	43.3
5 Strongly agree	14	46.7
Total	30	100.0

Q14b The operational risk appetite statement has been defined by means of a bottom-up process, which includes the level where the risk exposure originated from.

	Frequency	Per cent
2 Disagree	2	6.7
3 Neutral	9	30.0
4 Agree	14	46.7
5 Strongly agree	5	16.7
Total	30	100.0

Q15a.1 The following operational risk methodologies should be used as an input to determine operational risk appetite: Key Risk Indicators (KRI)

	Frequency	Per cent
4 Agree	10	33.3
5 Strongly agree	20	66.7
Total	30	100.0

Q15a.2 The following operational risk methodologies should be used as an input to determine operational risk appetite: Loss data analysis/Incident management

	Frequency	Per cent
4 Agree	8	26.7
5 Strongly agree	22	73.3
Total	30	100.0

Q15a.3 The following operational risk methodologies should be used as an input to determine operational risk appetite: Risk control self-assessment (RCSA)

	Frequency	Per cent
2 Disagree	2	6.7
4 Agree	6	20.0
5 Strongly agree	22	73.3
Total	30	100.0

Q15a.4 The following operational risk methodologies should be used as an input to determine operational risk appetite: Scenarios

	Frequency	Per cent
4 Agree	9	30.0
5 Strongly agree	21	70.0
Total	30	100.0

Q15b.1 The following operational risk methodologies are used as an input to determine the operational risk appetite in my bank: Key Risk Indicators (KRI)

	Frequency	Per cent
2 Disagree	1	3.3
3 Neutral	5	16.7
4 Agree	9	30.0
5 Strongly agree	15	50.0
Total	30	100.0

Q15b.2 The following operational risk methodologies are used as an input to determine operational risk appetite in my bank: Loss data analysis/Incident management

	Frequency	Per cent
2 Disagree	1	3.3
3 Neutral	5	16.7
4 Agree	11	36.7
5 Strongly agree	13	43.3
Total	30	100.0

Q15b.3 The following operational risk methodologies are used as an input to determine operational risk appetite in my bank: Risk control self-assessment (RCSA)

	Frequency	Per cent
2 Disagree	2	6.7
3 Neutral	5	16.7
4 Agree	9	30.0
5 Strongly agree	14	46.7
Total	30	100.0

Q15b.4 The following operational risk methodologies are used as an input to determine operational risk appetite in my bank: Scenarios

	Frequency	Per cent
2 Disagree	1	3.3
3 Neutral	6	20.0
4 Agree	8	26.7
5 Strongly agree	15	50.0
Total	30	100.0

Q16a The operational risks should be managed within the approved limits of the operational risk appetite.

	Frequency	Per cent
1 Strongly disagree	1	3.3
2 Disagree	1	3.3
3 Neutral	1	3.3
4 Agree	10	33.3
5 Strongly agree	17	56.7
Total	30	100.0

Q16b The operational risks are managed within the approved limits of the operational risk appetite of my bank.

	Frequency	Per cent
1 Strongly disagree	1	3.3
3 Neutral	4	13.3
4 Agree	14	46.7
5 Strongly agree	11	36.7
Total	30	100.0

Q17a Operational risks should continuously be monitored against the operational risk appetite statement.

	Frequency	Per cent
2 Disagree	1	3.3
4 Agree	10	33.3
5 Strongly agree	19	63.3
Total	30	100.0

Q17b The operational risks are continuously monitored against the operational risk appetite statement in my bank.

	Frequency	Per cent
3 Neutral	4	13.3
4 Agree	13	43.3
5 Strongly agree	13	43.3
Total	30	100.0

Q18a Operational risks should be monitored to ensure that it is managed according to the approved operational risk appetite statement.

	Frequency	Per cent
4 Agree	9	30.0
5 Strongly agree	21	70.0
Total	30	100.0

Q18b The operational risks are monitored to ensure that it is managed according to the approved operational risk appetite statement of my bank.

	Frequency	Per cent
3 Neutral	5	16.7
4 Agree	12	40.0
5 Strongly agree	13	43.3
Total	30	100.0

Q19a Regular operational risk reporting should include the performance of the business compared to the tolerance levels of the operational risk appetite statement.

	Frequency	Per cent
4 Agree	12	40.0
5 Strongly agree	18	60.0
Total	30	100.0

Q19b The performance of the business is compared to the tolerance levels of the operational risk appetite statement included in operational risk reporting in my bank.

	Frequency	Per cent
3 Neutral	6	20.0
4 Agree	14	46.7
5 Strongly agree	10	33.3
Total	30	100.0

Q20a Operational risk reporting should indicate how changes in the operational risk appetite statement are managed.

	Frequency	Per cent
4 Agree	14	46.7
5 Strongly agree	16	53.3
Total	30	100.0

Q20b My bank’s operational risk reporting indicates how the changes in the operational risk appetite statement are managed.

