OPERATIONAL RISK MANAGEMENT IN THE SHORT-TERM INSURANCE INDUSTRY AND RISK BASED CAPITAL

RESEARCH REPORT: MBL3

A Research Report

presented to the

Graduate School of Business Leadership

University of South Africa

In partial fulfilment of the

requirements for the

MASTERS DEGREE IN BUSINESS LEADERSHIP,

UNIVERSITY OF SOUTH AFRICA

By

M C LE ROUX
STUDENT NUMBER 7176-843-2
22nd November 2010

ABSTRACT

Operational risk management has been identified as one of the primary risk types that short-term insurance companies will have to deal with on a rigorous basis in the future. The implied future importance of operational risk management to short-term insurance companies has come about due to the South African Financial Services Board's decision to develop and institute a new solvency regime for the South African short-term insurance industry.

The South African Financial Services Board has decided to implement a risk based capital approach to insurance company solvency requirements in line with approaches adopted in the European Union. The new proposed risk based capital solvency requirements are being designed to ensure that insurers have sufficient capital to withstand adverse events, both in terms of insurance risk, as well as in terms of economic, market and operational risk. A key divergence from the current capital regime is that under a risk based capital approach insurers will have to put rigorous risk management strategies into practice and to consider all the risks that may affect their business, including operational risks, and not only the underwriting risks.

Under the current solvency regime many insurance companies pay scant attention to operational risk. Solvency Assessment and Management aims to create a more realistic measure of solvency capital requirements based on all the risks an insurer faces, including all categories of risk and in particular bringing in the effect of operational risk.

In light of the above, this study, which consists of a literature review as well as experiential research in the form of a survey, was conducted:

- To identify and present the various elements, practices, processes, techniques and methods that can and should be recognised, considered and employed by insurers in terms of their operational risk management programmes.
- To investigate insurers current approaches, as well as their recommended views, towards the recognition, consideration and use of various elements, practices, processes, techniques and methods employed in operational risk management

practice.

- To investigate whether insurers approaches and views towards operational risk management, and their recognition, consideration and use of various elements, practices, processes, techniques and methods employed in operational risk management are being significantly altered by the current importance being attached to operational risk management as part of the requirements of the Solvency Assessment and Management risk based capital regime being implemented in 2014.

The literature review delineated operational risk as being the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events; and operational risk management as consisting of a continuing process of operational risk identification; measurement and evaluation; mitigation and control; and monitoring and reporting by means of various practices, processes, techniques and methods of operational risk management.

The results of the research indicate that insurers approaches and views towards operational risk management, and their recognition, consideration and use of various elements, practices, processes, techniques and methods employed in operational risk management are being significantly altered. In the majority of instances, insurers current approaches towards the recognition, consideration and use of various elements, practices, processes, techniques and methods employed in operational risk management practice differed significantly from their recommended views. It is this author's opinion that a major contributor to this phenomenon is the current importance being attached to operational risk management as part of the requirements of the Solvency Assessment and Management risk based capital regime being implemented in 2014.

Due to operational risk management in the short-term insurance industry being a relatively new concept still in a developmental stage, it is this author's opinion that this study could assist short-term insurers with founding formal operational risk management processes and programmes within their organisations, and key recommendations are:

- A structured approach to operational risk management should be instituted by short-term insurers.
- In line with a structured approach, the framework, practices, processes, techniques and methods identified and described by this study should be implemented by short-term insurers in designing and instituting their own operational risk management programmes.
- The adoption / institution of a structured, formalized operational risk management programme / processes should be commenced as soon as possible so that insurers can begin managing the operational risks inherent in their businesses to an optimal level.
- The adoption / institution of a structured, formalized operational risk management programme / processes should be commenced as soon as possible so as to integrate operational risk management processes and practices as well as an operational risk management culture into insurers businesses well in advance of the implementation of the SAM risk based capital regime.
- The adoption / institution of a structured, formalized operational risk management programme / processes should be commenced as soon as possible so that insurers are in a position to comply regulatorily with the pending SAM risk based capital regime which is being implemented on the 01st of January 2014.
- The adoption / institution of a structured, formalized operational risk management programme / processes should be commenced as soon as possible so that insurers have practiced, embedded and integrated structured operational risk management processes and practices into their businesses to such a degree that they are able to completely satisfy the regulator's (FSB) requirement of the insurer's operational risk management programme passing a "use" test at the time of the introduction of the SAM risk based capital regime on the 01st of January 2014.

The main recommendation for further study emanating from the research is for research to be conducted on insurers approaches towards operational risk management at the time of the Solvency Assessment and Management regime implementation on 01st January 2014, to assess their levels of institutionalization of formal operational risk management programmes at the time.

ACKNOWLEDGEMENTS

I wish to express my sincere gratitude and acknowledgements to the following:

- To Chanine and Daryl, thank you for your patience, understanding and support.
- To my late father, Martin, who unfortunately did not live to see the completion of my studies.
- To all of the people who made the completion of this Research Report possible through giving of their valuable time and input in answering questionnaires and participating in personal interviews.
- To Stephen Ndlovu, my Research Report Supervisor.

STATEMENT

It is hereby certified that the Research Report on:

"OPERATIONAL RISK MANAGEMENT IN THE SHORT-TERM INSURANCE INDUSTRY AND RISK BASED CAPITAL" is my own work and that all references have been acknowledged under the references section.

Signed:.....

M C Le Roux

Date:

Table of Contents

List of Tables

List of Figures

1 CHAPTER 1: ORIENTATION

1.1 Introduction

The South African Financial Services Board is in the process of developing and instituting a new solvency regime for the South African short-term insurance industry, to be in line with international standards. The South African Financial Services Board has decided to implement a risk based capital approach to insurance company solvency requirements in line with approaches adopted in the European Union.

Solvency capital requirements imposed by financial regulators mainly serve the following purposes:

- To reduce the risk that an insurer would be unable to meet claims.
- To reduce the losses suffered by policyholders in the event that a firm is unable to meet all claims fully.
- To provide supervisors early warning so that they can intervene promptly if capital falls below the required level.
- To promote confidence in the financial stability of the insurance sector.
- To ensure the financial stability of insurance companies.

Currently, South African short-term insurers are required to hold capital equal to 25% of their net written premiums. This is governed by the South African Short Term Insurance Act of 1998. The Short-Term Insurance Act, 1998 (Act No. 53 of 1998) under Section 29(1) and Part 2 of the Regulations stipulates that an insurer must hold capital equal to 15 per cent of the greater of the amount of the premium income of the short-term insurer after deduction of all premiums payable by it in terms of any short-term reinsurance policies entered into by it, plus a contingency reserve amount defined under Section 6 of Part II of the act as being equal to 10% of the total amount of all the premiums payable to the short-term insurer under short-term policies entered into by it. The total capital required therefore being equal to 25% of the insurer's net written premiums.

The principal of insurers holding capital equal to 25% of their net written premiums is applied across the board to all South African short-term insurers, but experts contend that this is a very simplistic approach and does not take into account the underlying

risk profile of each insurer (Nyamakanga, 2007). One of the criticisms of the current solvency regime is that merely meeting the current capital requirement is no indication that an insurer will not experience financial difficulty in the future and vice versa. Similarly, it is felt that the Financial Services Board cannot accurately judge the financial soundness of an insurer based on the current capital measurement (Nyamakanga, 2007).

Liberalization and emerging business models have led to changes in the risk profile of insurance companies. Insurers now need to manage risks in a more structured and informed manner (ChandraShekhar and Warrier, 2010), and the importance of risk management has assumed much larger proportions than it used to (ChandraShekhar and Warrier, 2010). Regulators around the world are now emphasizing on risk based capital as the basis for capital adequacy and insurer solvency (ChandraShekhar and Warrier, 2010). In this approach the minimum acceptable capital depends upon how risky the underwriting and investment operations of the company are. This is a major deviation from the fixed ratio approach currently in force in South Africa. Insurance companies will need to align their risk management practices with regulatory solvency and capital requirements and need to move up from being risk evaluators to total risk managers (ChandraShekhar and Warrier, 2010).

Implementing a risk based approach to solvency capital in line with similar regimes being adopted in the European Union and elsewhere however, means adopting regulatory capital requirements that are closely aligned to the risks in the specific insurance business. Under the existing fixed ratio solvency regime, no account is taken of the fact that certain lines or classes of insurance business are inherently riskier than others, for example motor insurance business versus fixed property insurance business.

The change from existing regulation is therefore to establish a risk-based capital regime as a tool to assist the regulator both in measuring risk and in determining appropriate levels of capitalisation for each specific short-term insurer based on their risk profile and types of insurance business conducted and underwritten. Under a risk based capital model insurers will have to hold solvency capital that can relate more accurately to the risks taken on by insurers and inherent in their businesses.

1.2 Objectives of the study

The objectives of the study are:

- To identify and present the various elements, practices, processes, techniques and methods that can and should be recognised, considered and employed by insurers in terms of their operational risk management programmes.
- To investigate insurers current approaches, as well as their recommended views, towards the recognition, consideration and use of various elements, practices, processes, techniques and methods employed in operational risk management practice.
- To investigate whether insurers approaches and views towards operational risk management, and their recognition, consideration and use of various elements, practices, processes, techniques and methods employed in operational risk management are being significantly altered by the current importance being attached to operational risk management as part of the requirements of the Solvency Assessment and Management risk based capital regime being implemented in 2014.

1.3 Delineation of scope of the study

The study covers licensed short-term insurance companies registered in South Africa.

1.4 Assumptions

All licensed short-term insurance companies registered in South Africa will be subject to and affected by the Financial Services Board's impending regulatory change to a risk based capital model known as Solvency Assessment and Management (SAM) which the Financial Services Board (FSB) is intending to have fully implemented on the 01st of January 2014 (FSB, 2010). Furthermore, it is assumed that the basis of the Solvency Assessment and Management regime will be the principles of the European Solvency II Directive as contained in the Financial Services Board's Information Letter 8/2009 (FSB, 2009), and the Solvency Assessment and

Management regime will at a minimum meet the requirements of a third country equivalence assessment under Solvency II (FSB, 2009).

1.5 Limitations

The study was conducted amongst short-term insurers only and did not include reinsurers or long-term (life) insurers.

1.6 Importance of the study

According to Capgemini (2006), times have changed for insurance companies. The operating environment has seen change brought about by complexity in markets, new products, evolving technology standards and conglomeration.

A recent survey provided a comprehensive overview of the strategic issues and challenges facing the South African insurance industry currently. The rate of premium growth in the South African insurance market considerably outstrips its counterparts in the rest of Africa and the South African insurance industry accounts for 71% of Africa's premiums (Metcalfe, 2010).

Amongst the most pressing issues facing the South African short-term industry cited was the proposed transition to the Solvency Assessment and Management regime with respondents believing it likely to have a significant impact. The survey indicated however, that most participants believe that the Solvency Assessment and Management regime will be of great benefit and indicated that in their opinion Solvency Assessment and Management will bring more confidence and stability; allow for a more professional approach to risk management and enable insurers to better understand and manage their risks (Metcalfe, 2010).

Respondents in the recent survey also made mention that risk management has started to play an increasingly more prominent role in their businesses. Participants noted that risk management has added substantially more value to their businesses over the past three years (Metcalfe, 2010). Companies are now monitoring and, in most cases, measuring a wide variety of risks including political, environmental and

latent claims risks.

The new envisaged Solvency Assessment and Management approach envisages enterprise-wide risk management as the basis for capital requirements, with one of the aims being to align capital requirements more closely with actual risks, and with a specific emphasis being placed on operational risk management.

Due to operational risk management in the short-term insurance industry being a relatively new concept still in a developmental stage, it is this author's opinion that this study could assist short-term insurers with founding formal operational risk management processes and programmes within their organisations.

1.7 Industry overview

1.7.1 Insurance overview

Short-term insurance is a form of risk management which is mainly used to hedge or protect against the risk of a contingent, uncertain loss. We can define insurance as the equitable transfer of the risk of a loss, from one entity to another, in exchange for payment. The insurer is a company selling the insurance, and the insured or policyholder is the person or entity buying the insurance policy.

The insurance rate is a factor used to determine the amount to be charged for a certain amount of insurance coverage, which is called the premium. The insurance transaction essentially involves the insured assuming a guaranteed and known relatively small loss in the form of payment of the premium to the insurer in exchange for the insurer's promise to compensate or indemnify the insured in the case of a loss. The insured receives a contract called the insurance policy which details the conditions and circumstances under which the insured will be compensated or indemnified.

Insurance involves the concept of pooling funds by insurers from many insured's in order to pay for losses which can occur to these insured's. The insured's are therefore protected from risk for a fee or premium, with the fee being dependent upon

various factors germane to the insurer including the type of policy, value at risk, and the potential frequency and severity of the event occurring (Wikipedia, 2010).

In South Africa the short-term insurance industry is governed by the Short-Term Insurance Act, 1998 (Act No. 53 of 1998) and overseen by the Financial Services Board, which oversees the South African Non-Banking Financial Services Industry and is committed to promoting and maintaining a sound financial investment environment in South Africa (FSB, 2009). The South African insurance industry is a well established and mature part of the South African financial services industry; it accounts for 71% of Africa's total premiums and has the third-highest insurance penetration in the world at 15.3% (Metcalfe, 2010).

1.7.2 Industry statistics

Table 1.1 below details the number and type of short-term insurers registered in South Africa.

Table 1.1 Number and type of short-term insurers

Type of insurers	2008	2009
Insurers		
Typical insurers	25	26
Niche insurers	34	35
Cell captive insurers	10	11
Captive insurers	10	11
Insurers in run-off	15	13
Other	3	3
Total	**97**	**99**

Source: Financial Services Board, 2009.

Details concerning short-term insurance premiums are detailed in figures 1.1 to 1.4. The premium details include premiums at both a gross level (including short-term reinsurance premiums) as well as at a net level (excluding short-term reinsurance premiums) at an insurer type level. Premium details at class of short-term business

level are also reflected. Figure 1.5 reflects short-term insurer underwriting results and investment income as a percentage of net premiums.

For purposes of the above mentioned the Financial Services Board's latest Annual Report (2009) has been utilised. The report contains premium and return detail for the previous financial period hence premium and return details are to 2008.

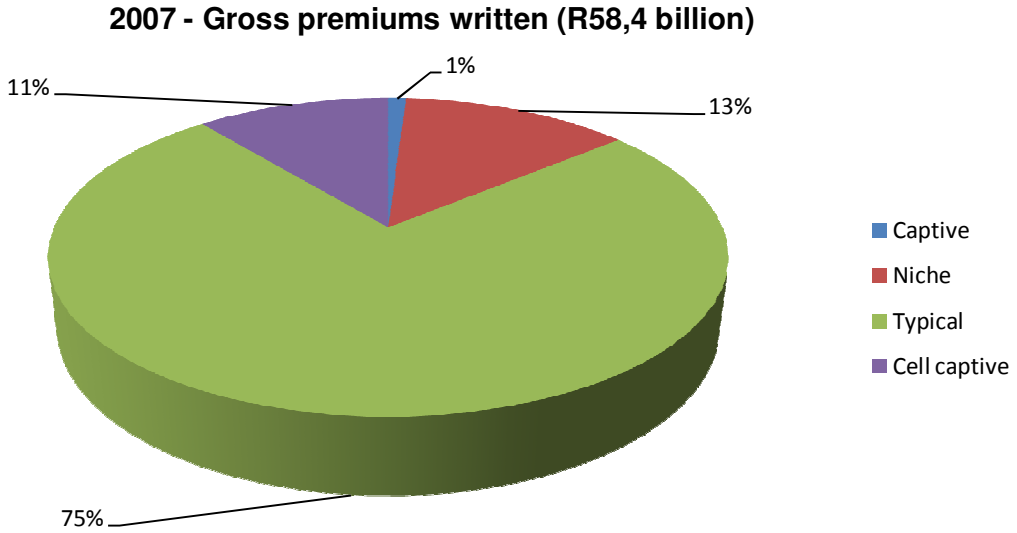

Figure 1.1 Gross premiums for 2007 split per insurer type

Source: Financial Services Board, 2009.

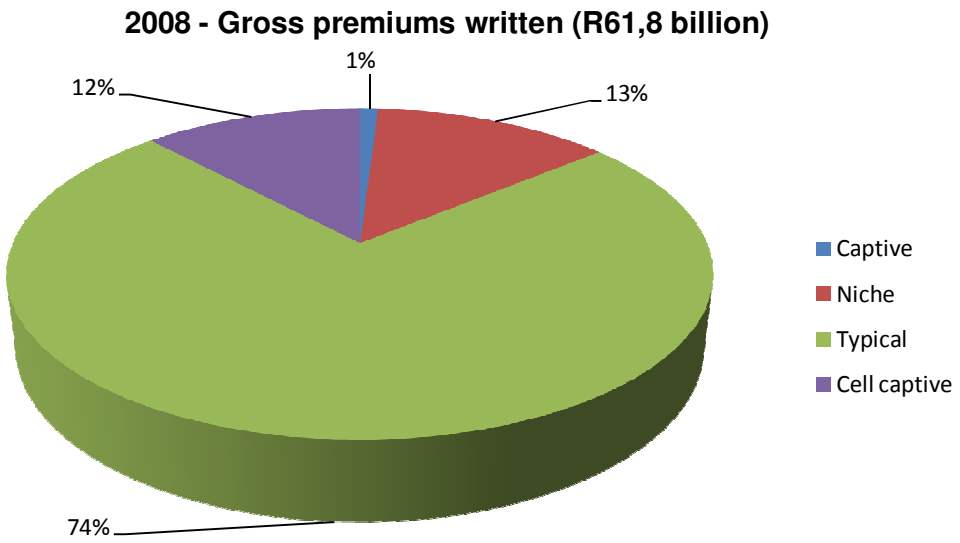

Figure 1.2 Gross premiums for 2008 split per insurer type

Source: Financial Services Board, 2009.

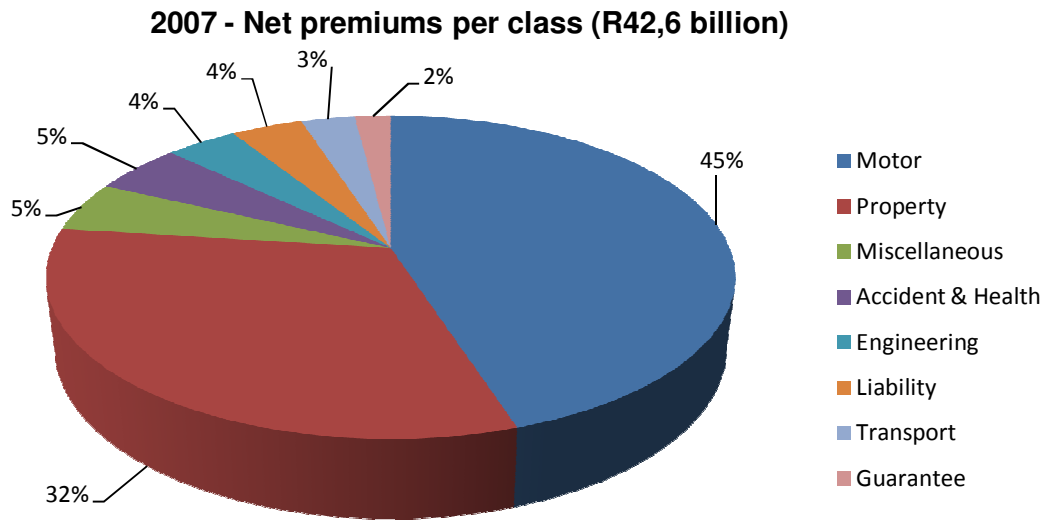

Figure 1.3 Net premiums for 2007 split per class of business

Source: Financial Services Board, 2009.

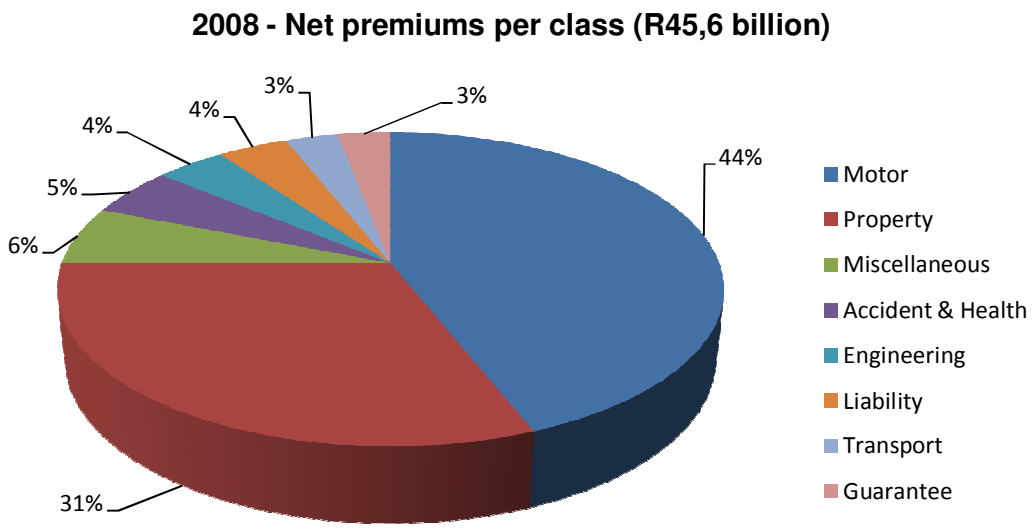

Figure 1.4 Net premiums for 2008 split per class of business

Source: Financial Services Board, 2009.

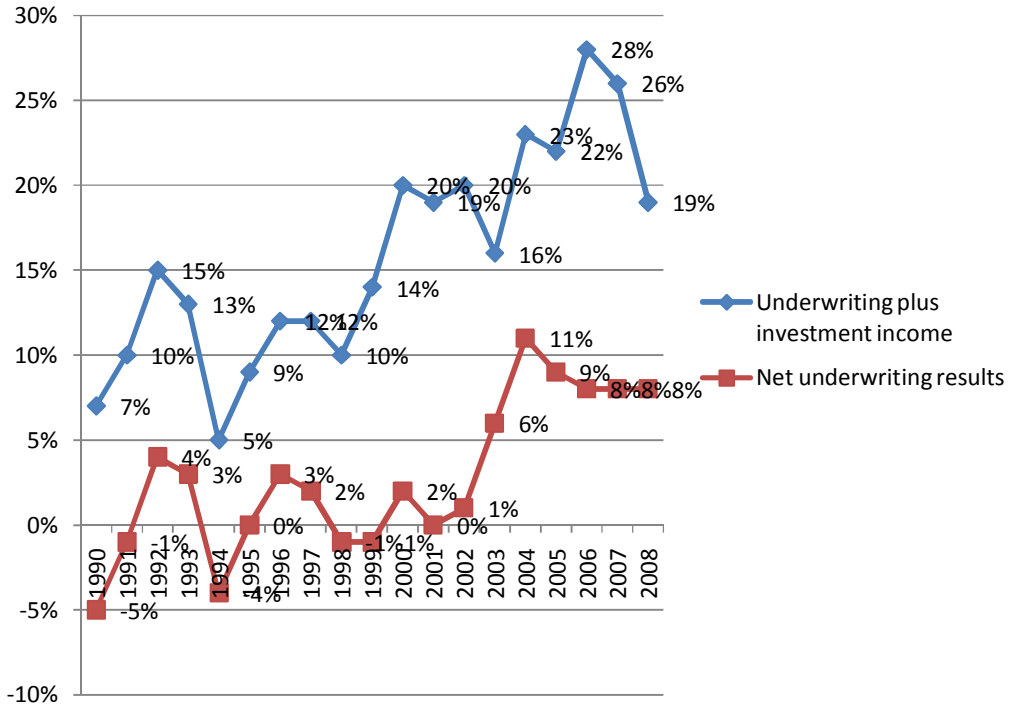

Figure 1.5 Underwriting results and investment income (as a percentage of net premiums)

Source: Financial Services Board, 2009.

As is evident, typical short-term insurers who offer most types of policies to, mostly, the general public as well as commercial businesses and corporate enterprises, write the majority of the short-term premium written (74% in 2008). This segment of the industry is also known as the primary market (Metcalfe, 2010). Within the primary market the majority of premium is underwritten in two main classes, namely the motor and property classes of business (44% and 31% respectively in 2008). The motor class is clearly concerned with motor vehicle insurance, and the property class with insurance of property such as domestic and commercial buildings, plant and machinery and other tangible assets.

Table 1.2 details the market shares of the five largest short-term insurers as well as what is attributable to the rest of the short-term primary market insurers, which amounts to a further 17 short-term insurers (Metcalfe, 2010).

Table 1.2 Market shares – primary market

Insurer (short name)	**Market share**
Santam	19%
Mutual & Federal	13%
Hollard	8%
Zurich	7%
Outsurance	5%
Rest of the short-term market	48%
Total	**100%**

Source: Metcalfe, 2010.

1.7.3 Performance

The industry faced some challenges in the past 2 years precipitated by the global financial crisis which saw the industry only grow at 5% in 2008 and 6% in 2009 (Kirk 2009; Metcalfe 2010). Investment performance of the insurers was obviously affected, but other difficulties also manifested in the form of reduced new business growth prospects and the durability of existing policies being adversely affected by

reduced consumer discretionary income, leading to client attrition (Santam Limited, 2010). In recessionary times, insurance markets soften, premium growth slows and claims rise (Santam Limited, 2010).

Notwithstanding this, the industry has recovered relatively quickly and remains robust, pointing towards the resilience of the insurance industry in South Africa (Metcalfe, 2010).

Expectations are that it will take two years for industry growth and underwriting margins to show substantial improvement (Kirk 2009; Metcalfe 2010), with most short-term insurers aiming for 15% annual premium growth between 2010 and 2013 (Metcalfe, 2010).

The South African insurance industry faces unique challenges and it is important that it evaluates and adapts to the needs of the emerging market (Metcalfe, 2010).

1.7.4 The future - specific concerns and pressing issues

Specific concerns for short-term insurers are the problems being experienced with motor insurance business (Kirk 2009; Matthew 2010; Ndururi 2010; Santam Limited 2010; South African Insurance Association 2009). Motor insurance is the largest class of short-term business, encompassing more than 40% of the industry's gross premium. Half the net costs of all industry claims are in respect of motor claims, with approximately 70% of these motor claims relating to vehicle crashes (South African Insurance Association, 2008). Reasons cited for problems being experienced with motor insurance business include driver behaviour and the poor state of some of South Africa's roads (South African Insurance Association, 2009). Other reasons include the difficulty in securing premium increases from insured's, an inability to price correctly for risk, an increase in claims frequency, as well as claims value as a result of increases in average repair costs for motor vehicle accidents which increased by 6% in 2005 and 6.7% in 2006, but by 13% in 2007 and 13.5% in 2008 (Kirk, 2009).

Risk management is set to receive much more emphasis by insurers going forward (Metcalfe, 2010). The need for effective risk management by short-term insurers has been labelled as essential and higher than ever before, with concerns that failure to manage risk down by insurers will lead to inefficiencies flowing through to consumers and resulting in further reductions in insurance penetration (Kirk, 2009). A recent survey of the insurance industry revealed that as insurers pursue growth strategies, risk management has started to play an increasingly more prominent role. Participants in the survey noted that risk management has added substantially more value to their businesses over the past three years, and companies are now monitoring and, in most cases, measuring a wide variety of risks including political, environmental and latent claims risks (Metcalfe, 2010).

Participants in the recent survey mentioned above also stated that the implementation of the proposed Solvency Assessment and Management risk based capital regime based on Solvency II principles will trigger major changes in the industry. Participants stated that the proposed transition to the Solvency Assessment and Management regime is likely to have a significant impact (Metcalfe, 2010). The majority of participants did however also state that their belief was that the Solvency Assessment and Management regime will be of benefit, notwithstanding that it was still early days to predict the full impact of the proposed capital regime and that it would lead to more confidence as well as stability, and also allow for a more professional approach to operational risk management and enable insurers to better understand and manage their risks (Metcalfe, 2010).

The recent survey of the insurance industry conducted by Metcalfe (2010) revealed participants perceptions of industry strengths and weaknesses as follows (Metcalfe, 2010):

1.7.5 Industry strengths

- Financial soundness and stability
- Highly competitive and innovative marketplace
- Well capitalized
- Seen as unique in the sense of being both an established and emerging market
- Entrepreneurial orientation

- Strong brands
- Good competencies for expansion into Africa
- Strong partnerships with banks
- Strong broker market
- Creative product design
- Well regulated
- Good underwriting practices

1.7.6 Industry weaknesses

- Skills shortages
- Poor market practice
- Large number of legacy products
- Weak client service
- Too few black intermediaries
- Products too complex for the market
- Too much delegation to the broker base
- Lack of a strong competitive reinsurance market
- Inability as an industry to collect and share data
- Need to focus on adding value for consumers

1.8 Clarification of acronyms, concepts and terms

- **ARROW** - Advanced Risk Reporting Operating Framework.
- **Cell captive insurers** - Insurers who offer insurance structures on a cell ownership basis for first party and third party cell owners.
- **FSA** – Financial Services Authority. Regulator of the financial services industry in the United Kingdom.
- **FSB** - Financial Services Board. Independent institution established by statute to oversee the South African Non-Banking Financial Services Industry in the public interest.
- **MCR** - Minimum Capital Requirement.
- **Niche insurers** - Insurers who offer, mostly, specialised cover only, in certain niche markets).

- **ORSA** - Own Risk & Solvency Assessment.
- **SAIA** - South African Insurance Association. Association which represents most of the short-term insurance companies in South Africa, with 55 members that include traditional short-term insurers, specialist and niche short-term insurance companies and reinsurers. Represents the industry at all levels, and with all stakeholders, including Government and the media.
- **SCR** - Solvency Capital Requirement
- **SFC** - Solvency & Financial Condition Report
- **STA** - Short-Term Insurance Act, 1998 (Act No. 53 of 1998). The Act which governs short-term insurance in South Africa.
- **Typical insurers** - Insurers who offer most types of policies to, mostly, the general public.

1.9 Plan of the research report

Chapter 1 provides for an orientation of the study. It provides a general outline of the new risk based capital model that is to be introduced to the South African short-term insurance industry. A brief overview of the South African short-term insurance industry is given. This chapter also mentions the objectives, scope, limitations and importance of the study.

Chapter 2 provides the foundation of the study. It includes an explanation surrounding the concept of a risk based capital approach to insurer solvency capital regimes. The chapter explores the nature of a risk based capital regime in the form of the European Solvency II directive which the FSB is developing for a South African context in the form of Solvency Assessment and Management. The risk management requirements imposed by a Solvency II type regime are specifically explored.

Chapter 3 is a literature review of operational risk management.

Chapter 4 details the research methodology employed in the research undertaken. The chapter details the objectives of the research; research method used; the population studied; the research instrument used as well as the data collection method.

Chapter 5 contains the results and analysis of the research.

Chapter 6 consists of a discussion, conclusions drawn from the study and recommendations.

2 CHAPTER 2: FOUNDATION OF THE STUDY

2.1 Overview of Solvency II / Solvency Assessment and Management

South Africa's current short-term solvency regime is over 10 years old and financial markets have developed significantly since then, leading to a large discrepancy between the reality of the insurance business of today and its regulation.

Solvency II is a fundamental review of the capital adequacy regime for European insurers and reinsurers, planned to take effect from October 2012. It aims to establish a revised set of EU-wide capital requirements, valuation techniques and risk management standards that will replace the current Solvency I requirements. The new regime is expected to apply to all insurance firms with gross premium income exceeding EUR5m or gross technical provisions in excess of EUR25m (FSA, 2008).

According to the FSB (2009), it aims to promote the soundness of insurance companies through the effective application of international regulatory and supervisory standards, and in line with this objective, their intent is to introduce a solvency regime along the principles set out in the new Solvency II Directive being applied in Europe. The introduction of a solvency regime such as this should help to protect policyholders' interests more effectively, by making firm failure less likely and reducing the probability of consumer loss or market disruption. The new FSB approach has been termed Solvency Assessment and Management (SAM) and it will be implemented fully at the beginning of 2014. The SAM approach to solvency capital for short-term insurers is a divergence from the current solvency regime of simply applying a statutory solvency provision currently equal to a holding of 25% of net written premiums across the board to all insurers.

According to the Financial Services Board (2009), the basis of the SAM regime will be the principles of the Solvency II Directive, as adopted by the European Parliament, but adapted to South African specific circumstances where necessary. As an overarching principle, and as a measure of the closeness that the Financial Services Board is hoping to achieve between the South African SAM regime and the European Solvency II initiative, it has been stated that the recommendations arising from the SAM project should meet the requirements of a third country equivalence

assessment under Solvency II (FSB, 2009). A risk based approach to solvency rules will both stipulate the minimum amounts of financial resources that insurers must have in order to cover the risks to which they are exposed as well as lay down the principles that should guide insurers overall operational risk management.

The Solvency II Directive was adopted by the European Parliament on 22 April 2009 and endorsed by the Council of Ministers on 5 May 2009. The implementation date for EU countries is October 2012 (FSA, 2008).

The new proposed SAM risk based capital solvency requirements are being designed to ensure that insurers have sufficient capital to withstand adverse events, both in terms of insurance risk, as well as in terms of economic, market and operational risk. Risk based capital models considers the underlying risk of the insurer to determine the capital levels needed, which should, if calculated correctly, minimise the possibility of future financial difficulty as well as lead to a more efficient allocation of capital between different risks (Nyamakanga, 2007). A key divergence from the current capital regime is that under a risk based capital approach insurers will have to put rigorous risk management strategies into practice and to consider all the risks that may affect their business, not only the underwriting risks (Nyamakanga, 2007).

Risks faced by the insurance company are diverse in nature and complexity. Risks that are straightforward and already form an important aspect of product design and pricing such as underwriting risks are already receiving attention from insurers due to it being fundamental to their business (ChandraShekhar and Warrier, 2010). It is the identification of risks and their interdependence at the enterprise level that will require expertise in risk management, as a solvency assessment based on risk involves considering the risks that the company is exposed to and factoring in these risks while addressing the capital needs (ChandraShekhar and Warrier, 2010).

The key drivers for the new solvency regime are fundamentally (Capgemini, 2006):

- Regulators want to protect the stability of the insurance financial system.
- The insurance sector has grown significantly in recent years. Due to this growth, any negative disturbances within the industry can potentially affect the entire financial system.

- Companies and markets are becoming increasingly complex, creating new types of risk, such as operational risk. Insurers may not be able to manage these new risks as well as they manage those that are core to their business, such as insurance technical or underwriting risks. To preserve systemic stability, regulations must therefore tackle a broader range of risks.
- An underlying tenet of Solvency II / SAM is that the regime should help to protect policyholders' interests more effectively, by making firm failure less likely and reducing the probability of consumer loss or market disruption (FSA, 2008).
- The promotion of improved and consistent risk management standards (FSA, 2008).

Solvency II / SAM is underpinned by a methodology which stresses enterprise-wide risk management as the basis for capital requirements and is built on a three-pillar approach which seeks to align capital requirements more closely with actual risks (FSA, 2008).

One of the drivers behind Solvency II / SAM is the promotion of improved and consistent risk management standards within insurers. Under the Solvency II pillar dealing with qualitative requirements (Pillar II) which the FSB have adopted, there is specific reference to the system of governance including risk management insurers are required to maintain (FSA, 2008).

Under its Solvency II directive the FSA contends that effective risk management and enterprise-wide governance are cornerstones of a sound solvency system (FSA, 2008). The FSA has stated in its information letter DP08/4 that “while it is necessary for insurers to hold adequate capital, the decisions of senior management and the quality of group controls are potentially even more crucial for an insurer's long-term health”, and that “weaknesses in such areas made firms susceptible to an external trigger event that caused adverse financial outcomes” (FSA, 2008: 2).

Solvency II requires insurers to have an effective risk management system (FSA, 2008). Specifically, it requires firms to consider all risks to which they are or could be exposed and for the risk management system to be fully integrated into the organisation as a fundamental part of the running of the firm (FSA, 2008). In this context, the concept of risk management being integrated is taken to mean that it is

owned, monitored and managed at a local level within the organisation (A.M. Best, 2010).

Solvency II / SAM suggests a two-tiered approach for the determination of regulatory capital adequacy. The first tier is known as the Minimum Capital Requirement (MCR). The MCR represents the threshold below which an insurer will not be able to write business. The second tier is known as the Solvency Capital Requirement (SCR). The SCR represents the level below which an insurer will likely need to discuss remedies with the regulator.

The MCR will be set by the regulator, and the methods used to calculate it will be based around “clear and simple” calculation methods that are proven to be consistent with confidence levels in the 80%-90% range over a one year period (FSA, 2008: 25). The MCR is designed to be the lower solvency calculation. This corresponds to a solvency level, below which policyholders and beneficiaries are exposed to an unacceptable level of risk, if the insurer were allowed to continue its operations (FSA, 2008).

The aim of the second tier of capital required, namely the SCR, is to reflect a level of eligible own funds that enables insurers to absorb losses to a confidence level of 99.5% over one year (FSA, 2008). The SCR imposes a higher capital requirement. This requirement basically reflects the capital needed to achieve a certain safety level. If an insurance company falls below this SCR level, this can be interpreted as an early-warning sign (Liebwein, 2006). For calculating the SCR, there will be a calibrated standard model which all insurers will be able to make use of, however, for SCR specifically, insurers will alternatively also be able to make use of so-called ‘‘internal’’ models. Internal models will in essence be a model that the insurer themselves have built which they believe details the level of SCR that they hold. The result of an insurer derived SCR as a result of them having built an internal model and having had it approved for use by them by the regulator might be lower (or at least more individual) than the SCR obtained by that insurer using the standard model for calculation of SCR derived by the regulator (Liebwein, 2006).

Therefore, in order to calculate their SCR, insurers will have the choice of the standard model, an internal capital model or a combination of both. The formulaic

standard model for SCR will be easier to implement and will treat risks consistently across companies (Guy Carpenter, 2010). This stands to reason as, in having derived its standard calculation methodology for calculation of an insurer's SCR, the regulator will have used statistics for the industry as a whole, not for individual companies. Insurers will therefore be able to calculate the Solvency Capital Requirement (SCR) using their own full or partial internal model, as approved by the regulator. Partial internal models will also be able to be used to calculate the SCR for one or more risk modules or sub-modules as well as for one or more major business units.

For small companies without complicated or highly unique risks, the standard model approach may be adequate. However the standard model will not reflect any characteristics specific to an insurer such as (Guy Carpenter, 2010):

- Focus on particular business niches and / or risk mitigation strategies in place by that insurer.
- Reinsurance programmes with features such as profit commissions, caps, indexes or corridors put in place by the insurer.
- Changes over time in the insurer's business strategy which affect its portfolio makeup.

Internal models can overcome these drawbacks, as the internal model derived by an insurer would have been modelled on their specific portfolio makeup and risk mitigation factors in place endemic only to their business. The costs of the internal model approach however, is that they require expertise and resources for parameterization, model building, validation, interpretation and communication. Internal models will also require supervisory approval by the regulator before an insurer will be able to use their own specific internal model to derive the amount of SCR that they need to hold.

Notwithstanding the costs mentioned above, there are still many advantages to using an internal model for the calculation of an insurer's SCR, in addition to its value in meeting supervisory solvency requirements (Guy Carpenter, 2010). Some of these advantages are:

- An internal model can be used for evaluating the insurer's risk profile and related reinsurance and investment strategies in the context of its risk appetite.
- An internal model can be useful for discussing capital management with other external parties, such as rating agencies.
- An internal can be used for evaluating returns on risk-adjusted capital for individual business segments.

2.2 Solvency II / Solvency Assessment and Management and the implications for operational risk management in insurers

Under the Solvency II regime, the FSA stipulates the role that risk management systems must play in any internal model the insurer presents for approval, as a means of calculating regulatory capital (FSA, 2008). The insurer must consider all risks that are included in the calculation of the SCR as well as the risks that are not, or not fully, captured in the calculation, examples of which would be liquidity risk and reputational risks (FSA, 2008).

In order to fulfil these requirements the insurer must first be able to monitor and understand all the risks to which it is exposed, by having a robust operational risk management system in place.

For an internal model to be approved for deriving the SCR, the insurer will need to satisfy the requirements related to internal models. Integration into the insurer of the insurer's risk management activity will be a key requirement (FSA, 2008), and the FSA have stated that the internal model is "owned by a firm's risk management function" (FSA, 2008: 25) and have also stated that the internal model "refers to a risk management system developed by an insurer to analyse the overall risk position, to quantify risks and to determine the economic capital required to meet those risks" (FSA, 2008: 20).

As part of having their internal model approved, an insurer will have to undertake an Own Risk and Solvency Assessment (ORSA) as well as be able to satisfy a use test.

The ORSA is defined as “the entirety of the processes and procedures employed to identify, assess, monitor, manage and report the short and long term risks an insurance undertaking faces or may face and to determine the own funds necessary to ensure that the undertaking's overall solvency needs are met at all times” (FSA, 2008: 20). The ORSA represents an assessment of the risks within the insurer and the level of solvency required to mitigate those risks.

An ORSA is an internal risk assessment process that aims to ensure senior management have conducted their own review of the risks to which they are exposed and that they hold sufficient capital against those risks (FSA, 2008). The FSA (2008) have stated that the ORSA must reflect the insurer’s own risk appetite.

According to the FSA (2008), the ORSA should be an integral part of managing the business against the company's chosen strategy and it should thus be an important tool in assisting strategic decision-making, as given the requirement for the integrated management of risk and capital, when making changes to their business strategy or the organisation’s risk appetite, senior management should demonstrate that they have considered the effects of these changes to their solvency requirements and record this in their ORSA. A robust risk management function will assist the firm to undertake a robust ORSA.

The use tests imply that the internal model must reflect the realities of the business and the operational processes of the firm, hence the need to fully integrate the insurer’s risk management processes within the organisation. To embed the internal model into the business, the FSA have stated that it is first necessary to embed the business into the model (FSA, 2008).

In order to assess whether the internal model plays an important role in managing the business, the use test looks at the processes by which the firm uses it within business decision-making, in terms of inputs to and output from the model (FSA, 2008). Key decision makers within the insurers will need to be able to demonstrate their understanding of the key elements and results from the internal model and according to the FSA an insurer’s internal model should be integrated within its overall risk management and decision-making activities (FSA, 2008).

Furthermore, full integration of the internal model into the business implies, according to the FSA (2008), that senior management is clearly responsible for the risk management system and ensuring that it is used in managing the business, including how it influences business decisions, and that risks identified by the risk management function are also a key input into the capital model in order to reflect the nature of the business and the environment in which the firm operates. The FSA (2008) also state that the risk management function should be such that it allocates economic capital at an appropriate level of granularity, such as by business unit, line of business, homogeneous risk group etc. to enable management to use this within internal reporting and to ensure that the capital allocation reflects the risks inherent in each area of the business.

Under the current solvency regime many insurance companies pay scant attention to operational risk. The new proposed FSB Solvency Assessment and Management regime, which is being principally modelled on the Solvency II regime in order to meet third country equivalence requirements, aims to create a more realistic measure of solvency capital requirements based on all the risks an insurer faces, including all categories of risk and in particular bringing in the effect of operational risk.

The FSB's envisaged implementation of SAM, specifically as concerns Pillar II - Qualitative requirements, will, as already disclosed by the FSB be based on the European Solvency II Directive and will entail inter alia that insurers:

- Develop and embed a formal set of governance requirements.
- Develop an effective operational risk management system, owned and implemented by senior management.
- Undertake a formalised risk-based evaluation of the whole firm, based on management's chosen risk appetite and level of capital required to run the business.

2.3 Further implications for robust operational risk management approaches by insurers

Having a more robust approach to operational risk management is not just a matter of compliance under a Solvency Assessment and Management / Solvency II regime

however. Other benefits in addition to regulatory compliance are believed to materialise as a result of better operational risk management.

In today's economic climate rating agencies, analysts and shareholders, as well as regulators, are all taking more interest in risk management and specifically the enterprise risk management practiced by insurance companies (Q Finance, 2010).

Global ratings agency A.M. Best believe that establishing a risk-aware culture, using sophisticated tools to consistently identify and manage, as well as measure risk and risk correlations is an increasingly important component of an insurer's risk management framework (A.M. Best, 2008).

However, A.M. Best believe that if an insurer is practicing sound risk management and executing its strategy effectively, it will maintain a prudent level of risk adjusted capital and perform successfully over the long term, both being common objectives of both A.M. Best ratings and risk management (A.M. Best, 2008). According to A.M. Best (2008) therefore, being adept at risk management practice will not only serve to make an insurer compliant with regard to a Solvency Assessment and Management / Solvency II regime, it will also serve to assist the insurer to remain competitive in the current dynamic environment, build sustainable earnings and capital accumulation, and ultimately, maintain high ratings (with their attendant benefits relative to accessing capital and credit and an increased reputational and corporate profile).

A.M. Best (2008) therefore contend that insurers participating in the global markets must develop and constantly refine a risk management framework (A.M. Best, 2008), and have stated that they "perceive risk management as paramount to an insurer's long term success. As such, within the rating process, each company, regardless of its size or complexity, is expected to explain how it identifies, measures, monitors and manages risk. An insurer that can demonstrate strong risk management practices integrated into its core operating processes, and effectively execute its business plan, will maintain favourable ratings" (A.M. Best, 2008: 5).

Accenture (2010: 10) state that "at the same time, more and more European insurers are investing in risk management capabilities to influence their evaluations by the rating agencies. The idea is that rating agencies' evaluations would be positively

influenced by the company's enterprise-wide risk management scores".

According to EMB (2010), notwithstanding the fact that risk management is such an integral part of compliance related to a Solvency II type regime, by considering not only the requirement to quantify the risks and calculate the capital requirements but also the general model of risk governance and the whole approach to management information and reporting, insurers can in fact build a more effective business operation that serves their long-term strategy (EMB, 2010).

Capgemini (2006), assert that the benefits of a more robust approach towards risk management over and above regulatory compliance are:

- Improved management of risk and capital. Effective risk management will enable insurance company business to be more predictable and stable, thereby leading to a less volatile capital position.
- Better risk management should bring closer alignment of organisational goals and allow an enterprise-wide understanding of business risks, thereby informing the planning process and ensuring that key objectives are consistent across the whole organisation.
- An increase in transparency as the transparency of roles and responsibilities improves, making clear where responsibilities lie and identifying areas of overlap and gaps, leading to an improvement in business efficiency and overall quality.
- Improved risk management should result in a competitive edge for insurers as a more robust approach to risk management should enable better identification and management of risks, allowing insurer's to understand which types and sources of risk can be opportunities to improve business performance.
- A better understanding of the insurer's risk profile can help the insurer to create better and more profitable products. A better understanding of risk pricing and capital requirements enables more accurate pricing decisions to be made.
- Better risk management should allow for greater visibility of business drivers as an improved assessment of risks as well as rewards will provide greater visibility of the real drivers of business value, thereby creating an environment for better planning and decision-making.

3 CHAPTER 3: LITERATURE REVIEW-OPERATIONAL RISK MANAGEMENT

3.1 Definition of operational risk

Many definitions of operational risk can be found. Whilst not specifically aimed at insurance companies, but undoubtedly having relevance to them in the form of financial institutions, the Basel Committee on Banking Supervision (Basel) for the purposes of the implementation of Basel II for banks in Europe defined operational risk as being "the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events" (Basel, 2003: 2).

Zurich (2010) define operational risk as "operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events" (Zurich, 2010: 10). It is therefore clear that notwithstanding the fact that they are an insurer, they seem to have fundamentally adopted the definition of operational risk as described by Basel (2003).

The FSA have also adopted the definition of operational risk defined by Basel. Under section 1.2.32 of the FSA's Integrated Prudential sourcebook for insurers, the FSA defines operational risk as being "operational risk refers to the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events" (FSA, 2004: 83).

Dowd (1998), whilst not offering a definition of operational risk, states that "these risks cover a huge variety of specific risks: risk from unauthorised trading, fraud, and human error, loss of personnel, communication failures and breakdown of control systems, computer breakdowns and other technological problems, natural disasters and many others" (Dowd, 1998: 191). According to Dowd (1998), "operational risks are everywhere, ranging from the very small to the very large, and encompass every level of the organisation" (Dowd, 1998: 191).

Lam (2003) also states agreement with the definition of operational risk as defined by Basel and also adopted by the FSA. Lam (2003) contends that whilst this definition does represent common ground "there is still considerable debate on how it should be applied" (Lam, 2003: 210).

According to Young (2001), operational risk is defined as “the exposure to potential losses, resulting from shortcomings and/or 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, 2001: 96).

Young’s (2005) definition of operational risk is defined as “operational risk is the exposure of an organisation to potential losses, resulting from shortcomings and/or 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, 2005: 11).

Tripp, Bradley, Devitt, Orros, Overton, Pryor & Shaw (2004), state that “there is no single risk classification that suits all purposes. However it seems that many U.K. insurance companies are adopting the definition used by the Basel committee as a starting point” (Tripp, *et al*., 2004: 21).

According to Tripp, *et al.* (2004), what matters more in practice is that the organisation has good definitions for all its risk categories and uses them consistently, bearing also in mind that it may well be necessary to use different definitions for different purposes.

Lam (2003), would seem to be in agreement with what Tripp, *et al*. (2004) suggest as he contends that “individual companies should establish an overall definition of operational risk, as well as its subcomponents” (Lam, 2003: 210).

According to Dickstein and Flast (2008) operational risk is different from all other risks. They contend that operational risk is typically defined by a variety of international sources, including government agencies, quasi-governmental bodies, professional organisations, and consulting firms, as the risk of loss resulting from inadequate or failed internal processes, people, and systems, or from external events.

In light of the fact that no single classification of operational risk seems to have been globally adopted, but bearing in mind the nature of the study being undertaken, it would seem that the FSA adopted definition of operational risk as being "operational risk refers to the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events" (FSA, 2004: 83) would provide the best fit in terms of a definition of operational risk in an insurance context.

3.2 Definition of risk management

The Oxford Advanced Learner's Dictionary defines the word risk as being "the possibility of something bad happening at some time in the future" (Oxford Advanced Learner's Dictionary, 2010).

The Institute of Risk Management (IRM) defines risk as "the combination of the probability of an event and its consequences" (IRM, 2002: 2) and asserts that in all types of endeavours there exists the potential for events and consequences that constitute threats which form the basis of risk (IRM, 2002). The IRM definition is taken from the International Organisation for Standardization's (ISO) ISO 31000 standard for risk management (ISO, 2009).

ISO 31000 is intended to be a family of standards relating to risk management codified by ISO. According to ISO, the purpose of ISO 31000 is to provide principles and generic guidelines on risk management. ISO 31000 seeks to provide a universally recognised paradigm for practitioners and companies employing risk management processes (ISO, 2009).

Blokdijk states that risk is "a source of danger with the possibility of incurring loss or misfortune" (Blokdijk, 2010: 46).

According to the IRM, risk management is "the process whereby organisations methodically address the risks attaching to their activities with the goal of achieving sustained benefit within each activity and across the portfolio of all activities. The focus of good risk management is the identification and treatment of these risks. Its objective is to add maximum sustainable value to all the activities of the organisation.

It marshals the understanding of the potential upside and downside of all those factors which can affect the organisation. It increases the probability of success, and reduces both the probability of failure and the uncertainty of achieving the organisation's overall objectives" (IRM, 2002: 2).

The American Committee of Sponsoring Organizations of the Treadway Commission (COSO), defines risk management as "a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting 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).

The Casualty Actuarial Society of America (CAS) states that risk management refers to "the discipline by which an organisation in any industry assesses, controls, exploits, finances and monitors risks from all sources for the purposes of increasing the organisation's short and long term value to its shareholders" (CAS, 2003: 8).

The International Actuarial Association (IAA) defined risk management from an insurer perspective with a definition of being "concerned with the totality of systems, structures and processes within an insurer that identify, assess, treat, monitor, report and/or communicate all internal and external sources of risk that could impact on the insurer's operations" (IAA, 2009: 8).

According to the Institute of Actuaries (2009), risk management is "the ongoing proactive process of adopting a holistic approach across the enterprise to all the uncertainty which may affect either positively or negatively the achievement of its key purposes and objectives, leading to action to achieve greater business robustness and flexibility, efficient risk taking and an appropriate risk-reward balance" (Institute of Actuaries, 2009).

ISO (2009) believe that risk management includes the application of logical and systematic methods for identifying, analysing, evaluating and treating risk associated with any activity, process, function or product as well as the actions of monitoring and reviewing risks and reporting and recording the results appropriately.

Q Finance (2010) believes that risk management is the process by which companies systematically identify measure and manage the various types of risk inherent within their operations. The fundamental objectives of a sound risk management programme are to manage the organisation's exposure to potential earnings and capital volatility and to maximize value to the organisation's various stakeholders (Q Finance, 2010).

Whilst the above definitions all represent different points of view on the concept of risk management, some commonality within the descriptions seems to emerge. To varying degrees the descriptions of risk management above speak to it being concerned with:

- a process, system or discipline; that
- addresses the risks within an organisation; through the
- identification, assessment, analysis, control and monitoring of risk

For the purposes of considering risk management in the context of insurance companies then, an adequate definition of risk management may be that it is the identification, assessment and treatment of all sources of risk within the insurer as well as the ongoing monitoring of risk and the reporting thereon through the use of systems, structures and processes.

3.3 Application of risk management – A Risk Management Framework

Accepting that risk management is an activity that takes place in the context of systems, structures and processes suited to it implies that it needs to follow a logical, disciplined approach within the bounds of a set down framework in order for it to be most effective.

The FSA have proposed a risk assessment framework for the insurers and other institutions under their direction known as ARROW (Advanced, Risk-Responsive Operating FrameWork). According to the FSA (2006), ARROW covers all of the risks that are of concern, i.e. firm-specific, thematic and internal. The ARROW framework is designed to identify the main risks; measure the importance of those risks; mitigate

those risks where their size justifies this; and monitor and report on the progress of risk management.

The FSA ARROW framework follows a methodology as follows:

- All risks are firstly identified
- Risks are then measured in terms of probability of occurrence and severity of occurrence
- Risk mitigation techniques are applied to the risks as appropriate
- The risks are monitored and reported on as part of ongoing activities

ARROW is detailed per figure 3.1 below.

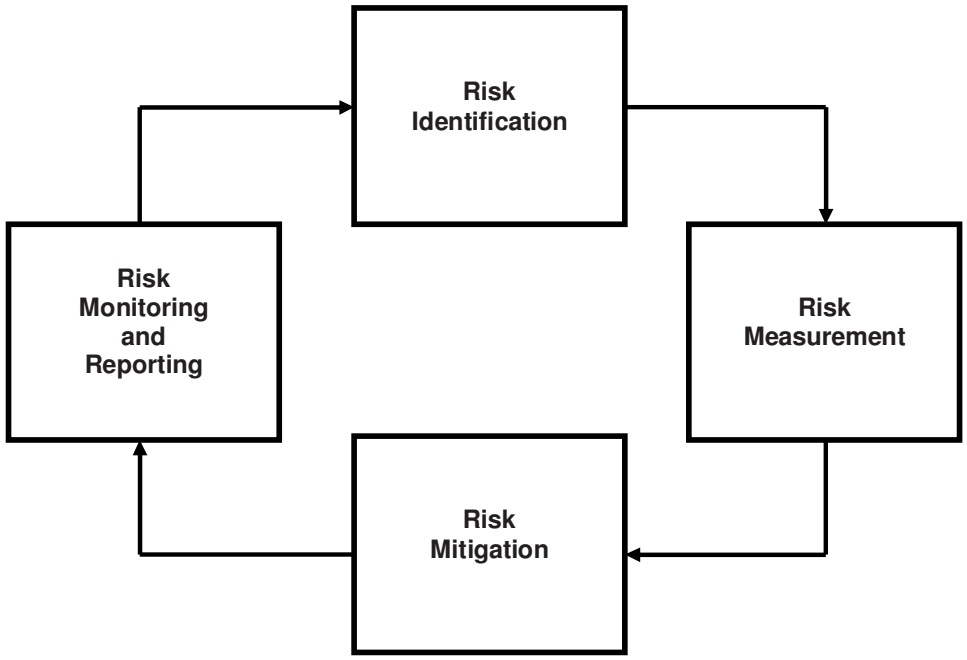

Figure 3.1 ARROW Risk management framework

Source: FSA, 2006.

In terms of ISO 31000, the following approach is adopted:

- Risks are first placed into context
- All risks are then identified
- Risks are analysed in terms of probability / severity
- Risks are evaluated in terms of probability / severity
- The appropriate treatment (mitigation) is applied to the risks

- The risks are monitored and reviewed as part of ongoing activities

Figure 3.2 below reflects the framework approach recommended in terms of ISO 31000 (ISO, 2009) diagrammatically:

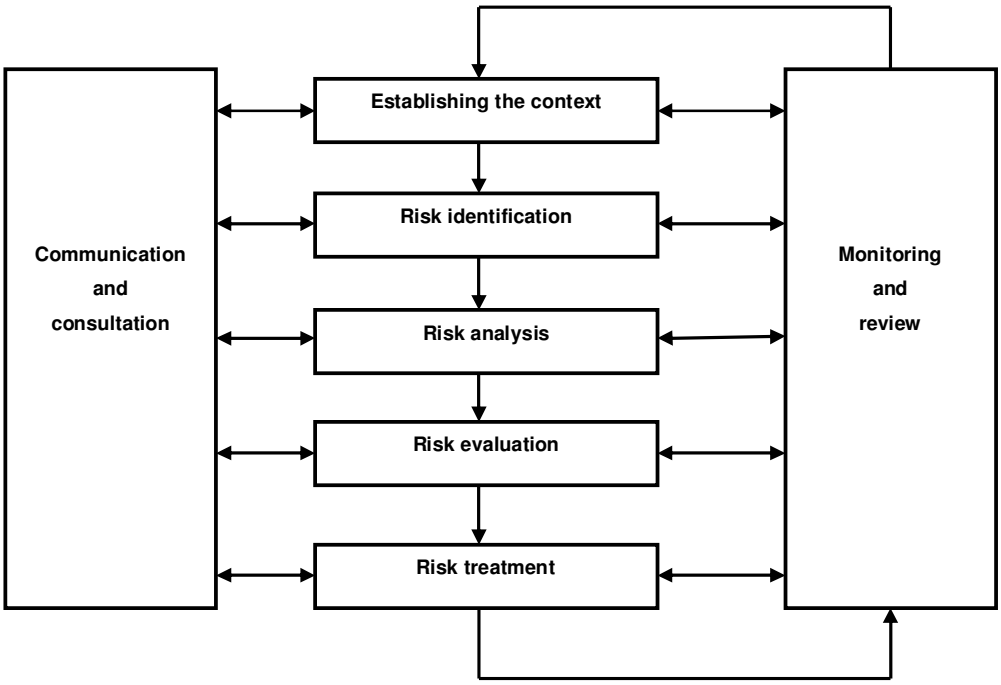

Figure 3.2 ISO 31000 Risk management framework

Source: ISO, 2009

Global Insurance Company Zurich, in their approach to risk management makes use of a framework that is applied as follows (Zurich, 2009) and per figure 3.3:

- Identification of potential risk issues via brainstorming / review of generic scenarios
- Development of risk scenarios
- Assessment and quantification of risks in terms of severity / probability
- Definition of risk priority boundaries and prioritisation of risk scenarios
- Develop improvement actions for the prioritised scenarios (mitigation)
- Follow–up on actions (reporting)

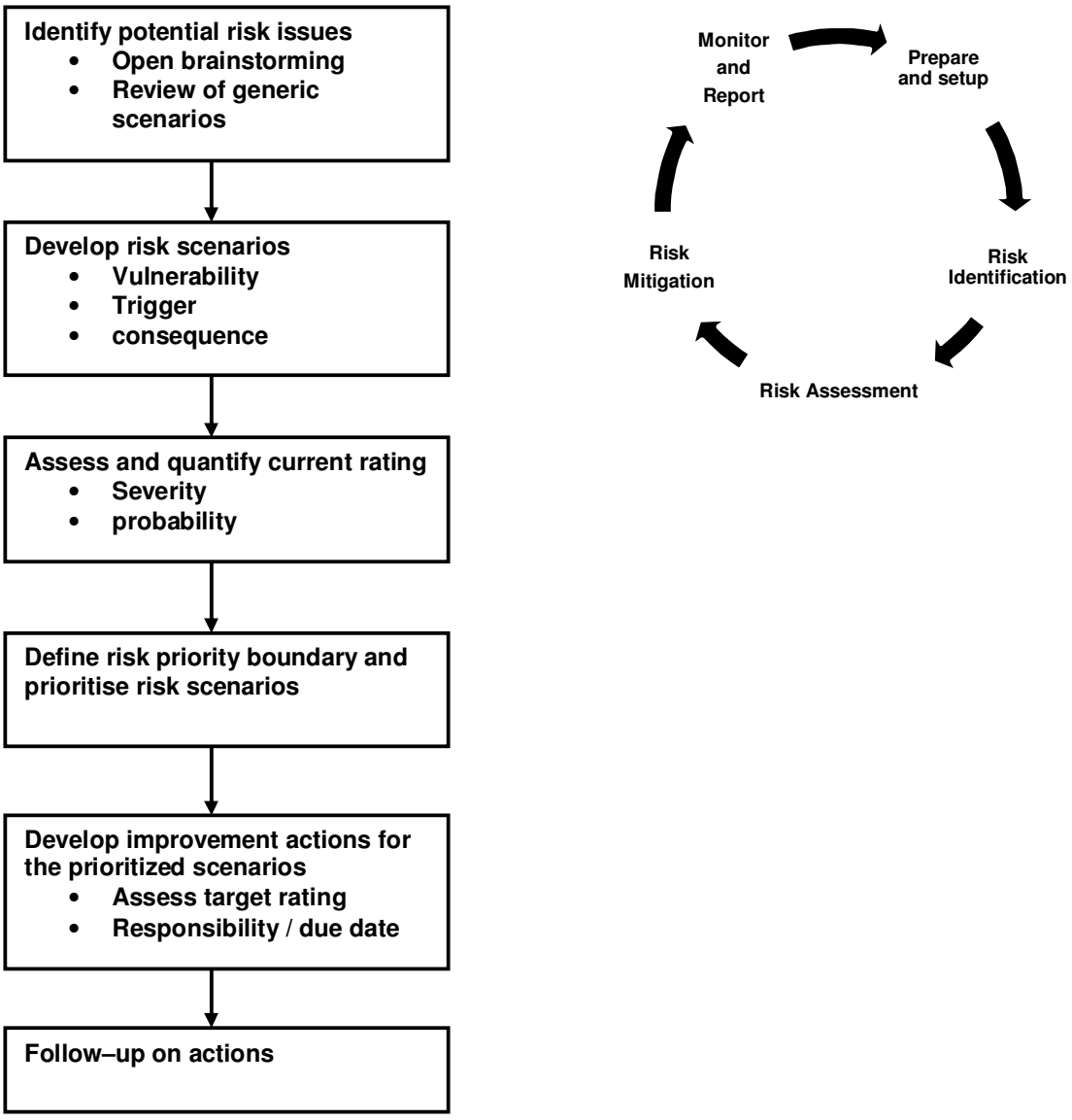

Figure 3.3 Zurich Insurance risk management framework

Source: Zurich, 2009

As a final example of a typical risk management framework, the framework proposed by the Casualty Actuary Society of America (CAS) is considered who propose a tabular framework detailed per figure 3.4 (CAS, 2003):

Process Steps	**Types of Risk**			
	Hazard	**Financial**	**Operational**	**Strategic**
Establish context				
Identify risks				
Analyse / quantify risks				
Integrate risks				
Treat risks				
Monitor and review				

Figure 3.4 Casualty Actuary Society risk management framework
Source: CAS, 2003

The abovementioned figures and discussion represent the details of four separate examples of typical risk management frameworks. Whilst each individual framework may use a different terminology, it is noted that all four of the above examples share some commonality in terms of their use of the following elements within their respective risk management framework:

- Risks are placed into context.
- Risks are identified.
- Risks are analysed in terms of probability / severity (measurement / evaluation).
- Risks are evaluated in terms of probability / severity (measurement / evaluation).
- The appropriate treatment (mitigation) is applied to the risks (mitigation / control).
- The risks are monitored and reviewed as part of ongoing activities (monitoring / reporting).

3.4 Definition of operational risk management

Previously the concept of risk management was explored such that an overarching definition of risk management was obtained in the sense of it being described as the identification, assessment and treatment of all sources of risk within the insurer as well as the ongoing monitoring of risk and the reporting thereon through the use of systems, structures and processes.

When viewed alongside the FSA view of operational risk, the definition above can be extrapolated to provide a definition of operational risk management as being the identification, assessment and treatment of all sources of risk resulting from inadequate or failed internal processes, people and systems within the insurer or from external events as well as the ongoing monitoring of risk and the reporting thereon through the use of systems, structures and processes.

3.5 The components of operational risk

The FSA (2004) definition of operational risk breaks the concept of operational risk into four separate components, which is concurred with by the literature (Dickstein and Flast 2008; Dowd 1998; Hoffman 2002; Hussain 2000; Lam 2003; Loader 2007; Young 2005; Zurich 2009), namely:

- Internal processes risk
- People risk
- Systems risk
- External events risk

3.5.1 Internal processes risk

Lam (2003) states that operational risk occurs through ineffective or inefficient processes. Ineffective processes are defined as being those that fail to achieve their objectives, whilst inefficient processes are defined as those that achieve their objectives but at excessive costs. Process risk can occur during various processes including errors in transactions such as sales, pricing and documentation.

Process risk can also include contract / transactional documentation failures such as incorrect policy issuance; process documentation failures; process design failures; process execution failures; internal data flaws; external data flaws; and internal / external reporting flaws (Zurich, 2009).

According to Basel (2003), process risk includes data entry errors; collateral management failures; incomplete legal documentation; unapproved access; and non-client counterparty misperformance.

Young (2005) believes that as processes form an integral part of operational risk they can thus be seen as one of its main underlying risk factors, and also affirms that process risk is the risk of business processes being insufficient and causing unexpected losses. The elements of process risk according to Young (2005) include the risk of errors arising from information being incorrect or incorrectly processed; the risks arising from inadequate processes, including time delays and inefficiencies and resulting in losses and loss of business; the risk of failure inherent in the processing of data resulting in processing failures or transactional errors.

According to Dickstein and Flast (2008) process risk is seen as risks that arise as a result of deficiencies in an existing procedure, or the absence of a procedure which could result in losses.

3.5.2 People risk

People are arguably an organisation's most important resource, however they have been historically overlooked when operational risk has been evaluated, as it is very difficult to measure and model the risks posed by inexperience; human error; unauthorised activity; lack of integrity and honesty; lack of segregation of duties; lack of customer focus and professionalism; incompetence; reliance on key individuals; insufficient skills, training, management or supervision; lack of control or lack of motivation (Young, 2005).

The risks associated with people arise from employees intentionally or unintentionally making mistakes or failing to follow existing policies or procedures, resulting in losses (Dickstein and Flast, 2008).

People risk concerns risks associated with the employment of people. Some examples of specific loss scenarios concerning people risk are employee errors; employee misdeeds; employee unavailability; employment practices; and the risk of key people leaving the organisation leading to loss of intellectual capital for the organisation (Hoffman, 2002).

Zurich (2009) identify loss / lack of key personnel; skills/capability gaps amongst employees; employee fraud; unauthorized activity; workplace safety; employee relations; and discrimination as falling under the domain of people risk.

According to Young (2005), there is always a human factor to consider when undertaking any business activity. The knowledge, experience, capability and reliability of the persons involved in all of the business processes are critical risk factors. Accordingly, people risk can be defined as the risk of loss caused intentionally or unintentionally by an employee (for example, an employee error or employee misdeed).

The concept of people risk however, also extends to an organisation's inability to recruit, train and retain the correct mix of skilled staff. This may occur as a result of inappropriate training or remuneration policies. Failure to meet objectives relating to equity targets will increase this risk. Regardless of the difficulties of measuring it, people risk continues to be a major contributing factor in many operational failures and therefore, it must be a focal point in a risk management programme (Young, 2005).

Various elements of people risk are identified in the literature (Basel 2003; Dickstein and Flast 2008; FSA 2004; Hoffman 2002; Hussain 2000; Lam 2003; Loader 2007; Young 2005; Zurich 2009) as follows:

- Internal fraud such as intentional misreporting of positions by employees.
- Employee theft.
- Insider trading on an employee’s own account.

- Employment practices issues including discrimination issues / claims.
- Violation of employee health and safety rules
- Organised labour activities.
- Inexperienced staff.
- Incompetent staff.
- Unsuitable staff.
- Negligent staff.
- Unauthorised and / or ill informed decision-making.
- Lack of integrity and honesty.
- No appropriate segregation of duties.
- Lack of customer focus and service.
- Lack of teamwork.
- Overreliance on key individuals (key person risk).
- Insufficient skills or training.
- Insufficient management.
- Lack of a culture of control.

3.5.3 Systems risk

As technology has become increasingly necessary in more and more areas of business, operational risk events due to systems failures have become an increasing concern. This is specifically relevant also bearing in mind that in today's organisation systems are often both integrated across the firm as well as custom tailored for their organisation's specific business needs (Lam, 2003).

According to Dickstein and Flast (2008), systems risk is created when automated processes and systems plus the underlying technology, security or infrastructure break down or fail and cause losses.

Hoffman (2002) defines systems risk as risks posed by an organisation's systems and concerning risks that an organisation's business is interrupted by technology related problems.

Systems risk includes all technology risks, including external pressure such as the risk of not keeping up with the progress of changing or developing a technology, as it is generally accepted that the newer the technology the greater the risk that it may not perform as expected. Organisation's also face systems risk when the systems they choose are not well designed or implemented (Young, 2005).

Several risks are identified falling under the domain of systems risk in the literature (Basel 2003; Dickstein and Flast 2008; Hoffman 2002; Lam 2003; Young 2005; Zurich 2010), these are depicted as follows:

- Hardware failures including obsolescence
- Software failures
- Network failures
- Interface failures
- Communications failures
- Security breaches such as hacking
- Business system disruptions and failures
- Hardware and software failures
- Telecommunication problems
- Utility outages
- Money laundering
- Computer hacking
- Insufficient systems capacity
- Systems failures
- Security breaches
- Insufficient systems capacity
- Poor data integrity
- Data theft
- Obsolescence of systems
- Computer viruses

3.5.4 External events risk

External factors, beyond the direct control and influence of the organisation, could have an adverse effect on the internal, underlying operational factors (people, processes and systems). It is imperative, therefore, that these external factors be considered during an operational risk management process, and it is they that constitute external events risk (Young, 2005).

According to Dickstein and Flast (2008), external risks arise as a result of third party actions and other artificial or natural forces that create losses for a company.

External events risks identified in the literature (Basel 2003; Dickstein and Flast 2008; Hoffman 2002; Hussain 2000; Loader 2007; Young 2005; Zurich 2010) include:

- External fraud including robbery, forgery, cheque kiting, money laundering
- Damage to physical assets
- Terrorism
- Vandalism
- Earthquakes
- Fires
- Floods
- Risks posed by outsourcing partners / outsourcing risk
- Natural or manmade events such as war or earthquakes
- Legislation and regulation
- External fraud and criminal activity
- Supplier risk
- Physical security risks
- Compliance risks
- Financial reporting requirements
- Legal risks
- Strikes
- Economic circumstances
- Political activity risks

3.6 The constituents of the operational risk management framework

3.6.1 Identification of operational risks

Risk identification is the process of finding, recognizing and recording risks. The purpose of risk identification is to identify what might happen or what situations might exist that might affect the achievement of the objectives of the system or organisation. As part of the identification phase of the risk management process, once a risk is identified, the organisation should identify any existing controls for that specific risk in the organisation. The risk identification process includes identifying the causes and source of the risk or hazard in the context of physical harm, events, situations or circumstances which could have a material impact upon objectives and the nature of that impact (ISO, 2009).

During the risk identification process, it is imperative that the risk exposure that the organisation faces be identified. Only when the risk exposure has been identified, can management work to transform it into an acceptable risk element (Young, 2005).

The risk identification processes can be either a continuous or a once-off risk identification process. As a continuous process, risk identification is regarded as an ongoing process in order to enable the identification of risk exposures in the business strategy. As circumstances change, it is imperative that the risks involved, which could have a negative influence on the achievement of business objectives, are understood and appreciated. A once-off risk identification process entails the identification of operational risk during a process so that the feasibility of a proposed business decision is proactively determined (Young, 2005).

Regarding the identification of operational risk, the FSA (2004) suggest that organisation's should try to understand the types of operational risk that are relevant to their specific circumstances and the impact that these risks may have on the incidence of financial crime, the fair treatment of its customers and its own solvency.

Hoffman (2002) states that an organisation can use either a bottom up strategy or a top down strategy to identify, evaluate, and quantify risk potential. A bottom up strategy is used to identify, evaluate, and quantify the risk potential at a transaction or business unit level in order to assist in day-to-day risk / reward business decision making and for the allocation of risk control resources. A top down strategy is used to identify, evaluate, and quantify the risk potential at an enterprise-wide and / or top line business level in order to support firm wide risk quantification and / or risk capital calculations; for the allocation of enterprise-wide internal audit resources; and to assist in making risk finance and insurance decisions.

The IRM (2002) recommends that risk identification should be approached in a methodical way to ensure that all significant activities within the organisation have been identified and all the risks flowing from these activities defined. The IRM also contend that all associated volatility related to the identified risks should also be identified and categorised.

According to the International Association of Actuaries (2009), the identification of risk should include the development of a risk profile for the particular risk. The risk profile should include the following:

- Description of the risk in enough detail for each risk to be understood in isolation.
- The causes or underlying conditions giving rise to a given risk actually occurring or crystallising.
- The consequences of the risk, typically expressed in both financial and non-financial terms (loss of customers, supervisory sanction, etc).
- An appropriate categorisation of each risk.

CAS (2003) states that identifying risks involves documenting the conditions and events that represent material threats to the achievement of the organisation's objectives. Several methods for risk identification are proposed including surveys, internal workshops, brainstorming sessions and internal auditing.

Risk identification should be approached systematically. This can be achieved by understanding the strategic and operational objectives of the organisation, including critical success factors, risk drivers, and the opportunities and threats (risks) related to the achievement of these

objectives; as well as by analysing the processes within the organisation in order to identify the significant risks that flow from these processes. A systematic approach is required, furthermore, in order to ensure that all risk types are identified, including all forms of underlying risk factors per risk type, which can be listed and subjected to the risk management process. It needs to be borne in mind that risk identification is a continuous process in the sense that identified risks must be regularly monitored and new risks highlighted, hence the need for a systematic process for the identification of risk exposures (Young, 2005).

According to Young (2005), once the objectives of a risk identification process have been determined, the second step is the choice of the method to be used. It is important that the method used is the one that will best suit the purpose of the process. According to Young (2005), for example, work-shops are a better option if all the role-players can attend, while questionnaires might be a better option when personal attendance poses a problem.

According to the literature (CAS 2003; FSA 2004; Hoffman 2002; International Association of Actuaries 2009; IRM 2002; ISO 2009; Young 2005) there are various methods or techniques for the identification of risks, but it is unlikely that one particular method will be sufficient for the identification of all the risk exposures. A combination of methods might be required to identify effectively an organisation's total exposure to risk. These are detailed as follows:

- Risk inventories.
- Risk maps.
- Business wide or enterprise-wide scenario analysis of different risk scenarios.
- Trends / Regression analysis of past business performance.
- Score cards.
- Control self assessments.
- Risk Assessment Interviews with staff members.
- Workshops and interviews with staff members where individual interviewees are asked a set of prepared questions from a prompting sheet which

encourages the interviewee to view a situation from a different perspective and thus identify risks from that perspective.

- Questionnaires and checklists, where the check-lists are lists of hazards, risks or control failures that have been developed usually from organisational experience, either as a result of a previous risk assessment or as a result of past failures.
- Risk process flow analysis, which involves mapping the processes of the business and determining the risk exposures that exist in these processes.
- Comparisons with other organisations.
- Discussions with peers.
- Previous loss history analysis.
- Systematic team approaches where a team of experts follow a systematic process to identify risks by means of a structured set of prompts or questions.
- Brainstorming by stimulating and encouraging free-flowing conversation amongst a group of knowledgeable people to identify risks and associated hazards as well as the criteria for decisions and options for treatment / mitigation.
- Delphi technique, which is a procedure to obtain a reliable consensus of opinion from a group of experts. To use the technique experts are questioned using a semi-structured questionnaire. The experts do not meet so their opinions are independent.
- Structured "What-if" Technique (SWIFT). SWIFT is a systematic, team based study, utilizing a set of prompt words or phrases that is used by the facilitator within a workshop to stimulate participants to identify risks. The facilitator and team use standard what-if type phrases in combination with the prompts to investigate how a system, organisation or procedure will be affected by deviations from normal operations and behaviour.

According to Young (2005), after a method for the identification of the risk has been decided upon, the next step is the customization of the method in order to ensure a structured approach during the risk identification process. For example, when a workshop is chosen as the risk identification method, the following guidelines could be useful:

- Specify the business area to be considered.

- Elect appropriate staff at the right management levels to participate.
- Develop a format that can serve as a guideline during the process.
- Appoint an expert facilitator.
- During the workshop, identify the inherent risks for the business, as well as the measures required to eliminate or reduce the potential effect of the risks.

3.6.2 Measurement and evaluation of operational risks

Young (2005) believes that there is a close and integrated link between risk identification and risk evaluation. The result of the risk identification process should be analysed to serve as input for the risk evaluation process. Risk evaluation is the assessment and measurement of the identified risk exposures with the aim of managing and controlling the risks that could negatively influence the business strategy and the achievement of objectives. From a risk management perspective, one of the most fundamental considerations is the quantification of the risk exposures, as once a risk is measured, it can be managed. The evaluation of risk can be qualitative or quantitative in nature. The quantitative approach aims to quantify risk in numerical terms and determine the potential impact of the risk on the organisation. The qualitative assessment of risk aims to evaluate the risk exposures that cannot be numerically calculated. The aim of risk evaluation is also to determine the potential impact of a loss event and the likelihood of a risk event occurring, which will provide management with guidelines on what control measures are required to prevent the event from occurring.

According to Tripp, *et al.* (2004), operational risks contain aspects that are not so easy to quantify and hence to model, therefore the accuracy of risk measurement methods depends on the risk model and data availability. Risk models require a thorough understanding of recurrent risk patterns, and their appropriateness is inherently linked to data availability and the occurrence of events. Operational risk encompasses risks with very different frequencies and possible patterns of occurrence relative to other risks.

The FSA (2002) state that operational risk measurement is a key issue to them. However, they also state that due to both data limitations and lack of high-powered analysis tools, a number of operational risks cannot be measured accurately in a quantitative manner at the present time. The FSA therefore use the term risk assessment in place of measurement, to encompass more qualitative processes, including for example the scoring of risks as high, medium and low. The FSA does however encourage firms to collect data on their operational risks and to use measurement tools where this is possible and appropriate.

Hoffman (2002) contends that risk assessment and risk measurement are fundamental in the operational risk management process, and that understanding and measuring the risks are key, but because of the difficulty in measuring operational risk, however, a balanced qualitative and quantitative approach is necessary in order to achieve a complete picture of the risk.

The FSA believe that using a combination of both quantitative and qualitative tools is the best approach to understanding the significance of a firm's operational risks (FSA, 2002).

The assessment of the potential impact of a particular risk can be a complicated task, as a number of possible outcomes may exist or the risk may occur a number of times in a given time period. Such complications should be anticipated and a consistent approach should therefore be adopted. The assessment of the impact of the risk on the organisation should take the financial impact, the impact on the organisation's viability and the impact on business objectives into account. The analysis may either be qualitative or quantitative, or a combination of both, but should be consistent to permit justifiable comparisons (Young, 2005).

According to Young (2005), a generally accepted measure of risk is a combination of the potential impact (the consequence or severity of the risk) and the frequency (how likely it is to occur) of a risk event. The impact of a potential risk is the potential financial, reputational or other damage as evaluated through the use of a combination of both quantitative and qualitative factors.

The above-mentioned approach is also used by the FSA in terms of its ARROW framework for risk management. According to the FSA's ARROW framework, risk is considered to be the combination of impact (the potential harm that could be caused) and probability (the likelihood of the particular event occurring). In terms of the ARROW framework the impact and probability factors are combined to derive a measure of the overall risk posed (FSA, 2006).

With regard to the judgment of the impact on the organisation, Dickstein and Flast (2008) contend that measurement of the significance or severity of this effect is necessary to determine the complete and accurate impact of the risk on the organisation, and it requires judgment and a combination of quantitative and qualitative analysis. With regard to the judgment of the probability of occurrence or recurrence, they believe that this relates to the probability of the failure's repeating itself, and as in the case of measuring impact, the measurement of probability requires both quantitative and qualitative analysis.

According to Tripp, *et* al. (2004), the highest attention will then obviously be paid to the high frequency / high severity risks, which threaten the very existence of the operation. By contrast relatively little attention will be paid to low frequency/low severity risk risks.

According to Young (2005), the following factors should be considered during risk evaluation:

- The significance of the risk and whether the likelihood of a loss is high, medium or low.
- The potential time at which the risk event is most likely to occur.
- The likelihood that the risk, if not controlled, will eventually turn into a material financial loss.
- The potential financial impact of the risk event.
- The potential reputational effect if a loss should occur.
- The manner in which the risk should be controlled.
- The cost of risk controls in relation to the potential loss.

The literature (Basel 2003; Dickstein and Flast 2008; FSA 2002; FSA 2003; FSA 2004; FSA 2006; Hoffman 2002; Institute of Actuaries 2009; International Actuarial Association 2009; Soprano, Crielaard, Piacenza & Ruspantini 2009; Tripp, *et al.* 2004; Young 2005) describes several methods that may be used for the purposes of measurement and evaluation of operational risks, which are described below:

3.6.2.1 Risk maps

Risk maps are also known as profiles of risks. They display the risks according to their frequency and severity of the loss when an event occurs. The process is internally driven and often incorporates checklists and / or workshops to identify the strengths and weaknesses of the operational risk environment. Scorecards, for example, provide a means of translating qualitative assessments into quantitative metrics that give a relative ranking of different types of operational risk exposures. Some scores may relate to risks unique to a specific business line while others may rank risks that cut across business lines. Scores may address inherent risks, as well as the controls to mitigate them. The exercise of risk mapping can reveal areas of weakness and help prioritise subsequent management action. The information required for risk mapping is obtained mainly through interviews, focus groups, facilitated meetings or workshops with the businesses. The key activities are outlined in terms of a process flow, highlighting the main responsibilities. After the documentation of the main activities, the next step involves the identification of the risk exposures (inherent risks) linked to each of these activities. The identification of the control measures to mitigate each risk is then possible.

3.6.2.2 Stress tests and Scenario analysis

Stress testing typically refers to shifting the values of individual parameters that affect the financial position of a firm and determining the effect on the firm's business, whilst scenario analysis typically refers to a wider range of parameters being varied at the same time.

Stress testing is concerned with downside risk and starts with an analysis of the kind of scenario which could cause the business to fail or suffer serious loss. Stress

testing then attempts to analyse how likely such scenarios are to occur and to suggest actions which could reduce the likelihood of occurrence or minimise the impact if they do occur.

Scenario analyses often examine the impact of catastrophic events on the firm's financial position, for example, simultaneous movements in a number of risk categories. Scenario analysis is the process of considering a limited number of future scenarios and working through their possible consequences for the business. Ideally the scenarios should be based on quite different circumstances which between them span as much of the future business environment as is likely to be experienced. The results will probably indicate a wide range of possible threats and opportunities, and lead to suggestions for managing them. This entails using disaster scenarios as part of business continuity management activities.

Scenario analysis can also involve the use of expert opinions, concerns and experience of key role-players in the business. After the assessment of the risk, a panel of experts can be assembled to generate scenarios by looking forward in time and identifying what can go wrong in terms of causes, effects, likelihood and impact of events. These scenarios can be based on the results of the assessment processes, with the main aim being the confirmation and validation of the subjective, qualitative assessments of operational risk.

In applying stress tests and scenario analysis the firm needs to decide how far forward to look. Ideally this should depend upon how quickly it would be able to identify events or changes in circumstances that might lead to a risk crystallising resulting in a loss, and after it has identified the event or circumstance, how quickly and effectively it could act to prevent or mitigate any loss resulting from the risk crystallising and to reduce exposure to any further adverse event or change in circumstance. As a guide, it is recommended that firms should consider conducting stress tests and scenario analyses which enable them to assess their exposure not only in their current position in the economic and business cycles, but also the possible changes in the cycles which might be expected over next three to five years.

3.6.2.3 Self risk assessment

This is described as a typical bottom-up approach to evaluating operational risk. In this approach, each business unit, in collaboration with the central operational risk control unit, assesses the operational risk to which it is exposed, on the basis of inside and expert knowledge, and also according to wider thinking, in order to include extreme events and experiences. Self risk assessments are internally driven analyses of risks, controls and their implementation, with the objective of determining a common understanding of the strengths and weaknesses of the operational risk environment. They can also be used as a key method for the identification of issues, the raising of risk awareness, the creation of a common understanding, and the recognition of the business units that manage and mitigate operational risks.

The process of executing a self risk assessment can be accomplished through various means, including by:

- Questionnaires: Involves starting with a comprehensive list of controls and requesting compliance with them. Best-practice lists, that are unique for each type of business or process, may then be accumulated and turned into a checklist questionnaire.
- Issue-orientated forms: Has a shorter duration than the questionnaires approach. Can start with a risk map, then a request for textual, open-ended responses to the following: how are risks being controlled; to what extent are controls in place; how are risks monitored and measured in order to ensure that controls are operating; and what improvements can be made to the organisation?
- Facilitated workshops: These workshops are usually attended by a cross-section of a business unit's operational and support staff, and are facilitated by a facilitator from the operational risk management function. In most workshops, the delegates identify the risk issues, the biggest risks facing the organisation, and the steps needed to take corrective action.
- Independent assessments: An independent party, whether risk management or internal audit, performs a comprehensive review of operations, risks and controls, and prepares an assessment report that is

reviewed with the business unit.

3.6.2.4 Using risk indicators

Risk indicators are mostly quantitative measures intended to provide insight into operational risk exposures and control measures. The current method is for organisations to develop risk indicators, which will provide management with early warning signals of operational risk issues. Indicators are presented to management in various forms of management information. Although the objectives of operational risk indicators are the support of strategic decision-making, the performance of trend analysis and the support of the goals of the operational risk management initiative, their real benefit lies in the provision of predictive information to facilitate decision-making and enable preventative actions. Risk indicators involve metrics, often financial, which can provide insight into a risk position. These indicators tend to be reviewed on a periodic basis (such as monthly or quarterly) to alert to changes that may be indicative of risk concerns.
A list of key risk indicators could include:

- Customer complaints and commendations.
- Staff resignations.
- Payment delays by third parties.
- Media reports about the business (positive, neutral and negative).
- Production downtime.
- Time taken to process customer's orders.
- Error rates in processing customer's orders.
- IT system availability.
- Key financial data.
- Other risk indicators specific to the individual business.

Risk indicators such as these should be analysed carefully, to see whether there are any indications of a changing trend which needs further enquiries and research. Risk indicators are useful in terms of the assessment and evaluation of operational risks, and for that purpose should be both easy to calculate and predictive, although this can be difficult to achieve. Nonetheless, they can help with a qualitative assessment

of risk, as even if an organisation cannot yet measure operational risk quantitatively, some sort of assessment is needed.

The behaviour of risk indicators can indicate that qualitative, subjective assessments need to be changed or updated. Another advantage is that risk indicators can be used for all risks, not only those with past losses. Risk indicators can also be used to gauge the effectiveness of systems and controls. When a risk indicator falls outside its normal range, it indicates a possible operational issue.

Risk indicators can also be the basis of penalties and positive incentives that encourage managers to operate in a way that contributes to the reduction of enterprise wide operational risk exposures. They thus help to create a culture of risk awareness throughout the company.

It can be quite difficult to find good indicators, insurance companies have a plethora of risks and identifying the most appropriate is not simple, and in practice, the difficulty of finding good indicators may limit the choice. Risk indicators can also be difficult to use unless the company already has at least a rudimentary risk management framework. Therefore, a key challenge in dealing with risk indicators is in identifying or constructing metrics that serve as predictors of operational risk.

Risk indicators may be classified in a number of ways, including indicators by type, risk class, or breadth of application to the business:

- Risk indicator by type includes inherent risk indicators, control risk indicators, composite indicators, and model risk factors.
- Indicators by risk class includes a mapping of the indicators to risk classes, i.e. people, relationships, technology / processing, physical assets, and other external risk classes.
- Business specific versus firm wide risk indicators categorizes indicators by the breadth of their application across the entire firm.