	Frequency	Per cent
3 Neutral	7	23.3
4 Agree	18	60.0
5 Strongly agree	5	16.7
Total	30	100.0

APPENDIX H: CORRELATION COEFFICIENTS

	Question 4B: The operational risk appetite framework is considered in my bank's strategic planning process.	Significance
Question 4A: An operational risk appetite framework should assist a bank with its strategic planning process to achieve business objectives.	0.454*	0.012

	Question 5B My bank's operational risk appetite framework informs decision-making.	Significance
Question 5A The operational risk appetite framework informs decision-making throughout the bank.	0.836**	0.000

	Question 6B My bank has a common risk language which includes operational risk appetite.	Significance
Question 6A The bank should have a common risk language including the understanding of operational risk appetite.	0.249	0.184

	Question 7B Operational risk appetite should be clearly defined throughout the bank	Significance
Question 7A Operational risk appetite should be clearly defined throughout the bank.	0.245	0.192

	Question 8B The operational risk appetite definition is included in the operational risk appetite framework of my bank.	Significance
Question 8A An operational risk appetite definition should be included in an operational risk appetite framework.	0.542**	0.002

	Question 9B My bank's operational risk appetite framework includes an operational risk appetite statement.	Significance
Question 9A An operational risk appetite framework should include an operational risk appetite statement.	0.684**	0.000

	Question 10B My bank's Board approves the operational risk appetite statement.	Significance
Question 10A The Board should approve the operational risk appetite statement.	0.561**	0.0001

	Question 11B My bank's top management submits the operational risk appetite statement to the Risk/Audit Committee for recommendation to the Board.	Significance
Question 11A Top management should submit the operational risk appetite statement to the Risk/Audit Committee for recommendation to the Board.	0.611**	0.0000

	Question 12B My bank's operational risk appetite statement includes quantitative expressions.	Significance
Question 12A The operational risk appetite statement should include quantitative expressions.	0.665**	0.000

	Question 13B My bank's operational risk appetite statement includes qualitative expressions.	Significance
Question 13A The operational risk appetite statement should include qualitative expressions.	0.770**	0.000

	Question 14B The operational risk appetite statement has been defined by means of a bottom-up process, which includes the level where the risk exposure originated from.	Significance
Question 14A To define an operational risk appetite statement should be a bottom-up process including the level where the risk exposure originated from.	0.053	0.780

	Question 15B.1 Key Risk Indicators (KRI) are used as an input to determine the operational risk appetite in my bank.	Significance
Question 15A.1 Key Risk Indicators (KRI) should be used as an input to determine operational risk appetite.	0.676**	0.000

	Question 15B.2 Loss data analysis/Incident management is used as an input to determine operational risk appetite in my bank.	Significance
Question 15A.2 Loss data analysis/Incident management should be used as an input to determine operational risk appetite.	0.402*	0.027

	Question 15B.3 Risk control self-assessment (RCSA) is used as an input to determine the operational risk appetite in my bank.	Significance
Question 15A.3 Risk control self-assessment (RCSA) should be used as an input to determine operational risk appetite.	0.489**	0.006

	Question 15B.4 Scenarios are used as an input to determine the operational risk appetite in my bank.	Significance
Question 15A.4 Scenarios should be used as an input to determine operational risk appetite.	0.511**	0.004

	Question 16B The operational risks are managed within the approved limits of the operational risk appetite of my bank.	Significance
Question 16A The operational risks should be managed within the approved limits of the operational risk appetite.	0.744**	0.000

	Question 17B The operational risks are continuously monitored against the operational risk appetite statement in my bank.	Significance
Question 17A Operational risks should continuously be monitored against the operational risk appetite statement.	0.421*	0.020

	Question 18B The operational risks are monitored to ensure that it is managed according to the approved operational risk appetite statement of my bank.	Significance
Question 18A Operational risks should be monitored to ensure that it is managed according to the approved operational risk appetite statement.	0.483**	0.007

	Question 19B The performance of the business is compared to the tolerance levels of the operational risk appetite statement included in operational risk reporting in my bank.	Significance
Question 19A Regular operational risk reporting should include the performance of the business compared to the tolerance levels of the operational risk appetite statement.	0.459*	0.011

	Question 20B My bank's operational risk reporting indicates how the changes in the operational risk appetite statement are managed.	Significance
Question 20A Operational risk reporting should indicate how changes in the operational risk appetite statement are managed.	0.106	0.578

APPENDIX I: CHECKLIST

Principles for an Operational Risk Appetite Framework

Nr.	Principles for an operational risk appetite framework	Checkmark (√) the appropriate column	
		Yes	No
1	An operational risk appetite framework should inform decision-making throughout the organisation.		
2	An operational risk appetite framework should assist with an organisation's strategic planning process and the achievement of objectives.		
3	An operational risk appetite framework should include a formal definition of operational risk appetite.		
4	An operational risk appetite framework should define operational risk appetite that is understood and accepted throughout the bank.		
5	An operational risk appetite framework should support the implementation of a common risk language throughout the organisation including the understanding of operational risk appetite.		
6	An operational risk appetite framework should include an operational risk appetite statement.		
7	An operational risk appetite framework should include the process of the board to approve the operational risk appetite statement.		
8	An operational risk appetite framework should include the practice of a bank's top management submitting the operational risk appetite statement to the risk or audit committee for recommendation to the board.		
9	An operational risk appetite framework should indicate how an operational risk appetite statement must be defined from a bottom-up process, which includes the level where the risk exposure originated.		
10	An operational risk appetite framework should have an operational risk appetite statement expressed in qualitative terms.		

11	An operational risk appetite framework should have an operational risk appetite statement expressed in quantitative measures.		
12	An operational risk appetite framework should contain the different metrics/measures used to determine an organisation's operational risk appetite and tolerance namely, Key Risk Indicators (KRIs), loss data analysis or incident management, Risk Control Self-Assessments (RCSA) and scenarios.		
13	An operational risk appetite framework should indicate the approved operational risk appetite limits to ensure that operational risks are managed within the limits of the organisation.		
14	An operational risk appetite framework should include the monitoring of operational risks to ensure that it is managed against the organisation's approved operational risk appetite statement.		
15	An operational risk appetite framework should include a process where operational risks are continuously monitored against the operational risk appetite statement.		
16	An operational risk appetite framework should include a reporting process on how changes in the operational risk appetite statement are managed within the organisation.		
17	An operational risk appetite framework should include a process for the regular reporting of the performance of the business compared to the tolerance levels of the operational risk appetite statement.		