3.6.2.5 Operational risk modelling

These methods include the more mathematical methods of analysis such as Value-at-Risk (VaR) analysis as well as stochastic modelling methods. Operational Value-at-Risk (OpVaR) is arrived at as a function of determining the severity and frequency of operational losses. Modelling approaches such as this focus on estimating the risk of the specific processes, using loss data to determine a loss distribution from which the operational risk is derived. The ultimate objective of models such as these is the performance of an estimation of the frequency of operational risk events in the future. Other examples of operational risk modelling include:

- Economic pricing models, which base forecasts on economic models.
- Scenario analysis / subjective loss estimate models, which are used to capture diverse opinions, concerns, and experience / expertise of key managers and represent them in matrix and graphic form.
- Expected loss models, which are simplistic models based on expectations of loss and derived by a multiple of expected frequency and expected severity.
- Statistical / actuarial / loss distribution loss models, which use actual loss data and are used to construct representations of loss frequencies and severities in the form of statistical probability distributions. Simulation techniques are then used to combine the distributions in modelling expected losses for the future.
- Factor-derived models, which apply loss and / or causal factors to build a bottom-up prediction of loss expectancies.

3.6.2.6 Internal and external loss / event databases

A loss event database captures operational loss events across businesses and risk types. The creation of a loss database, whether an internal or external one, has become recognised as being of utmost importance in any operational risk management effort. A well designed and thorough database will enable the user to identify key facts and trends, which can be used to perform rigorous analysis.

The type of information that could be used in the construction of a loss database includes:

- The identification of the institution or department that incurred losses.

- The amount of loss suffered as a result of the loss incident.
- The date the loss was realized.
- The occurrence period, or the time interval for the reported loss.
- The insurance recovery, if any, of all or a portion of the loss.
- The location of the reported loss.

The following are important points to be considered when a centralised loss event database is developed for operational risk:

- Operational losses must be clearly defined and categorised in order to ensure a standard for the capturing of losses.
- Events that have resulted in losses must be captured in order to ensure effective management information.
- Losses must not be double-counted on the database.
- A loss event database and process must be centrally administered.
- The capture of losses must be a simple and easily understood process.
- Loss reports must be easy to produce.
- Recoveries must be taken into account in determining the net loss.
- A loss must be captured as soon as possible and as close as possible to the place at which it occurred.
- The loss amounts must reconcile with the general ledger in order to ensure accuracy.
- Senior management must support the loss management system.
- The system must reflect the actual loss amount, and the date on which the loss occurred, for effective management information purposes.

Loss event database models are currently the only tools that are seen to provide both financial and quantitative measures of operational risk, in that for example, the likelihood of losses occurring is represented by the number of incidents and the impact of losses by the value of the loss events.

The advantages of loss event databases are considered to be:

- Analysis of losses can provide information for trend analysis, which can serve as a basis for the implementation or upgrading of risk control measures.

- The value of losses indicates the effectiveness of the operational risk management process.
- The loss data can serve as an input for operational risk modelling.
- A loss event also provides a standard for the collation of operational losses throughout the organisation. This will allow for a comparison of businesses in order to determine the influence of the losses on the overall organisation.
- A loss event database also serves as a platform for determining accountability and responsibility for the management and control of the losses, and for subsequent management information.

Lastly, with regard to the measurement and evaluation of operational risk, Young (2005) offers the following guidelines:

- Reliability: The information being analysed / evaluated should be validated in order to ensure accurate measurement.
- Audit-ability: The process of identifying and evaluating risk should be auditable in order to assure management that the use of information was objective and accurate.
- Objectivity: The measurement of operational risk should be executed through the use of standard, objective criteria.
- Consistency: The use of operational risk information should be used in a consistent way in order to ensure that different risk profiles of similar business areas can be compared.
- Relevance: The information used to identify operational risk should be relevant to the business in order to allow management to make accurate decisions based on the risk measurements.
- Transparency: All the essential operational risk information should be reported and assessed in a way that makes risk management transparent to senior managers.
- Enterprise-wide: Operational risk measurements should be designed in such a way that the results can be aggregated across the entire organisation.
- Completeness: All material operational risks should be identified and captured.

3.6.3 Risk mitigation and control of operational risks

Risk control involves the activities designed for the purpose of eliminating or reducing the factors that may negatively influence the strategic objectives and may cause a loss to the organisation. The controls should minimise the loss when it occurs and when preventative methods have not been fully effective. This component of the risk management process can include activities such as the implementation of policies and procedures, internal controls, risk reporting and decision-making, as well as the determination of an organisational structure to form the basis of the process – all of which management needs to ensure are aligned with the original business objectives (Young, 2005).

According to Tripp, *et al.* (2004), a basic understanding of controlling risk may be achieved by understanding that companies take a number of inputs or resources (capital, people, fixed assets, brand, intellectual capital) and use them to achieve certain outputs or objectives, (e.g. dividends, debt repayment, growth). In order to achieve the objectives the company must expose the resources to certain risks. The company must make critical decisions on:

- The level of risk to which it is prepared to expose its resources in order to achieve its objectives;
- The level of risk which it is prepared to accept of not achieving its objectives; and
- Whether the level of potential reward is consistent with the risks.

The important challenge for a business is to set up a system for managing all kinds of operational risk. The best way of doing this will vary from one organisation to another, but there should be a systematic and methodical approach to seeking out and controlling all the various risks which could arise, with particular emphasis on the underlying causes of risk, chain reactions, connections between risks, and the identification of risks which might well occur simultaneously in various parts of the business due to their having the same underlying causes. With regard to risk control activities, an understanding is needed of whether the assessed impacts if a risk materialises include the knock-on effects or not. Therefore, determining whether to respond to perceived risks, and how far such responses should go, are essentially matters of judgement (Institute of Actuaries, 2009).

According to Dickstein and Flast (2008), the process of mitigation and control of operational risks includes conducting an assessment of the risk, and after determining that there is indeed a risk worthy of attention, an analysis of benefits and costs. This entails answering the following two questions:

- What does the control deficiency cost? Costs can be financial and qualitative and would include both current and future expectations.
- What is the cost of mitigating the deficiency?

According to Dowd (1998) the key to handling operational risk is to get the right control systems in place and to have good staff running them, as if the staff are incompetent or the control systems wrong then it is only a matter of time before major problems emerge.

Tripp, *et al.* (2004) states that unfortunately it is often the case that in order to achieve the objectives the company might undertake activities which expose the resources to risks which are beyond its risk appetite. The company then has three options:

- Find an alternative approach to achieving the objectives that allows it to avoid those activities and hence the risks;
- Put in place some sort of mitigating process which reduces the impact of the risk if and when it crystallises; or
- Put in place some sort of mitigating processes which are designed to reduce the likelihood of the risk crystallising.

Tripp, *et al.* (2004) says the last item of putting in place mitigating processes would be what many would recognise as internal risk controls, but in reality risk controls are the combination of all three items above.

According to Tripp, *et al.* (2004) it is also important to note that an internal control cannot remove a risk altogether and therefore ensure that a company achieves its objectives with no unintended destruction of resources. Risk control only provides a certain level of assurance, and there is a clear trade-off between the cost of the control process chosen and the level of assurance achieved (Tripp, *et al.*, 2004).

According to Young (2005), the overarching principles guiding the control of operational risk procedures are that they:

- Should ensure the orderly and efficient execution of business activities.
- Should ensure adherence to management policies.
- Are there to safeguard the assets of the business.
- Should ensure the efficiency and effectiveness of activities.
- Should produce reliable, complete and timely financial and management information.
- Should ensure compliance with applicable laws and regulations.

Tripp, *et al.* (2004), identify six possible treatments of risks:

- Control.
- Mitigate.
- Exploit.
- Fund.
- Ignore.
- Postpone.

Sadgrove (2005) suggests that risks can be treated by means of the following four ways:

- Avoidance – choosing not to accept the risk (e.g. by discontinuing activities in a certain business line).
- Minimisation – minimising a risk through improved monitoring, process changes or substitution of different processes.
- Spread – transferring of a risk or sharing it by means of diversification, sub-contracting, outsourcing, joint ventures or insurance.
- Acceptance – accepting the risk provided that it falls within agreed risk tolerances.

According to the Institute of Actuaries (2009), responding to risk effectively is an essential part of risk management. The Institute states that there are several possible ways of responding to threats – reducing the risk by altering the situation, transferring the risk (e.g. by insurance or by outsourcing), pooling it with another party, or taking no action.

According to Damodaran (2008), deciding which risks to avoid, which ones to pass through and which ones to exploit is the key to good risk management. Damodaran (2008) believes that firms that are good at making the correct selection between the choices outlined above have a better chance of succeeding.

According to Young (2005), as risk control entails any activity that is aimed at the prevention of losses, the minimisation of the consequences of losses that may arise from any risks facing an organisation, and the handling of an adverse event in advance or as it occurs, it is important that the following three types of risk control are in place in order to mitigate operational risk:

- Preventative controls: These are control measures that are put in place in order to prevent a loss event from occurring.
- Detective controls: These are control measures that ensure that a loss event is identified as soon as it occurs, in order to control the effect on the organisation and to put preventative controls in place to prevent a re-occurrence.
- Contingency controls: These control measures are necessary in order to ensure the sustainability of the organisation or business area once a risk event has occurred.

Young (2005) believes that whilst risk controls will never be faultless, there are some characteristics of good controls as follows:

- Controls should be logical, focused and verifiable.
- Controls need to be timely and accurate to be effective.
- Controls should be reviewed when deficiencies are identified.
- Controls should be constantly monitored and adapted to changing circumstances.

The literature (Basel 2003; Damodaran 2008; Dickstein and Flast 2008; Dowd 1998; Institute of Actuaries 2009; Sadgrove 2005; Tripp, *et al.* 2004; Young 2005) recommends certain best practice principles in terms of risk mitigation and control of operational risks which are detailed below:

3.6.3.1 Policies, processes and procedures

- Policies, processes and procedures to control and / or mitigate material operational risks should be in place.
- A risk management policy statement that defines the organisation's approach to risk management and provides for the overall roles and responsibilities should be drawn up. This statement should be approved by the board of directors and adopted by senior management.
- A consistent methodology of updating the formal policies and procedures should be adhered to.
- In order to ensure that all policies are carried out, thorough operating procedures should be documented and communicated to the appropriate staff. The procedures should contain detail on specific actions to be taken for the effective management and control of risks.
- Policies must be concise and clear.
- Once policies and procedures have been approved, internal controls should be established in order to ensure the implementation and effectiveness of these policies and procedures.
- Policies, processes and procedures should be periodically reviewed and adjusted.
- A system should be in place for ensuring compliance with a documented set of internal policies concerning the risk management system.
- The framework of formal, written policies and procedures must be reinforced through a strong control culture that promotes sound risk management practices.
- There should be appropriate segregation of duties, so that personnel are not assigned responsibilities which may create a conflict of interest.
- Control systems should be such that they allow recognition and continual assessment of the risks that could adversely affect the achievement of an organisation's goals.
- Control activities should be an integral part of the daily activities of an organisation. This necessitates an appropriate control structure with the performance of defined control activities on every business level.
- Comprehensive internal financial, operational and compliance information, as well as external market information regarding events and conditions that are relevant to decision-making is required.
- An effective communication system should exist in order to ensure that the

information is available to those who need it.

- The overall effectiveness of an organisation's internal controls should be monitored continuously.
- The monitoring of key risks should be part of both the daily activities of an organisation, and the periodic evaluations by the business lines and internal audit.
- Procedures must be introduced to review periodically the risks which have been identified and the extent to which the agreed risk responses have been actually implemented.
- Policies for managing the risks associated with outsourcing activities should be established. Outsourcing of activities can reduce the institution's risk profile by transferring activities to others with greater expertise and scale to manage the risks associated with specialised business activities. However, use of third parties can also add risk.
- Outsourcing arrangements should be based on robust contracts and / or service level agreements that ensure a clear allocation of responsibilities between external service providers and the outsourcer.
- There should be periodic review of disaster recovery and business continuity plans so that they are consistent with current operations and business strategies. These plans should be tested periodically.

3.6.3.2 Risk treatment

- For all material operational risks that have been identified, the decision must be made whether to use appropriate procedures to control and / or mitigate the risks, or bear the risks.
- For those risks that cannot be controlled, it must be decided whether to accept the risks, reduce the level of business activity involved, or withdraw from this activity completely.
- Risk mitigation tools should be viewed as complementary to, rather than a replacement for, thorough internal operational risk control.
- A system should be in place to analyse the organisation's failures and successes as a matter of course and ensure that the lessons from them are distributed to staff who could learn from them.

3.6.3.3 The Board of Directors and senior management

- The board of directors as well as senior management are responsible for establishing a strong internal control culture in which control activities are an integral part.
- The board of directors, should provide governance, guidance and direction to senior management. The board is also responsible for the approval and review of the overall business strategies and significant policies of the organisation, as well as the organisational structure.
- Top management is also responsible for the promotion of integrity and high standards of ethics, and for the establishment of a culture within the organisation that emphasises and demonstrates, to all levels of personnel, the importance of internal control.
- Other procedures should be put in place throughout the organisation to ensure that higher management, and the Board if necessary, are notified promptly of significant changes in risk exposure or of any concerns expressed by regulatory authorities.
- All managers should be required to report at least annually, as a matter of routine, on the risks in areas for which they are responsible, and the actions they have taken to respond to the risks or control them.
- Project managers in particular should be required to report regularly on the projects for which they are responsible, including any significant concerns they may have developed about future risks once the project becomes operational.
- Since it is vital that risk management has the support of the CEO, consideration should be given to adding suitable responsibilities into his or her job description and reward criteria, requiring promotion of a risk management framework and culture, and the provision of regular information and assurances to the Board about opportunities as well as threats.
- Senior management must understand the business that they are in.
- Senior management should employ good risk management staff and pay them well. This should include appropriate incentive structures which reward on a risk-adjusted basis.
- Senior management should be able to delegate to risk management personnel below them and should work on the presumption that the risk management specialists know more about risk management than they do.

- Everyone involved should understand that no risk management system is perfect and should be aware of the weaknesses of whatever risk management system they work with. They should also understand that the ultimate protection against risk is simply vigilance.

3.6.3.4 Independent risk management function

- A credible, independent risk management function should be established.
- The risk management function should ensure that risks are managed on a firm-wide basis to ensure consistency.
- The risk management unit should be independent of front and back offices and report directly to the Chief Executive of the organisation.
- The risk management unit should have control over risk measurement and risk reporting issues below board level and should have a consistent and integrated approach towards different risks.
- The risk management unit should set decision rules, position and other limits and monitor compliance within those limits.
- The risk management unit should undertake stress testing and contingency planning.
- The risk management unit should periodically review and update risk management systems.
- The risk management unit should advise senior management on risk management issues and warn them of outstanding / prospective problems.
- The risk management unit should involve internal audit in conducting risk audits.

3.6.4 Monitoring and reporting of operational risks

The final stage of the risk management process is to monitor risks. This includes regularly measuring the risk to ensure that it remains within stated tolerances, and auditing to ensure that the procedure is being followed. The auditors should report findings to the chief executive officer or risk manager, who in turn should discuss the findings. This review is the time to consider how the company's risk exposure could be reduced (Sadgrove, 2005).

According to Sadgrove (2005), a process of continuous improvement will help to keep the company abreast of best practice, reduce its risks, and lower its costs. Because there is so much information in the business, monitoring should focus on the most important risks and managers should examine:

- Trends that indicate a growing danger.
- Data that shows variances from the norm.
- Key performance indicators.
- One-off reports on new areas of risk.
- Information from a range of sources.
- Key findings from audits.

The need for continuous and dynamic reviews is more evident today than ever before, fortunately, advancements in technology, frequent reporting, and interactive systems will support a more timely response to risks. Effective operational risk management begins with each employee having an understanding of the potential benefits and harm in each risk faced. This requires a process at a sufficiently detailed and specific level for identifying and evaluating new risks on a continuous basis, but in addition, senior management at a firm wide level must have an aggregate view of operational risk in terms of reporting. Therefore, the organisation must have the ability to track operational risk issues, incidents, and losses by developing a process to capture and track them, including their cost and causative factors, at both business and corporate levels firm wide (Hoffman, 2002).

According to the FSA (2008), Solvency II requires every insurance firm to have an internal audit function, which shall provide for an effective and permanent internal audit function and include a report of whether the internal control system of the firm remains sufficient and appropriate for its business.

From a reporting perspective, according to the Institute of Actuaries (2009), there needs to be an annual independent audit of the risk management process itself, which could well be carried out by the organisation's internal audit department. The results of the audit should be reported to the Board, and should cover such matters as:

- The progress which has been made towards achieving a suitable risk aware culture and communications system throughout the business.
- Progress on the risk training of managers and other staff.
- The effectiveness of risk-related communication with suppliers and customers.
- The documentation of risks and responses, including evidences.
- The effectiveness of reporting systems - risk occurrences, risk indicators and data accuracy.
- The extent to which the Central Risk Function has discharged its tasks.
- Regulatory compliance.
- The effectiveness of the mechanism for categorising certain risks as strategic, so that they receive special attention.
- The amount of time which the Board itself has devoted to risk management.
- Progress on the action plan for eventual full implementation of risk management.
- Priorities for improvement.

Solvency II (and by implication SAM, based on third country equivalence) is likely to require two different types of report: the public, annual Solvency and Financial Condition report, as well as further information that is considered inappropriate to disclose publicly but is needed for the purposes of supervision. In addition to key financial information, firms will have to provide, publicly, a description of their business and financial performance, their systems of governance and the different risks they face, including for each risk category the risk exposure, concentration, mitigation and sensitivity (FSA, 2008).

According to the IRM (2002), different levels within an organisation need different information from the risk management process:

- The Board of Directors should:
    - Know about the most significant risks facing the organisation.
    - Know the possible effects on shareholder value of deviations to expected performance ranges.
    - Ensure appropriate levels of awareness throughout the organisation.
    - Know how the organisation will manage a crisis.
    - Know the importance of stakeholder confidence in the organisation.

    - Be assured that the risk management process is working effectively by receiving adequate information.
    - Publish a clear risk management policy covering risk management philosophy and responsibilities.
- Business units should:
    - Be aware of risks which fall into their area of responsibility, the possible impacts these may have on other areas and the consequences other areas may have on them.
    - Have performance indicators which allow them to monitor the key business and financial activities, progress towards objectives and identify developments which require intervention.
    - Report systematically and promptly to senior management any perceived new risks or failures of existing control measures.
- Individuals should:
    - Understand their accountability for individual risks.
    - Understand how they can enable continuous improvement of risk management responses.
    - Understand that risk management and risk awareness are a key part of the organisation's culture.
    - Report systematically and promptly to senior management any perceived new risks or failures of existing control measures.

According to the IRM (2002), the arrangements for the formal reporting of risk management should be clearly stated and be available to the stakeholders. The formal reporting should address:

- The control methods, particularly management responsibilities for risk management.
- The processes used to identify risks and how they are addressed by the risk management systems.
- The primary control systems in place to manage significant risks.
- The monitoring and review system in place.
- Any significant deficiencies uncovered by the system, or in the system itself, should be reported together with the steps taken to deal with them.

Effective risk management relies on quality risk management information because better risk management information means better decisions. The insurer's risk management function should form a view as to whether executive management and the board are receiving the right information, and risk reporting should seek to answer questions surrounding current and emerging key risks in the business and within the wider environment; changes in risk indicators; the organisation's capability for identifying and managing risks (International Actuarial Association, 2009).

As indicated by Dickstein and Flast (2008), the monitoring and reporting of operational risks is a routine function embedded within the organisation once it is fully implemented. The collection of daily, weekly, and monthly data is an essential part of this monitoring, and the difficulty of gathering the correct and complete amount of data should not be minimized.

Part of the process of monitoring operational risks includes determining what to measure. Dickstein and Flast (2008) suggest the creation of relevant risk metrics, indicators and control standards, and also state that performance and environmental indicators help measure how well a business process is operating. Once relevant risk metrics, indicators and control standards have been established, they state that target levels for the specific measures should be identified.

According to Dickstein and Flast (2008), the data required for monitoring purposes may be gathered as a by-product of performing the process, and may be gathered by various means including collecting process performance data and using checklists. Once gathered the data needs to be compared to the previously mentioned target levels and standards, with ongoing monitoring being performed using these standards as the benchmark. Dickstein and Flast (2008) state that risk monitoring concludes with the comparison of actual results against these standards to determine if control deficiencies, control failures, or risk issues exist.

The final part of the monitoring and reporting of operational risk process is the reporting of the risk indicators and any operational or control failures in order to ensure that management is aware of everything that is happening. An organisation should ensure that this set of activities is a part of everyday management and supervision, as communication and reporting to senior

management is essential for the organisation to ensure that the determination of potential risk feeds into and influences the appropriate next action, so that if potential control deficiencies were found and mitigated, then the new process could be placed into production. Conversely, if potential control deficiencies were found and a decision was made to not mitigate them and instead live with the risk, then reporting to senior management to review the risk appetite of the organisation would be necessary (Dickstein and Flast, 2008).

Young (2005) maintains that risk reporting is the process whereby an organisation reports on risk internally, through its management information system, and externally, to its regulators and shareholders, and that this is an important aspect of risk control and should be enhanced in order to ensure that the applicable data is available to management for decision making.

According to Young (2005), it is critical that risk management provides accurate and timely information regarding risk exposures. The information must be concise, unambiguous, standardised and integrated with existing reporting processes in order to ensure timely and efficient decisions on risk control measures.

An effective risk reporting framework focuses on the generation of risk management information that meets the objectives and needs of different target audiences, and the main objectives of risk reporting are as follows (Young, 2005):

- Increased awareness and transparency of risk exposures.
- The provision of qualitative and quantitative risk information.
- The generation of risk management information for decision-making.
- The provision of risk information that is timeous.

According to Young (2005), monitoring operational risk is a continuous process, which forms an integral part of operational risk management. In order to ensure an appropriate and timely response to risk, an organisation should have a mechanism in place to allow the organisation to monitor its risks and controls. The monitoring process should aim to assist management in understanding the operational risk profile of the organisation, how

changes or developments influence the profile and what must be done in order to protect the organisation against operational risk exposures.

The main objective of operational risk monitoring is the evaluation of the effectiveness of the operational risk management process. The aim is the provision, for management, of timely information on any shortcomings and deficiencies that could negatively influence the achievement of the business objectives. The main focus of this monitoring process is the effectiveness of the operational risk management components, namely risk identification, risk evaluation and risk control as follows (Young, 2005):

- Risk identification: During this process, monitoring plays an important role by ensuring that all the operational risk exposures are identified and that the methods used are sound.
- Risk evaluation: The monitoring of this component of the operational risk management process ensures that all identified risks are assessed and measured. It also determines the effectiveness of the methods and systems used for the evaluation of the risks. It will ensure that the evaluated risks are those that must be subjected to control measures.
- Risk control: The monitoring process will ensure that the optimum control measures are used for the elimination or minimisation of risk.

Young (2005) stresses the importance of critical risks being identified and managed in the most effective way so that the less critical risks do not become critical, and advises that a monitoring system should be linked to the other components of an operational risk management process, and should provide management with an early warning system in order to identify areas which could potentially lead to risk exposures.

It is important that the monitoring of risk involves senior management in the organisation and that a risk monitoring programme is established to perform the following (Young, 2005):

- Monitor the qualitative assessments and quantitative measurements of operational risk exposures.
- Assess the quality and appropriateness of mitigating actions, including the extent to which risks can be transferred.

- Ensure that adequate internal controls, processes and systems are in place to identify and address problems on a proactive basis.
- Ensure the optimum operational risk management process and ensure that the cost of risk does not exceed the risk reward.
- Ensure efficient reporting of operational risk management information.
- Ensure the efficiency of operational risk management systems.
- Ensure the efficiency of the operational risk management strategy.

Continuous monitoring of operational risk is essential in order to ensure the quality of the operational risk management process and to ensure that changing circumstances do not alter risk management priorities. As few risks remain constant, an ongoing review of the exposures is necessary in order to ensure that management action plans remain relevant, therefore the monitoring of the operational risk management process is a continuous action taken in order to ensure the effectiveness of each of the components of the process (Young, 2005).

3.7 Integrating operational risk management into the organisation

The key to managing operational risk successfully rests with one element - the environment, or culture of an organisation. Whilst risk oversight committees, risk management officers, and related staff and departments may be established, the fact remains that an organisation will manage risk only if the organisation's management wants to manage risk. Regulators can force companies to implement risk management processes and systems, but they cannot force companies and their employees to effectively manage risk. It is therefore crucial for organisations to have a corporate culture of rewarding risk management behaviour, as without an appropriate culture all of the risk management tools will be wasted (Dickstein and Flast, 2008).

With regard to the implementation of a risk based capital model such as Solvency II (and by implication SAM, due to third country equivalence), the FSA (2008) expects full integration of risk management into the organisation such that:

- Senior management is clearly responsible for the risk management system and ensuring that it is used in managing the business, including how it influences business decisions.
- Each function within the organisation should be expected to understand how its decisions affect the risk and capital profile of the firm.

Everyone in an entity has some responsibility for enterprise risk management. The chief executive officer is ultimately responsible and should assume ultimate ownership. Other managers support the entity's risk management philosophy, promote compliance with its risk appetite, and manage risks within their spheres of responsibility consistent with risk tolerances. A risk officer, financial officer, internal auditor, and others usually have key support responsibilities. Other entity personnel are responsible for executing enterprise risk management in accordance with established directives and protocols, and the board of directors provides important oversight to enterprise risk management, and is aware of and concurs with the entity's risk appetite (COSO, 2004).

According to Damodaran (2008), risk management was traditionally viewed as a finance function, with the Chief Financial Officer playing the role of risk measurer, assessor, and punisher. Damodaran (2008) contends however that although there are some aspects of risk management and hedging that may be finance related and thus logically embedded in Treasury departments, there are many aspects of risk management that cut across functional areas, and therefore every decision made by a firm in any functional area has a risk management component. Therefore although there may be a centralized group to aggregate these risks and look at the portfolio, individual decision makers have to be aware of how their decisions play out in the big picture.

Deighton, Dix, Graham, & Skinner (2009) maintain that risk is not only the responsibility of the risk department, all people employed and engaged by a company must take responsibility for risk.

According to the IRM (2002), risk management needs to be a concern of everybody employed in the organisation. They delineate responsibility of the various organisational groups as follows:

- Board's have responsibility for determining the strategic direction of the organisation and for creating the environment and the structures for risk management to operate effectively.
- Business units have primary responsibility for managing risk on a day to day basis.
- Business unit management is responsible for promoting risk awareness within their operations and should introduce risk management objectives into their business.
- The risk management function is responsible for setting policy and strategy for risk management; being the primary champion of risk management at strategic and operational level; building a risk aware culture within the organisation; establishing internal risk policy and structures for business units; designing and reviewing processes for risk management; co-ordinating the various functional activities which advise on risk management issues within the organisation; developing risk response processes, including contingency and business continuity programmes; and preparing reports on risk for the board and other stakeholders.
- Internal audit's role should include focusing the internal audit work on the significant risks, as identified by management; auditing the risk management processes across an organisation; providing assurance on the management of risk; providing active support and involvement in the risk management process; facilitating risk identification / assessment and educating line staff in risk management and internal control; and co-ordinating risk reporting to the board.

Organisations should have a risk management culture. Appropriate risk management behaviours may vary according to the organisation, the industry context, the location of operations both within and across national boundaries together with the resultant jurisdictional requirements, however, behaviours that allow responsibility for dealing with risk to be unclear or that inspire a culture of fear or retribution are not likely to be conducive to good risk management. People need to be willing and able to use the appropriate behaviours to support risk related activities. It is these behaviours that over time will create the desired risk management culture (International Actuarial Association, 2009).

The International Actuarial Association (2009) also believe that positioning risk management behaviours as part of "business as usual" also serves to bind the whole organisation to the concept because everyone is on the implementation team.

The FSA (2003: 16) state that "in assessing the effectiveness of a firm's approach to the development and implementation of an OR Framework, we will consider for example ownership at business and corporate / group level – the level of senior management sponsorship, and clarity in the apportionment of roles and responsibilities for OR management throughout the organisation".

Patel and George (2009) point out that by integrating risk management within the organisation and effectively de-centralising it, the "risk culture" can spread beyond core risk functions in an organisation (Patel and George, 2009).

According to KPMG (2010) "In recent years, Operational Risk Management (ORM) has received increased regulatory attention. Regulatory focus continues to escalate, but more and more, Boards, Executives and Senior Managers are driving the need for ORM. This is partly due to highly-publicised operational risk events, but also due to the improved traction of the discipline" (KPMG, 2010: 1).

Dickstein and Flast (2008) consider that senior management is responsible for setting the appropriate tone for the rest of the company, including integrity, ethical values, and competence with regard to the risk environment. Therefore, in order to integrate operational risk management into the organisation it is necessary that the tone be set from the top of the organisation.

According to EMB (2010), in an insurer context, true risk management revolves around understanding the nature (causes, effects and likelihood) and scale of risks faced by an insurer. In order to be successful, risk management should become integral to the strategic planning of an organisation, to its day-to-day operations and to its capital modelling and actuarial practices, and that perhaps the biggest and most endemic change is the likely impact on culture. Specifically with regard to a risk based capital approach to capital, it necessitates the whole organisation to understand its roles, its interdependencies and its responsibilities towards risk. All

employees must share the responsibility for risk, and the board needs to demonstrate that the awareness is across the whole organisation.

Standard & Poor's (2005) assert that the company's risk management culture underpins the effectiveness of the entire risk-management process. They define a risk management culture as the degree to which risk and risk management are important considerations in all aspects of corporate decision making, as well as the degree to which there is broad understanding and participation in risk management across the company.

According to Hoffman (2002), although measuring risk adds much value in drawing attention for mitigation and management purposes, in isolation the measurement process does not have much value until the numbers are integrated back into management and used in a performance management or behaviour modification sense, and therefore, without a doubt, the most effective methods are those that have a direct impact on incentive compensation. Other key benefits from using a fully integrated approach to operational risk management according to Hoffman (2002) are that the organisation is able to create forums for collaboration by getting different groups to work together; measure exposures more completely; develop incentives for productive behaviour; and streamline internal risk controls, eliminating redundancy.

Hoffman (2002) believes that any enterprise-wide programme must be evident to stakeholders both internally and externally, and the commitment must be as clear to the investment community as it is to the employee and client base. Therefore, it is essential to begin with top level issues of vision, reputation, culture, and definition as follows:

- Operational risk must be defined and that definition communicated throughout an organisation before it can be measured or managed effectively.
- The firm wide vision, values, and mandate with regard to enterprise risk management generally, and operational risk management specifically, must be formulated at the highest levels of the organisation and communicated outward to the organisation.

The organisation's corporate culture will make or break a risk management programme. If quality and risk management is stressed at senior levels and driven throughout the organisation, the operational risk management programme will be more likely to succeed. In contrast, if control is simply viewed by management or conveyed in the organisation as an obligatory task, but not nearly as important as developing business, serving clients, and producing revenue, then the operational risk management effort will fail (Hoffman, 2002).

Hoffman (2002) argues that the defence against operational risk and losses flows from the highest level of the organisation - the board of directors and executive management. The board, the management team that they hire, and the policies that they develop, all set the tone for a corporation, its external face and image, and internal culture. At the end of the day, they will have a huge impact on the chances for success of most initiatives, including an operational risk management programme.

Hoffman (2002) also considers that far too often risk management only focuses on negatives, and thus risk managers fall into the trap of penalizing staff and units for risks identified, poor performance, and loss results. According to Hoffman (2002), the most effective programmes balance this with a system of rewards for productive risk management behaviour and investment by both business and corporate units and staff alike.

Hoffman (2002) advises the following with regard to integrating risk management into the organisation:

- Corporate culture and ethos are the least recognised components of an operational risk management programme but, at the same time, can have the greatest positive or negative impact on an organisation's risk profile. A senior level commitment and a risk-aware culture are both essential.
- Delineate risk management roles and responsibilities of the business units. Business units on a local level manage operational risk most effectively.
- Define roles and responsibilities of corporate units firm wide.
- Provide clear, useful, and actionable information about operational risks, losses, and the status of risk response and control efforts such that business unit managers and staff firm wide are in a position to manage them on a day-to-day basis.

- Use incentives and disincentive systems as a means to balance strategic risk and reward. Provide both incentives and disincentives for the management of risk.
- Empower business units with responsibility for the management of operational risks.

Young (2005) contends that the way in which an organisation is structured to undertake risk management is of the utmost importance, and that unless risk management is fully endorsed and actively supported by the board and by the senior management of an organisation as an integral part of the way the organisation is managed, it cannot be effective.

In light of the above, the establishment of a culture for managing operational risk within an organisation is a difficult but necessary task, and although there are various ways of achieving this, the most important aspect seems to be the achievement of the active involvement of all staff members in managing operational risk. This means that the operational risk policies and procedures, the principles whereby operational risk should be managed, and the value adding activities that must be performed must be understood by all staff members. Risk management needs the support and involvement of senior management, which can set a tone for the organisation which indicates that operational risks are important and deserve attention. This originates with the board and filters down to every management and operating level throughout the organisation (Young, 2005).

According to Young (2005), the creation of a fair payment scheme for employees is both a major challenge as well as a critical element of risk management, as an organisation may have all the risk management tools, processes and systems in place, but that these would be worthless without motivated personnel. According to Young (2005), if incentive compensation is a key driver of employee performance, then it is also by extension a key driver of risk management, therefore it is important to ensure the existence of an effective incentive scheme to ensure a motivated workforce.

According to Young (2005), the board of directors and senior management should be actively involved in overseeing the operational risk management framework, therefore the board needs to clearly formulate the organisation's attitude towards risk and the assignment of responsibilities for assessing and controlling risks.

It is essential that the risk management function is established independently of the business operations, and operated as a controlling or monitoring function. This will allow risk management to provide assurance to senior management and the board that the organisation is assessing its risk effectively and complying with its own risk management policies. The internal audit function of the organisation needs to ensure and provide assurance that the operational risk management process has integrity and is being implemented along with the appropriate controls. Internal audit should also offer an independent assessment of the underlying design of the operational risk management process (Young, 2005).

4 CHAPTER 4: RESEARCH METHODOLOGY

4.1 Research method

Leedy and Ormrod (2005) define descriptive research as "identifying the characteristics of an observed phenomenon or exploring possible correlations among two or more phenomena. In every case, descriptive research examines a situation as it is. It does not involve changing or modifying the situation under investigation, nor is it intended to determine cause-and-effect relationships" (Leedy and Ormrod, 2005: 179). In terms of the data that the researcher gathered, namely an investigation into identifying and assessing the current as well as proposed approach by South African short-term insurers towards operational risk management, a descriptive research methodology was followed.

Leedy and Ormrod (2005) state that in terms of descriptive research designs, the following approaches may be utilised:

4.1.1 Observation studies

Observation studies include the observing of the phenomena under investigation, including through using field notes and videotapes such that the variety of ways in which people act and interact are captured (Leedy and Ormrod, 2005).

4.1.2 Correlational research

Correlational research examines the extent to which differences in a certain characteristic or variable correspond or are related to one or more characteristics or variables. In Correlational studies, researchers gather concerning two or more characteristics for a specific group of people or other units of study (Leedy and Ormrod, 2005).

4.1.3 Developmental designs

Developmental designs are most often found in developmental research, such that might be conducted in child developmental research which is an observational type of research that either compares people in different age groups or follows particular groups of people over a lengthy period of time (Leedy and Ormrod, 2005).

4.1.4 Survey research

According to Leedy and Ormrod (2005), survey research "involves acquiring information about one or more groups of people – perhaps about their characteristics, opinions, attitudes, or previous experiences – by asking them questions and tabulating their answers. The ultimate goal is to learn about a large population by surveying a sample of that population, thus, we might call this approach a descriptive survey or normative survey" (Leedy and Ormrod, 2005: 183).

Based on the above descriptions of the various descriptive research designs, a survey research was utilised to gather the data for this study. Leedy and Ormrod (2005) propose two methods that may be used to conduct survey research, namely face-to-face interviews and questionnaires.

Based on the time constraints posed by the research and the fact that a census of the population was proposed, face-to-face interviews as a method of data collection were not seen as a viable option and the data was gathered by means of questionnaires. Some of the reasons for this include:

- It was seen as the most efficient way to reach all of the participants within the time frame available for the research to be conducted.
- The questionnaires could be distributed via either email or standard post.
- Participants in the research would be able to complete the questionnaire in their own time and at their own convenience.

According to Leedy and Ormrod (2005), questionnaires present several advantages in that they can be sent to a large group of people who may be spatially separated from the researcher; respondents can answer the questions under the veil of

anonymity and the cost of the research is relatively low relative to telephone or face-to-face interviews.

Leedy and Ormrod (2005) do however, also note that questionnaire research has some disadvantages as well in that they typically have low response rates as respondents simply fail to return them and that the answers to the questions posed may exhibit bias in the sense that they reflect more the reading and writing skills of the respondents which may have led to misinterpretation of questions.

4.2 Population

The latest list of registered South African short-term insurers available from the Financial Services Board in June 2010 is attached as Appendix 5 (Financial Services Board, 2010). The list details a total of 98 currently registered short-term insurers. Of the 98 currently registered short-term insurers, 2 are in a runoff position and a further 11 insurers are parts of larger insurance groups which exhibit common shareholding and who hold more than one short-term insurance license.

4.3 Census

As described above, excluding the 2 insurers in runoff as well as the 11 insurers which form part of larger insurance groups produces a population of 85 short-term insurers from whom data could be gathered.

In light of the size of the population, a census of the population was conducted as opposed to only selecting a sample from the population.

4.4 Instrument design

According to Leedy and Ormrod (2005), questionnaires should be designed to fulfil a specific research objective and the researcher must consider the respondent when constructing the questionnaire. Accordingly Leedy and Ormrod (2005) offer the following with regard to developing a questionnaire:

- Try to keep the questionnaire as short as possible.
- Use simple, clear and unambiguous language.
- Check for unwarranted assumptions implicit in the questions.
- Word questions in such a way that no clues are provided with regard to preferred or more desirable responses.
- Check for consistency.
- Determine in advance how responses will be coded.
- Make the respondents task as simple as possible.
- Provide instructions that are clear.
- Provide a rationale for any items whose purpose may be unclear.
- Make the questionnaire professional looking.
- Conduct a pilot test.
- Ensure that every question is essential for addressing the research problem.

Accordingly the questionnaire attached as Appendix 2 was formulated. In formulating the questionnaire, questions were largely based on the following:

- Operational risk management best practice identified in the literature review.
- Operational risk management requirements as outlined in the Solvency II Directive (FSA, 2006).
- Previous research done on short-term insurance approaches to risk management conducted by Capgemini in 2006 (Capgemini, 2006).
- Previous research done on banking approaches to risk management conducted by Young in 2001 (Young, 2001).

Leedy and Ormrod (2005) state that “a rating scale is more useful when a behaviour, attitude, or other phenomenon of interest needs to be evaluated on a continuum of say, inadequate to excellent, never to always, or strongly disapprove to strongly approve” (Leedy and Ormrod, 2005: 185). As the research focused on to what degree certain elements of operational risk management are currently being implemented as well as to what degree the participants in the survey believe they should be implemented, a Likert scaled questionnaire was deemed appropriate. The participants were requested to rate both their responses to how certain operational risk management elements are currently being approached within their organisations as well as their beliefs, opinions etc. in terms of how they believe the same

operational risk management elements should be approached within their organisations according to the following scale:

1 = Not at all
2 = To a lesser degree
3 = To a fair degree
4 = To a high degree
5 = Totally
6 = Unsure

The majority of the questions were close-ended requiring the participant to simply state to what degree a certain element is currently being implemented as well as to what degree they believe it should be implemented. In order for participants to provide some additional information or personal opinions some questions contained an item under the label of "other" which could be used for this purpose.

4.5 Data collection

The questionnaire was sent out to the identified short-term insurers under cover of the letter attached as Appendix 1 with a request for it to be returned to the researcher by no later than 31st August in order to facilitate meaningful interpretation of the data. The questionnaire was addressed to the Chief Executive Officer or Managing Director of each respective insurer but it was anticipated that some of them would request that the questionnaire actually be completed by another senior person within the organisation who may have responsibility for operational risk management within the organisation, such as Financial Directors or Chief Financial Officers; Chief Operating Officers; Risk Managers; Actuaries or other senior line managers.

4.6 Data analysis

Simple descriptive statistics have been used to describe the research findings in the form of tables which detail the percentage of respondents who responded to a specific question with their specific preference with regard to their current as well as future opinion of the question being asked. Bar graphs have also been utilised which

detail the arithmetic mean of the responses received per question and which allow visual comparison of the differences in arithmetic means between respondents current as well as future opinions with regard to each specific question and which facilitate and allow for conclusions to be drawn.

Lastly, and where appropriate, a statistical test known as a Paired-Sample t-test has been performed on the data. According to Diamantopoulos and Schlegelmilch (2006), a Paired-Sample t-test "is the related measures equivalent to the two-sample t-test for differences in means. It lends itself nicely to comparisons of two interval or ratio-level measures, the null hypothesis being that the mean difference in the population is zero" (Diamantopoulos and Schlegelmilch, 2006: 195). The Paired-Sample t-test is therefore deemed to be an appropriate test to apply to this research.

In each case where the Paired-Sample t-test is utilised therefore, the null hypothesis is deemed to be that the mean difference in the population is zero versus the alternative hypothesis that a difference does exist at an appropriate statistical significance level. In all instances where applied, the Paired-Sample t-test has been performed at both a 5% significance level as well as at a 10% significance level.

4.7 Limitations

4.7.1 Response rate

As previously mentioned, Leedy and Ormrod (2005) note that questionnaire research has some disadvantages in that they typically have low response rates as respondents simply fail to return them. In order to motivate participants to participate in the research and to return and complete the questionnaire the following methods were adopted:

- A postage paid, self addressed envelope to the researcher was enclosed with surveys sent in the mail.
- Participants had the option of mailing back the completed questionnaire; faxing it or emailing it back to the researcher.
- The results of the study were offered to participants if they indicated their preference to receive them on the questionnaire.

- Gently persistent telephone calls and follow up emails were made towards the end of August to participants who had not returned their completed questionnaire by then.

A total of 27 (31.76%) completed questionnaires were ultimately received back from a population of 85 short-term insurers to whom the questionnaire was distributed, therefore 58 (68.24%) were not returned. No declinature to participate responses were received.

The questionnaire responses received are detailed in the data tables attached to this report as Appendix 6.

4.7.2 Response bias

Leedy and Ormrod (2005) describe bias as "any influence, condition, or set of conditions that singly or together distort the data" (Leedy and Ormrod, 2005: 208). Response bias refers to the situation where bias arises due to response rate in terms of the potential differences between respondents and nonrespondents as nonrespondents are often different to respondents in ways such as having less interest in the topic being studied or having other factors present that prevent them from responding (Leedy and Ormrod, 2005). The element of response bias has been dealt with as follows (Leedy and Ormrod, 2005):

- The percentages of participants who have participated; not participated due to non return of the questionnaire or declined entirely to participate have been fully reported.
- Based on the percentages of respondents versus nonrespondents as defined above, attempts have been made to identify possible sources of bias so that these can be factored into the research conclusions, although no sources are outwardly apparent.
- Responses on questionnaires that were returned quickly have been compared with responses on questionnaires that were returned later as significant differences between early returned and late returned questionnaires can indicate bias in the results.

- A small number of respondents were randomly selected for contact by telephone for the administration of an abridged version of the questionnaire via telephonic interview for comparison with their original answers in the questionnaire.

4.8 Validity and reliability

Content validity would seem to be the best validity criteria for this study as the questionnaire seeks to measure the attitude and opinions of insurers on current as well as future approaches towards operational risk management. Content validity refers to the degree to which the question is answered "are we in fact measuring what we think we are measuring" (Diamantopoulos and Schlegelmilch, 2006: 34). It is believed in this instance that content validity should be evaluated by experts in the field involved. In order for this to be accomplished discussions were held with the Actuarial Department of a large insurer (gross premium in excess of R2 billion per annum) which is responsible for risk management within the organisation in addition to fulfilling other normal actuarial functions such as pricing and modelling. The Actuarial Department consisted of Actuaries, Actuaries in training, and qualified Quantitative Analysts. The members of the department were briefed as to the objectives of the research being undertaken and were given a copy of the questionnaire to comment and provide feedback on. The results were as follows:

- No negative feedback on the understandability of the questions was received.
- No negative feedback on the content of the questions was received.
- The instructions for completing the questionnaire were noted as being clear and understandable.
- The questionnaire was simple to complete.
- The questionnaire was regarded as asking the correct questions for the objectives it was seeking to establish.

Accordingly the researcher has regarded the questionnaire as being valid for the purposes of the research undertaken.

Reliability refers to the degree to which the question is answered "are we getting consistent results from our measures" (Diamantopoulos and Schlegelmilch, 2006: 35). According to Diamantopoulos and Schlegelmilch (2006), two types of

consistency should be considered, one is consistency over time, which is the extent to which similar results are obtained from repeated applications of the same or similar measurement instrument to the same set of respondents, also known as the stability aspect of reliability (Diamantopoulos and Schlegelmilch, 2006).

The other type of consistency is known as equivalence and according to Diamantopoulos and Schlegelmilch (2006) it indicates the extent to which the same set of respondents replies in a consistent manner on similar items or it can also be seen as the extent to which different but comparable sets of respondents produce similar results on the same measurement instrument (Diamantopoulos and Schlegelmilch, 2006). Unfortunately due to the time constraints that the research took place under it was not feasible to administer repeated applications of the questionnaire to the same set of respondents who had replied.

The concept of equivalence was however tested via the administration of a split-sample reliability test wherein the consistency of results of applications of the same measures across randomly selected sub-samples of the respondents were applied. According to Diamantopoulos and Schlegelmilch (2006) this is achieved through the assessment of the degree of correspondence between random sub-samples of respondents (usually split on a 50:50 basis) on the same measure (Diamantopoulos and Schlegelmilch, 2006).

Accordingly the group of respondents was randomly split into a group of 13 respondents and a group of 14 respondents. A two sample t-test was then administered on the two groups in order test for differences in means on a question-by-question basis, so that for example the mean of the answers of the group of 13 respondents with regard to question 3.1 was compared to the mean of the answers of the group of 14 respondents with regard to question 3.1. This was done for each question. The degrees of freedom were set at 25 [(n1 + n2) – 2] and the resultant test t-values compared against the standard t-test table p values as follows:

df = 25

p = 0.05 – 1.706

p = 0.10 – 1.315

A resultant t-value greater than the above indicated t-table critical value for a given significance level would indicate significance. The highest t-value obtained across all questions answered by respondents in the t-test administered was 0.49. There is therefore no significant differences in the means between the two groups of respondents at a 5% level of significance.

4.9 Ethical issues

The researcher is employed in the short-term insurance industry and thus respondents may have had concerns relating to confidentiality. To mitigate against this the covering letter which accompanied the questionnaire contained the following statement:

"The findings will be kept confidential and the report will only refer to respondents as Respondent X or Y. No organisation will be referred to by name. I am employed in the short-term insurance industry and would be willing to sign a confidentiality agreement if so required."

5 CHAPTER 5: RESULTS

5.1 Introduction

Sub-sections 5.2, 5.3 and 5.4 deal with demographic information of the respondents.

Sub-sections 5.5 through to 5.44 deal with the responses received to the questions posed in the questionnaire.

Sub-section 5.45 discusses the results of the items evaluated in the questions posed in the questionnaire.

Tables representing the summarised results of the answers provided by respondents to the questions in the questionnaire from both a current as well as a recommended perspective are provided.

Tables representing the results of the Paired-Sample t-test conducted on the summarised results of the answers provided by respondents are provided. The tables specify whether the statistical test was significant or not at both a 5% as well as a 10% level of significance.

The Paired-Sample t-test is based on the following Hypothesis:

- Null: There is no significant difference between the means of the two responses.
- Alternate: There is a significant difference between the means of the two responses.

Bar graphs representing the summarised results of the answers provided by respondents to the questions in the questionnaire from both a current as well as a recommended perspective are provided.

5.2 Demographic information – Type of insurer

Table 5.1 Demographic of type of insurer

Indicate the type of organisation that you are representing

1.1. Typical insurer	74.07%
1.2. Niche insurer	18.52%
1.3. Cell captive insurer	7.41%
1.4. Captive insurer	
1.5. Reinsurer	

1.6. Other

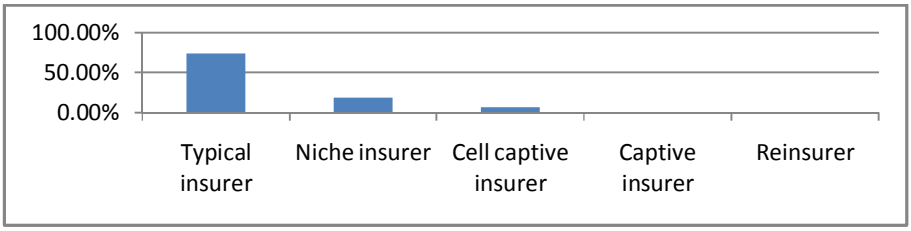

Figure 5.1 Graphical representation of type of insurer

The respondent base was comprised of typical insurers (74.07%), followed by niche insurers (18.52%) and cell captive insurers (7.41%).

5.3 Demographic information – Position

Table 5.2 Demographic of role within organisation

Indicate your role within the organisation

1. Managing Director / Chief Executive Officer	29.63%
2. Financial Director / Chief Financial Officer	22.22%
3. Chief Operating Officer	25.93%
4. Risk Manager	22.22%
5. Line Manager	
6. Actuarial	
7. Internal Audit	

8. Other (specify):

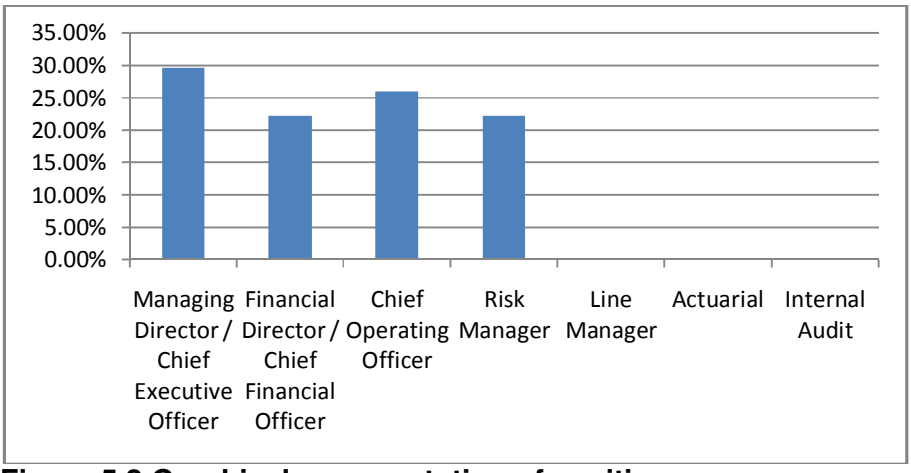

Figure 5.2 Graphical representation of position

The majority of the respondents occupied the position or role of Managing Director / Chief Executive Officer (29.63%), followed by Chief Operating Officers (25.93%) and Financial Directors / Chief Financial Officers as well as Risk Managers (22.22% each respectively).

5.4 Demographic information – Experience

Table 5.3 Demographic of years of experience

Indicate your number of years of experience in the short-term insurance industry

1.	Less than 5 years	
2.	Between 5 and 10 years	
3.	Between 10 and 15 years	66.67%
4.	Between 15 and 20 years	25.93%
5.	Greater than 20 years	7.41%

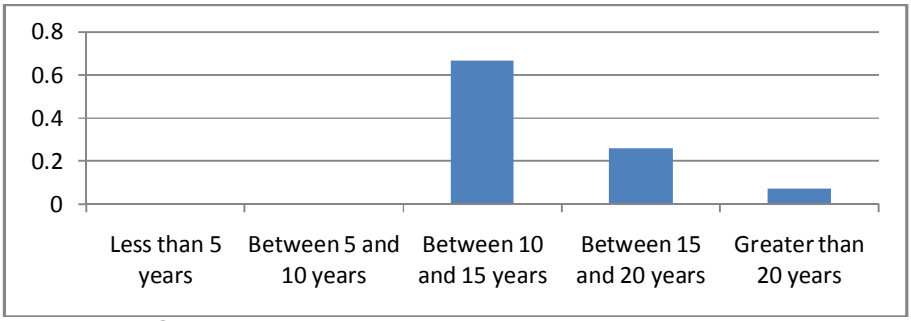

Figure 5.3 Graphical representation of experience

The majority of respondents had between 10 and 15 years of experience (66.67%), followed by respondents with between 15 and 20 years of experience (25.93%) and respondents with more than 20 years of experience (7.41%). On the whole it would appear that the respondents base was therefore comprised of senior to relatively

senior short-term industry participants with a considerable amount of short-term insurance industry experience.

5.5 Questions 1 and 41 – Importance of risk elements

Table 5.4 Current importance of risk areas

1. To what degree of primary importance would you rate the following areas of risk within your organisation?	1	2	3	4	5	6
1.1. Insurance risk				70.37%	29.63%	
1.2. Market risk	25.93%	59.26%	14.81%			
1.3. Credit risk			14.81%	70.37%	14.81%	
1.4. Operational risk			66.67%	29.63%	3.70%	
1.5. Liquidity risk		25.93%	70.37%	3.70%		
1.6. Reputation risk				44.44%	55.56%	
1.7. Political risk		66.67%	33.33%			
1.8. Legal risk			81.48%	18.52%		
1.9. Other:						

Table 5.5 Future importance of risk areas

41. In your opinion to what degree of primary importance should your organisation rate the following areas of risk?	1	2	3	4	5	6
41.1. Insurance risk					100%	
41.2. Market risk	3.70%	48.15%	48.15%			
41.3. Credit risk				77.78%	22.22%	
41.4. Operational risk					100%	
41.5. Liquidity risk		3.70%	74.07%	22.22%		
41.6. Reputation risk				40.74%	59.26%	
41.7. Political risk		3.70%	66.67%	29.63%		
41.8. Legal risk			7.41%	70.37%	22.22%	
41.9. Other:						

Table 5.6 Data analysis of questions 1 and 41

	Q	**Q**	**Q**	**Q**	**Q**	**Q**	**Q**	**Q**	**Q**
	1.1	**1.2**	**1.3**	**1.4**	**1.5**	**1.6**	**1.7**	**1.8**	**1.9**
Mean	4.30	1.89	4.00	3.37	2.78	4.56	2.33	3.19	0.00
	Q	**Q**	**Q**	**Q**	**Q**	**Q**	**Q**	**Q**	**Q**
	41.1	**41.2**	**41.3**	**41.4**	**41.5**	**41.6**	**41.7**	**41.8**	**41.9**
Mean	5.00	2.44	4.22	5.00	3.19	4.59	3.26	4.15	0.00
t-value	1.2E-08	1.7E-05	0.00567	1.3E-14	0.00051	0.16326	7.2E-08	1.8E-08	
df=26									
p = 0.05	1.71	1.71	1.71	1.71	1.71	1.71	1.71	1.71	
p = 0.10	1.32	1.32	1.32	1.32	1.32	1.32	1.32	1.32	
Sig. 0.05	**YES**	**YES**	NO	**YES**	NO	NO	**YES**	**YES**	
Sig. 0.10	**YES**	**YES**	NO	**YES**	NO	NO	**YES**	**YES**	

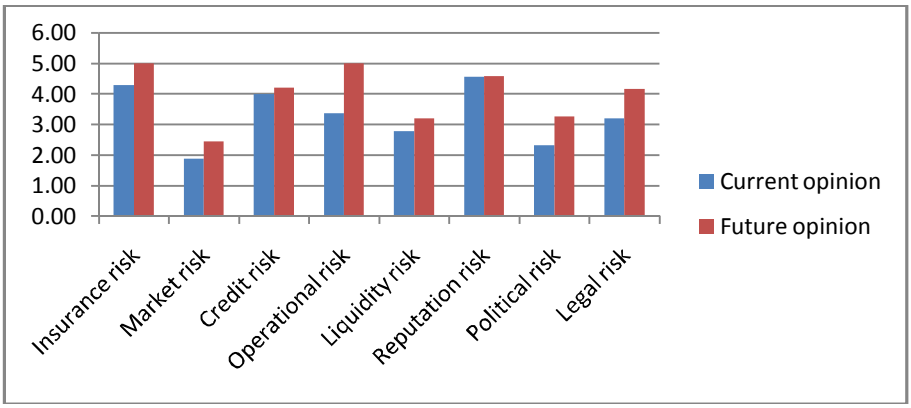

Figure 5.4 Comparison of mean values of current and future opinions of various risk areas

With regard to what degree of primary importance insurers rated / believed should be rated various areas of risk within their organisation, insurers currently recognise all areas of risk as being an area of risk within their organisations to a greater or lesser degree (insurance; market; credit; operational; liquidity; reputation; political; and legal risk). However, only insurance risk, credit risk and reputation risk are currently rated as primarily important. Insurers recommended view is that operational risk and legal risk also need to be considered as primarily important in addition to insurance risk, credit risk and reputation risk. The test results indicate significance at the 5% level of significance for insurance risk; market risk; operational risk; political risk and legal risk.

5.6 Questions 2 and 42 – Factors of operational risk

Table 5.7 Current factors of operational risk

2. To what degree does your organisation believe that the following are factors of operational risk?	1	2	3	4	5	6
2.1. People			11.11%	85.19%	3.70%	
2.2. Processes			33.33%	62.96%	3.70%	
2.3. Systems				96.30%	3.70%	
2.4. Other external factors (fraud, natural disasters)			48.15%	51.85%		
2.5. Other:						

Table 5.8 Future factors of operational risk

42. In your opinion to what degree should your organisation believe that the following are factors of operational risk?	1	2	3	4	5	6
42.1. People				40.74%	59.26%	
42.2. Processes				48.15%	51.85%	
42.3. Systems				33.33%	66.67%	
42.4. Other external factors (fraud, natural disasters)			7.41%	70.37%	22.22%	
42.5. Other:						

Table 5.9 Data analysis of questions 2 and 42

	Q	Q	Q	Q	Q
	2.1	**2.2**	**2.3**	**2.4**	**2.5**
Mean	3.93	3.70	4.04	3.52	0.00
	Q	**Q**	**Q**	**Q**	**Q**
	42.1	**42.2**	**42.3**	**42.4**	**42.5**
Mean	4.59	4.52	4.67	4.15	0.00
t-value	5.9E-08	7.1E-07	2.4E-07	2.1E-06	
df=26					
p = 0.05	1.71	1.71	1.71	1.71	
p = 0.10	1.32	1.32	1.32	1.32	
Sig. 0.05	**YES**	**YES**	**YES**	**YES**	
Sig. 0.10	**YES**	**YES**	**YES**	**YES**	

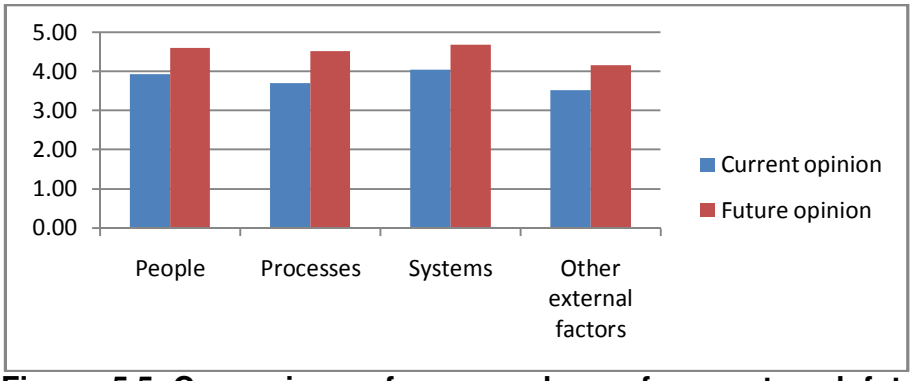

Figure 5.5 Comparison of mean values of current and future opinions of various factors of operational risk

In connection with to what degree do / should insurers believe that various elements are factors of operational risk only systems risk is currently considered a major factor of operational risk. However, insurers recommended view is that all four of the identified elements be in fact considered major factors of operational risk, which would include people; processes and other external events risks. The test results indicate significance at the 5% level of significance for all elements.

5.7 Questions 3 and 43 – Human factors as elements of operational risk

Table 5.10 Current human factors of operational risk

3. To what degree has your organisation recognised the following human factors as an important element of operational risk?	1	2	3	4	5	6
3.1. Incompetence			11.11%	88.89%		
3.2. Negligence			33.33%	66.67%		
3.3. Human error			29.63%	66.67%	3.70%	
3.4. Low morale		62.96%	37.04%			
3.5. High staff turnover		18.52%	55.56%	25.93%		
3.6. Criminal activities (fraud)			37.04%	62.96%		
3.7. Lack of skills or training			22.22%	77.78%		
3.8. Other:						

Table 5.11 Future human factors of operational risk

43. In your opinion to what degree should your organisation recognise the following human factors as an important element of operational risk?	1	2	3	4	5	6
43.1. Incompetence				51.85%	48.15%	
43.2. Negligence				55.56%	44.44%	
43.3. Human error				55.56%	44.44%	
43.4. Low morale				55.56%	44.44%	
43.5. High staff turnover			74.07%	22.22%	3.70%	
43.6. Criminal activities (fraud)			3.70%	96.30%		
43.7. Lack of skills or training				88.89%	11.11%	
43.8. Other:						

Table 5.12 Data analysis of questions 3 and 43

	Q	**Q**	**Q**	**Q**	**Q**	**Q**	**Q**	**Q**
	3.1	**3.2**	**3.3**	**3.4**	**3.5**	**3.6**	**3.7**	**3.8**
Mean	3.89	3.67	3.74	2.37	3.07	3.63	3.78	0.00
	Q	**Q**	**Q**	**Q**	**Q**	**Q**	**Q**	**Q**
	43.1	**43.2**	**43.3**	**43.4**	**43.5**	**43.6**	**43.7**	**43.8**
Mean	4.48	4.44	4.44	4.44	3.30	3.96	4.11	0.00
t-value	8.4E-07	2.1E-06	1.2E-06	8.9E-14	0.04151	0.00065	0.00065	
df=26								
p = 0.05	1.71	1.71	1.71	1.71	1.71	1.71	1.71	
p = 0.10	1.32	1.32	1.32	1.32	1.32	1.32	1.32	
Sig. 0.05	**YES**	**YES**	**YES**	**YES**	NO	NO	NO	
Sig. 0.10	**YES**	**YES**	**YES**	**YES**	NO	NO	NO	

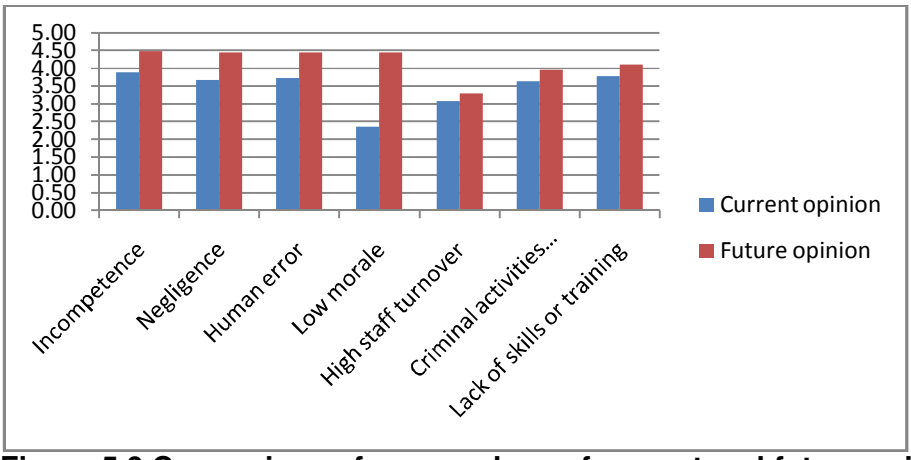

Figure 5.6 Comparison of mean values of current and future opinions of human elements as factors of operational risk

None of the factors of people risk is currently recognised as being an important element of operational risk (incompetence; negligence; human error; low morale; high staff turnover; criminal activities; lack of skill or training). However, insurers recommended view is that all factors with the exception of high staff turnover and criminal activities should be recognised as important elements of operational risk. The test results indicate significance at the 5% level of significance for incompetence; negligence; human error and low morale.

5.8 Questions 4 and 44 – Recognition of process exposures

Table 5.13 Current process exposures

4. To what degree has your organisation recognised the following process exposures as an important element of operational risk?	1	2	3	4	5	6
4.1. Errors in procedures or methodologies			37.04%	62.96%		
4.2. Execution errors			29.63%	66.67%		
4.3. Documentation errors			40.74%	59.26%		
4.4. Product complexity			37.04%	59.26%	3.70%	
4.5. Security risks			85.19%	14.81%		
4.6. Other:						

Table 5.14 Future process exposures

44. In your opinion to what degree should your organisation recognise the following process exposures as an important element of operational risk?	1	2	3	4	5	6
44.1. Errors in procedures or methodologies				70.37%	29.63%	
44.2. Execution errors				55.56%	44.44%	
44.3. Documentation errors				48.15%	51.85%	
44.4. Product complexity			25.93%	70.37%	3.70%	
44.5. Security risks			62.96%	37.04%		
44.6. Other:						

Table 5.15 Data analysis of questions 4 and 44

	Q	Q	Q	Q	Q	Q
	4.1	**4.2**	**4.3**	**4.4**	**4.5**	**4.6**
Mean	3.63	3.74	3.59	3.67	3.15	0.00
	Q	**Q**	**Q**	**Q**	**Q**	**Q**
	44.1	**44.2**	**44.3**	**44.4**	**44.5**	**44.6**
Mean	4.30	4.44	4.52	3.78	3.37	0.00
t-value	1.3E-05	1.5E-05	2.7E-07	0.04151	0.00567	
df=26						
p = 0.05	1.71	1.71	1.71	1.71	1.71	
p = 0.10	1.32	1.32	1.32	1.32	1.32	
Sig. 0.05	**YES**	**YES**	**YES**	NO	NO	
Sig. 0.10	**YES**	**YES**	**YES**	NO	NO	

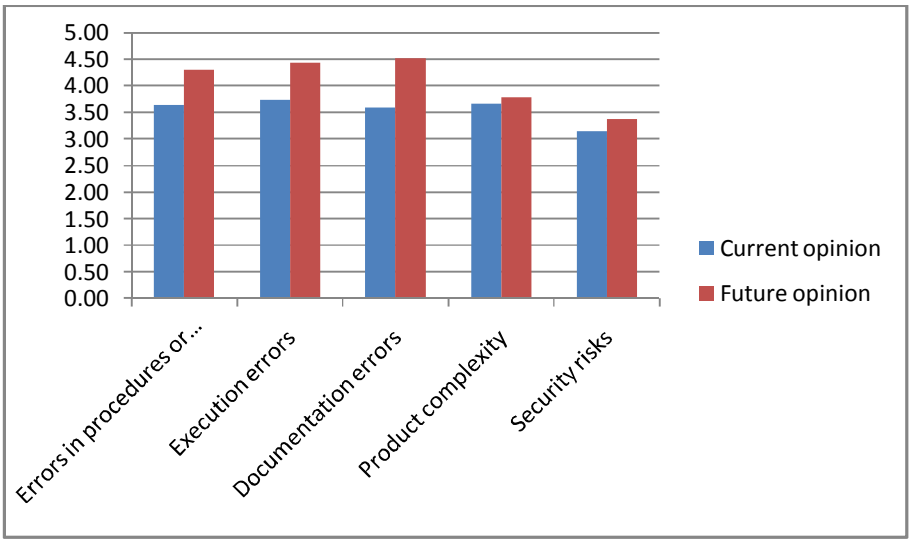

Figure 5.7 Comparison of mean values of current and future opinions of recognition of process exposures

All of the elements of process exposures are only recognised to a fair degree currently (errors in procedures or methodologies; execution errors; documentation errors; product complexity; security risks). Insurers do however recommend that with the exception of product complexity and security risks, all of the exposures should be recognised to a high degree. The test results indicate significance at the 5% level of

significance for errors in procedures or methodologies; execution errors and documentation errors.

5.9 Questions 5 and 45 – Recognition of systems exposures

Table 5.16 Current systems exposures

5. To what degree has your organisation recognised the following systems exposures as an important element of operational risk?	1	2	3	4	5	6
5.1. System infiltration		3.70%	14.81%	81.48%		
5.2. System failure			7.41%	92.59%		
5.3. Third party computer fraud			29.63%	70.37%		
5.4. Programming errors			44.44%	55.56%		
5.5. Information risk			40.74%	55.56%	3.70%	
5.6. Telecommunications risk			33.33%	66.67%		
5.7. System obsolescence		3.70%	77.78%	18.52%		
5.8. Other:						

Table 5.17 Future systems exposures

45. In your opinion to what degree should your organisation recognise the following systems exposures as an important element of operational risk?	1	2	3	4	5	6
45.1. System infiltration		3.70%		92.59%	3.70%	
45.2. System failure				74.07%	25.93%	
45.3. Third party computer fraud				81.48%	18.52%	
45.4. Programming errors			3.70%	85.19%	11.11%	
45.5. Information risk				77.78%	22.22%	
45.6. Telecommunications risk				92.59%	7.41%	
45.7. System obsolescence				85.19%	14.81%	
45.8. Other:						

Table 5.18 Data analysis of questions 5 and 45

	Q	**Q**	**Q**	**Q**	**Q**	**Q**	**Q**	**Q**
	5.1	**5.2**	**5.3**	**5.4**	**5.5**	**5.6**	**5.7**	**5.8**
Mean	3.78	3.93	3.70	3.56	3.63	3.67	3.15	0.00
	Q	**Q**	**Q**	**Q**	**Q**	**Q**	**Q**	**Q**
	45.1	**45.2**	**45.3**	**45.4**	**45.5**	**45.6**	**45.7**	**45.8**
Mean	3.96	4.26	4.19	4.07	4.22	4.07	4.15	0.00
t-value	0.01113	0.00065	0.00031	0.00035	6.2E-06	0.00131	4.1E-10	
df=26								
p = 0.05	1.71	1.71	1.71	1.71	1.71	1.71	1.71	
p = 0.10	1.32	1.32	1.32	1.32	1.32	1.32	1.32	
Sig. 0.05	NO	NO	NO	NO	**YES**	NO	**YES**	
Sig. 0.10	NO	NO	NO	NO	**YES**	NO	**YES**	

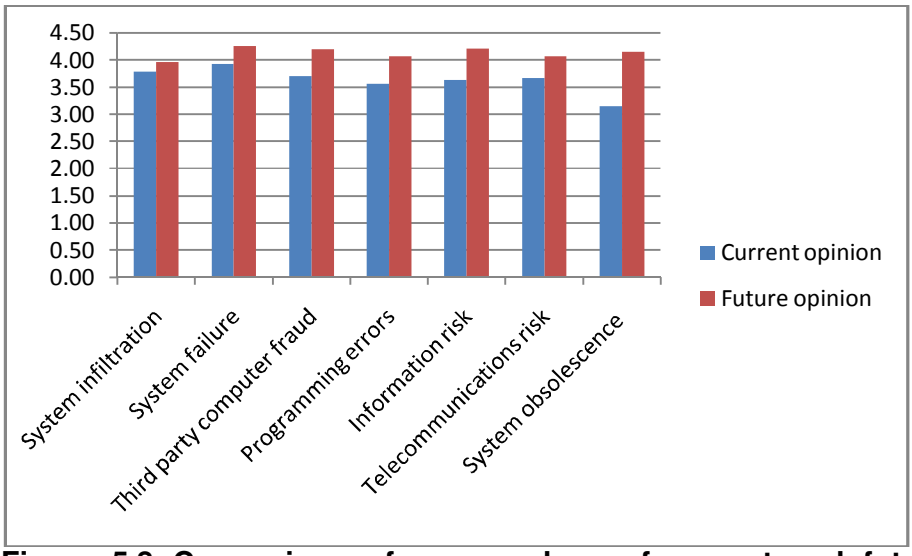

Figure 5.8 Comparison of mean values of current and future opinions of recognition of systems exposures

All of the elements of systems exposures are only recognised to a fair degree currently (system infiltration; system failure; third party computer fraud; programming errors; information risk; telecommunications risk; system obsolescence). Insurers do however recommend that with the exception of system infiltration, all of the exposures should in fact be recognised to a high degree. The test results indicate significance at the 5% level of significance for information risk and system obsolescence.

5.10 Questions 6 and 46 – Recognition of external exposures

Table 5.19 Current external exposures

6. To what degree has your organisation recognised the following external exposures as an important element of operational risk?	1	2	3	4	5	6
6.1. Acts of God		74.07%	25.93%			
6.2. Crime		37.04%	62.96%			
6.3. Regulation and compliance				48.15%	51.85%	
6.4. Legal actions			33.33%	59.26%	7.41%	
6.5. Changes in the business environment			62.96%	37.04%		
6.6. Other:						

Table 5.20 Future external exposures

46. In your opinion to what degree should your organisation recognise the following external exposures as an important element of operational risk?	1	2	3	4	5	6
46.1. Acts of God		3.70%		70.37%	25.93%	
46.2. Crime				40.74%	59.26%	
46.3. Regulation and compliance				40.74%	59.26%	
46.4. Legal actions				85.19%	14.81%	
46.5. Changes in the business environment				55.56%	44.44%	
46.6. Other:						

Table 5.21 Data analysis of questions 6 and 46

	Q	Q	Q	Q	Q	Q
	6.1	**6.2**	**6.3**	**6.4**	**6.5**	**6.6**
Mean	2.26	2.63	4.52	3.74	3.37	0.00
	Q	**Q**	**Q**	**Q**	**Q**	**Q**
	46.1	**46.2**	**46.3**	**46.4**	**46.5**	**46.6**
Mean	4.19	4.59	4.59	4.15	4.44	0.00
t-value	1.9E-20	2.5E-28	0.08059	0.00013	1.9E-07	
df=26						
p = 0.05	1.71	1.71	1.71	1.71	1.71	
p = 0.10	1.32	1.32	1.32	1.32	1.32	
Sig. 0.05	**YES**	**YES**	NO	NO	**YES**	
Sig. 0.10	**YES**	**YES**	NO	NO	**YES**	

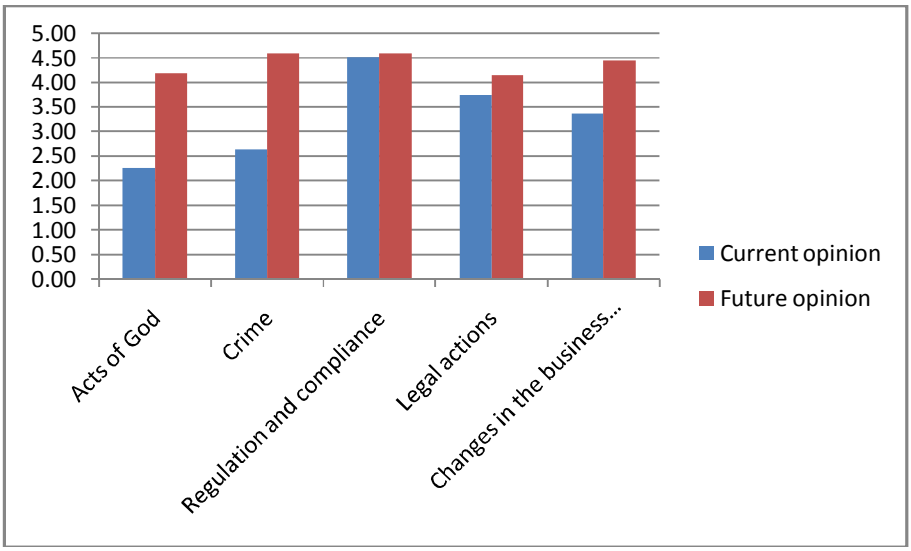

Figure 5.9 Comparison of mean values of current and future opinions of recognition of external exposures

Of the various external exposures (acts of God; crime; regulation and compliance; legal actions; changes in the business environment) only regulation and compliance are currently recognised to a high degree, with the balance of exposures being recognised to a lesser or fair degree. Insurers do however recommend that all of the exposures should in fact be recognised to a high degree. The test results indicate

significance at the 5% level of significance for acts of God; crime and changes in the business environment.

5.11 Questions 7 and 47 – Importance of an ERM programme

Table 5.22 Current importance of risk management process

	1	2	3	4	5	6
7. To what degree does your organisation recognise the importance of implementing a formal risk management (ERM) process?				18.52%	81.48%	

Table 5.23 Future importance of risk management process

	1	2	3	4	5	6
47. In your opinion to what degree should your organisation recognise the importance of implementing a formal risk management (ERM) process?					100%	

Table 5.24 Data analysis of questions 7 and 47

	Q
	7
Mean	4.81
	Q
	47
Mean	5.00
t-value	0.01113
df=26	
p = 0.05	1.71
p = 0.10	1.32
Sig. 0.05	NO
Sig. 0.10	NO

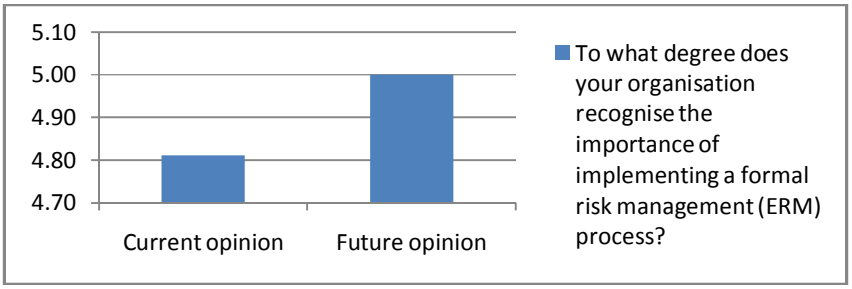

Figure 5.10 Comparison of mean value of current and future opinion of degree of recognition of importance of implementing an ERM process

Insurers indicated recognition of implementing an enterprise risk management process to a high degree currently, with insurers recommended view being that it should be totally implemented.

5.12 Questions 8 and 48 – Formal definition of operational risk

Table 5.25 Current definition of operational risk

	1	2	3	4	5	6
8. To what degree has your organisation adopted a formal definition of operational risk?			7.41%	40.74%	51.85%	

Table 5.26 Future definition of operational risk

	1	2	3	4	5	6
48. In your opinion to what degree should your organisation adopt a formal definition of operational risk?					100%	

Table 5.27 Data analysis of questions 8 and 48

	Q
	8
Mean	4.44
	Q
	48
Mean	5.00
t-value	6.2E-05
df=26	
p = 0.05	1.71
p = 0.10	1.32
Sig. 0.05	**YES**
Sig. 0.10	**YES**

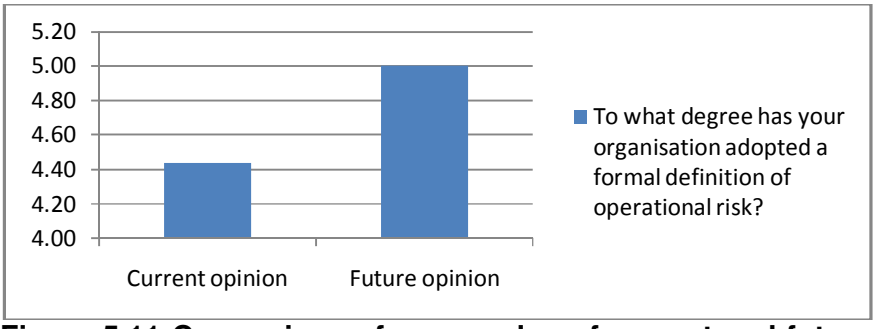

Figure 5.11 Comparison of mean value of current and future opinion of degree of adoption of formal definition of operational risk

Insurers indicated adoption of a formal definition of operational risk to a high degree currently, with insurers recommended view that it should be totally adopted. The test results indicate significance at the 5% level of significance.

5.13 Questions 9 and 49 – Elements of operational risk management

Table 5.28 Current elements of operational risk

9. To what degree has your organisation recognised the following as important elements of an operational risk management process?	1	2	3	4	5	6
9.1. Risk identification				55.56%	44.44%	
9.2. Risk measurement and evaluation			7.41%	77.78%	14.81%	
9.3. Risk control			55.56%	40.74%	3.70%	
9.4. Other:						

Table 5.29 Future elements of operational risk

49. In your opinion to what degree should your organisation recognise the following as important elements of an operational risk management process?	1	2	3	4	5	6
49.1. Risk identification					100%	
49.2. Risk measurement and evaluation					100%	
49.3. Risk control					100%	
49.4. Other:						

Table 5.30 Data analysis of questions 9 and 49

	Q	Q	Q	Q
	9.1	**9.2**	**9.3**	**9.4**
Mean	4.44	4.07	3.48	0.00
	Q	**Q**	**Q**	**Q**
	49.1	**49.2**	**49.3**	**49.4**
Mean	5.00	5.00	5.00	0.00
t-value	2.7E-06	7.9E-11	1.2E-13	
df=26				
p = 0.05	1.71	1.71	1.71	
p = 0.10	1.32	1.32	1.32	
Sig. 0.05	**YES**	**YES**	**YES**	
Sig. 0.10	**YES**	**YES**	**YES**	

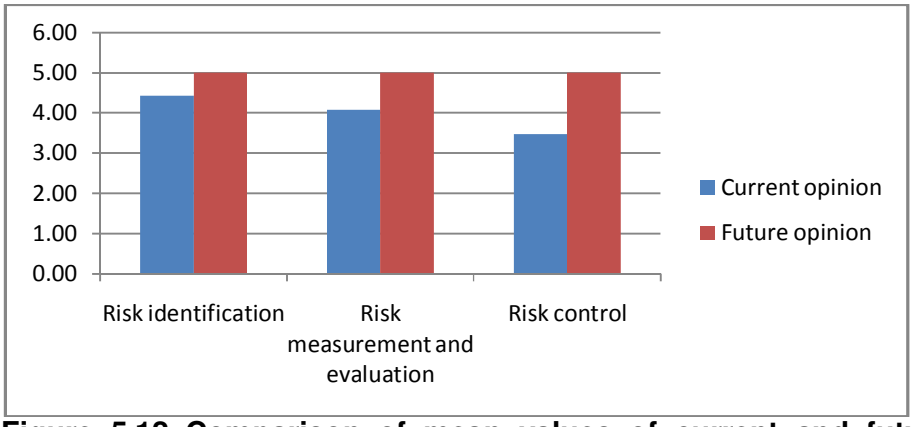

Figure 5.12 Comparison of mean values of current and future opinions of recognition of elements of operational risk management process

All of the elements of an operational risk management process (risk identification; risk measurement and evaluation; risk control) are recognised to a high degree currently, with insurers recommended view that they should be recognised totally. The test results indicate significance at the 5% level of significance for all elements.

5.14 Questions 10 and 50 – Risk management alignment to strategy

Table 5.31 Current alignment of risk management

	1	2	3	4	5	6
10. To what degree is risk management currently aligned to the overall business strategy, including covering the planned risk profile of the organisation and the approach to managing those risks?			37.04%	62.96%		

Table 5.32 Future alignment of risk management

	1	2	3	4	5	6
50. In your opinion to what degree should risk management be aligned to the overall business strategy, including covering the planned risk profile of the organisation and the approach to managing those risks?					100%	

Table 5.33 Data analysis of questions 10 and 50

	Q
	10
Mean	3.63
	Q
	50
Mean	5.00
t-value	3E-14
df=26	
p = 0.05	1.71
p = 0.10	1.32
Sig. 0.05	**YES**
Sig. 0.10	**YES**

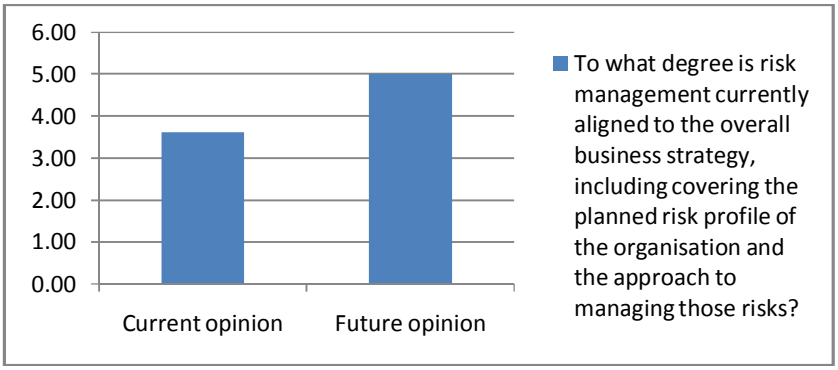

Figure 5.13 Comparison of mean value of current and future opinion of degree of risk alignment to business strategy

Insurers indicated that risk management is aligned to the overall business strategy, including covering the planned risk profile of the organisation and the approach to managing those risks to a fair degree currently, with insurers recommended view that alignment should be total. The test results indicate significance at the 5% level of significance.

5.15 Questions 11 and 51 – Integration of operational risk management

Table 5.34 Current integration of risk management

	1	2	3	4	5	6
11. To what degree is an operational risk management process recognised as an important and integral part of your organisation's overall management process?			62.96%	37.04%		

Table 5.35 Future integration of risk management

	1	2	3	4	5	6
51. In your opinion to what degree should an operational risk management process be recognised as an important and integral part of your organisation's overall management process?					100%	

Table 5.36 Data analysis of questions 11 and 51

	Q
	11
Mean	3.37
	Q
	51
Mean	5.00
t-value	5E-16
df=26	
p = 0.05	1.71
p = 0.10	1.32
Sig. 0.05	**YES**
Sig. 0.10	**YES**

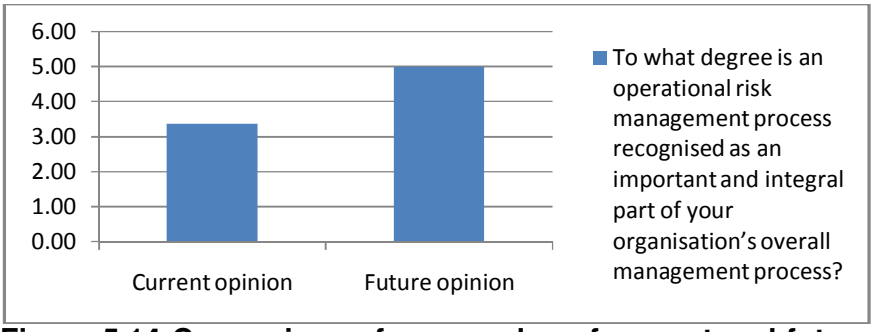

Figure 5.14 Comparison of mean value of current and future opinion of degree of recognition of risk management process as integral to overall organisation management process

Insurers indicated that an operational risk management process is recognised as an important and integral part of their organisation's overall management process to a fair degree currently, with insurers recommended view that recognition should be total. The test results indicate significance at the 5% level of significance.

5.16 Questions 12 and 52 – Board involvement in risk management

Table 5.37 Current board involvement in risk management

	1	2	3	4	5	6
12. To what degree does the board currently set the strategies, policies and processes surrounding risk management?			33.33%	66.67%		

Table 5.38 Future board involvement in risk management

	1	2	3	4	5	6
52. In your opinion to what degree should the board set the strategies, policies and processes surrounding risk management?					100%	

Table 5.39 Data analysis of questions 12 and 52

	Q
	12
Mean	3.67
	Q
	52
Mean	5.00
t-value	3.2E-14
df=26	
p = 0.05	1.71
p = 0.10	1.32
Sig. 0.05	**YES**
Sig. 0.10	**YES**

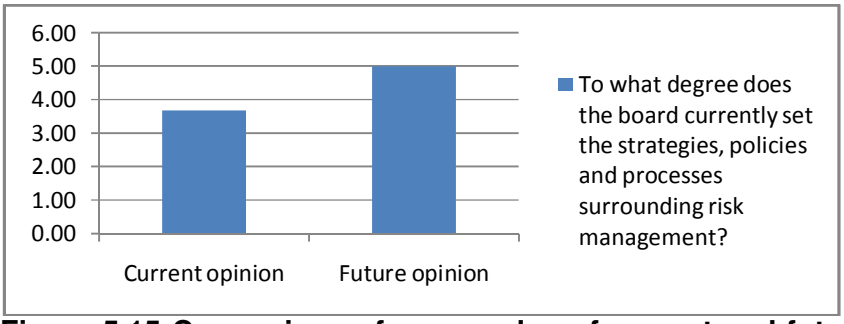

Figure 5.15 Comparison of mean value of current and future opinion of degree of board involvement in risk management strategies, policies and processes

Insurers indicated that their boards set the strategies, policies and processes surrounding risk management to a fair degree currently, with insurers recommended view that this should be implemented totally. The test results indicate significance at the 5% level of significance.

5.17 Questions 13 and 53 – Board oversight of risk management

Table 5.40 Current board oversight of risk management

	1	2	3	4	5	6
13. To what degree does the board currently actively provide oversight to risk management strategies?			18.52%	81.48%		

Table 5.41 Future board oversight of risk management

	1	2	3	4	5	6
53. In your opinion to what degree should the board actively provide oversight to risk management strategies?					100%	

Table 5.42 Data analysis of questions 13 and 53

	Q
	13
Mean	3.81
	Q
	53
Mean	5.00
t-value	5.5E-15
df=26	
p = 0.05	1.71
p = 0.10	1.32
Sig. 0.05	**YES**
Sig. 0.10	**YES**

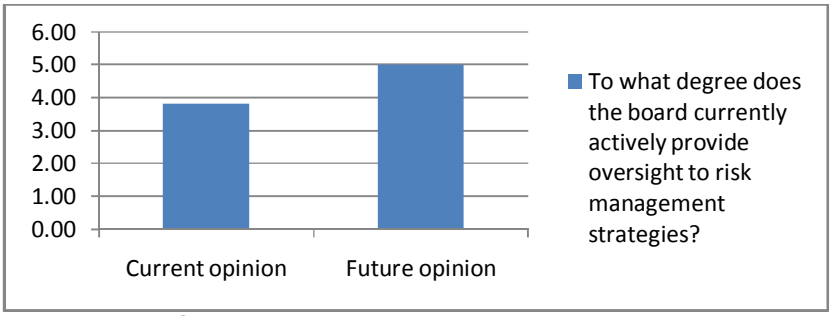

Figure 5.16 Comparison of mean value of current and future opinion of degree of board oversight to risk management strategies

Insurers indicated that their boards actively provide oversight to risk management strategies to a fair degree currently, with insurers recommended view that this should be the case totally. The test results indicate significance at the 5% level of significance.

5.18 Questions 14 and 54 – Board engagement on risk management

Table 5.43 Current board engagement

	1	2	3	4	5	6
14. To what degree does the board currently actively challenge management's assessment of key risks and their approach to managing those risks?			25.93%	74.07%		

Table 5.44 Future board engagement

	1	2	3	4	5	6
54. In your opinion to what degree should the board actively challenge management's assessment of key risks and their approach to managing those risks?					100%	

Table 5.45 Data analysis of questions 14 and 54

	Q
	14
Mean	3.74
	Q
	54
Mean	5.00
t-value	2.2E-14
df=26	
p = 0.05	1.71
p = 0.10	1.32
Sig. 0.05	**YES**
Sig. 0.10	**YES**

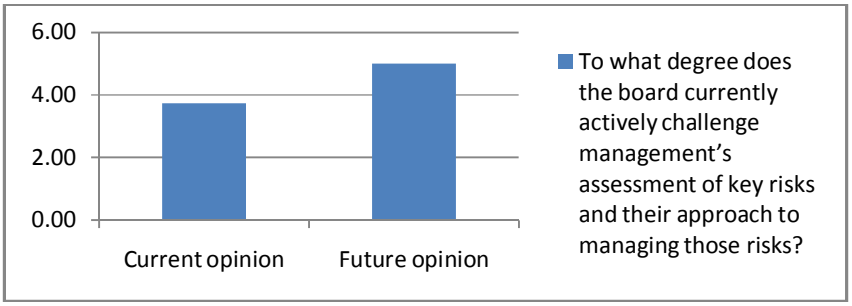

Figure 5.17 Comparison of mean value of current and future opinion of degree of board challenging of management's assessment of and approach to managing key risks

Insurers indicated that their boards actively challenge management's assessment of key risks and their approach to managing those risks to a fair degree currently, with insurers recommended view that this should occur totally. The test results indicate significance at the 5% level of significance.

5.19 Questions 15 and 55 – Risk appetite

Table 5.46 Current risk appetite

	1	2	3	4	5	6
15. To what degree is there a comprehensive understanding of and agreement on the organisation's risk appetite within the organisation?		48.15%	48.15%	3.70%		

Table 5.47 Future risk appetite

	1	2	3	4	5	6
55. In your opinion to what degree should there be a comprehensive understanding of and agreement on the organisation's risk appetite within the organisation?					100%	

Table 5.48 Data analysis of questions 15 and 55

	Q
	15
Mean	2.56
	Q
	55
Mean	5.00
t-value	1.2E-18
df=26	
p = 0.05	1.71
p = 0.10	1.32
Sig. 0.05	**YES**
Sig. 0.10	**YES**

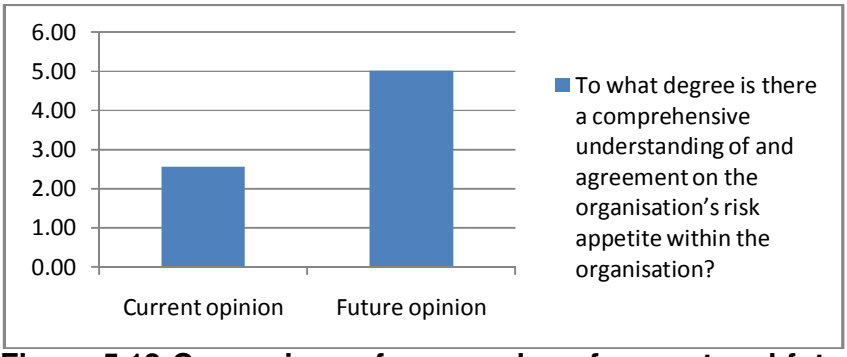

Figure 5.18 Comparison of mean value of current and future opinion of degree of understanding and agreement on the organisation's risk appetite

Insurers indicated that there is a comprehensive understanding of and agreement on the organisation's risk appetite within the organisation to a lesser degree currently, with insurers recommended view that understanding and agreement should be total. The test results indicate significance at the 5% level of significance.

5.20 Questions 16 and 56 – Integration of risk management

Table 5.49 Current integration of risk management

	1	2	3	4	5	6
16. To what degree is your organisation's risk management process integrated? (That is, to what extent is risk management owned, monitored and managed at a local level within the organisation?)		33.33%	66.67%			

Table 5.50 Future integration of risk management

	1	2	3	4	5	6
56. In your opinion to what degree should your organisation's risk management process be integrated? (That is, to what extent should risk management be owned, monitored and managed at a local level within the business?)					100%	

Table 5.51 Data analysis of questions 16 and 56

	Q
	16
Mean	2.67
	Q
	56
Mean	5.00
t-value	4.1E-20
df=26	
p = 0.05	1.71
p = 0.10	1.32
Sig. 0.05	**YES**
Sig. 0.10	**YES**

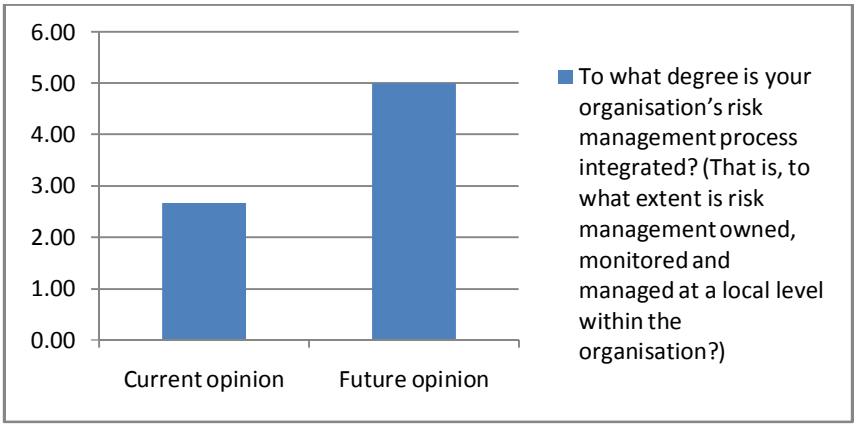

Figure 5.19 Comparison of mean value of current and future opinion of degree of integration of organisation's risk management processes

Insurers indicated that their organisation's risk management processes are integrated to a lesser degree currently, with insurers recommended view that integration should be total. The test results indicate significance at the 5% level of significance.

5.21 Questions 17 and 57 – Communication of risk appetite

Table 5.52 Current communication of risk appetite

	1	2	3	4	5	6
17. To what degree is the organisational risk appetite clearly communicated to business unit managers who are required to implement operational risk management processes?		55.56%	44.44%			

Table 5.53 Future communication of risk appetite

	1	2	3	4	5	6
57. In your opinion to what degree should the organisational risk appetite be clearly communicated to business unit managers who are required to implement operational risk management processes?					100%	

Table 5.54 Data analysis of questions 17 and 57

	Q
	17
Mean	2.44
	Q
	57
Mean	5.00
t-value	1.6E-20
df=26	
p = 0.05	1.71
p = 0.10	1.32
Sig. 0.05	**YES**
Sig. 0.10	**YES**

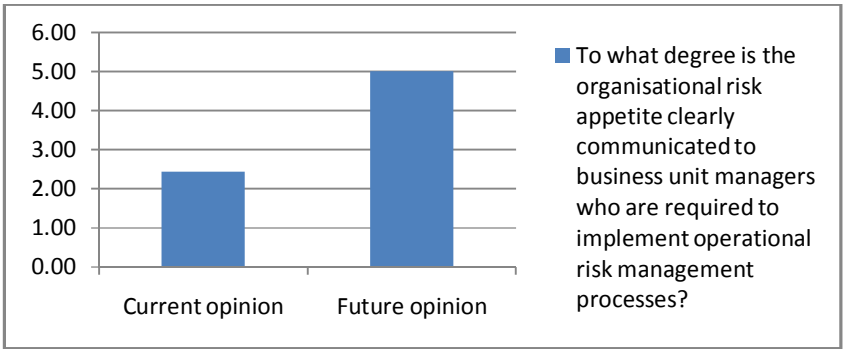

Figure 5.20 Comparison of mean value of current and future opinion of degree of communication organisation's risk appetite to business unit managers

Insurers indicated that the organisational risk appetite is clearly communicated to business unit managers who are required to implement operational risk management processes to a lesser degree currently, with insurers recommended view that communication should be total. The test results indicate significance at the 5% level of significance.

5.22 Questions 18 and 58 – Incentive compensation

Table 5.55 Current incentive compensation

	1	2	3	4	5	6
18. To what degree is current management incentive compensation tied to organisational risk objectives and risk / return measures approved by the board?		85.19%	14.81%			

Table 5.56 Future incentive compensation

	1	2	3	4	5	6
58. In your opinion to what degree should management incentive compensation be tied to organisational risk objectives and risk / return measures approved by the board?					100%	

Table 5.57 Data analysis of questions 18 and 58

	Q
	18
Mean	2.15
	Q
	58
Mean	5.00
t-value	1.9E-25
df=26	
p = 0.05	1.71
p = 0.10	1.32
Sig. 0.05	**YES**
Sig. 0.10	**YES**

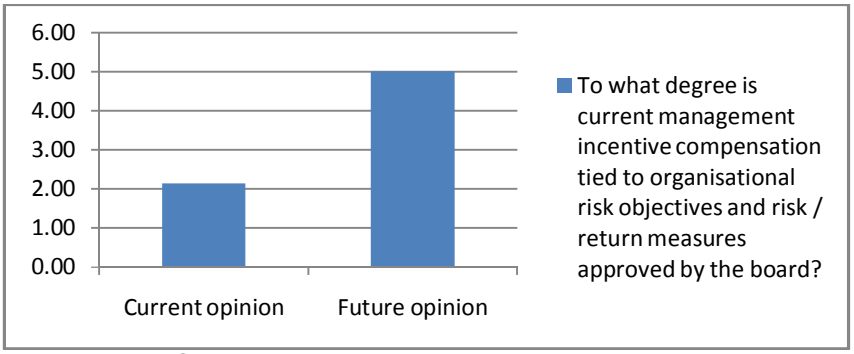

Figure 5.21 Comparison of mean value of current and future opinion of degree of management incentive compensation being tied to organisational risk objectives and risk / return measures

Insurers indicated that current management incentive compensation is tied to organisational risk objectives and risk / return measures approved by the board to a lesser degree currently, with insurers recommended view that this should occur totally. The test results indicate significance at the 5% level of significance.

5.23 Questions 19 and 59 – Segregation of duties

Table 5.58 Current segregation of duties

	1	2	3	4	5	6
19. To what degree is there appropriate segregation of duties between those responsible for monitoring and measuring risk and those responsible for making decisions?		48.15%	51.85%			

Table 5.59 Future segregation of duties

	1	2	3	4	5	6
59. In your opinion to what degree should there be appropriate segregation of duties between those responsible for monitoring and measuring risk and those responsible for making decisions?				59.26%	40.74%	

Table 5.60 Data analysis of questions 19 and 59

	Q
	19
Mean	2.52
	Q
	59
Mean	4.41
t-value	5.8E-14
df=26	
p = 0.05	1.71
p = 0.10	1.32
Sig. 0.05	**YES**
Sig. 0.10	**YES**

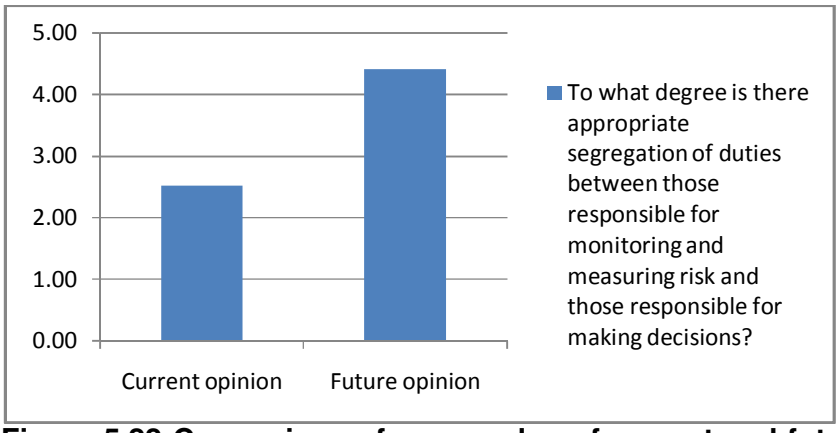

Figure 5.22 Comparison of mean value of current and future opinion of degree of segregation of duties between risk monitors and decision makers

Insurers indicated that there is appropriate segregation of duties between those responsible for monitoring and measuring risk and those responsible for making decisions to a lesser degree currently, with insurers recommended view that

segregation should be in place to a high degree. The test results indicate significance at the 5% level of significance.

5.24 Questions 20 and 60 – Risk control measures

Table 5.61 Current risk control measures

20. To what degree has your organisation recognised the importance of and implemented the following operational risk control measures?	1	2	3	4	5	6
20.1. Policies and procedures			77.78%	22.22%		
20.2. Internal controls			7.41%	92.59%		
20.3. Risk reporting			29.63%	66.67%	3.70%	
20.4. Other:						

Table 5.62 Future risk control measures

60. In your opinion to what degree should your organisation recognise the importance of and implement the following operational risk control measures?	1	2	3	4	5	6
60.1. Policies and procedures					100%	
60.2. Internal controls					100%	
60.3. Risk reporting					100%	
60.4. Other:						

Table 5.63 Data analysis of questions 20 and 60

	Q	Q	Q	Q
	20.1	**20.2**	**20.3**	**20.4**
Mean	3.22	3.93	3.74	0.00
	Q	**Q**	**Q**	**Q**
	60.1	**60.2**	**60.3**	**60.4**
Mean	5.00	5.00	5.00	0.00
t-value	1.6E-18	4.4E-18	9.3E-13	
df=26				
p = 0.05	1.71	1.71	1.71	
p = 0.10	1.32	1.32	1.32	
Sig. 0.05	**YES**	**YES**	**YES**	
Sig. 0.10	**YES**	**YES**	**YES**	

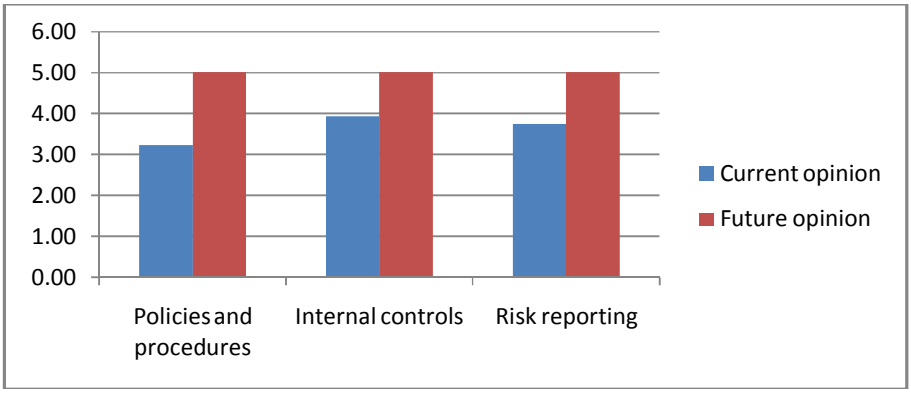

Figure 5.23 Comparison of mean values of current and future opinions of various operational risk control measures

All of the operational risk controls (policies and procedures; internal controls; risk reporting) were only recognised by insurers to a fair degree currently, with insurers recommended view that they should all be recognised totally. The test results indicate significance at the 5% level of significance for all measures.

5.25 Questions 21 and 61 – Measurement of operational risk

Table 5.64 Current measurement of operational risk

21. To what degree does your organisation use the following methods to measure operational risk?	1	2	3	4	5	6
21.1. Stress testing	88.89%	11.11%				
21.2. Scenario analysis	51.85%	48.15%				
21.3. Simulation techniques	88.89%	11.11%				
21.4. Actuarial methods		66.67%	33.33%			
21.5. Historical data to forecast potential losses		59.26%	40.74%			
21.6. Self-risk assessments		22.22%	74.07%	3.70%		
21.7. Risk maps and process flows		62.96%	33.33%	3.70%		
21.8. Other:						

Table 5.65 Future measurement of operational risk

61. In your opinion to what degree should your organisation use the following methods to measure operational risk?	1	2	3	4	5	6
61.1. Stress testing			85.19%	14.81%		
61.2. Scenario analysis			48.15%	51.85%		
61.3. Simulation techniques			81.48%	18.52%		
61.4. Actuarial methods				66.67%	33.33%	
61.5. Historical data to forecast potential losses				51.85%	48.15%	
61.6. Self-risk assessments				25.93%	74.07%	
61.7. Risk maps and process flows			3.70%	62.96%	33.33%	
61.8. Other:						

Table 5.66 Data analysis of questions 21 and 61

	Q	Q	Q	Q	Q	Q	Q	Q
	21.1	**21.2**	**21.3**	**21.4**	**21.5**	**21.6**	**21.7**	**21.8**
Mean	1.11	1.48	1.11	2.33	2.41	2.81	2.41	0.00
	Q	**Q**	**Q**	**Q**	**Q**	**Q**	**Q**	**Q**
	61.1	**61.2**	**61.3**	**61.4**	**61.5**	**61.6**	**61.7**	**61.8**
Mean	3.15	3.52	3.19	4.33	4.48	4.74	4.30	0.00
t-value	9.7E-29	9.7E-29	2.7E-25	7E-219	2.7E-25	1.8E-24	3.5E-19	
df=26								
p = 0.05	1.71	1.71	1.71	1.71	1.71	1.71	1.71	
p = 0.10	1.32	1.32	1.32	1.32	1.32	1.32	1.32	
Sig. 0.05	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	
Sig. 0.10	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	

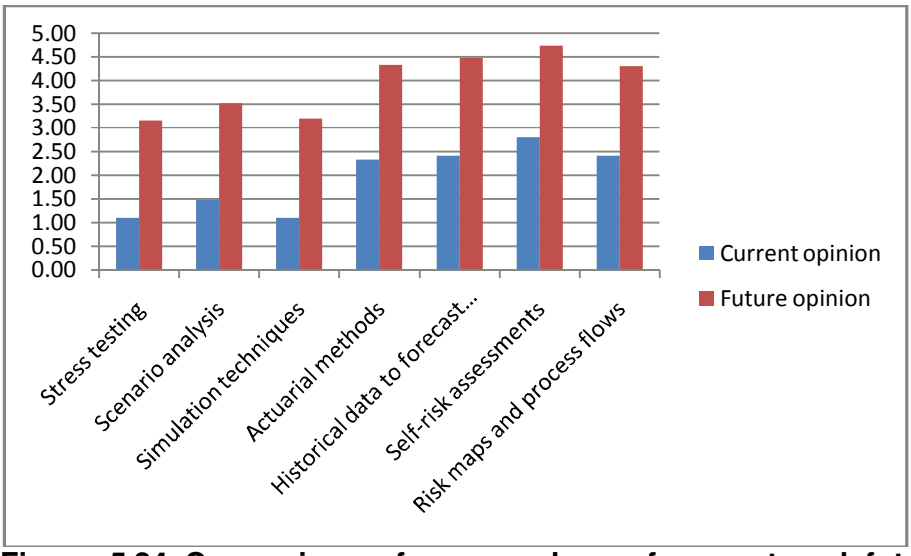

Figure 5.24 Comparison of mean values of current and future opinions of various methods to measure operational risk

Insurers indicated that whilst not currently the case, their recommended view is that all of the various methods identified to measure operational risk should be used to a greater or lesser degree (stress testing; scenario analysis; simulation techniques; actuarial methods; historical data to forecast potential losses; self-risk assessments; risk maps and process flows). The test results indicate significance at the 5% level of significance for all methods.

5.26 Questions 22 and 62 – Ongoing identification of operational risks

Table 5.67 Current ongoing identification of operational risks

	1	2	3	4	5	6
22. To what degree does your organisation currently have an ongoing process in place for identifying / managing significant operational risks?		18.52%	70.37%	11.11%		

Table 5.68 Future ongoing identification of operational risks

	1	2	3	4	5	6
62. In your opinion to what degree should your organisation have an ongoing process in place for identifying / managing significant operational risks?					100%	

Table 5.69 Data analysis of questions 22 and 62

	Q
	22
Mean	2.93
	Q
	62
Mean	5.00
t-value	2.1E-17
df=26	
p = 0.05	1.71
p = 0.10	1.32
Sig. 0.05	**YES**
Sig. 0.10	**YES**

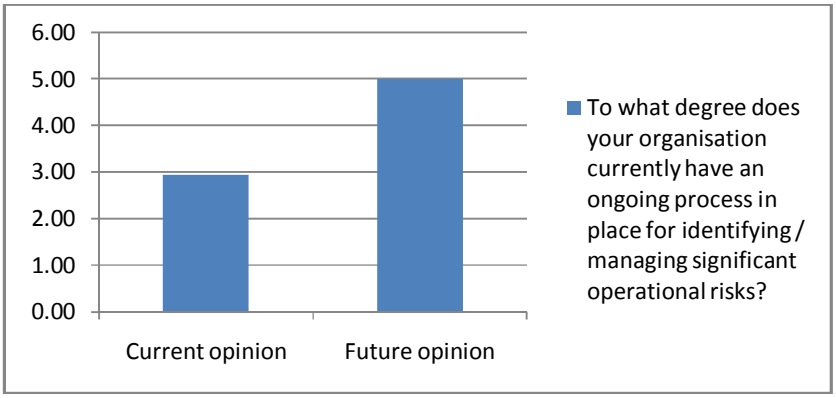

Figure 5.25 Comparison of mean value of current and future opinion of degree of ongoing process in place for identifying / managing significant operational risks

Insurers indicated that their organisations have an ongoing process in place for identifying / managing significant operational risks to a lesser degree currently, with insurers recommended view being that this should be in place totally. The test results indicate significance at the 5% level of significance.

5.27 Questions 23 and 63 – Risk strategy alignment

Table 5.70 Current risk strategy alignment

	1	2	3	4	5	6
23. To what degree does your organisation have a risk strategy related to risk classes as well as overall risk exposure?		22.22%	77.78%			

Table 5.71 Future risk strategy alignment

	1	2	3	4	5	6
63. In your opinion to what degree should your organisation have a risk strategy related to risk classes as well as overall risk exposure?					100%	

Table 5.72 Data analysis of questions 23 and 63

	Q
	23
Mean	2.78
	Q
	63
Mean	5.00
t-value	6E-21
df=26	
p = 0.05	1.71
p = 0.10	1.32
Sig. 0.05	**YES**
Sig. 0.10	**YES**

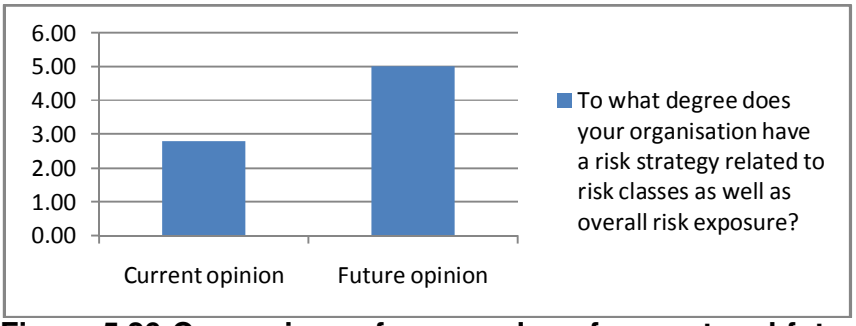

Figure 5.26 Comparison of mean value of current and future opinion of degree of a risk strategy related to risk classes as well as overall risk exposure

Insurers indicated that their organisations have a risk strategy related to risk classes as well as overall risk exposure to a lesser degree currently, with insurers recommended view being that a strategy should be in place totally. The test results indicate significance at the 5% level of significance.

5.28 Questions 24 and 64 – Methods to identify operational risk

Table 5.73 Current methods to identify operational risk

24. To what degree has your organisation recognised the following methods as the most appropriate to identify risks?	1	2	3	4	5	6
24.1. Workshops		18.52%	77.78%		3.70%	
24.2. Brainstorming		33.33%	62.96%	3.70%		
24.3. Questionnaires	22.22%	74.07%		3.70%		
24.4. Process mapping	40.74%	59.26%				
24.5. Comparison with other organisations	59.26%	40.74%				
24.6. Peer discussions			77.78%	22.22%		
24.7. Other:						

Table 5.74 Future methods to identify operational risk

64. In your opinion to what degree should your organisation recognise the following methods as the most appropriate to identify risks?	1	2	3	4	5	6
64.1. Workshops			44.44%	51.85%	3.70%	
64.2. Brainstorming			48.15%	51.85%		
64.3. Questionnaires		44.44%	51.85%		3.70%	
64.4. Process mapping		33.33%	62.96%	3.70%		
64.5. Comparison with other organisations			70.37%	29.63%		
64.6. Peer discussions			3.70%	66.67%	29.63%	
64.7. Other:						

Table 5.75 Data analysis of questions 24 and 64

	Q	**Q**	**Q**	**Q**	**Q**	**Q**	**Q**
	24.1	**24.2**	**24.3**	**24.4**	**24.5**	**24.6**	**24.7**
Mean	2.89	2.70	1.85	1.59	1.41	3.22	0.00
	Q	**Q**	**Q**	**Q**	**Q**	**Q**	**Q**
	64.1	**64.2**	**64.3**	**64.4**	**64.5**	**64.6**	**64.7**
Mean	3.59	3.52	2.63	2.70	3.30	4.26	0.00
t-value	1.2E-06	1.6E-07	9.8E-08	6.5E-12	3.1E-13	4.4E-09	
df=26							
p = 0.05	1.71	1.71	1.71	1.71	1.71	1.71	
p = 0.10	1.32	1.32	1.32	1.32	1.32	1.32	
Sig. 0.05	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	
Sig. 0.10	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	

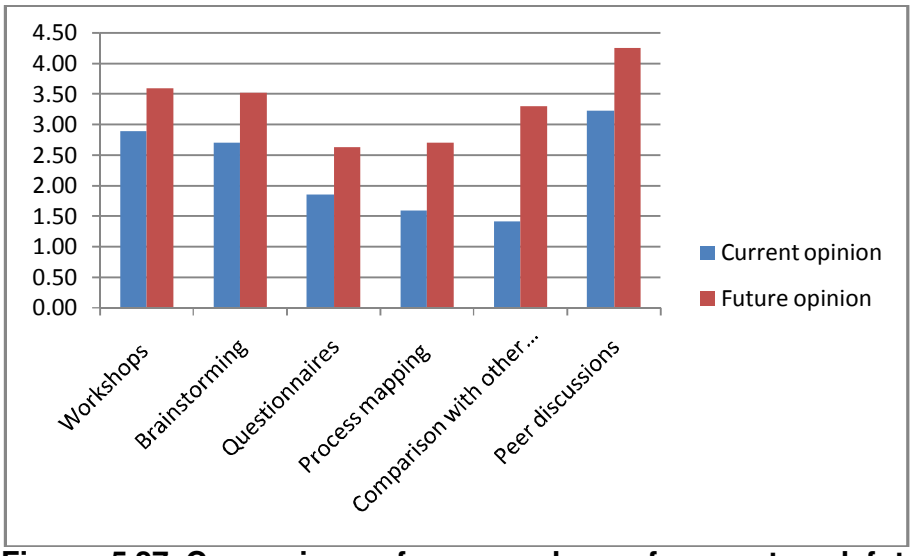

Figure 5.27 Comparison of mean values of current and future opinions of various methods to identify risks

Insurers indicated that whilst not currently the case, their recommended view is that all of the various methods recognised as appropriate to identify risks (workshops; brainstorming; questionnaires; process mapping; comparison with other organisations; peer discussions) should be used to a greater or lesser degree. The test results indicate significance at the 5% level of significance for all methods.

5.29 Questions 25 and 65 – Independent risk management structure

Table 5.76 Current state of independent risk management structure

	1	2	3	4	5	6
25. To what degree has your organisation established a separate operational risk management structure?		40.74%	59.26%			

Table 5.77 Future state of independent risk management structure

	1	2	3	4	5	6
65. In your opinion to what degree should your organisation establish a separate operational risk management structure?			3.70%	48.15%	48.15%	

Table 5.78 Data analysis of questions 25 and 65

	Q
	25
Mean	2.59
	Q
	65
Mean	4.44
t-value	8.4E-13
df=26	
p = 0.05	1.71
p = 0.10	1.32
Sig. 0.05	**YES**
Sig. 0.10	**YES**

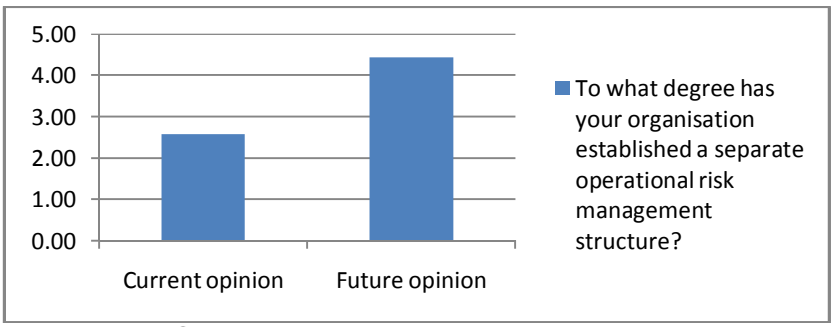

Figure 5.28 Comparison of mean value of current and future opinion of degree of establishment of a separate operational risk management structure

Insurers indicated that their organisations have established a separate operational risk management structure to a lesser degree currently, with insurers recommended view being that it should occur to a high degree. The test results indicate significance at the 5% level of significance.

5.30 Questions 26 and 66 – Access of risk manager to CEO

Table 5.79 Current access of risk manager to CEO

	1	2	3	4	5	6
26. To what degree does a risk manager have direct access to the CEO of your organisation?			11.11%	51.85%	37.04%	

Table 5.80 Future access of risk manager to CEO

	1	2	3	4	5	6
66. In your opinion to what degree should a risk manager have direct access to the CEO of your organisation?					100%	

Table 5.81 Data analysis of questions 26 and 66

	Q
	26
Mean	4.26
	Q
	66
Mean	5.00
t-value	1.7E-06
df=26	
p = 0.05	1.71
p = 0.10	1.32
Sig. 0.05	**YES**
Sig. 0.10	**YES**

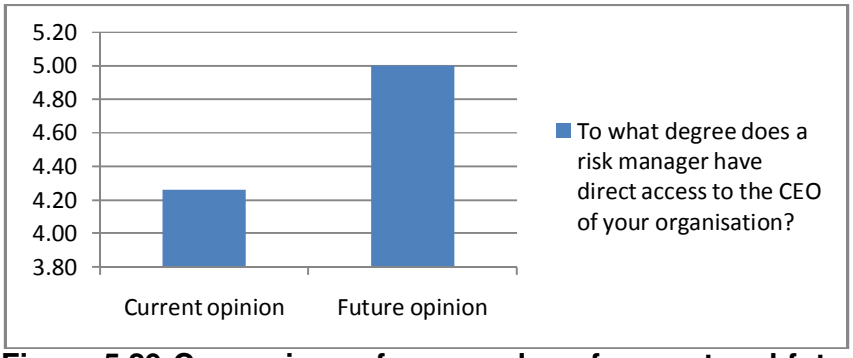

Figure 5.29 Comparison of mean value of current and future opinion of degree of direct access a risk manager should have to the CEO of the organisation

Insurers indicated that risk managers have direct access to the CEO of their organisations to a high degree currently, with insurers recommended view being that access should be total. The test results indicate significance at the 5% level of significance.

5.31 Questions 27 and 67 – Involvement of internal audit

Table 5.82 Current involvement of internal audit

	1	2	3	4	5	6
27. To what degree does your organisation involve internal audit to manage operational risk?			29.63%	40.74%	29.63%	

Table 5.83 Future involvement of internal audit

	1	2	3	4	5	6
67. In your opinion to what degree should your organisation involve internal audit to manage operational risk?				48.15%	51.85%	

Table 5.84 Data analysis of questions 27 and 67

	Q
	27
Mean	4.00
	Q
	67
Mean	4.52
t-value	0.00283
df=26	
p = 0.05	1.71
p = 0.10	1.32
Sig. 0.05	NO
Sig. 0.10	NO

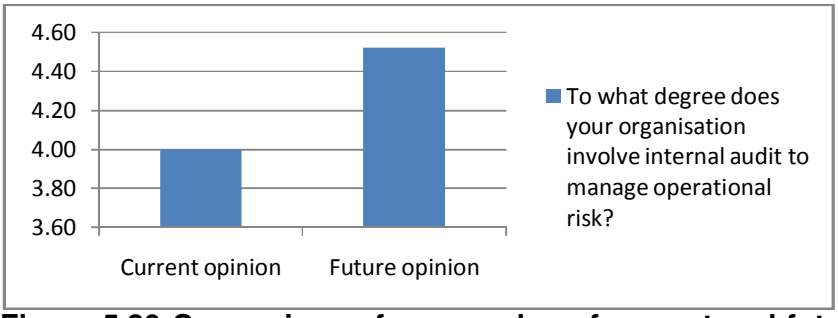

Figure 5.30 Comparison of mean value of current and future opinion of degree to which the organisation involves internal audit to manage operational risk

Insurers indicated that their organisations involve internal audit to manage operational risk to a high degree currently, with insurers recommended view that this should occur to a high degree.

5.32 Questions 28 and 68 – Involvement of business unit managers

Table 5.85 Current involvement of business unit managers

	1	2	3	4	5	6
28. To what degree does your organisation involve business unit managers in operational risk management processes?			29.63%	66.67%	3.70%	

Table 5.86 Future involvement of business unit managers

	1	2	3	4	5	6
68. In your opinion to what degree should your organisation involve business unit managers in operational risk management processes?					100%	

Table 5.87 Data analysis of questions 28 and 68

	Q
	28
Mean	3.74
	Q
	68
Mean	5.00
t-value	9.3E-13
df=26	
p = 0.05	1.71
p = 0.10	1.32
Sig. 0.05	**YES**
Sig. 0.10	**YES**

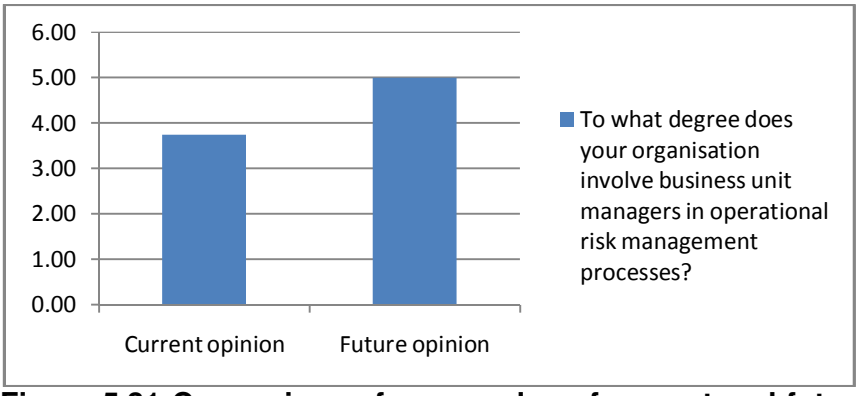

Figure 5.31 Comparison of mean value of current and future opinion of degree to which the organisation involves business unit managers in operational risk management processes

Insurers indicated that their organisations involve business unit managers in operational risk management processes to a fair degree currently, with insurers recommended view being that involvement should be total. The test results indicate significance at the 5% level of significance.

5.33 Questions 29 and 69 – Adjustment of organisational risk appetite

Table 5.88 Current adjustment of organisational risk appetite

	1	2	3	4	5	6
29. To what degree does your organisation on an ongoing, immediate basis adjust the organisation's risk appetite and risk processes based on past experiences, pro forma results, future stakeholder expectations and existing market conditions?	11.11%	77.78%	11.11%			

Table 5.89 Future adjustment of organisational risk appetite

	1	2	3	4	5	6
69. In your opinion to what degree should your organisation on an ongoing, immediate basis adjust the organisation's risk appetite and risk processes based on past experiences, pro forma results, future stakeholder expectations and existing market conditions?			3.70%		96.30%	

Table 5.90 Data analysis of questions 29 and 69

	Q
	29
Mean	2.00
	Q
	69
Mean	4.93
t-value	9.9E-23
df=26	
p = 0.05	1.71
p = 0.10	1.32
Sig. 0.05	**YES**
Sig. 0.10	**YES**

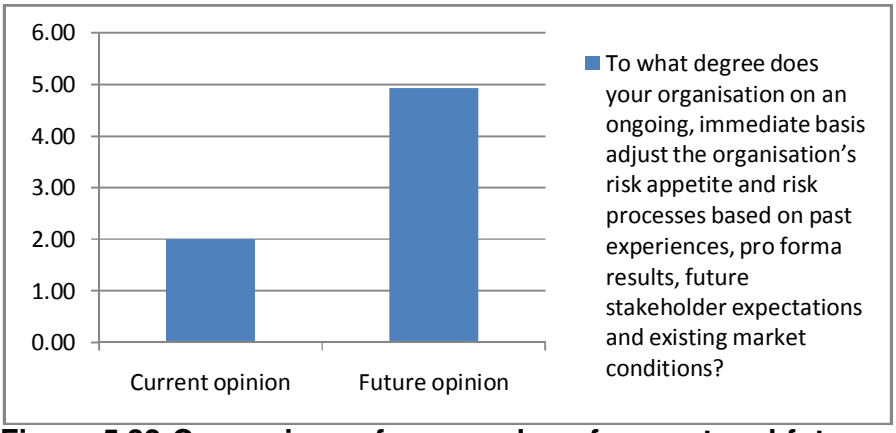

Figure 5.32 Comparison of mean value of current and future opinion of degree to which the organisation adjusts its risk appetite / processes based on experiences, pro forma results, future stakeholder expectations and existing market conditions

Insurers indicated that their organisations on an ongoing, immediate basis adjust the organisation's risk appetite and risk processes based on past experiences, pro forma results, future stakeholder expectations and existing market conditions to a lesser degree currently, with insurers recommended view being that this should occur to a high degree. The test results indicate significance at the 5% level of significance.

5.34 Questions 30 and 70 – Influences on risk management processes

Table 5.91 Current influences on risk management processes

30. To what degree do the following factors influence your organisation's development and improvement of risk management processes?	1	2	3	4	5	6
30.1. Compliance - regulatory				85.19%	14.81%	
30.2. Compliance - shareholders				88.89%	11.11%	
30.3. Compliance - market			33.33%	62.96%	3.70%	
30.4. Business driven logic		22.22%	66.67%	11.11%		
30.5. Losses made by others		40.74%	59.26%			
30.6. Being a pioneer in risk management	3.70%	59.26%	37.04%			
30.7. Image		22.22%	62.96%	14.81%		
30.8. Other:						

Table 5.92 Future influences on risk management processes

70. In your opinion to what degree should the following factors influence your organisation's development and improvement of risk management processes?	1	2	3	4	5	6
70.1. Compliance - regulatory					100%	
70.2. Compliance - shareholders				55.56%	44.44%	
70.3. Compliance - market				96.30%	3.70%	
70.4. Business driven logic				66.67%	33.33%	
70.5. Losses made by others				74.07%	25.93%	
70.6. Being a pioneer in risk management			70.37%	29.63%		
70.7. Image			33.33%	66.67%		
70.8. Other:						

Table 5.93 Data analysis of questions 30 and 70

	Q	**Q**	**Q**	**Q**	**Q**	**Q**	**Q**	**Q**
	30.1	**30.2**	**30.3**	**30.4**	**30.5**	**30.6**	**30.7**	**30.8**
Mean	4.15	4.11	3.70	2.89	2.59	2.33	2.93	0.00
	Q	**Q**	**Q**	**Q**	**Q**	**Q**	**Q**	**Q**
	70.1	**70.2**	**70.3**	**70.4**	**70.5**	**70.6**	**70.7**	**70.8**
Mean	5.00	4.44	4.04	4.33	4.26	3.30	3.67	0.00
t-value	1.4E-12	0.00218	0.00065	3.5E-13	5E-15	2.6E-09	3.6E-07	
df=26								
p = 0.05	1.71	1.71	1.71	1.71	1.71	1.71	1.71	
p = 0.10	1.32	1.32	1.32	1.32	1.32	1.32	1.32	
Sig. 0.05	**YES**	NO	NO	**YES**	**YES**	**YES**	**YES**	
Sig. 0.10	**YES**	NO	NO	**YES**	**YES**	**YES**	**YES**	

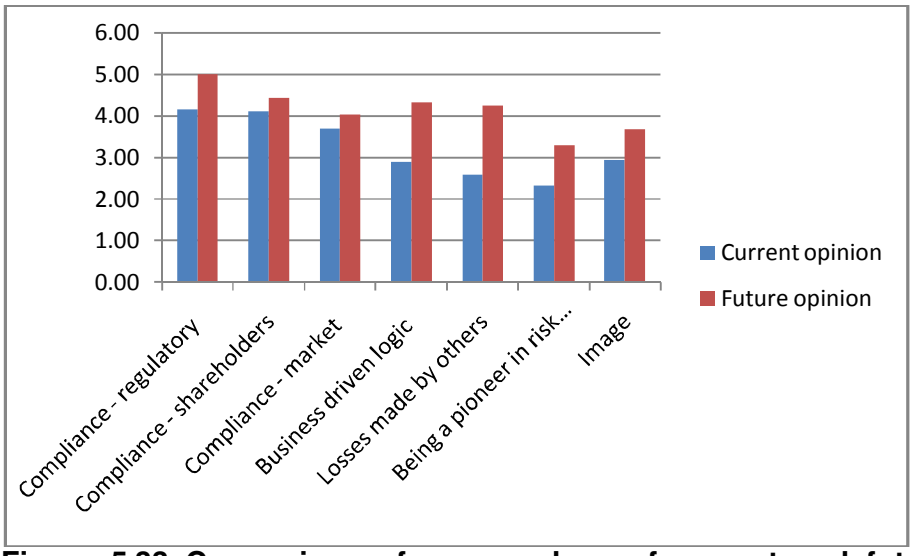

Figure 5.33 Comparison of mean values of current and future opinions of various factors influencing organisation's development and improvement of risk management processes

Of the various factors which can influence their organisation's development and improvement of risk management processes (regulatory compliance; shareholder compliance; market compliance; business driven logic; losses made by others; being a pioneer in risk management; image), only shareholder and market compliance was rated as influencing factors to a high degree currently, with all other factors being considered influencing factors to a lesser or fair degree. Insurers recommended view was that being a pioneer in risk management and image should be rated as influencing factors to a fair degree whilst all other factors should be considered as influencing factors to a high degree. The test results indicate significance at the 5% level of significance for regulatory compliance; business driven logic; losses made by others; being a pioneer in risk management and image.

5.35 Questions 31 and 71 – Risk / return based decision making

Table 5.94 Current risk / return based decision making

	1	2	3	4	5	6
31. To what degree are decisions to enter or withdraw from certain lines of business based upon their potential impact on the organisation's risk / return measures?			66.67%	33.33%		

Table 5.95 Future risk / return based decision making

	1	2	3	4	5	6
71. In your opinion to what degree should decisions to enter or withdraw from certain lines of business be based upon their potential impact on the organisation's risk / return measures?				74.07%	25.93%	

Table 5.96 Data analysis of questions 31 and 71

	Q
	31
Mean	3.33
	Q
	71
Mean	4.26
t-value	1.6E-09
df=26	
p = 0.05	1.71
p = 0.10	1.32
Sig. 0.05	**YES**
Sig. 0.10	**YES**

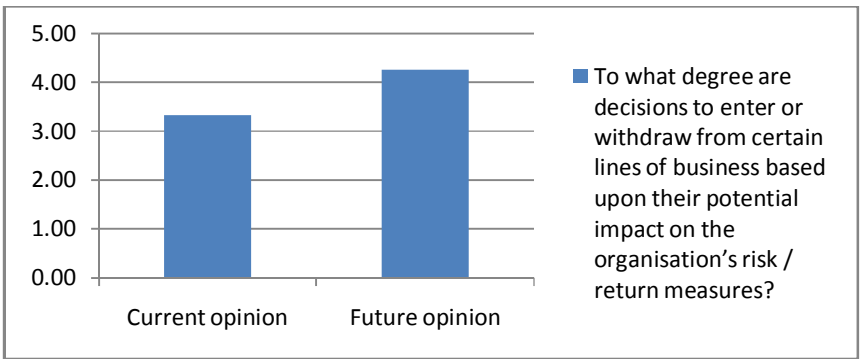

Figure 5.34 Comparison of mean value of current and future opinion of degree to which decisions to enter or withdraw from certain lines of business are based upon their potential impact on the organisation's risk / return measures

Insurers indicated that decisions to enter or withdraw from certain lines of business are based upon their potential impact on the organisation's risk / return measures to a fair degree currently, with insurers recommended view being that it should occur to a high degree. The test results indicate significance at the 5% level of significance.

5.36 Questions 32 and 72 – Dependencies between risks

Table 5.97 Current dependencies between risks

	1	2	3	4	5	6
32. To what degree does your organisation account for dependencies between risks?	7.41%	74.07%	18.52%			

Table 5.98 Future dependencies between risks

	1	2	3	4	5	6
72. In your opinion to what degree should your organisation account for dependencies between risks?				77.78%	22.22%	

Table 5.99 Data analysis of questions 32 and 72

	Q
	32
Mean	2.11
	Q
	72
Mean	4.22
t-value	1.8E-18
df=26	
p = 0.05	1.71
p = 0.10	1.32
Sig. 0.05	**YES**
Sig. 0.10	**YES**

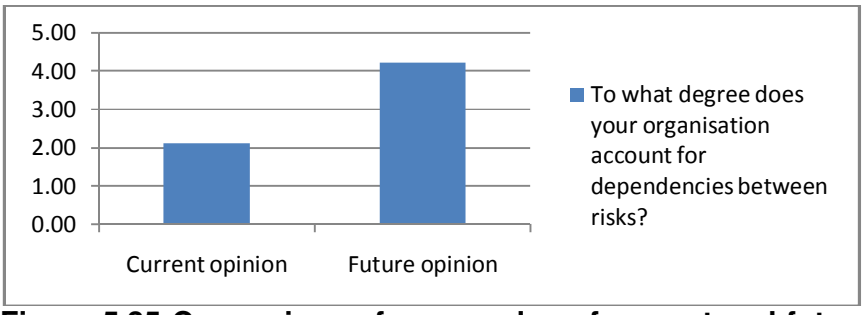

Figure 5.35 Comparison of mean value of current and future opinion of degree to which organisation accounts for dependencies between risks

Insurers indicated that their organisations account for dependencies between risks to a lesser degree currently, with insurers recommended view being that it should occur to a high degree. The test results indicate significance at the 5% level of significance.

5.37 Questions 33 and 73 – Outsourcing of risk management functions

Table 5.100 Current outsourcing of risk management functions

	1	2	3	4	5	6
33. To what degree does your organisation currently outsource any of the risk management functions within your organisation?	22.22%	62.96%	11.11%	3.70%		

Table 5.101 Future outsourcing of risk management functions

	1	2	3	4	5	6
73. In your opinion to what degree should your organisation outsource any of the risk management functions within your organisation?	33.33%	37.04%	22.22%	7.41%		

Table 5.102 Data analysis of questions 33 and 73

	Q
	33
Mean	1.96
	Q
	73
Mean	2.04
t-value	0.33902
df=26	
p = 0.05	1.71
p = 0.10	1.32
Sig. 0.05	NO
Sig. 0.10	NO

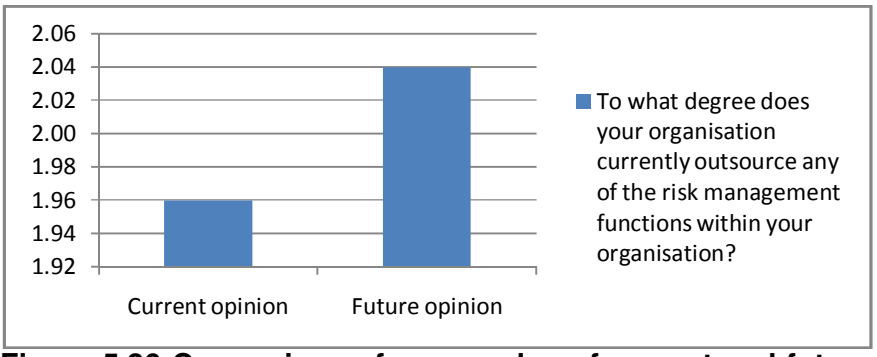

Figure 5.36 Comparison of mean value of current and future opinion of degree to which organisation outsources any of the risk management functions within the organisation

Insurers indicated that their organisations outsource risk management functions within the organisation to no degree currently, with insurers recommended view that this should occur to a lesser degree.

5.38 Questions 34 and 74 – Use of a corporate scorecard

Table 5.103 Current use of a corporate scorecard

	1	2	3	4	5	6
34. To what degree does your organisation use some form of corporate scorecard to assess risk and measure it against predetermined tolerances?		18.52%	74.07%	7.41%		

Table 5.104 Future use of a corporate scorecard

	1	2	3	4	5	6
74. In your opinion to what degree should your organisation use some form of corporate scorecard to assess risk and measure it against predetermined tolerances?			3.70%	70.37%	25.93%	

Table 5.105 Data analysis of questions 34 and 74

	Q
	34
Mean	2.89
	Q
	74
Mean	4.22
t-value	8.6E-13
df=26	
p = 0.05	1.71
p = 0.10	1.32
Sig. 0.05	**YES**
Sig. 0.10	**YES**

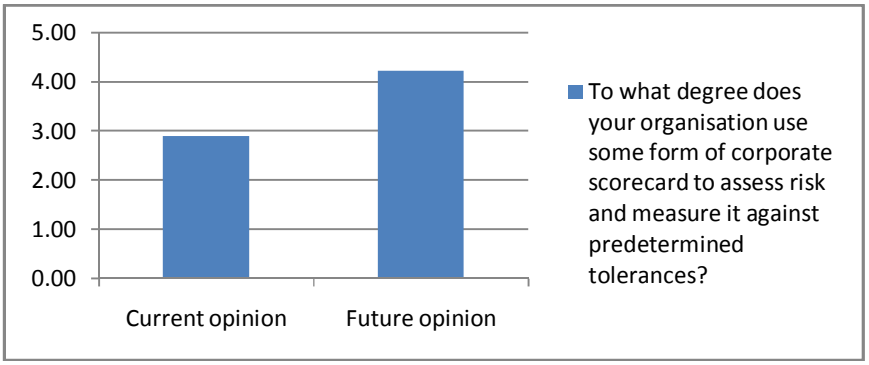

Figure 5.37 Comparison of mean value of current and future opinion of degree to which organisation uses some form of corporate scorecard to assess risk and measure it against predetermined tolerances

Insurers indicated that their organisations use some form of corporate scorecard to assess risk and measure it against predetermined tolerances to a lesser degree currently, with insurers recommended view being that it should occur to a high degree. The test results indicate significance at the 5% level of significance.

5.39 Questions 35 and 75 – Management reporting

Table 5.106 Current management reporting

	1	2	3	4	5	6
35. To what degree do your organisational management reports supply information using measures that identify areas where risk tolerances are being exceeded or risk objectives not met?		37.04%	62.96%			

Table 5.107 Future management reporting

	1	2	3	4	5	6
75. In your opinion to what degree should your organisational management reports supply information using measures that identify areas where risk tolerances are being exceeded or risk objectives not met?					100%	

Table 5.108 Data analysis of questions 35 and 75

	Q
	35
Mean	2.63
	Q
	75
Mean	5.00
t-value	5E-20
df=26	
p = 0.05	1.71
p = 0.10	1.32
Sig. 0.05	**YES**
Sig. 0.10	**YES**

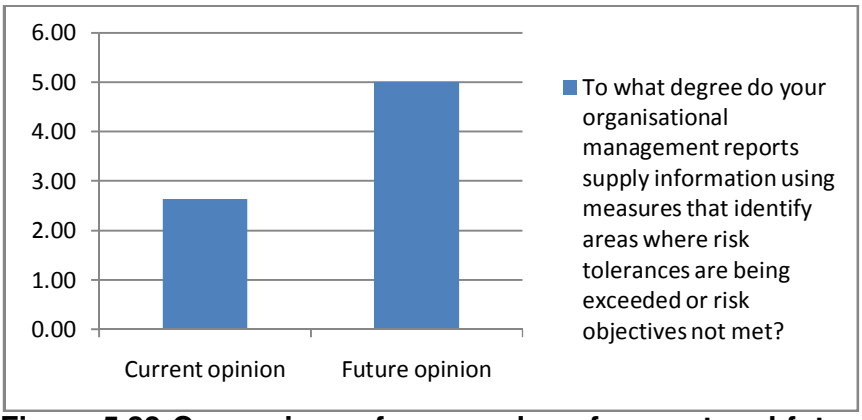

Figure 5.38 Comparison of mean value of current and future opinion of degree to which organisational management reports supply information using measures that identify areas where risk tolerances are being exceeded or risk objectives not met

Insurers indicated that their organisational management reports supply information using measures that identify areas where risk tolerances are being exceeded or risk objectives not met to a lesser degree currently, with insurers recommended view that this should occur totally. The test results indicate significance at the 5% level of significance.

5.40 Questions 36 and 76 – Effectiveness of risk mitigation techniques

Table 5.109 Current effectiveness of risk mitigation techniques

	1	2	3	4	5	6
36. To what degree does your organisation have processes or measures in place that are able to determine the effectiveness of risk mitigation techniques that have been implemented?	3.70%	29.63%	66.67%			

Table 5.110 Future effectiveness of risk mitigation techniques

	1	2	3	4	5	6
76. In your opinion to what degree should your organisation have processes or measures in place that are able to determine the effectiveness of risk mitigation techniques that have been implemented?				66.67%	33.33%	

Table 5.111 Data analysis of questions 36 and 76

	Q
	36
Mean	2.63
	Q
	76
Mean	4.33
t-value	1.7E-15
df=26	
p = 0.05	1.71
p = 0.10	1.32
Sig. 0.05	**YES**
Sig. 0.10	**YES**

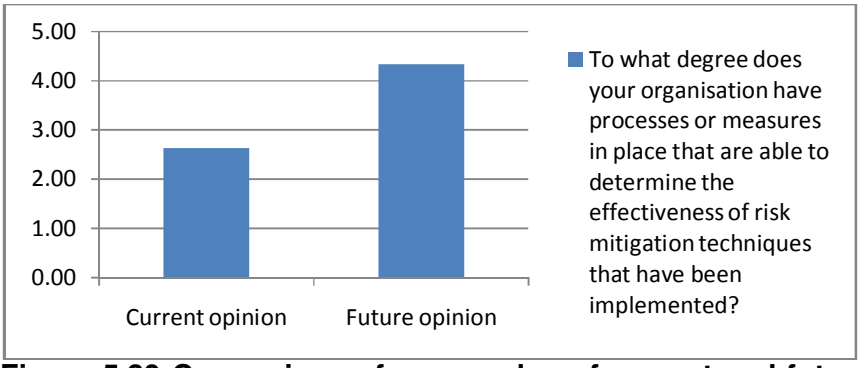

Figure 5.39 Comparison of mean value of current and future opinion of degree to which the organisation has processes or measures in place that are able to determine the effectiveness of risk mitigation techniques that have been implemented

Insurers indicated that their organisations have processes or measures in place that are able to determine the effectiveness of risk mitigation techniques that have been implemented to a lesser degree currently, with insurers recommended view being

that these processes should be in place to a high degree. The test results indicate significance at the 5% level of significance.

5.41 Questions 37 and 77 – Use of a risk register

Table 5.112 Current use of a risk register

	1	2	3	4	5	6
37. To what degree does your organisation keep an updated risk register?			59.26%	40.74%		

Table 5.113 Future use of a risk register

	1	2	3	4	5	6
77. In your opinion to what degree should your organisation keep an updated risk register?					100%	

Table 5.114 Data analysis of questions 37 and 77

	Q
	37
Mean	3.41
	Q
	77
Mean	5.00
t-value	1.3E-15
df=26	
p = 0.05	1.71
p = 0.10	1.32
Sig. 0.05	**YES**
Sig. 0.10	**YES**

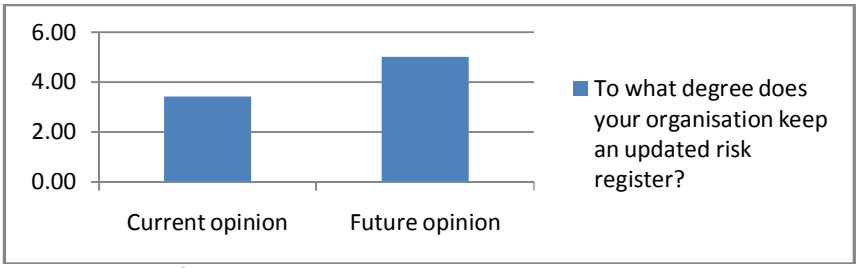

Figure 5.40 Comparison of mean value of current and future opinion of degree to which the organisation keeps an updated risk register

Insurers indicated that their organisations keep an updated risk register to a fair degree currently, with insurers recommended view being that this should occur totally. The test results indicate significance at the 5% level of significance.

5.42 Questions 38 and 78 – Interdependencies between risks

Table 5.115 Current interdependencies between risks

	1	2	3	4	5	6
38. To what degree does your organisation have a reporting process that takes into account both individual categories of risks and the interdependencies between them?	29.63%	66.67%	3.70%			

Table 5.116 Future interdependencies between risks

	1	2	3	4	5	6
78. In your opinion to what degree should your organisation have a reporting process that takes into account both individual categories of risks and the interdependencies between them?			11.11%	70.37%	18.52%	

Table 5.117 Data analysis of questions 38 and 78

	Q
	38
Mean	1.74
	Q
	78
Mean	4.07
t-value	2.3E-17
df=26	
p = 0.05	1.71
p = 0.10	1.32
Sig. 0.05	**YES**
Sig. 0.10	**YES**

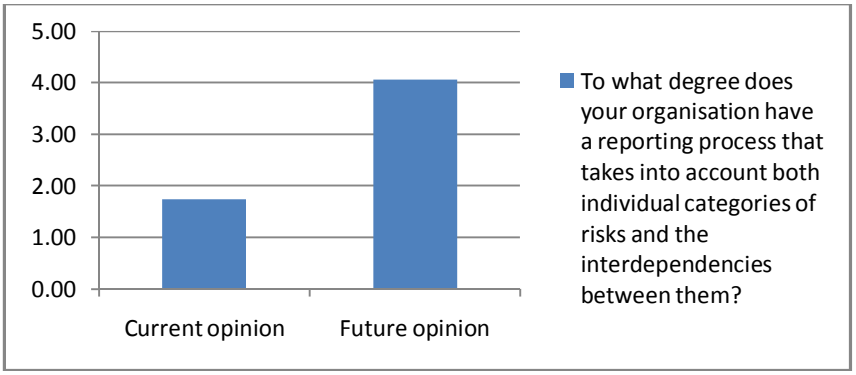

Figure 5.41 Comparison of mean value of current and future opinion of degree to which the organisation has a reporting process that takes into account both individual categories of risks and the interdependencies between them

Insurers indicated that their organisations have reporting processes that take into account both individual categories of risks and the interdependencies between them to no degree currently, with insurers recommended view that this should be the case to a high degree. The test results indicate significance at the 5% level of significance.

5.43 Questions 39 and 79 – Perception of risk management

Table 5.118 Current perception of risk management

	1	2	3	4	5	6
39. To what degree does your organisation view risk management processes as methods of actively creating value through prudent risk taking as opposed to only as tools to avoid organisational value deterioration?		11.11%	81.48%	7.41%		

Table 5.119 Future perception of risk management

	1	2	3	4	5	6
79. In your opinion to what degree should your organisation view risk management processes as methods of actively creating value through prudent risk taking as opposed to only tools to avoid organisational value deterioration?				51.85%	48.15%	

Table 5.120 Data analysis of questions 39 and 79

	Q
	39
Mean	2.96
	Q
	79
Mean	4.48
t-value	1.3E-12
df=26	
p = 0.05	1.71
p = 0.10	1.32
Sig. 0.05	**YES**
Sig. 0.10	**YES**

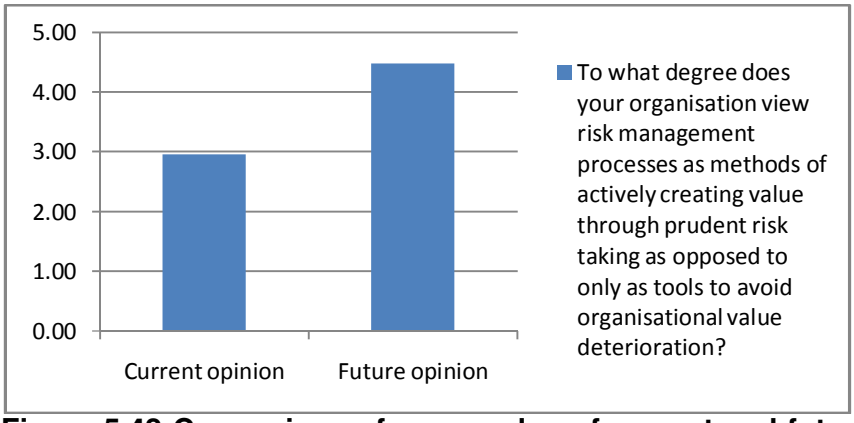

Figure 5.42 Comparison of mean value of current and future opinion of degree to which the organisation views risk management processes as methods of actively creating value through prudent risk taking as opposed to only as tools to avoid organisational value deterioration

Insurers indicated that their organisations viewed risk management processes as methods of actively creating value through prudent risk taking as opposed to only as

tools to avoid organisational value deterioration to a lesser degree currently, with insurers recommended view being that this view should be held to a high degree. The test results indicate significance at the 5% level of significance.

5.44 Questions 40 and 80 – Perception of introduction of SAM regime

Table 5.121 Current perception of introduction SAM regime

	1	2	3	4	5	6
40. To what degree does your organisation regard the introduction of a risk based capital regime such as Solvency Assessment and Management / Solvency II as essential?			33.33%	44.44%	22.22%	

Table 5.122 Future perception of introduction SAM regime

	1	2	3	4	5	6
80. In your opinion to what degree should your organisation regard the introduction of a risk based capital regime such as Solvency Assessment and Management / Solvency II as essential?				18.52%	81.48%	

Table 5.123 Data analysis of questions 40 and 80

	Q
	40
Mean	3.89
	Q
	80
Mean	4.81
t-value	8.1E-07
df=26	
p = 0.05	1.71
p = 0.10	1.32
Sig. 0.05	**YES**
Sig. 0.10	**YES**

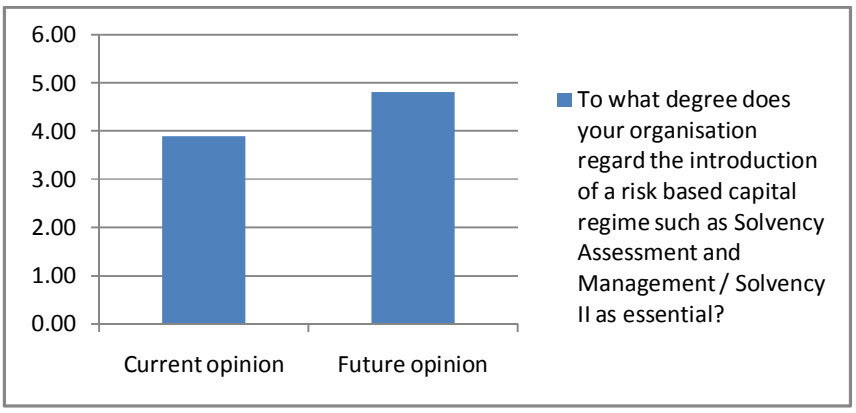

Figure 5.43 Comparison of mean value of current and future opinion of degree to which the organisation regards the introduction of a risk based capital regime such as Solvency Assessment and Management / Solvency II as essential

Insurers indicated that their organisations regard the introduction of a risk based capital regime such as Solvency Assessment and Management / Solvency II as essential to a fair degree currently, with insurers recommended view being that this should be regarded as essential to a high degree. The test results indicate significance at the 5% level of significance.

5.45 Analysis of items evaluated

Table 5.124 Analysis of items evaluated

	Number	Proportion
Total number of items evaluated	91	100.00%
Total number of items indicating significance at the 5% level of significance	**71**	**78.02%**
Total number of items not reflecting significance at the 5% level of significance	20	21.98%

The questionnaire required a total of 91 items to be evaluated from a current (what is) as well as a recommended (what should be) perspective. The results of the Paired-Sample t-tests reveal that in 78.02% of cases the null hypothesis (that there is no significant difference between the means of the two responses) is rejected, and the alternate hypothesis supported (that there is a significant difference between the means of the two responses). This is an indication that insurers approaches and

views towards operational risk management, and their recognition, consideration and use of various elements, practices, processes, techniques and methods employed in operational risk management are being significantly altered. It is this author's opinion that a major contributor to this phenomenon is the current importance being attached to operational risk management as part of the requirements of the Solvency Assessment and Management risk based capital regime being implemented in 2014.

6 CHAPTER 6: DISCUSSION, CONCLUSIONS AND RECOMMENDATIONS

6.1 Discussion and conclusions

At an overarching level the survey research indicates that insurers approaches and views towards operational risk management, and their recognition, consideration and use of various elements, practices, processes, techniques and methods employed in operational risk management are being significantly altered. As previously stated, it is this author's opinion that a major contributor to this phenomenon is the current importance being attached to operational risk management as part of the requirements of the Solvency Assessment and Management risk based capital regime being implemented in 2014.

The discussion and conclusions that follow are based on the findings of the research with regard to insurers current approaches towards the recognition, consideration and use of various elements, practices, processes, techniques and methods employed in operational risk management practice, with commentary delivered from the perspective of best practice identified in the literature review which should serve as a guide to insurers in terms of shifting from their current operational risk management reality to a paradigm more in line with best practice.

6.1.1 Definition of operational risk

The research indicates that insurers at least currently recognise all areas of risk as being an area of risk within their organisations to a greater or lesser degree (insurance; market; credit; operational; liquidity; reputation; political; and legal risk). However, only insurance risk, credit risk and reputation risk are currently rated as primarily important.

The new proposed SAM risk based capital solvency requirements are being designed to ensure that insurers have sufficient capital to withstand adverse events, both in terms of insurance risk, as well as in terms of economic, market and operational risk (Nyamakanga, 2007). Due to the importance being attached to operational risk management under the proposed SAM risk based capital regime, it is vitally

important that insurers recognise operational risk as a primary risk factor in their businesses so that it can be afforded the level of attention that it deserves and that will be mandated under the new capital regime.

The Basel Committee on Banking Supervision (Basel), for the purposes of the implementation of Basel II for banks in Europe, defined operational risk as being "the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events" (Basel, 2003: 2). The FSA, responsible for the regulation of insurers in the United Kingdom, have adopted the definition of operational risk defined by Basel for the purposes of insurer regulation and the implementation of Solvency II.

Tripp, *et al*. (2004) state that "there is no single risk classification that suits all purposes. However it seems that many U.K. insurance companies are adopting the definition used by the Basel committee as a starting point" (Tripp, *et al*., 2004: 21), whilst Zurich Insurance Company (2009), also following the FSA's lead, define operational risk as "operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events" (Zurich, 2009: 10).

In light of the FSA adoption of the Basel definition of operational risk for the purposes of insurer regulation in the UK, allied with the fact that a global insurer such as Zurich Insurance Company has adopted the same definition, a logical conclusion would be that South African insurers would be well served by adopting the same definition of operational risk, that is that "operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events".

6.1.2 Definition of risk management

According to the Institute of Risk Management (IRM), "The focus of good risk management is the identification and treatment of these risks. Its objective is to add maximum sustainable value to all the activities of the organisation. It marshals the understanding of the potential upside and downside of all those factors which can affect the organisation" (IRM, 2002: 2).

The American Committee of Sponsoring Organizations of the Treadway Commission (COSO), defines risk management as “a process, effected by an entity’s board of directors, management and other personnel, applied in strategy setting 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).

The International Actuarial Association (IAA) characterize risk management from an insurer perspective, as being “concerned with the totality of systems, structures and processes within an insurer that identify, assess, treat, monitor, report and/or communicate all internal and external sources of risk that could impact on the insurer’s operations” (IAA, 2009: 8). The International Organization for Standardization (ISO) (2009) believe that risk management includes the application of logical and systematic methods for identifying, analysing, evaluating and treating risk, and monitoring and reviewing risks and reporting and recording the results appropriately.

According to Q Finance (2010) risk management is the process by which companies systematically identify, measure and manage the various types of risk inherent within their operations. The fundamental objectives of a sound risk management programme are to manage the organisation's exposure to potential earnings and capital volatility and to maximize value to the organisation's various stakeholders (Q Finance, 2010).

The above definitions all represent different points of view on the concept of risk management, but some commonality within the descriptions seems to emerge. To varying degrees the descriptions of risk management above speak to it being concerned with a process, system or discipline; that addresses the risks within an organisation; through the identification, assessment, analysis, control and monitoring of risk.

6.1.3 Application of risk management – A Risk Management Framework

The FSA have proposed a risk assessment framework for the insurers and other institutions under their direction known as ARROW (Advanced, Risk-Responsive Operating FrameWork). According to the FSA (2006), the ARROW framework is designed to identify the main risks; measure the importance of those risks; mitigate those risks where their size justifies this; and monitor and report on the progress of risk management. The FSA ARROW framework follows a methodology as follows:

- All risks are firstly identified.
- Risks are then measured in terms of probability of occurrence and severity of occurrence.
- Risk mitigation techniques are applied to the risks as appropriate.
- The risks are monitored and reported on as part of ongoing activities.

The research indicates that insurers currently recognise the importance of implementing an enterprise risk management process, as well as recognise all of the elements of an operational risk management process to a high degree.

Insurers must ensure that their operational risk management practice takes place within the ambit of a logical sequence of events that can be systematically implemented. Based in part on the fact that the UK's regulator of insurer's (the FSA) have proposed a specific risk assessment framework for insurers, and based also in part on the fact that the South African FSB is establishing much of its own SAM risk based capital regime on the work previously done by the FSA in order to satisfy the requirements of SAM meeting third country equivalence with overseas financial regulators, it appears logical that South African insurers should adopt a similar framework.

6.1.4 Definition of operational risk management

As detailed in the literature review, in view of the FSA (2006) proposed risk assessment framework for insurers (ARROW), and their adoption of the Basel (2003) definition of operational risk, a definition of operational risk management was derived as being the identification, assessment and treatment of all sources of risk resulting

from inadequate or failed internal processes, people and systems within the insurer or from external events as well as the ongoing monitoring of risk and the reporting thereon through the use of systems, structures and processes (FSA, 2008).

6.1.5 The components of operational risk

The research indicates that for insurers only systems risk is currently considered a major factor of operational risk.

The literature (Abkowitz 2008; Dickstein and Flast 2008; Dowd 1998; Hoffman 2002; Hussain 2000; Lam 2003; Loader 2007; Young 2005; Zurich 2009) identifies the components of operational risk as comprising of four central components, namely internal processes; people; systems; and external events.

- Internal processes

  Internal processes risk is associated with operational risk occurring through ineffective or inefficient processes (Lam, 2003), defined as being those that fail to achieve their objectives. Internal processes risk can result from transactional documentation failures; process documentation failures; process design failures; internal data flaws; data entry errors; and incomplete legal documentation (Basel 2003; Young 2005; Dickstein and Flast 2008; Zurich 2009).

  The research indicates that all of the elements of process exposures surveyed are only recognised to a fair degree currently (errors in procedures or methodologies; execution errors; documentation errors; product complexity; security risks). Based on the literature above, all of the exposures should in fact be recognised to a high degree.

- People

  People risk is related to risk arising from loss / lack of key personnel; skills / capability gaps amongst employees; employee fraud; unauthorized activity; workplace safety; employee relations; inexperienced staff; incompetent staff; unsuitable staff; negligent staff; human error; fraud and theft and unauthorised and / or ill informed decision-making (Basel 2003; Dickstein and Flast 2008; FSA

2004; Hoffman 2002; Hussain 2000; Lam 2003; Loader 2007; Young 2005; Zurich 2009).

The research indicates that none of the factors of people risk surveyed is currently recognised as being a major or important element of operational risk (incompetence; negligence; human error; low morale; high staff turnover; criminal activities; lack of skill or training). Based on the literature above, all of the exposures should in fact be recognised to a high degree.

- Systems

  Systems risk concerns risks surfacing as a result of hardware failures including obsolescence; software failures; network failures; interface failures; communications failures; and security breaches such as hacking (Basel 2003; Dickstein and Flast 2008; Hoffman 2002; Zurich 2009). Lam (2003) contends that as technology has become increasingly necessary in more and more areas of business, operational risk events due to systems failures have become an increasing concern. According to Young (2005), an organisation faces risk when the systems it chooses are not well designed or implemented. Young (2005) states that system risk includes all technology risks, including external pressure such as the risk of not keeping up with the progress of changing or developing a technology.

  The research indicates that all of the elements of systems exposures surveyed are only recognised to a fair degree currently (system infiltration; system failure; third party computer fraud; programming errors; information risk; telecommunications risk; system obsolescence). Based on the literature above, all of the exposures should in fact be recognised to a high degree.

- External events

  External events risk is associated with external fraud including robbery; forgery; cheque kiting; damage to physical assets; terrorism; vandalism; earthquakes; fires and floods (Basel, 2003). Zurich (2009), identify risks posed by outsourcing partners; natural or manmade events such as war or earthquakes; and legislation and regulation as being part of the domain of external events risk. Other factors inherent under the domain of external events risk identified by the literature

(Dickstein and Flast 2008; Hoffman 2002; Hussain 2000; Loader 2007) include supplier risk; physical security risks; compliance risks; financial reporting requirements; legal risks; strikes; economic circumstances and political activity risks. According to Young (2005), external factors, beyond the direct control and influence of the organisation, could have an adverse effect on the internal, underlying operational factors (people, processes and systems). It is imperative, therefore, that these external factors be considered during an operational risk management process.

The research indicates that of the various external exposures surveyed (acts of God; crime; regulation and compliance; legal actions; changes in the business environment), only regulation and compliance is currently recognised to a high degree, with the balance of exposures being recognised to a lesser or fair degree. Based on the literature above, all of the exposures should in fact be recognised to a high degree.

6.1.6 Identification of operational risks

According to ISO (2009), risk identification is the process of finding, recognising and recording risks. The purpose of risk identification is to identify what might happen or what situations might exist that might affect the achievement of the objectives of the system or organisation. The FSA (2004) suggest that organisation's should try to understand the types of operational risk that are relevant to their specific circumstances and the impact that these risks may have on the incidence of financial crime, the fair treatment of its customers and its own solvency.

According to Young (2005), during the risk identification process, it is imperative that the risk exposure that the organisation faces be identified, as only when the risk exposure has been identified, can management work to transform it into an upside of risk.

The research indicates that insurers currently only recognise peer discussions to a fair degree, whilst all other methods (workshops; brainstorming; questionnaires; process mapping; and comparison with other organisations) are only recognised to a lesser degree or not at all.

Young (2005) contends that a systematic approach is required, furthermore, in order to ensure that all risk types are identified, including all forms of underlying risk factors per risk type, which can be listed and subjected to the risk management process.

Hoffman (2002) states that an organisation can use either a bottom up strategy or a top down strategy to identify, evaluate, and quantify risk potential. A bottom up strategy is used to identify, evaluate, and quantify the risk potential at a transaction or business unit level, and a top down strategy is used to identify, evaluate, and quantify the risk potential at an enterprise-wide and / or top line business level.

The IRM (2002) recommends that risk identification should be approached in a methodical way to ensure that all significant activities within the organisation have been identified and all the risks flowing from these activities defined.

According to the literature (CAS 2003; ISO 2009; Young 2005), key risks can be identified in a number of ways and methods such as:

- Workshops and interviews.
- Brainstorming sessions.
- Questionnaires.
- Risk process flow analysis (mapping the processes of the business and determining the risk exposures that exist in these processes).
- Comparisons with other organisations.
- Discussions with peers.
- Checklists.
- Previous loss history analysis.
- Control self assessments.
- Business unit level scenario analysis.
- Risk Assessment Interviews.
- Unit level trends and regressions.
- Risk inventories.
- Risk maps.
- Score cards.

Per Young (2005), there are various methods or techniques for the identification of risks, but it is unlikely that one particular method will be sufficient for the identification of all the risk exposures. A combination of methods might be required to identify effectively the insurers total exposure to risk

.

6.1.7 Measurement and evaluation of operational risks

According to Young (2005), risk evaluation is the assessment and measurement of the identified risk exposures with the aim of managing and controlling these risks. The aim of risk evaluation is also to determine the potential impact of a loss event in terms of financial, reputational or other damage and the likelihood of a risk event occurring (Young, 2005). A generally accepted measure of risk is a combination of the potential impact (the consequence or severity of the risk) and the frequency (how likely it is to occur) of a risk event (FSA 2006; Tripp, *et al.* 2004; Young 2005).

The research indicates that all of the methods surveyed (stress testing; scenario analysis; simulation techniques; actuarial methods; historical data to forecast potential losses; self risk assessments; and risk maps and process flows) are currently only used by insurers to a lesser degree or not at all.

According to Tripp, *et al.* (2004), operational risks contain aspects that are not so easy to quantify and hence to model, therefore the accuracy of risk measurement methods depends on the risk model and data availability. According to Tripp, *et al.* (2004), the accuracy of risk models depends upon the measurability of outcomes and therefore goes hand in hand with sound risk definition. Therefore, in order to quantify risk effectively insurers need to conduct a combination of quantitative and qualitative techniques to assess risk (Hoffman 2002; IAA 2009).

Various methods are identified and recommended in the literature for the measurement and evaluation of operational risks (Basel 2003; FSA 2004; FSA 2006; Hoffman 2002; IAA 2009; Soprano, Crielaard, Piacenza & Ruspantini 2009; Tripp, *et al.* 2004; Young 2005) as follows:

- Risk maps include the profiling of risks. These display the risks according to their frequency and severity of the loss when an event occurs. For risk mapping, various business units, organisational functions or process flows are mapped by risk type.
- Stress tests and scenario analysis is the process of considering a limited number of future scenarios and working through their possible consequences for the business. Both stress tests and scenario analyses can be undertaken by firms to further a better understanding of the vulnerabilities that they face under extreme conditions, and are based on the analysis of the impact of unlikely, but not impossible, events. Scenario analysis specifically involves the use of expert opinions, concerns and experience of key role-players in the business.
- Internal and external loss databases involve the collection and capturing of data on operational risk incidents. The data includes the identification of new risk categories, the frequency and severity of incidents, and lessons learnt from operational exposures. The databases enable users to identify key facts and trends, which can be used to perform rigorous analysis.
- Self risk assessments entail operations and activities being assessed against a menu of potential operational risk vulnerabilities. By way of example, in this approach, each business unit, in collaboration with the central operational risk control unit, assesses the operational risk to which it is exposed, on the basis of inside and expert knowledge, and also according to wider thinking, in order to include extreme events and experiences.
- Using risk indicators involves employing statistics and / or metrics, often financial, which can provide insight into risk positions. These indicators tend to be reviewed on a periodic basis (such as monthly or quarterly) to alert to changes that may be indicative of risk concerns. Examples of some commonly used risk indicators include the number of failed transactions; staff turnover rates; the frequency and / or severity of process errors; customer complaints and commendations; payment delays by third parties; media reports about the business (positive, neutral and negative); error rates in processing customer's orders; IT system availability; and key financial data.
- Mathematical methods of analysis such as Value-at-Risk (VaR) analysis as well as stochastic modelling methods. Operational Value-at-Risk (OpVaR) is arrived at as a function of determining the severity and

frequency of operational losses. Modelling approaches such as this focus on estimating the risk of the specific processes, using loss data to determine a loss distribution from which the operational risk is derived. The ultimate objective of models such as these is the performance of an estimation of the frequency of operational risk events in the future.

6.1.8 Risk mitigation and control of operational risks

Risk control involves the activities designed for the purpose of eliminating or reducing the factors that may negatively influence the strategic objectives and may cause a loss to the organisation (Young, 2005).

Six possible treatments of risks predominate in the literature (Basel 2003; Damodaran 2008; Dickstein and Flast 2008; Institute of Actuaries 2009; Sadgrove 2005; Tripp, *et al.* 2004; Young 2005), which are detailed as follows:

- Controlling the risk.
- Mitigating the risk.
- Exploiting the risk.
- Funding the risk.
- Ignoring the risk.
- Postponing the risk.

The research indicates that there is currently only to a lesser degree a comprehensive understanding of and agreement on the organisation's risk appetite within insurers, and that insurers organisational risk appetite is again only to a lesser degree clearly communicated to business unit managers who are required to implement operational risk management processes. The research indicates that insurers only to a lesser degree currently make adjustments to their risk appetite and processes on an ongoing, immediate basis based on past experiences, pro forma results, future stakeholder expectations and existing market conditions.

The literature (Basel 2003; Dickstein and Flast 2008; Dowd 1998; Institute of Actuaries 2009; Young 2005) states that although a framework of formal, written policies and procedures is critical, it must be reinforced through a strong (i.e. high

degree) control culture that promotes sound risk management practices. The board of directors as well as senior management are responsible for establishing a strong internal control culture in which control activities are an integral part.

Tripp, *et al.* (2004) states that with regard to risk mitigation and control, the organisation needs to ask itself questions relating to the level of risk to which it is prepared to expose its resources in order to achieve its objectives; the level of risk which it is prepared to accept of not achieving its objectives; and whether the level of potential reward is consistent with the risks.

The research indicates that all of the operational risk controls surveyed (policies and procedures; internal controls; risk reporting) are only recognised by insurers to a fair degree currently. The literature (Basel 2003; Young 2005) argues that this component of the risk management process should be recognised to a much higher degree, and formulated to include activities such as the implementation of policies and procedures, internal controls, risk reporting and decision-making, as well as the determination of an organisational structure to form the basis of the process – all focused on the ultimate control and mitigation and risks, and all of which management needs to ensure are aligned with the original business objectives.

The literature (Basel 2003; Dickstein and Flast 2008; Dowd 1998; Institute of Actuaries 2009; Young 2005) states that policies, processes and procedures to control and / or mitigate material operational risks should be in place and should be periodically reviewed and adjusted, and that furthermore, organisations must ensure that the risk management control infrastructure keeps pace with the growth in the business activity.

The research indicates that insurers base decisions to enter or withdraw from certain lines of business based upon their potential impact on the organisation's risk / return measures only to a fair degree currently. Furthermore, the research indicates that insurers have ongoing processes in place for identifying / managing significant operational risks only to a lesser degree currently. According to Young (2005), risk controls should be reviewed when deficiencies are identified; and should be constantly monitored and adapted to changing circumstances.

The research indicates that insurers outsource risk management functions within the organisation to no degree currently. The literature best practice states that policies for managing the risks associated with outsourcing activities should be established, as outsourcing of activities can reduce the institution's risk profile by transferring activities to others with greater expertise and scale to manage the risks associated with specialised business activities, but can also attach additional risk. Therefore, outsourcing arrangements should be based on robust contracts and / or service level agreements that ensure a clear allocation of responsibilities between external service providers and the outsourcer (Basel 2003; Dickstein and Flast 2008; Dowd 1998; Institute of Actuaries 2009; Young 2005).

The literature (Basel 2003; Dickstein and Flast 2008; Dowd 1998; Institute of Actuaries 2009; Young 2005) advises that control processes and procedures should be established and a system should be in place for ensuring compliance with a documented set of internal policies concerning the risk management system. Principal elements of this could include top-level reviews of progress towards the stated objectives and checking for compliance with management controls. Furthermore, risk mitigation tools should be viewed as complementary to, rather than a replacement for, thorough internal operational risk control. Having mechanisms in place to quickly recognise and rectify legitimate operational risk errors can greatly reduce exposures.

6.1.9 Monitoring and reporting of operational risks

The final stage of the risk management process is to monitor and report on risks, which forms an integral part of operational risk management. This includes regularly measuring the risk to ensure that it remains within stated tolerances, and auditing to ensure that the procedure is being followed. In order to ensure an appropriate and timely response to risk, an organisation should have a mechanism in place to allow the organisation to monitor its risks and controls. The monitoring process should aim to assist management in determining what to measure, understanding the operational risk profile of the organisation, how changes or developments influence the profile and what must be done in order to protect the organisation against operational risk exposures (Dickstein and Flast 2008; Sadgrove 2005; Young 2005).

The need for continuous and dynamic reviews is more evident today than ever before, fortunately, advancements in technology, frequent reporting, and interactive systems support a more timely response to risks (Hoffman 2002; IAA 2009).

The research indicates that insurers boards actively provide oversight to risk management strategies, and that insurers boards actively challenge management's assessment of key risks and their approach to managing those risks, as well as involve business unit managers in operational risk management processes only to a fair degree currently. The literature (IAA 2009; IRM 2002; Young 2005) affirms that the reporting process should ensure that the board of directors are assured of the risk management process working effectively by receiving adequate information, and that they further know about the most significant risks facing the organisation and their possible effects on shareholder value of deviations to expected performance ranges.

Furthermore, the board should have responsibility in terms of determining the strategic direction of the organisation and for creating the environment and the structures for risk management to operate effectively. Unless risk management is fully endorsed and actively supported by the board and by the senior management of an organisation as an integral part of the way the organisation is managed, it cannot be effective (IRM 2002; Young 2005).

The research indicates that insurers have appropriate segregation of duties between those responsible for monitoring and measuring risk and those responsible for making decisions, and have established a separate operational risk management structure, only to a lesser degree currently. However, the research also indicates that risk managers have direct access to the CEO of their organisations, and that internal audit is involved to manage operational risk to a high degree currently. The literature (Basel 2003; Dickstein and Flast 2008; Dowd 1998; Institute of Actuaries 2009; Young 2005) best practice states that an effective internal control system requires that there be appropriate segregation of duties and that personnel are not assigned responsibilities which may create a conflict of interest, furthermore, the reporting process must report systematically and promptly to senior management any perceived new risks or failures of existing control measures.

The research indicates that currently insurers reporting processes do not take into account both individual categories of risks and the interdependencies between. Furthermore, insurers only account for dependencies between risks or use some form of corporate scorecard to report on risk to a lesser degree currently. Insurers also indicated that organisational reports that supply information using measures that identify areas where risk tolerances are being exceeded or risk objectives not met are only utilised to a lesser degree currently, although they report the use of updated risk registers to a fair degree. The research indicates that insurers have processes or measures in place that are able to determine the effectiveness of risk mitigation techniques that have been implemented only to a lesser degree currently.

According to Dickstein and Flast (2008), risk metrics, indicators and control standards for risk reporting should be established, with target levels for the specific measures being set such that they can be used to help measure how well a business process is operating. Consistent with the literature (Hoffman 2002; IRM 2002; IAA 2009; Sadgrove 2005), it is crucial from a risk monitoring perspective that organisations focus on the most important risks such as:

- Trends that indicate a growing danger.
- Data that shows variances from the norm.
- Key performance indicators.
- One-off reports on new areas of risk.
- Information from a range of sources.
- Key findings from audits.
- The processes used to identify risks and how they are addressed by the risk management systems.
- The primary control systems in place to manage significant risks.
- The organisation's ability to track operational risk issues, incidents, and losses by developing a process to capture and track them, including their cost and causative factors.

According to Young (2005), it is critical that risk management provides accurate and timely information regarding risk exposures. The information must be concise, unambiguous, standardised and integrated with existing reporting processes in order to ensure timely and efficient decisions on risk control measures. Different levels within an organisation need different information

from the risk management process. The risk management process must operate at a sufficiently detailed and specific level for identifying and evaluating new risks on a continuous basis, but in addition, senior management at a firm wide level must have an aggregate view of operational risk in terms of reporting. Any significant deficiencies uncovered by the system, or in the system itself, should be reported together with the steps taken to deal with them (IAA 2009; IRM 2002; Young 2005).

6.1.10 Integrating operational risk management into the organisation

In order to be successful, risk management should become integral to the strategic planning of an organisation, to its day-to-day operations and to its capital modelling and actuarial practices (EMB, 2010). Specifically as regards a risk based capital regime, the FSA (2008) state that it expects full integration of risk management into the organisation, such that senior management is clearly responsible for the risk management system and ensuring that it is used in managing the business, including how it influences business decisions, and that each function within the organisation should be expected to understand how its decisions affect the risk and capital profile of the firm.

The research indicates that insurers consider their risk management processes to be integrated and have risk strategies related to risk classes as well as overall risk exposure only to a lesser degree currently.

Ernst & Young (2009) state that it is necessary to truly embed risk management into the operations of the organisation, starting by effectively articulating risk strategy and risk appetite and cascading through to use within the organisation. Patel and George (2009) point out that by integrating risk management within the organisation and effectively de-centralising it, the “risk culture” can spread beyond core risk functions in an organisation (Patel and George, 2009).

According to the International Actuarial Association (2009), positioning risk management behaviours as part of “business as usual” also serves to bind the whole organisation to the concept because everyone is on the implementation team. The Institute of Actuaries (2009) state that risk management processes should come to be embedded in all the activities of the organisation in a holistic way.

The research indicates that insurers boards set the strategies, policies and processes surrounding risk management to a fair degree currently, but that current management incentive compensation is tied to organisational risk objectives and risk / return measures approved by the board to only a lesser degree currently.

Specifically with regard to a risk based capital approach to capital, a regime such as SAM / Solvency II necessitates the whole organisation to understand its roles, its interdependencies and its responsibilities towards risk. All employees must share the responsibility for risk, and the board needs to demonstrate that the awareness is across the whole organisation - top to bottom, front line to back office (EMB, 2010). Everyone in an entity has some responsibility for enterprise risk management (COSO 2004; Deighton, Dix, Graham, & Skinner 2009; IRM 2002).

According to the IRM (2002), integrating risk management into every level of the organisation is necessary for the effective functioning of the risk management process, and is a function of commitment from the chief executive and executive management of the organisation; the allocation of appropriate resources for training; and the development of enhanced risk awareness by all stakeholders.

Organisation's may have all the risk management tools, processes and systems in place, but these are considered to be of not much use without motivated personnel. Therefore, it is crucial for organisations to have a corporate culture of rewarding risk management behaviour, and the creation of a fair payment scheme for employees is seen as both a major challenge as well as a critical element of risk management. If incentive compensation is a key driver of employee performance, then it is also by extension a key driver of risk management. The existence of an effective incentive scheme to ensure a motivated workforce is therefore stressed as being an important element of integrating operational risk management into the organisation (Dickstein and Flast 2008; Young 2005).

The research indicates that insurers view risk management processes as methods of actively creating value through prudent risk taking as opposed to only as tools to avoid organisational value deterioration only to a lesser degree currently, but that insurers currently regard the introduction of a risk based capital regime such as SAM as essential to a fair degree.

According to IRM (2002), as well as ISO (2009), having structured risk management processes in place leads to several benefits in addition to providing a framework that enables operational risk management to take place in a consistent and controlled manner. These other benefits are identified as being:

- Improved decision making and planning.
- Improved prioritization through a structured understanding of business activity and volatility.
- A more efficient use and allocation of capital and resources within the organisation.
- The reduction of volatility in non essential areas of the business.
- The protection and enhancement of assets and company image.
- The optimisation of operational efficiency.
- Assistance with the selection of different forms of risk treatment; and assistance with meeting regulatory requirements.

Capgemini (2006), assert that the benefits of a more robust approach towards risk management over and above regulatory compliance are:

- Improved management of risk and capital.
- Better risk management should bring closer alignment of organisational goals and allow an enterprise-wide understanding of business risks.
- Improved risk management should result in a competitive edge for insurers as a more robust approach to risk management should enable better identification and management of risks, allowing insurer's to understand which types and sources of risk can be opportunities to improve business performance.
- A better understanding of the insurer's risk profile can help the insurer to create better and more profitable products.
- A better understanding of risk pricing and capital requirements enables more accurate pricing decisions to be made.

- Better risk management should allow for greater visibility of business drivers as an improved assessment of risks as well as rewards will provide greater visibility of the real drivers of business value, thereby creating an environment for better planning and decision-making.

6.2 Recommendations

- A structured approach to operational risk management should be instituted by short-term insurers.
- In line with a structured approach, the framework, practices, processes, techniques and methods identified and described by this study should be implemented by short-term insurers in designing and instituting their own operational risk management programmes. Individual insurers will ascertain and institute their own individual operational risk management programmes and processes, however, the framework, practices, processes, techniques and methods identified and described by this research encompass the major constituents of operational risk management that should be focused on during the development and institution of an operational risk management programme.
- The adoption / institution of a structured, formalized operational risk management programme / processes should be commenced as soon as possible so that insurers can begin managing the operational risks inherent in their businesses to an optimal level.
- The adoption / institution of a structured, formalized operational risk management programme / processes should be commenced as soon as possible so as to integrate operational risk management processes and practices as well as an operational risk management culture into insurers businesses well in advance of the implementation of the SAM risk based capital regime.
- The adoption / institution of a structured, formalized operational risk management programme / processes should be commenced as soon as possible so that insurers are in a position to comply regulatorily with the pending SAM risk based capital regime which is being implemented on the 01st of January 2014.
- The adoption / institution of a structured, formalized operational risk management programme / processes should be commenced as soon as possible so that insurers have practiced, embedded and integrated structured operational risk

management processes and practices into their businesses to such a degree that they are able to completely satisfy the regulator's (FSB) requirement of the insurer's operational risk management programme passing a "use" test at the time of the introduction of the SAM risk based capital regime in January 2014.

The main recommendation for further study emanating from the research is for research to be conducted on insurers approaches towards operational risk management at the time of the Solvency Assessment and Management regime implementation on 01st January 2014, to assess their levels of institutionalization of formal operational risk management programmes at the time.

7 List of References

A.M. Best. 2008. *Risk Management and the Rating Process for Insurance Companies*. New Jersey: A.M. Best.

Abkowitz, M.D. 2008. *Operational Risk Management – A Case Study Approach To Effective Planning And Response*. New Jersey: John Wiley & Sons.

Accenture. 2010. *In Full, On Time—and Beyond High Performance through Solvency II* [online]. New York: Accenture.
Available from: <http://www.accenture.com/NR/rdonlyres/F7B47EDF-1BB7-4FA0-93C9-3A2DC4BD89D7/0/Accenture_Solvency_II_PoV.pdf>
[Accessed 10 June 2010]

Basel Committee on Banking Supervision. 2003. *Sound Practices for the Management and Supervision of Operational Risk*. Washington: Bank for International Settlements.

Blokdijk, G. 2010. *Risk Management 100 Success Secrets - Identifying and project managing Risk Management research, design, training and operations in the Enterprise* [online]. E-book.
Available from: <http://www.emereo.org>
[Accessed 10 June 2010]

Capgemini. 2006. *Risk Management in the Insurance Industry and Solvency II*. London: Capgemini.

Casualty Actuarial Society. 2003. *Overview of Enterprise Risk Management*. Schaumberg: Casualty Actuarial Society.

ChandraShekhar, P. and Warrier, S. R. 2010. *Risk Based Capital Management: a "principles based approach" to insurer solvency management* [online]. Available from: <http://www.rmi.nccu.edu.tw/apria/docs/concurrent%20i/session%205/13007risk%20based%20capital%20-%20warrier%20&%20preeti%20-%20apria%202007.pdf> [Accessed 15 June 2010]

Committee of Sponsoring Organizations of the Treadway Commission. 2004. *Enterprise Risk Management — Integrated Framework*. New York: PricewaterhouseCoopers LLP.

Damodaran, A. 2008. *Strategic Risk Taking – A Framework for Risk Management*. New Jersey: Wharton School Publishing.

Deighton, S. P., Dix, R. C., Graham, J. R. & Skinner, J. M. E. 2009. *GOVERNANCE AND RISK MANAGEMENT IN UNITED KINGDOM INSURANCE COMPANIES*. London: Institute of Actuaries

Diamantopoulos, A. and Schlegelmilch, B. B. 2006. *Taking the Fear Out of Data Analysis.* London: Thomson.

Dickstein, D.I. and Flast, R.H. 2008. *No Excuses: A Business Process Approach to Managing Operational Risk*. New Jersey: John Wiley & Sons.

Dowd, K. 1998. *Beyond Value At Risk – The new science of risk management*. West Sussex: John Wiley & Sons Ltd.

EMB Actuaries and Consultants. 2010. *Solvency II and Risk Management* [online]. New York: EMB Actuaries and Consultants. Available from: <http://www.solvency-2.com/news/OperationalRisk2.php> [Accessed 10 June 2010]

EMB Actuaries and Consultants. 2010. *Solvency II: Gaining maximum benefit from the new legislation* [online]. New York: EMB Actuaries and Consultants. Available from: <http://www.emb.com/EMBDOTCOM/Global/Solvency%20II%20Brochure_Gaining%20benefit%20brochure_web%20version.pdf> [Accessed 10 June 2010]

Financial Services Authority. 2003. *Building a framework for operational risk management: the FSA's observations*. London: The Financial Services Authority.

Financial Services Authority. 2004. *Integrated Prudential sourcebook for insurers*. London: The Financial Services Authority.

Financial Services Authority. 2006. *The FSA's risk assessment framework*. London: The Financial Services Authority.

Financial Services Authority. 2008. *Insurance Risk Management: The Path To Solvency II*. London: The Financial Services Authority.

Financial Services Board. 2009. *Annual Report 2009*. Menlo Park: Financial Services Board.

Financial Services Board. 2009. *Information letter 8/2009 – Solvency Assessment and Management regime*. Menlo Park: Financial Services Board.

Financial Services Board. 2010. *List of registered insurers* [online]. Menlo Park: Financial Services Board. Available from: <http://www.fsb.co.za/Magic94Scripts/mgrqispi94.dll?APPNAME=Web&PRGNAME=List_Of_Registered_Insurers> [Accessed 10 June 2010]

Financial Services Board. 2010. *Solvency Assessment and Management Project* [online]. Menlo Park: Financial Services Board. Available from: <http://www.fsb.co.za/public/Insurance/SAMProjectworkshop2010.pdf> [Accessed 10 June 2010]

Guy Carpenter. 2010. *Internal Models – A Winning Solution for Solvency II* [online]. New York: Guy Carpenter. Available from: <www.guycarp.com/portal/extranet/insights/.../Solvency%20II_07.pdf> [Accessed 10 June 2010]

Hoffman, D. 2002. *Managing Operational Risk: 20 Firmwide Best Practice Strategies*. New Jersey: John Wiley & Sons.

Hussain, A. 2000. *Managing Operational Risk in Financial Markets*. Burlington, MA: Elsevier.

Institute of Actuaries. 2009. *ERM – a guide to implementation*. London: Institute of Actuaries.

Institute of Risk Management. 2002. *A Risk Management Standard*. London: The Institute of Risk Management.

International Actuarial Association. 2009. *Note on Enterprise Risk Management for Capital and Solvency Purposes in the Insurance Industry*. Ontario: International Actuarial Association.

International Organization for Standardization. 2009. *Risk management — Risk assessment techniques*. Geneva, Switzerland: International Organization for Standardization.

Kirk, I. 2009. *Insurance Institute of South Africa 2009 Annual Conference: Sun City, May 2009*. Insurance Institute of South Africa.

KPMG. 2010. *Operational Risk Management*. Johannesburg: KPMG.

Lam, J. 2003. *Enterprise Risk Management – From Incentives to Controls*. New Jersey: John Wiley & Sons Ltd.

Leedy, P. D., and Ormrod, J. E. 2005. *Practical Research, Planning and Design*. 8th ed. New Jersey: Pearson Education, Inc.

Liebwein, P. 2006. 'Risk Models for Capital Adequacy: Applications in the Context of Solvency II and Beyond', *The Geneva Papers*, 2006 (31): 528–550.

Loader, D. 2007. *Operations risk: managing a key component of operations risk under Basel II*. Oxford : Butterworth-Heinemann.

Matthew, Q. M. Executive Head Portfolio Services, Santam Insurance Company Limited. 2010. Personal interview. 09 June, Illovo.

Metcalfe, B. 2010. *Strategic and Emerging Issues in South African Insurance*. Johannesburg: PricewaterhouseCoopers.

Ndururi, P. Senior Actuary, Centriq Insurance Company Limited. 2010. Personal interview. 09 June, Illovo.

Nyamakanga, R. 2007. *A risk-based regulatory framework set to transform the industry* [online]. Johannesburg: Financial Mail.
Available from: <http://free.financialmail.co.za/report07/short07/ashort.htm>
[Accessed 05 June 2010]

Oxford Advanced Learner's Dictionary. 2010. *Oxford Advanced Learner's Dictionary* [online]. Oxford: Oxford University Press.
Available from:
<http://www.oxfordadvancedlearnersdictionary.com/dictionary/risk>
[Accessed 05 June 2010]

Patel, N.S. and George, G. 2009. *Integrated Operational Risk Management Beyond Basel II* [online]. New York: Infosys.
Available from: <http://www.infosys.com/offerings/industries/banking-capital-markets/Documents/operational-risk-management-basel.pdf>
[Accessed 06 June 2010]

Q Finance. 2010. *Enterprise Risk Management and Solvency II* [online]. London: Q Finance.
Available from: <http://www.qfinance.com/insurance-markets-best-practice/enterprise-risk-management-and-solvency-ii?full>
[Accessed 06 June 2010]

Sadgrove, K. 2005. *The Complete Guide to Business Risk Management*. 2nd ed. Aldershot: Gower Publishing Company.

Santam Limited. 2010. *Annual Report 2009*. Bellville: Santam Limited.

South Africa. Registrar of Short-term Insurance. 1998. *Short-Term Insurance Act, 1998 (Act No. 53 of 1998)*. Pretoria: Registrar of Short-term Insurance.

Soprano, A., Crielaard, B., Piacenza, F. & Ruspantini, D. 2009. *Measuring Operational and Reputational Risk: A Practitioner's Approach*. New Jersey: John Wiley & Sons.

South African Insurance Association. 2008. *Annual Review 2008*. Milpark: South African Insurance Association.

South African Insurance Association. 2009. *Annual Review 2009*. Milpark: South African Insurance Association.

Standard & Poor's. 2005. *Evaluating The Enterprise Risk Management Practices Of Insurance Companies*. New York: Standard & Poor's.

Tripp, M.H., Bradley, H.L., Devitt, R., Orros, G.C., Overton, G.L., Pryor, L. & Shaw, R.A. 2004. *QUANTIFYING OPERATIONAL RISK IN GENERAL INSURANCE COMPANIES*. London: Institute of Actuaries.

Wikipedia. 2010. *Insurance* [online]. Wikipedia.
Available from: <http://en.wikipedia.org/wiki/Insurance>
[Accessed 06 June 2010]

Young, J. 2001. A STRUCTURED APPROACH TO OPERATIONAL RISK MANAGEMENT IN A BANKING ENVIRONMENT. DCOM thesis. University of South Africa, Pretoria.

Young, J. 2005. *Operational Risk Management: The Practical Application of a Qualitative Approach*. Pretoria: Van Schaik Publishers.

Zurich Insurance Company USA. 2009. *Operational Risk Management*. New York: Zurich Insurance Company USA.

Appendix 1: Example of letter accompanying questionnaire

The Managing Director / Chief Executive Officer
Name of Company
Address 1
Address 2
Address 3
Address 4

01 July 2010

Dear XXX

RESEARCH TOWARDS COMPLETION OF MBL DEGREE:
"OPERATIONAL RISK MANAGEMENT IN THE SHORT-TERM INSURANCE INDUSTRY AND RISK BASED CAPITAL"

I am completing a Master of Business Leadership degree through the Graduate School of Business Leadership at the University of South Africa. For my final year Research Report I have selected operational risk management in the short-term insurance industry as my topic, with specific reference to the role that operational risk management will play in the future in light of the new Solvency Assessment and Management regime being developed by the Financial Services Board in line with the European Solvency II Directive.

All registered short-term insurers have been requested to participate in this research and I would be grateful for your organisation's contribution to this research by requesting you to kindly complete and return the attached questionnaire.

The aims of the survey are as follows:

- To ascertain the current status of operational risk management in the short-term insurance industry; and
- To determine the views and opinions of experts on how certain aspects relating to operational risk management in the short-term insurance industry should be approached.

The findings will be kept confidential and the report will only refer to respondents as Respondent X or Y. No organisation will be referred to by name. I am employed in the short-term insurance industry and would be willing to sign a confidentiality agreement if so required.

After completing the questionnaire please return it via the provided self addressed prepaid envelope, or fax it to 011-268-6495 for my attention or email it to me at mleroux@centriq.co.za

Should you desire a copy of the results please indicate accordingly where provided for on the questionnaire and they will be forwarded to you after completion of the research.

I would appreciate it if I could receive your reply by 31st August 2010.

Yours sincerely,

Martin Le Roux

Appendix 2: Questionnaire on operational risk management

QUESTIONNAIRE ON OPERATIONAL RISK MANAGEMENT

This questionnaire is comprised of three sections:

Section 1 consists of demographic information.

Section 2 seeks to determine your organisation's current approach towards operational risk management.

Section 3 seeks to determine what your organisation's approach towards operational risk management **should be**, based on your views, experience as well as knowledge.

Please indicate your choice by marking the applicable box with a cross (X) or specify your answer under "other".

Section 1: Demographic Information

1. Indicate the type of organisation that you are representing

1.1. Typical insurer	
1.2. Niche insurer	
1.3. Cell captive insurer	
1.4. Captive insurer	
1.5. Reinsurer	

1.6. Other:

2. Indicate your role within the organisation

2.1. Managing Director / Chief Executive Officer	
2.2. Financial Director / Chief Financial Officer	
2.3. Chief Operating Officer	
2.4. Risk Manager	
2.5. Line Manager	
2.6. Actuarial	
2.7. Internal Audit	

2.8. Other (specify):

3. Indicate your number of years of experience in the short-term insurance industry

3.1. Less than 5 years	
3.2. Between 5 and 10 years	
3.3. Between 10 and 15 years	
3.4. Between 15 and 20 years	
3.5. Greater than 20 years	

4. If you would like a copy of the results, please indicate your email address below:

Sections 2 and 3

Please answer the following questions by indicating your answer with a cross (X) in the applicable box according to the following scale or specify your answer under "other":

Scale for answers:

1 = Not at all

2 = To a lesser degree

3 = To a fair degree

4 = To a high degree

5 = Totally

6 = Unsure

Section 2: Your organisation's current approach towards operational risk management

1. To what degree of primary importance would you rate the following areas of risk within your organisation?	1	2	3	4	5	6
1.1. Insurance risk						
1.2. Market risk						
1.3. Credit risk						
1.4. Operational risk						
1.5. Liquidity risk						
1.6. Reputation risk						
1.7. Political risk						
1.8. Legal risk						
1.9. Other:						

2. To what degree does your organisation believe that the following are factors of operational risk?	1	2	3	4	5	6
2.1. People						
2.2. Processes						
2.3. Systems						
2.4. Other external factors (fraud, natural disasters)						

2.5. Other:

3. To what degree has your organisation recognised the following human factors as an important element of operational risk?	1	2	3	4	5	6
3.1. Incompetence						
3.2. Negligence						
3.3. Human error						
3.4. Low morale						
3.5. High staff turnover						
3.6. Criminal activities (fraud)						
3.7. Lack of skills or training						

3.8. Other:

4. To what degree has your organisation recognised the following process exposures as an important element of operational risk?	1	2	3	4	5	6
4.1. Errors in procedures or methodologies						
4.2. Execution errors						
4.3. Documentation errors						
4.4. Product complexity						
4.5. Security risks						

4.6. Other:

5. To what degree has your organisation recognised the following systems exposures as an important element of operational risk?	1	2	3	4	5	6
5.1. System infiltration						
5.2. System failure						
5.3. Third party computer fraud						
5.4. Programming errors						
5.5. Information risk						
5.6. Telecommunications risk						
5.7. System obsolescence						

5.8. Other:

6. To what degree has your organisation recognised the following external exposures as an important element of operational risk?	1	2	3	4	5	6
6.1. Acts of God						
6.2. Crime						
6.3. Regulation and compliance						
6.4. Legal actions						
6.5. Changes in the business environment						

6.6. Other:

	1	2	3	4	5	6
7. To what degree does your organisation recognise the importance of implementing a formal risk management (ERM) process?						

	1	2	3	4	5	6
8. To what degree has your organisation adopted a formal definition of operational risk?						

9. To what degree has your organisation recognised the following as important elements of an operational risk management process?	1	2	3	4	5	6
9.1. Risk identification						
9.2. Risk measurement and evaluation						
9.3. Risk control						
9.4. Other:						

	1	2	3	4	5	6
10. To what degree is risk management currently aligned to the overall business strategy, including covering the planned risk profile of the organisation and the approach to managing those risks?						

	1	2	3	4	5	6
11. To what degree is an operational risk management process recognised as an important and integral part of your organisation's overall management process?						

	1	2	3	4	5	6
12. To what degree does the board currently set the strategies, policies and processes surrounding risk management?						

	1	2	3	4	5	6
13. To what degree does the board currently actively provide oversight to risk management strategies?						

	1	2	3	4	5	6
14. To what degree does the board currently actively challenge management's assessment of key risks and their approach to managing those risks?						

	1	2	3	4	5	6
15. To what degree is there a comprehensive understanding of and agreement on the organisation's risk appetite within the organisation?						

	1	2	3	4	5	6
16. To what degree is your organisation's risk management process integrated? (That is, to what extent is risk management owned, monitored and managed at a local level within the organisation?)						

	1	2	3	4	5	6
17. To what degree is the organisational risk appetite clearly communicated to business unit managers who are required to implement operational risk management processes?						

	1	2	3	4	5	6
18. To what degree is current management incentive compensation tied to organisational risk objectives and risk / return measures approved by the board?						

	1	2	3	4	5	6
19. To what degree is there appropriate segregation of duties between those responsible for monitoring and measuring risk and those responsible for making decisions?						

20. To what degree has your organisation recognised the importance of and implemented the following operational risk control measures?	1	2	3	4	5	6
20.1. Policies and procedures						
20.2. Internal controls						
20.3. Risk reporting						

20.4. Other:

21. To what degree does your organisation use the following methods to measure operational risk?	1	2	3	4	5	6
21.1. Stress testing						
21.2. Scenario analysis						
21.3. Simulation techniques						
21.4. Actuarial methods						
21.5. Historical data to forecast potential losses						
21.6. Self-risk assessments						
21.7. Risk maps and process flows						

21.8. Other:

	1	2	3	4	5	6
22. To what degree does your organisation currently have an ongoing process in place for identifying / managing significant operational risks?						

	1	2	3	4	5	6
23. To what degree does your organisation have a risk strategy related to risk classes as well as overall risk exposure?						

24. To what degree has your organisation recognised the following methods as the most appropriate to identify risks?	1	2	3	4	5	6
24.1. Workshops						
24.2. Brainstorming						
24.3. Questionnaires						
24.4. Process mapping						
24.5. Comparison with other organisations						
24.6. Peer discussions						

24.7. Other:

	1	2	3	4	5	6
25. To what degree has your organisation established a separate operational risk management structure?						

	1	2	3	4	5	6
26. To what degree does a risk manager have direct access to the CEO of your organisation?						

	1	2	3	4	5	6
27. To what degree does your organisation involve internal audit to manage operational risk?						

	1	2	3	4	5	6
28. To what degree does your organisation involve business unit managers in operational risk management processes?						

	1	2	3	4	5	6
29. To what degree does your organisation on an ongoing, immediate basis adjust the organisation's risk appetite and risk processes based on past experiences, pro forma results, future stakeholder expectations and existing market conditions?						

30. To what degree do the following factors influence your organisation's development and improvement of risk management processes?	1	2	3	4	5	6
30.1. Compliance - regulatory						
30.2. Compliance - shareholders						
30.3. Compliance - market						
30.4. Business driven logic						
30.5. Losses made by others						
30.6. Being a pioneer in risk management						
30.7. Image						

30.8. Other:

	1	2	3	4	5	6
31. To what degree are decisions to enter or withdraw from certain lines of business based upon their potential impact on the organisation's risk / return measures?						

	1	2	3	4	5	6
32. To what degree does your organisation account for dependencies between risks?						

	1	2	3	4	5	6
33. To what degree does your organisation currently outsource any of the risk management functions within your organisation?						

	1	2	3	4	5	6
34. To what degree does your organisation use some form of corporate scorecard to assess risk and measure it against predetermined tolerances?						

	1	2	3	4	5	6
35. To what degree do your organisational management reports supply information using measures that identify areas where risk tolerances are being exceeded or risk objectives not met?						

	1	2	3	4	5	6
36. To what degree does your organisation have processes or measures in place that are able to determine the effectiveness of risk mitigation techniques that have been implemented?						

	1	2	3	4	5	6
37. To what degree does your organisation keep an updated risk register?						

	1	2	3	4	5	6
38. To what degree does your organisation have a reporting process that takes into account both individual categories of risks and the interdependencies between them?						

	1	2	3	4	5	6
39. To what degree does your organisation view risk management processes as methods of actively creating value through prudent risk taking as opposed to only as tools to avoid organisational value deterioration?						

	1	2	3	4	5	6
40. To what degree does your organisation regard the introduction of a risk based capital regime such as Solvency Assessment and Management / Solvency II as essential?						

Section 3: What your organisation's approach towards operational risk management should be, based on your views, experience as well as knowledge

41. In your opinion to what degree of primary importance should your organisation rate the following areas of risk?	1	2	3	4	5	6
41.1. Insurance risk						
41.2. Market risk						
41.3. Credit risk						
41.4. Operational risk						
41.5. Liquidity risk						
41.6. Reputation risk						
41.7. Political risk						
41.8. Legal risk						

41.9. Other:

42. In your opinion to what degree should your organisation believe that the following are factors of operational risk?	1	2	3	4	5	6
42.1. People						
42.2. Processes						
42.3. Systems						
42.4. Other external factors (fraud, natural disasters)						

42.5. Other:

43. In your opinion to what degree should your organisation recognise the following human factors as an important element of operational risk?	1	2	3	4	5	6
43.1. Incompetence						
43.2. Negligence						
43.3. Human error						
43.4. Low morale						
43.5. High staff turnover						
43.6. Criminal activities (fraud)						
43.7. Lack of skills or training						

43.8. Other:

44. In your opinion to what degree should your organisation recognise the following process exposures as an important element of operational risk?	1	2	3	4	5	6
44.1. Errors in procedures or methodologies						
44.2. Execution errors						
44.3. Documentation errors						
44.4. Product complexity						
44.5. Security risks						

44.6. Other:

45. In your opinion to what degree should your organisation recognise the following systems exposures as an important element of operational risk?	1	2	3	4	5	6
45.1. System infiltration						
45.2. System failure						
45.3. Third party computer fraud						
45.4. Programming errors						
45.5. Information risk						
45.6. Telecommunications risk						
45.7. System obsolescence						

45.8. Other:

46. In your opinion to what degree should your organisation recognise the following external exposures as an important element of operational risk?	1	2	3	4	5	6
46.1. Acts of God						
46.2. Crime						
46.3. Regulation and compliance						
46.4. Legal actions						
46.5. Changes in the business environment						

46.6. Other:

	1	2	3	4	5	6
47. In your opinion to what degree should your organisation recognise the importance of implementing a formal risk management (ERM) process?						

	1	2	3	4	5	6
48. In your opinion to what degree should your organisation adopt a formal definition of operational risk?						

49. In your opinion to what degree should your organisation recognise the following as important elements of an operational risk management process?	1	2	3	4	5	6
49.1. Risk identification						
49.2. Risk measurement and evaluation						
49.3. Risk control						

49.4. Other:

	1	2	3	4	5	6
50. In your opinion to what degree should risk management be aligned to the overall business strategy, including covering the planned risk profile of the organisation and the approach to managing those risks?						

	1	2	3	4	5	6
51. In your opinion to what degree should an operational risk management process be recognised as an important and integral part of your organisation's overall management process?						

	1	2	3	4	5	6
52. In your opinion to what degree should the board set the strategies, policies and processes surrounding risk management?						

	1	2	3	4	5	6
53. In your opinion to what degree should the board actively provide oversight to risk management strategies?						

	1	2	3	4	5	6
54. In your opinion to what degree should the board actively challenge management's assessment of key risks and their approach to managing those risks?						

	1	2	3	4	5	6
55. In your opinion to what degree should there be a comprehensive understanding of and agreement on the organisation's risk appetite within the organisation?						

	1	2	3	4	5	6
56. In your opinion to what degree should your organisation's risk management process be integrated? (That is, to what extent should risk management be owned, monitored and managed at a local level within the business?)						

	1	2	3	4	5	6
57. In your opinion to what degree should the organisational risk appetite be clearly communicated to business unit managers who are required to implement operational risk management processes?						

	1	2	3	4	5	6
58. In your opinion to what degree should management incentive compensation be tied to organisational risk objectives and risk / return measures approved by the board?						

	1	2	3	4	5	6
59. In your opinion to what degree should there be appropriate segregation of duties between those responsible for monitoring and measuring risk and those responsible for making decisions?						

60. In your opinion to what degree should your organisation recognise the importance of and implement the following operational risk control measures?	1	2	3	4	5	6
60.1. Policies and procedures						
60.2. Internal controls						
60.3. Risk reporting						

60.4. Other:

61. In your opinion to what degree should your organisation use the following methods to measure operational risk?	1	2	3	4	5	6
61.1. Stress testing						
61.2. Scenario analysis						
61.3. Simulation techniques						
61.4. Actuarial methods						
61.5. Historical data to forecast potential losses						
61.6. Self-risk assessments						
61.7. Risk maps and process flows						

61.8. Other:

	1	2	3	4	5	6
62. In your opinion to what degree should your organisation have an ongoing process in place for identifying / managing significant operational risks?						

	1	2	3	4	5	6
63. In your opinion to what degree should your organisation have a risk strategy related to risk classes as well as overall risk exposure?						

64. In your opinion to what degree should your organisation recognise the following methods as the most appropriate to identify risks?	1	2	3	4	5	6
64.1. Workshops						
64.2. Brainstorming						
64.3. Questionnaires						
64.4. Process mapping						
64.5. Comparison with other organisations						
64.6. Peer discussions						

64.7. Other:

	1	2	3	4	5	6
65. In your opinion to what degree should your organisation establish a separate operational risk management structure?						

	1	2	3	4	5	6
66. In your opinion to what degree should a risk manager have direct access to the CEO of your organisation?						

	1	2	3	4	5	6
67. In your opinion to what degree should your organisation involve internal audit to manage operational risk?						

	1	2	3	4	5	6
68. In your opinion to what degree should your organisation involve business unit managers in operational risk management processes?						

	1	2	3	4	5	6
69. In your opinion to what degree should your organisation on an ongoing, immediate basis adjust the organisation's risk appetite and risk processes based on past experiences, pro forma results, future stakeholder expectations and existing market conditions?						

70. In your opinion to what degree should the following factors influence your organisation's development and improvement of risk management processes?	1	2	3	4	5	6
70.1. Compliance - regulatory						
70.2. Compliance - shareholders						
70.3. Compliance - market						
70.4. Business driven logic						
70.5. Losses made by others						
70.6. Being a pioneer in risk management						
70.7. Image						

70.8. Other:

	1	2	3	4	5	6
71. In your opinion to what degree should decisions to enter or withdraw from certain lines of business be based upon their potential impact on the organisation's risk / return measures?						

	1	2	3	4	5	6
72. In your opinion to what degree should your organisation account for dependencies between risks?						

	1	2	3	4	5	6
73. In your opinion to what degree should your organisation outsource any of the risk management functions within your organisation?						

	1	2	3	4	5	6
74. In your opinion to what degree should your organisation use some form of corporate scorecard to assess risk and measure it against predetermined tolerances?						

	1	2	3	4	5	6
75. In your opinion to what degree should your organisational management reports supply information using measures that identify areas where risk tolerances are being exceeded or risk objectives not met?						

	1	2	3	4	5	6
76. In your opinion to what degree should your organisation have processes or measures in place that are able to determine the effectiveness of risk mitigation techniques that have been implemented?						

	1	2	3	4	5	6
77. In your opinion to what degree should your organisation keep an updated risk register?						

	1	2	3	4	5	6
78. In your opinion to what degree should your organisation have a reporting process that takes into account both individual categories of risks and the interdependencies between them?						

	1	2	3	4	5	6
79. In your opinion to what degree should your organisation view risk management processes as methods of actively creating value through prudent risk taking as opposed to only tools to avoid organisational value deterioration?						

	1	2	3	4	5	6
80. In your opinion to what degree should your organisation regard the introduction of a risk based capital regime such as Solvency Assessment and Management / Solvency II as essential?						

THANK YOU FOR TAKING THE TIME TO COMPLETE THE QUESTIONNAIRE

Other comments:

Please add any other comments that you may wish to express with regard to operational risk management in the short-term insurance industry here:

Appendix 3: Schedule

DATE	DELIVERABLE	REMARKS
26 February 2010	Submit research topic to SBL.	
15 July	Submit research proposal electronically on the EDS.	• Introduction and background to the study • Statement of the problem and sub-problems and research objectives • Importance of the study and potential benefits • Literature Review • Research Methodology
20 July 2010	Survey questionnaire to be ready for delivery / posting.	
21 July 2010	Delivery / posting of survey questionnaires	
21 August 2010	Receipt of completed questionnaires	
22 August 2010 through to 21 September 2010	Inclusion of questionnaire data into research report.	• Collation of data • Interpretation of data • Formulation of findings • Conclusions
22 September	Submit first draft research report to SBL on EDS. Include comments from lecturer on the research proposal in track changes.	• Complete as possible. • Include all chapters, conclusions and recommendations.
31 October	Request permission to prepare final submission.	
22 November	Submit final report for examination.	
January 2010	Notification of pass or not.	• Insert minor changes if required. • Submit 2 leather bound copies after changes / corrections made.

Appendix 4: Consistency matrix

Objective	Literature Review (refs)	Research objective	Question	Data analysis method
Definition of operational risk.	Basel (2003) Dickstein and Flast (2008) Dowd (1998) FSA (2004) Lam (2003) Tripp, *et al*. (2004) Young (2001) Young (2005) Zurich (2010)	Identification of definition of operational risk. Evaluate insurers rating of primary importance.	1 8	Desc. Stats./t-test Desc. Stats./t-test
Definition of risk management.	Blokdijk (2010) CAS (2003) COSO (2004) IAA (2009) Institute of Actuaries (2009) IRM (2002) ISO (2009) Oxford Advanced Learner's Dictionary (2010) Q Finance (2010)	Identification of definition of risk management.	Not applicable	
Application of risk management – A Risk Management Framework.	CAS (2003) FSA (2006) ISO (2009) Zurich (2009)	Identification of a risk management framework. Evaluate insurers recognition of a framework.	7 9	Desc. Stats./t-test Desc. Stats./t-test
The components of operational risk.	Basel (2003) FSA (2004) Dickstein and Flast (2008) Dowd (1998) Hoffman (2002) Hussain (2000) Lam (2003) Loader (2007) Young (2005) Zurich (2009)	Identification of definition of the components of operational risk. Evaluate insurers recognition of the components of operational risk.	2 3 4 5 6	Desc. Stats./t-test Desc. Stats./t-test Desc. Stats./t-test Desc. Stats./t-test Desc. Stats./t-test
Identification of operational risks.	CAS (2003) FSA (2004) Hoffman (2002) International Association of Actuaries (2009) IRM (2002) ISO (2009)	Identification of operational risks. Evaluate insurers recognition of various methods.	24	Desc. Stats./t-test

	Young (2005)			
Measurement and evaluation of operational risks.	Basel (2003) Dickstein and Flast (2008) FSA (2002) FSA (2003) FSA (2004) FSA (2006) Hoffman (2002) Institute of Actuaries (2009) International Actuarial Association (2009) Soprano, Crielaard, Piacenza & Ruspantini (2009) Tripp, *et al.* (2004) Young (2005)	Identification of various methods of operational risk measurement and evaluation. Evaluate insurers recognition and use of the various methods.	21	Desc. Stats./t-test
Risk mitigation and control of operational risks.	Basel (2003) Damodaran (2008) Dickstein and Flast (2008) Dowd (1998) Institute of Actuaries (2009) Sadgrove (2005) Tripp, *et al.* (2004) Young (2005)	Identification of risk mitigation and control methods and practices. Evaluate insurers use and recognition of methods and practices.	15 17 20 22 23 29 30 31 33 36	Desc. Stats./t-test Desc. Stats./t-test Desc. Stats./t-test Desc. Stats./t-test Desc. Stats./t-test Desc. Stats./t-test Desc. Stats./t-test Desc. Stats./t-test Desc. Stats./t-test Desc. Stats./t-test
Monitoring and reporting of operational risks.	COSO (2004) Dickstein and Flast (2008) FSA (2008) Hoffman (2002) Institute of Actuaries (2009) International Actuarial Association (2009) IRM (2002) Sadgrove (2005) Young (2005)	Identification of risk monitoring and reporting methods and practices. Evaluate insurers use and recognition of methods and practices.	13 14 19 25 26 27 28 32 34 35 37 38	Desc. Stats./t-test Desc. Stats./t-test Desc. Stats./t-test Desc. Stats./t-test Desc. Stats./t-test Desc. Stats./t-test Desc. Stats./t-test Desc. Stats./t-test Desc. Stats./t-test Desc. Stats./t-test Desc. Stats./t-test Desc. Stats./t-test
Integrating operational risk management into the organisation.	Damodaran (2008) Deighton, Dix, Graham, & Skinner (2009) Dickstein and Flast (2008) EMB (2010) FSA (2003) Hoffman (2002) International Actuarial Association (2009) IRM (2002) KPMG (2010) Patel and George (2009)	Identification of importance of integration of operational risk management into the organisation. Evaluate insurers integration of practice into organisations.	10 11 12 16 18 39 40	Desc. Stats./t-test Desc. Stats./t-test Desc. Stats./t-test Desc. Stats./t-test Desc. Stats./t-test Desc. Stats./t-test Desc. Stats./t-test

	Standard & Poor's (2005) Young (2005)			

Appendix 5: List of registered short-term insurers

The below mentioned represents the list of registered South African short-term insurance companies (Financial Services Board, 2010).

ABSA IDIRECT LIMITED – **Excluded**
ABSA INSURANCE COMPANY LIMITED
ABSA INSURANCE RISK MANAGEMENT SERVICES LIMITED – **Excluded**
ACE INSURANCE LIMITED
AECI CAPTIVE INSURANCE COMPANY LIMITED
AEGIS INSURANCE COMPANY LIMITED - **Excluded**
AFRICAN GENERAL INSURANCE COMPANY LIMITED - **Excluded**
ALEXANDER FORBES INSURANCE COMPANY LIMITED
ALLIANZ INSURANCE LIMITED
ATTORNEYS INSURANCE INDEMNITY FUND
AURORA INSURANCE COMPANY LIMITED
AUTO AND GENERAL INSURANCE COMPANY LIMITED
AVIATION INSURANCE COMPANY LIMITED
BENSURE INSURANCE UNDERWRITERS LIMITED
CENTRAL REINSURANCE CORPORATION LIMITED
CENTRIQ INSURANCE COMPANY LIMITED
CGU INSURANCE LIMITED - **Excluded**
CHARTIS SOUTH AFRICA LIMITED
CLIENTELE GENERAL INSURANCE LIMITED
COFACE SOUTH AFRICA INSURANCE COMPANY LIMITED
COMPASS INSURANCE COMPANY LIMITED
CONSTANTIA INSURANCE COMPANY LIMITED
CORPORATE GUARANTEE (SOUTH AFRICA) LIMITED
CREDIT GUARANTEE INSURANCE CORPORATION OF AFRICA LIMITED
CUSTOMER PROTECTION INSURANCE COMPANY LIMITED
DENSECURE (EDMS) BPK
DIAL DIRECT INSURANCE LIMITED
EMERALD INSURANCE COMPANY LIMITED - **Excluded**
ENPET AFRICA INSURANCE LIMITED
ESCAP LIMITED
ETANA INSURANCE COMPANY LIMITED

EXPORT CREDIT INSURANCE CORPORATION OF SOUTH AFRICA LIMITED
EXXARO INSURANCE COMPANY LIMITED
FEDERATED EMPLOYERS` MUTUAL ASSURANCE COMPANY LIMITED
FIRST CENTRAL INSURANCE LIMITED - **Excluded**
FIRSTRAND INSURANCE SERVICES COMPANY LIMITED
FNB CREDIT GUARANTEE LIMITED
G4S INSURANCE LIMITED
GENERAL ACCIDENT INS. COMPANY SOUTH AFRICA LIMITED - **Excluded**
GUARDIAN NATIONAL INSURANCE COMPANY LIMITED - **Excluded**
GUARDRISK INSURANCE COMPANY LIMITED
HOLLARD INSURANCE COMPANY LIMITED,THE
HOME LOAN GUARANTEE COMPANY
INDEQUITY SPECIALISED INSURANCE LIMITED
INFINITI INSURANCE LIMITED
INTERMEDIARIES GUARANTEE FACILITY LTD
JDG MICRO INSURANCE LIMITED
KHULA CREDIT GUARANTEE LIMITED
KINGFISHER INSURANCE COMPANY
LEGAL EXPENSES INSURANCE SOUTHERN AFRICA LIMITED
LION OF AFRICA INSURANCE COMPANY LIMITED
LOMBARD INSURANCE COMPANY LIMITED
MCSURE LIMITED
MIWAY INSURANCE LIMITED
MOMENTUM SHORT-TERM INSURANCE COMPANY LIMITED
MOMENTUM STRUCTURED INSURANCE LIMITED
MONARCH INSURANCE COMPANY LIMITED
MUA INSURANCE COMPANY LIMITED
MUTUAL & FEDERAL INSURANCE COMPANY LIMITED
MUTUAL & FEDERAL RISK FINANCING LIMITED - **Excluded**
NATSURE LIMITED
NEDCOR (SA) INSURANCE COMPANY LIMITED
NEDGROUP INSURANCE COMPANY LIMITED - **Excluded**
NEW NATIONAL ASSURANCE COMPANY LIMITED
NMS INSURANCE COMPANY (SA) LIMITED
NOVA RISK PARTNERS LIMITED - **Excluded**

OAKHURST INSURANCE COMPANY LIMITED
ORANGE INSURANCE LIMITED
OUTSURANCE INSURANCE COMPANY LIMITED
PINNAFRICA INSURANCE LIMITED
REGENT INSURANCE COMPANY LIMITED
RELYANT INSURANCE COMPANY LIMITED
RENASA INSURANCE COMPANY LIMITED
RESOLUTION INSURANCE COMPANY LIMITED
RMB SPECIALISED LINES LIMITED
RMB STRUCTURED INSURANCE LIMITED
SABSURE LIMITED
SAFIRE INSURANCE COMPANY LIMITED
SAHL INSURANCE COMPANY LIMITED
SANTAM BEPERK
SASGUARD INSURANCE COMPANY LIMITED
SASRIA LIMITED
SAXUM INSURANCE LIMITED
SCOR AFRICA LIMITED
SENTRASURE LIMITED
SHOPRITE INSURANCE COMPANY LIMITED
SOUTH AFRICAN RESERVE BANK CAPTIVE INSURANCE COMPANY
STANDARD INSURANCE LIMITED
SUNDERLAND MARINE (AFRICA) LIMITED
THE PARKTOWN INSURANCE COMPANY LIMITED
TRUCK & GENERAL INSURANCE COMPANY LIMITED
UNITRANS INSURANCE LIMITED
UNITY INSURANCE LIMITED
WESTCHESTER INSURANCE COMPANY (PTY) LIMITED
WESTERN NATIONAL INSURANCE COMPANY LIMITED
XL INSURANCE COMPANY LIMITED
ZURICH INSURANCE COMPANY SOUTH AFRICA LIMITED
ZURICH RISK FINANCING SA LIMITED - **Excluded**

Appendix 6: Data tables

		Question	Question	Question	Q	Q	Q	Q
		Organisation	Role	Experience	1.1	1.2	1.3	1.4
Respondent	1	3	2	3	4	1	4	3
Respondent	2	3	1	3	5	2	5	5
Respondent	3	1	2	5	4	1	4	3
Respondent	4	1	2	4	4	2	5	4
Respondent	5	1	1	4	4	2	4	3
Respondent	6	1	3	3	4	3	4	3
Respondent	7	1	4	3	5	2	4	4
Respondent	8	2	4	3	4	2	5	3
Respondent	9	1	2	3	4	2	5	3
Respondent	10	1	1	4	4	3	4	3
Respondent	11	2	1	5	5	3	4	3
Respondent	12	1	1	4	4	2	3	3
Respondent	13	1	4	3	4	2	4	3
Respondent	14	1	3	3	4	1	4	4
Respondent	15	1	3	3	4	1	4	3
Respondent	16	1	1	4	5	2	4	3
Respondent	17	2	2	3	4	1	4	4
Respondent	18	1	1	4	4	2	4	3
Respondent	19	2	4	3	4	2	3	4
Respondent	20	1	1	4	5	1	4	4
Respondent	21	1	3	3	5	2	4	3
Respondent	22	1	3	3	5	2	4	3
Respondent	23	1	4	3	4	2	3	3
Respondent	24	2	4	3	4	1	4	4
Respondent	25	1	2	3	4	2	4	3
Respondent	26	1	3	3	5	3	3	3
Respondent	27	1	3	3	4	2	4	4
Count		27	27	27	27	27	27	27
Response	1	74.07%	29.63%	0.00%	0.00%	25.93%	0.00%	0.00%
Response	2	18.52%	22.22%	0.00%	0.00%	59.26%	0.00%	0.00%
Response	3	7.41%	25.93%	66.67%	0.00%	14.81%	14.81%	66.67%
Response	4	0.00%	22.22%	25.93%	70.37%	0.00%	70.37%	29.63%
Response	5	0.00%	0.00%	7.41%	29.63%	0.00%	14.81%	3.70%
Response	6	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	7	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	8	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Mean		N/A	N/A	N/A	4.30	1.89	4.00	3.37
Validate		100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%
t-value					1.2E-08	1.7E-05	0.00567	1.3E-14
df=26								
p = 0.05		1.706			1.71	1.71	1.71	1.71
p = 0.10		1.315			1.32	1.32	1.32	1.32
Sig. 0.05					**YES**	**YES**	NO	**YES**
Sig. 0.10					**YES**	**YES**	NO	**YES**

		Q	Q	Q	Q	Q	Q	Q	Q
		1.5	**1.6**	**1.7**	**1.8**	**1.9**	**2.1**	**2.2**	**2.3**
Respondent	1	2	5	2	3	0	4	4	4
Respondent	2	2	4	2	3	0	5	5	5
Respondent	3	2	4	2	3	0	4	4	4
Respondent	4	2	4	2	4	0	4	3	4
Respondent	5	3	4	2	3	0	4	4	4
Respondent	6	3	4	2	3	0	4	4	4
Respondent	7	3	4	2	3	0	4	4	4
Respondent	8	2	4	3	3	0	4	4	4
Respondent	9	3	5	2	4	0	3	3	4
Respondent	10	3	5	2	3	0	4	3	4
Respondent	11	2	4	3	3	0	3	3	4
Respondent	12	3	5	3	4	0	4	3	4
Respondent	13	3	5	2	3	0	4	4	4
Respondent	14	3	5	2	3	0	4	4	4
Respondent	15	3	5	2	3	0	4	4	4
Respondent	16	3	5	2	3	0	4	3	4
Respondent	17	3	4	2	3	0	3	4	4
Respondent	18	3	4	3	3	0	4	3	4
Respondent	19	2	5	2	3	0	4	4	4
Respondent	20	4	5	2	4	0	4	4	4
Respondent	21	3	5	3	3	0	4	4	4
Respondent	22	3	4	3	4	0	4	3	4
Respondent	23	3	5	3	3	0	4	4	4
Respondent	24	3	5	3	3	0	4	3	4
Respondent	25	3	4	2	3	0	4	4	4
Respondent	26	3	5	3	3	0	4	4	4
Respondent	27	3	5	2	3	0	4	4	4
Count		27	27	27	27	27	27	27	27
Response	1	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	2	25.93%	0.00%	66.67%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	3	70.37%	0.00%	33.33%	81.48%	0.00%	11.11%	33.33%	0.00%
Response	4	3.70%	44.44%	0.00%	18.52%	0.00%	85.19%	62.96%	96.30%
Response	5	0.00%	55.56%	0.00%	0.00%	0.00%	3.70%	3.70%	3.70%
Response	6	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	7	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	8	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Mean		2.78	4.56	2.33	3.19	0.00	3.93	3.70	4.04
Validate		100.00%	100.00%	100.00%	100.00%	0.00%	100.00%	100.00%	100.00%
t-value		0.00051	0.16326	7.2E-08	1.8E-08		5.9E-08	7.1E-07	2.4E-07
df=26									
p = 0.05		1.71	1.71	1.71	1.71		1.71	1.71	1.71
p = 0.10		1.32	1.32	1.32	1.32		1.32	1.32	1.32
Sig. 0.05		NO	NO	**YES**	**YES**		**YES**	**YES**	**YES**
Sig. 0.10		NO	NO	**YES**	**YES**		**YES**	**YES**	**YES**

		Q	Q	Q	Q	Q	Q	Q	Q
		2.4	2.5	3.1	3.2	3.3	3.4	3.5	3.6
Respondent	1	4	0	4	4	4	2	3	4
Respondent	2	3	0	4	3	5	3	4	3
Respondent	3	4	0	4	3	4	3	2	4
Respondent	4	3	0	4	4	4	2	3	4
Respondent	5	4	0	4	3	3	3	4	3
Respondent	6	3	0	4	3	4	3	3	4
Respondent	7	4	0	4	3	4	2	3	3
Respondent	8	4	0	4	4	3	2	2	4
Respondent	9	4	0	3	3	4	2	3	4
Respondent	10	3	0	4	4	4	3	3	3
Respondent	11	3	0	4	4	3	2	4	3
Respondent	12	3	0	4	4	4	2	3	4
Respondent	13	3	0	4	4	3	3	3	4
Respondent	14	4	0	4	4	4	2	4	4
Respondent	15	4	0	4	4	4	2	2	3
Respondent	16	3	0	3	4	3	2	3	4
Respondent	17	3	0	3	4	4	3	4	3
Respondent	18	4	0	4	4	4	2	2	4
Respondent	19	4	0	4	3	3	3	3	4
Respondent	20	4	0	4	3	4	2	3	4
Respondent	21	3	0	4	4	4	2	2	3
Respondent	22	4	0	4	4	3	2	4	4
Respondent	23	3	0	4	4	4	2	3	4
Respondent	24	4	0	4	3	3	2	3	3
Respondent	25	4	0	4	4	4	2	3	4
Respondent	26	3	0	4	4	4	3	3	3
Respondent	27	3	0	4	4	4	3	4	4
Count		27	27	27	27	27	27	27	27
Response	1	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	2	0.00%	0.00%	0.00%	0.00%	0.00%	62.96%	18.52%	0.00%
Response	3	48.15%	0.00%	11.11%	33.33%	29.63%	37.04%	55.56%	37.04%
Response	4	51.85%	0.00%	88.89%	66.67%	66.67%	0.00%	25.93%	62.96%
Response	5	0.00%	0.00%	0.00%	0.00%	3.70%	0.00%	0.00%	0.00%
Response	6	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	7	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	8	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Mean		3.52	0.00	3.89	3.67	3.74	2.37	3.07	3.63
Validate		100.00%	0.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%
t-value		2.1E-06		8.4E-07	2.1E-06	1.2E-06	8.9E-14	0.04151	0.00065
df=26									
p = 0.05		1.71		1.71	1.71	1.71	1.71	1.71	1.71
p = 0.10		1.32		1.32	1.32	1.32	1.32	1.32	1.32
Sig. 0.05		YES		YES	YES	YES	YES	NO	NO
Sig. 0.10		YES		YES	YES	YES	YES	NO	NO

		Q	Q	Q	Q	Q	Q	Q	Q
		3.7	3.8	4.1	4.2	4.3	4.4	4.5	4.6
Respondent	1	4	0	4	3	3	4	3	0
Respondent	2	4	0	4	5	4	5	4	0
Respondent	3	3	0	3	3	4	3	3	0
Respondent	4	4	0	3	3	4	3	3	0
Respondent	5	4	0	4	4	3	4	3	0
Respondent	6	4	0	3	4	3	4	3	0
Respondent	7	4	0	4	4	3	4	3	0
Respondent	8	3	0	4	4	4	3	4	0
Respondent	9	4	0	4	4	3	4	3	0
Respondent	10	3	0	3	4	4	4	3	0
Respondent	11	4	0	4	3	4	3	3	0
Respondent	12	4	0	4	4	4	3	3	0
Respondent	13	4	0	3	4	3	3	3	0
Respondent	14	3	0	3	3	3	4	3	0
Respondent	15	4	0	4	4	4	3	4	0
Respondent	16	3	0	4	4	4	4	4	0
Respondent	17	4	0	3	3	4	4	3	0
Respondent	18	4	0	4	4	4	4	3	0
Respondent	19	4	0	3	4	3	4	3	0
Respondent	20	4	0	4	4	3	4	3	0
Respondent	21	4	0	4	4	4	4	3	0
Respondent	22	4	0	4	4	3	3	3	0
Respondent	23	4	0	3	3	4	3	3	0
Respondent	24	3	0	4	4	4	4	3	0
Respondent	25	4	0	4	4	4	3	3	0
Respondent	26	4	0	4	4	3	4	3	0
Respondent	27	4	0	3	3	4	4	3	0
Count		27	27	27	27	27	27	27	27
Response	1	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	2	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	3	22.22%	0.00%	37.04%	29.63%	40.74%	37.04%	85.19%	0.00%
Response	4	77.78%	0.00%	62.96%	66.67%	59.26%	59.26%	14.81%	0.00%
Response	5	0.00%	0.00%	0.00%	3.70%	0.00%	3.70%	0.00%	0.00%
Response	6	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	7	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	8	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Mean		3.78	0.00	3.63	3.74	3.59	3.67	3.15	0.00
Validate		100.00%	0.00%	100.00%	100.00%	100.00%	100.00%	100.00%	0.00%
t-value		0.00065		1.3E-05	1.5E-05	2.7E-07	0.04151	0.00567	
df=26									
p = 0.05		1.71		1.71	1.71	1.71	1.71	1.71	
p = 0.10		1.32		1.32	1.32	1.32	1.32	1.32	
Sig. 0.05		NO		**YES**	**YES**	**YES**	NO	NO	
Sig. 0.10		NO		**YES**	**YES**	**YES**	NO	NO	

		Q	Q	Q	Q	Q	Q	Q	Q
		5.1	5.2	5.3	5.4	5.5	5.6	5.7	5.8
Respondent	1	4	4	3	3	3	4	3	0
Respondent	2	2	4	3	3	5	3	2	0
Respondent	3	4	4	3	3	3	3	3	0
Respondent	4	4	4	4	3	4	4	3	0
Respondent	5	4	4	4	4	3	4	3	0
Respondent	6	3	4	4	4	3	3	4	0
Respondent	7	4	4	3	4	4	4	4	0
Respondent	8	4	3	4	3	3	4	3	0
Respondent	9	3	4	4	4	4	4	3	0
Respondent	10	4	4	4	3	3	3	3	0
Respondent	11	4	4	3	4	4	4	3	0
Respondent	12	4	4	4	4	4	4	3	0
Respondent	13	4	4	4	4	4	4	3	0
Respondent	14	4	3	4	3	3	4	3	0
Respondent	15	4	4	4	4	4	3	4	0
Respondent	16	3	4	3	3	3	4	3	0
Respondent	17	4	4	4	3	3	3	3	0
Respondent	18	4	4	3	4	4	4	3	0
Respondent	19	4	4	4	4	3	3	3	0
Respondent	20	4	4	4	3	4	3	3	0
Respondent	21	4	4	3	4	4	4	3	0
Respondent	22	4	4	4	4	4	4	3	0
Respondent	23	4	4	4	4	4	4	4	0
Respondent	24	3	4	4	3	3	4	3	0
Respondent	25	4	4	4	4	4	4	3	0
Respondent	26	4	4	4	3	4	3	3	0
Respondent	27	4	4	4	4	4	4	4	0
Count		27	27	27	27	27	27	27	27
Response	1	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	2	3.70%	0.00%	0.00%	0.00%	0.00%	0.00%	3.70%	0.00%
Response	3	14.81%	7.41%	29.63%	44.44%	40.74%	33.33%	77.78%	0.00%
Response	4	81.48%	92.59%	70.37%	55.56%	55.56%	66.67%	18.52%	0.00%
Response	5	0.00%	0.00%	0.00%	0.00%	3.70%	0.00%	0.00%	0.00%
Response	6	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	7	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	8	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Mean		3.78	3.93	3.70	3.56	3.63	3.67	3.15	0.00
Validate		100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	0.00%
t-value		0.01113	0.00065	0.00031	0.00035	6.2E-06	0.00131	4.1E-10	
df=26									
p = 0.05		1.71	1.71	1.71	1.71	1.71	1.71	1.71	
p = 0.10		1.32	1.32	1.32	1.32	1.32	1.32	1.32	
Sig. 0.05		NO	NO	NO	NO	**YES**	NO	**YES**	
Sig. 0.10		NO	NO	NO	NO	**YES**	NO	**YES**	

		Q	Q	Q	Q	Q	Q	Q	Q
		6.1	6.2	6.3	6.4	6.5	6.6	7	8
Respondent	1	2	2	5	3	3	0	5	5
Respondent	2	2	3	5	3	4	0	5	4
Respondent	3	2	3	5	4	3	0	5	3
Respondent	4	2	2	5	4	3	0	5	4
Respondent	5	3	3	5	3	3	0	4	4
Respondent	6	2	3	4	3	3	0	4	5
Respondent	7	2	2	4	4	4	0	5	4
Respondent	8	2	2	4	4	3	0	5	5
Respondent	9	2	3	4	4	4	0	5	5
Respondent	10	3	3	4	4	3	0	5	5
Respondent	11	3	3	4	5	3	0	4	4
Respondent	12	2	2	5	5	4	0	5	4
Respondent	13	2	2	5	4	3	0	5	5
Respondent	14	3	3	4	4	3	0	4	4
Respondent	15	2	3	4	4	4	0	5	3
Respondent	16	2	3	5	3	3	0	5	4
Respondent	17	2	3	5	4	3	0	4	4
Respondent	18	2	2	5	3	3	0	5	5
Respondent	19	3	3	5	4	3	0	5	5
Respondent	20	3	3	4	3	3	0	5	5
Respondent	21	2	2	4	3	4	0	5	5
Respondent	22	2	2	5	4	3	0	5	5
Respondent	23	2	3	5	4	4	0	5	4
Respondent	24	2	3	4	4	4	0	5	5
Respondent	25	3	3	5	3	4	0	5	5
Respondent	26	2	2	4	4	3	0	5	4
Respondent	27	2	3	4	4	4	0	5	5
Count		27	27	27	27	27	27	27	27
Response	1	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	2	74.07%	37.04%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	3	25.93%	62.96%	0.00%	33.33%	62.96%	0.00%	0.00%	7.41%
Response	4	0.00%	0.00%	48.15%	59.26%	37.04%	0.00%	18.52%	40.74%
Response	5	0.00%	0.00%	51.85%	7.41%	0.00%	0.00%	81.48%	51.85%
Response	6	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	7	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	8	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Mean		2.26	2.63	4.52	3.74	3.37	0.00	4.81	4.44
Validate		100.00%	100.00%	100.00%	100.00%	100.00%	0.00%	100.00%	100.00%
t-value		1.9E-20	2.5E-28	0.08059	0.00013	1.9E-07		0.01113	6.2E-05
df=26									
p = 0.05		1.71	1.71	1.71	1.71	1.71		1.71	1.71
p = 0.10		1.32	1.32	1.32	1.32	1.32		1.32	1.32
Sig. 0.05		YES	YES	NO	NO	YES		NO	YES
Sig. 0.10		YES	YES	NO	NO	YES		NO	YES

		Q	Q	Q	Q	Q	Q	Q	Q
		9.1	9.2	9.3	9.4	10	11	12	13
Respondent	1	5	4	3	0	4	4	4	4
Respondent	2	5	4	5	0	4	4	4	4
Respondent	3	5	4	4	0	4	3	3	4
Respondent	4	4	3	3	0	3	3	4	4
Respondent	5	4	4	4	0	3	3	4	4
Respondent	6	5	4	4	0	3	3	3	4
Respondent	7	4	4	3	0	4	4	4	4
Respondent	8	5	4	4	0	4	4	4	4
Respondent	9	5	5	4	0	3	3	4	3
Respondent	10	4	4	3	0	4	3	3	4
Respondent	11	4	4	3	0	4	4	4	3
Respondent	12	4	4	3	0	3	3	4	4
Respondent	13	5	4	3	0	3	3	3	4
Respondent	14	4	4	3	0	3	3	4	4
Respondent	15	4	4	4	0	4	3	4	4
Respondent	16	4	4	3	0	3	3	4	4
Respondent	17	4	4	4	0	4	3	4	4
Respondent	18	5	5	4	0	4	4	4	3
Respondent	19	4	4	4	0	4	4	3	4
Respondent	20	5	3	3	0	4	4	3	4
Respondent	21	5	4	3	0	4	3	4	3
Respondent	22	4	4	3	0	3	3	3	4
Respondent	23	4	4	3	0	3	3	4	4
Respondent	24	5	5	4	0	4	3	3	4
Respondent	25	5	5	4	0	4	4	3	3
Respondent	26	4	4	3	0	4	4	4	4
Respondent	27	4	4	3	0	4	3	4	4
Count		27	27	27	27	27	27	27	27
Response	1	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	2	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	3	0.00%	7.41%	55.56%	0.00%	37.04%	62.96%	33.33%	18.52%
Response	4	55.56%	77.78%	40.74%	0.00%	62.96%	37.04%	66.67%	81.48%
Response	5	44.44%	14.81%	3.70%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	6	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	7	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	8	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Mean		4.44	4.07	3.48	0.00	3.63	3.37	3.67	3.81
Validate		100.00%	100.00%	100.00%	0.00%	100.00%	100.00%	100.00%	100.00%
t-value		2.7E-06	7.9E-11	1.2E-13		3E-14	5E-16	3.2E-14	5.5E-15
df=26									
p = 0.05		1.71	1.71	1.71		1.71	1.71	1.71	1.71
p = 0.10		1.32	1.32	1.32		1.32	1.32	1.32	1.32
Sig. 0.05		YES	YES	YES		YES	YES	YES	YES
Sig. 0.10		YES	YES	YES		YES	YES	YES	YES

		Q	Q	Q	Q	Q	Q	Q	Q
		14	15	16	17	18	19	20.1	20.2
Respondent	1	3	2	3	2	2	2	3	4
Respondent	2	4	2	3	2	3	3	4	4
Respondent	3	4	2	2	2	2	2	3	4
Respondent	4	3	3	3	3	2	3	3	4
Respondent	5	4	2	3	2	2	3	3	4
Respondent	6	4	2	3	3	2	2	3	4
Respondent	7	4	2	2	2	2	3	3	4
Respondent	8	4	2	3	2	2	3	3	4
Respondent	9	3	3	2	2	2	3	4	4
Respondent	10	4	2	2	2	2	3	3	4
Respondent	11	3	3	3	3	2	2	4	3
Respondent	12	4	4	3	3	2	3	4	4
Respondent	13	4	3	3	2	2	2	3	4
Respondent	14	4	2	2	2	2	2	4	4
Respondent	15	4	3	3	3	3	2	3	4
Respondent	16	4	3	3	3	2	3	3	4
Respondent	17	4	3	3	3	2	3	3	4
Respondent	18	3	3	3	3	3	2	3	4
Respondent	19	4	2	2	2	2	3	4	4
Respondent	20	4	2	3	2	2	3	3	4
Respondent	21	3	3	2	2	2	2	3	4
Respondent	22	4	2	2	2	2	2	3	4
Respondent	23	4	3	3	3	2	2	3	4
Respondent	24	4	3	3	3	2	3	3	4
Respondent	25	3	3	3	3	2	2	3	4
Respondent	26	4	3	3	3	3	3	3	3
Respondent	27	4	2	2	2	2	2	3	4
Count		27	27	27	27	27	27	27	27
Response	1	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	2	0.00%	48.15%	33.33%	55.56%	85.19%	48.15%	0.00%	0.00%
Response	3	25.93%	48.15%	66.67%	44.44%	14.81%	51.85%	77.78%	7.41%
Response	4	74.07%	3.70%	0.00%	0.00%	0.00%	0.00%	22.22%	92.59%
Response	5	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	6	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	7	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	8	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Mean		3.74	2.56	2.67	2.44	2.15	2.52	3.22	3.93
Validate		100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%
t-value		2.2E-14	1.2E-18	4.1E-20	1.6E-20	1.9E-25	5.8E-14	1.6E-18	4.4E-18
df=26									
p = 0.05		1.71	1.71	1.71	1.71	1.71	1.71	1.71	1.71
p = 0.10		1.32	1.32	1.32	1.32	1.32	1.32	1.32	1.32
Sig. 0.05		YES	YES	YES	YES	YES	YES	YES	YES
Sig. 0.10		YES	YES	YES	YES	YES	YES	YES	YES

		Q	Q	Q	Q	Q	Q	Q	Q
		20.3	20.4	21.1	21.2	21.3	21.4	21.5	21.6
Respondent	1	4	0	1	2	1	2	2	3
Respondent	2	4	0	1	1	1	2	2	4
Respondent	3	4	0	1	2	1	2	2	3
Respondent	4	3	0	2	2	2	3	3	3
Respondent	5	3	0	1	2	2	2	2	2
Respondent	6	4	0	1	1	1	2	2	3
Respondent	7	4	0	1	1	1	2	2	2
Respondent	8	4	0	1	2	1	2	2	2
Respondent	9	4	0	1	2	1	3	3	3
Respondent	10	3	0	1	1	1	2	2	3
Respondent	11	3	0	1	2	1	3	3	3
Respondent	12	4	0	1	1	1	3	3	3
Respondent	13	3	0	1	1	1	3	3	3
Respondent	14	4	0	2	2	1	2	2	2
Respondent	15	4	0	1	1	1	3	3	3
Respondent	16	4	0	1	2	1	2	2	3
Respondent	17	4	0	2	2	1	2	2	3
Respondent	18	3	0	1	1	1	2	2	3
Respondent	19	4	0	1	2	1	3	3	2
Respondent	20	3	0	1	2	1	3	3	3
Respondent	21	5	0	1	2	1	2	2	3
Respondent	22	4	0	1	1	2	2	2	3
Respondent	23	4	0	1	1	1	2	2	2
Respondent	24	3	0	1	1	1	3	3	3
Respondent	25	4	0	1	1	1	2	2	3
Respondent	26	4	0	1	1	1	2	3	3
Respondent	27	4	0	1	1	1	2	3	3
Count		27	27	27	27	27	27	27	27
Response	1	0.00%	0.00%	88.89%	51.85%	88.89%	0.00%	0.00%	0.00%
Response	2	0.00%	0.00%	11.11%	48.15%	11.11%	66.67%	59.26%	22.22%
Response	3	29.63%	0.00%	0.00%	0.00%	0.00%	33.33%	40.74%	74.07%
Response	4	66.67%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	3.70%
Response	5	3.70%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	6	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	7	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	8	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Mean		3.74	0.00	1.11	1.48	1.11	2.33	2.41	2.81
Validate		100.00%	0.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%
t-value		9.3E-13		9.7E-29	9.7E-29	2.7E-25	7E-219	2.7E-25	1.8E-24
df=26									
p = 0.05		1.71		1.71	1.71	1.71	1.71	1.71	1.71
p = 0.10		1.32		1.32	1.32	1.32	1.32	1.32	1.32
Sig. 0.05		YES		YES	YES	YES	YES	YES	YES
Sig. 0.10		YES		YES	YES	YES	YES	YES	YES

		Q	Q	Q	Q	Q	Q	Q	Q
		21.7	21.8	22	23	24.1	24.2	24.3	24.4
Respondent	1	2	0	3	3	3	3	2	2
Respondent	2	4	0	4	3	5	4	4	2
Respondent	3	3	0	3	3	3	3	2	1
Respondent	4	2	0	2	3	2	3	1	1
Respondent	5	2	0	3	3	3	3	2	2
Respondent	6	3	0	3	3	3	2	2	1
Respondent	7	2	0	2	2	3	3	2	2
Respondent	8	2	0	3	3	2	2	2	2
Respondent	9	3	0	3	3	3	3	1	1
Respondent	10	2	0	3	3	3	3	2	1
Respondent	11	2	0	3	3	3	3	2	2
Respondent	12	3	0	3	3	3	2	2	2
Respondent	13	3	0	3	3	3	3	2	2
Respondent	14	2	0	2	2	3	3	1	1
Respondent	15	3	0	4	3	2	2	1	2
Respondent	16	2	0	3	3	3	3	2	2
Respondent	17	2	0	4	3	2	2	1	1
Respondent	18	3	0	2	2	3	2	2	2
Respondent	19	2	0	3	3	3	3	2	2
Respondent	20	3	0	3	3	3	2	2	1
Respondent	21	2	0	3	2	3	3	2	2
Respondent	22	3	0	3	3	3	3	1	1
Respondent	23	2	0	2	2	2	2	2	1
Respondent	24	2	0	3	3	3	3	2	2
Respondent	25	2	0	3	2	3	2	2	1
Respondent	26	2	0	3	3	3	3	2	2
Respondent	27	2	0	3	3	3	3	2	2
Count		27	27	27	27	27	27	27	27
Response	1	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	22.22%	40.74%
Response	2	62.96%	0.00%	18.52%	22.22%	18.52%	33.33%	74.07%	59.26%
Response	3	33.33%	0.00%	70.37%	77.78%	77.78%	62.96%	0.00%	0.00%
Response	4	3.70%	0.00%	11.11%	0.00%	0.00%	3.70%	3.70%	0.00%
Response	5	0.00%	0.00%	0.00%	0.00%	3.70%	0.00%	0.00%	0.00%
Response	6	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	7	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	8	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Mean		2.41	0.00	2.93	2.78	2.89	2.70	1.85	1.59
Validate		100.00%	0.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%
t-value		3.5E-19		2.1E-17	6E-21	1.2E-06	1.6E-07	9.8E-08	6.5E-12
df=26									
p = 0.05		1.71		1.71	1.71	1.71	1.71	1.71	1.71
p = 0.10		1.32		1.32	1.32	1.32	1.32	1.32	1.32
Sig. 0.05		YES		YES	YES	YES	YES	YES	YES
Sig. 0.10		YES		YES	YES	YES	YES	YES	YES

		Q	Q	Q	Q	Q	Q	Q	Q
		24.5	**24.6**	**24.7**	**25**	**26**	**27**	**28**	**29**
Respondent	1	2	3	0	3	5	5	4	2
Respondent	2	2	4	0	3	5	4	5	1
Respondent	3	1	3	0	3	5	5	4	2
Respondent	4	1	3	0	2	3	3	3	2
Respondent	5	1	3	0	2	4	4	4	2
Respondent	6	1	4	0	3	5	3	3	1
Respondent	7	2	3	0	3	5	4	3	2
Respondent	8	1	3	0	2	4	3	4	1
Respondent	9	1	3	0	3	4	3	4	2
Respondent	10	1	3	0	3	4	3	3	2
Respondent	11	1	4	0	3	5	5	4	3
Respondent	12	2	3	0	2	4	5	4	2
Respondent	13	2	4	0	2	3	4	4	3
Respondent	14	1	3	0	2	3	3	4	2
Respondent	15	2	3	0	2	4	5	3	2
Respondent	16	1	3	0	3	4	4	4	2
Respondent	17	1	3	0	2	4	4	3	2
Respondent	18	2	3	0	3	5	4	3	2
Respondent	19	2	3	0	3	5	5	4	2
Respondent	20	1	4	0	3	4	3	4	2
Respondent	21	2	4	0	2	4	4	4	2
Respondent	22	1	3	0	3	4	4	4	2
Respondent	23	1	3	0	2	4	4	3	3
Respondent	24	2	3	0	2	4	3	4	2
Respondent	25	1	3	0	3	5	5	4	2
Respondent	26	1	3	0	3	4	5	4	2
Respondent	27	2	3	0	3	5	4	4	2
Count		27	27	27	27	27	27	27	27
Response	1	59.26%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	11.11%
Response	2	40.74%	0.00%	0.00%	40.74%	0.00%	0.00%	0.00%	77.78%
Response	3	0.00%	77.78%	0.00%	59.26%	11.11%	29.63%	29.63%	11.11%
Response	4	0.00%	22.22%	0.00%	0.00%	51.85%	40.74%	66.67%	0.00%
Response	5	0.00%	0.00%	0.00%	0.00%	37.04%	29.63%	3.70%	0.00%
Response	6	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	7	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	8	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Mean		1.41	3.22	0.00	2.59	4.26	4.00	3.74	2.00
Validate		100.00%	100.00%	0.00%	100.00%	100.00%	100.00%	100.00%	100.00%
t-value		3.1E-13	4.4E-09		8.4E-13	1.7E-06	0.00283	9.3E-13	9.9E-23
df=26									
p = 0.05		1.71	1.71		1.71	1.71	1.71	1.71	1.71
p = 0.10		1.32	1.32		1.32	1.32	1.32	1.32	1.32
Sig. 0.05		**YES**	**YES**		**YES**	**YES**	NO	**YES**	**YES**
Sig. 0.10		**YES**	**YES**		**YES**	**YES**	NO	**YES**	**YES**

		Q	Q	Q	Q	Q	Q	Q	Q
		30.1	30.2	30.3	30.4	30.5	30.6	30.7	30.8
Respondent	1	4	4	4	3	3	3	4	0
Respondent	2	5	5	3	4	2	1	2	0
Respondent	3	4	4	4	3	3	2	3	0
Respondent	4	5	5	5	2	3	2	2	0
Respondent	5	4	4	4	3	3	3	3	0
Respondent	6	4	4	4	3	3	3	3	0
Respondent	7	5	4	4	4	3	3	3	0
Respondent	8	4	4	3	3	2	2	3	0
Respondent	9	4	4	3	3	3	3	4	0
Respondent	10	4	4	4	4	3	2	2	0
Respondent	11	4	4	3	2	2	2	3	0
Respondent	12	4	4	3	2	2	2	2	0
Respondent	13	4	4	3	3	3	2	3	0
Respondent	14	5	4	4	3	3	3	3	0
Respondent	15	4	4	3	2	2	2	3	0
Respondent	16	4	4	4	3	3	3	3	0
Respondent	17	4	4	4	2	2	3	4	0
Respondent	18	4	4	4	2	2	2	3	0
Respondent	19	4	4	4	3	2	2	3	0
Respondent	20	4	4	4	3	3	3	3	0
Respondent	21	4	5	4	3	3	2	2	0
Respondent	22	4	4	3	3	3	2	4	0
Respondent	23	4	4	4	3	2	2	3	0
Respondent	24	4	4	3	3	3	2	2	0
Respondent	25	4	4	4	3	2	3	3	0
Respondent	26	4	4	4	3	3	2	3	0
Respondent	27	4	4	4	3	2	2	3	0
Count		27	27	27	27	27	27	27	27
Response	1	0.00%	0.00%	0.00%	0.00%	0.00%	3.70%	0.00%	0.00%
Response	2	0.00%	0.00%	0.00%	22.22%	40.74%	59.26%	22.22%	0.00%
Response	3	0.00%	0.00%	33.33%	66.67%	59.26%	37.04%	62.96%	0.00%
Response	4	85.19%	88.89%	62.96%	11.11%	0.00%	0.00%	14.81%	0.00%
Response	5	14.81%	11.11%	3.70%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	6	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	7	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	8	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Mean		4.15	4.11	3.70	2.89	2.59	2.33	2.93	0.00
Validate		100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	0.00%
t-value		1.4E-12	0.00218	0.00065	3.5E-13	5E-15	2.6E-09	3.6E-07	
df=26									
p = 0.05		1.71	1.71	1.71	1.71	1.71	1.71	1.71	
p = 0.10		1.32	1.32	1.32	1.32	1.32	1.32	1.32	
Sig. 0.05		**YES**	NO	NO	**YES**	**YES**	**YES**	**YES**	
Sig. 0.10		**YES**	NO	NO	**YES**	**YES**	**YES**	**YES**	

		Q	Q	Q	Q	Q	Q	Q	Q
		31	32	33	34	35	36	37	38
Respondent	1	3	2	4	4	3	3	4	2
Respondent	2	4	2	2	4	3	1	4	2
Respondent	3	3	2	2	3	3	3	4	2
Respondent	4	4	3	2	3	2	2	4	2
Respondent	5	3	2	2	3	2	3	3	1
Respondent	6	3	2	3	3	2	2	3	2
Respondent	7	3	2	2	3	3	3	3	1
Respondent	8	4	3	1	2	3	3	3	1
Respondent	9	3	2	1	2	3	3	4	1
Respondent	10	3	2	2	3	3	2	3	1
Respondent	11	3	2	1	3	2	3	3	2
Respondent	12	3	1	1	2	3	3	3	2
Respondent	13	3	3	1	3	2	2	4	1
Respondent	14	4	3	2	3	2	2	3	2
Respondent	15	3	2	2	3	3	3	3	2
Respondent	16	4	2	3	3	3	3	3	2
Respondent	17	4	3	1	2	3	3	3	2
Respondent	18	3	2	2	3	3	3	3	2
Respondent	19	4	2	2	3	3	2	3	2
Respondent	20	3	2	2	3	3	3	3	3
Respondent	21	3	2	2	3	3	3	4	2
Respondent	22	4	2	2	3	2	2	4	2
Respondent	23	3	1	2	3	3	3	4	2
Respondent	24	3	2	3	2	2	3	3	1
Respondent	25	3	2	2	3	2	3	4	2
Respondent	26	4	2	2	3	3	3	4	2
Respondent	27	3	2	2	3	2	2	3	1
Count		27	27	27	27	27	27	27	27
Response	1	0.00%	7.41%	22.22%	0.00%	0.00%	3.70%	0.00%	29.63%
Response	2	0.00%	74.07%	62.96%	18.52%	37.04%	29.63%	0.00%	66.67%
Response	3	66.67%	18.52%	11.11%	74.07%	62.96%	66.67%	59.26%	3.70%
Response	4	33.33%	0.00%	3.70%	7.41%	0.00%	0.00%	40.74%	0.00%
Response	5	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	6	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	7	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	8	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Mean		3.33	2.11	1.96	2.89	2.63	2.63	3.41	1.74
Validate		100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%
t-value		1.6E-09	1.8E-18	0.33902	8.6E-13	5E-20	1.7E-15	1.3E-15	2.3E-17
df=26									
p = 0.05		1.71	1.71	1.71	1.71	1.71	1.71	1.71	1.71
p = 0.10		1.32	1.32	1.32	1.32	1.32	1.32	1.32	1.32
Sig. 0.05		YES	YES	NO	YES	YES	YES	YES	YES
Sig. 0.10		YES	YES	NO	YES	YES	YES	YES	YES

		Q	Q	Q	Q	Q	Q	Q	Q
		39	40	41.1	41.2	41.3	41.4	41.5	41.6
Respondent	1	3	5	5	2	5	5	3	5
Respondent	2	3	4	5	2	5	5	2	4
Respondent	3	3	4	5	1	4	5	3	4
Respondent	4	3	3	5	2	5	5	3	4
Respondent	5	3	5	5	3	4	5	3	4
Respondent	6	3	4	5	3	5	5	3	4
Respondent	7	3	3	5	3	4	5	4	5
Respondent	8	3	3	5	2	5	5	3	4
Respondent	9	2	4	5	3	5	5	3	5
Respondent	10	3	5	5	3	4	5	3	5
Respondent	11	3	3	5	3	4	5	3	4
Respondent	12	2	4	5	2	4	5	3	5
Respondent	13	3	3	5	3	4	5	3	5
Respondent	14	3	3	5	2	4	5	3	5
Respondent	15	3	4	5	2	4	5	3	5
Respondent	16	3	3	5	2	4	5	3	5
Respondent	17	2	5	5	2	4	5	3	4
Respondent	18	3	4	5	3	4	5	3	4
Respondent	19	3	5	5	3	4	5	4	5
Respondent	20	3	3	5	2	4	5	4	5
Respondent	21	3	4	5	2	4	5	4	5
Respondent	22	3	4	5	3	4	5	4	4
Respondent	23	4	3	5	2	4	5	3	5
Respondent	24	3	4	5	3	4	5	4	5
Respondent	25	4	5	5	2	4	5	3	4
Respondent	26	3	4	5	3	4	5	3	5
Respondent	27	3	4	5	3	4	5	3	5
Count		27	27	27	27	27	27	27	27
Response	1	0.00%	0.00%	0.00%	3.70%	0.00%	0.00%	0.00%	0.00%
Response	2	11.11%	0.00%	0.00%	48.15%	0.00%	0.00%	3.70%	0.00%
Response	3	81.48%	33.33%	0.00%	48.15%	0.00%	0.00%	74.07%	0.00%
Response	4	7.41%	44.44%	0.00%	0.00%	77.78%	0.00%	22.22%	40.74%
Response	5	0.00%	22.22%	100.00%	0.00%	22.22%	100.00%	0.00%	59.26%
Response	6	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	7	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	8	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Mean		2.96	3.89	5.00	2.44	4.22	5.00	3.19	4.59
Validate		100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%
t-value		1.3E-12	8.1E-07						
df=26									
p = 0.05		1.71	1.71						
p = 0.10		1.32	1.32						
Sig. 0.05		YES	YES						
Sig. 0.10		YES	YES						

		Q	Q	Q	Q	Q	Q	Q	Q
		41.7	**41.8**	**41.9**	**42.1**	**42.2**	**42.3**	**42.4**	**42.5**
Respondent	1	4	5	0	5	5	5	4	0
Respondent	2	2	4	0	5	5	5	3	0
Respondent	3	4	4	0	5	5	5	4	0
Respondent	4	3	4	0	5	5	5	4	0
Respondent	5	3	4	0	4	4	4	5	0
Respondent	6	3	4	0	5	5	5	4	0
Respondent	7	3	4	0	5	5	5	5	0
Respondent	8	3	5	0	5	5	5	5	0
Respondent	9	3	5	0	4	4	4	4	0
Respondent	10	3	4	0	5	5	5	4	0
Respondent	11	4	5	0	4	4	4	3	0
Respondent	12	4	4	0	5	4	5	4	0
Respondent	13	4	3	0	5	5	5	4	0
Respondent	14	3	4	0	5	5	5	5	0
Respondent	15	3	4	0	4	4	4	4	0
Respondent	16	3	3	0	5	5	5	5	0
Respondent	17	4	4	0	4	4	4	4	0
Respondent	18	4	5	0	5	4	5	4	0
Respondent	19	3	4	0	4	4	5	4	0
Respondent	20	4	4	0	5	5	5	4	0
Respondent	21	3	4	0	5	5	5	4	0
Respondent	22	3	4	0	4	4	4	4	0
Respondent	23	3	4	0	4	4	4	4	0
Respondent	24	3	4	0	5	5	5	5	0
Respondent	25	3	5	0	4	4	5	4	0
Respondent	26	3	4	0	4	4	4	4	0
Respondent	27	3	4	0	4	4	4	4	0
Count		27	27	27	27	27	27	27	27
Response	1	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	2	3.70%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	3	66.67%	7.41%	0.00%	0.00%	0.00%	0.00%	7.41%	0.00%
Response	4	29.63%	70.37%	0.00%	40.74%	48.15%	33.33%	70.37%	0.00%
Response	5	0.00%	22.22%	0.00%	59.26%	51.85%	66.67%	22.22%	0.00%
Response	6	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	7	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	8	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Mean		3.26	4.15	0.00	4.59	4.52	4.67	4.15	0.00
Validate		100.00%	100.00%	0.00%	100.00%	100.00%	100.00%	100.00%	0.00%
t-value									
df=26									
p = 0.05									
p = 0.10									
Sig. 0.05									
Sig. 0.10									

		Q	Q	Q	Q	Q	Q	Q	Q
		43.1	43.2	43.3	43.4	43.5	43.6	43.7	43.8
Respondent	1	5	5	5	5	4	4	4	0
Respondent	2	5	5	5	4	5	3	5	0
Respondent	3	5	5	5	5	3	4	4	0
Respondent	4	5	5	5	5	3	4	5	0
Respondent	5	5	4	5	5	3	4	5	0
Respondent	6	4	4	4	4	3	4	4	0
Respondent	7	5	5	5	5	3	4	4	0
Respondent	8	4	4	4	4	3	4	4	0
Respondent	9	4	4	4	4	3	4	4	0
Respondent	10	5	5	4	4	3	4	4	0
Respondent	11	4	4	4	4	3	4	4	0
Respondent	12	5	5	5	5	3	4	4	0
Respondent	13	4	4	4	4	3	4	4	0
Respondent	14	4	4	4	4	4	4	4	0
Respondent	15	4	4	4	4	3	4	4	0
Respondent	16	4	4	4	5	3	4	4	0
Respondent	17	4	4	4	4	4	4	4	0
Respondent	18	5	5	5	5	3	4	4	0
Respondent	19	5	5	5	5	3	4	4	0
Respondent	20	4	4	4	4	3	4	4	0
Respondent	21	5	5	5	5	4	4	4	0
Respondent	22	4	4	4	4	4	4	4	0
Respondent	23	5	5	5	5	3	4	4	0
Respondent	24	4	4	4	4	3	4	4	0
Respondent	25	5	5	5	5	3	4	4	0
Respondent	26	4	4	4	4	3	4	4	0
Respondent	27	4	4	4	4	4	4	4	0
Count		27	27	27	27	27	27	27	27
Response	1	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	2	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	3	0.00%	0.00%	0.00%	0.00%	74.07%	3.70%	0.00%	0.00%
Response	4	51.85%	55.56%	55.56%	55.56%	22.22%	96.30%	88.89%	0.00%
Response	5	48.15%	44.44%	44.44%	44.44%	3.70%	0.00%	11.11%	0.00%
Response	6	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	7	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	8	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Mean		4.48	4.44	4.44	4.44	3.30	3.96	4.11	0.00
Validate		100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	0.00%
t-value									
df=26									
p = 0.05									
p = 0.10									
Sig. 0.05									
Sig. 0.10									

		Q	Q	Q	Q	Q	Q	Q	Q
		44.1	44.2	44.3	44.4	44.5	44.6	45.1	45.2
Respondent	1	5	5	5	4	4	0	4	4
Respondent	2	4	5	5	5	4	0	2	4
Respondent	3	5	5	5	4	4	0	5	5
Respondent	4	4	5	5	4	4	0	4	4
Respondent	5	5	5	5	4	4	0	4	4
Respondent	6	5	5	4	4	3	0	4	5
Respondent	7	4	5	5	4	4	0	4	5
Respondent	8	5	4	4	3	4	0	4	4
Respondent	9	4	4	5	4	3	0	4	4
Respondent	10	4	4	4	4	4	0	4	4
Respondent	11	5	4	5	3	3	0	4	5
Respondent	12	4	4	4	4	3	0	4	4
Respondent	13	4	5	4	3	3	0	4	5
Respondent	14	5	4	5	4	3	0	4	4
Respondent	15	4	4	4	3	4	0	4	5
Respondent	16	5	4	4	4	4	0	4	4
Respondent	17	4	4	5	4	3	0	4	4
Respondent	18	4	4	5	4	3	0	4	4
Respondent	19	4	5	4	4	3	0	4	4
Respondent	20	4	4	5	4	3	0	4	5
Respondent	21	4	5	4	4	3	0	4	4
Respondent	22	4	4	4	3	3	0	4	4
Respondent	23	4	5	5	3	3	0	4	4
Respondent	24	4	5	4	4	3	0	4	4
Respondent	25	4	4	5	3	3	0	4	4
Respondent	26	4	4	4	4	3	0	4	4
Respondent	27	4	4	4	4	3	0	4	4
Count		27	27	27	27	27	27	27	27
Response	1	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	2	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	3.70%	0.00%
Response	3	0.00%	0.00%	0.00%	25.93%	62.96%	0.00%	0.00%	0.00%
Response	4	70.37%	55.56%	48.15%	70.37%	37.04%	0.00%	92.59%	74.07%
Response	5	29.63%	44.44%	51.85%	3.70%	0.00%	0.00%	3.70%	25.93%
Response	6	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	7	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	8	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Mean		4.30	4.44	4.52	3.78	3.37	0.00	3.96	4.26
Validate		100.00%	100.00%	100.00%	100.00%	100.00%	0.00%	100.00%	100.00%
t-value									
df=26									
p = 0.05									
p = 0.10									
Sig. 0.05									
Sig. 0.10									

		Q	Q	Q	Q	Q	Q	Q	Q
		45.3	45.4	45.5	45.6	45.7	45.8	46.1	46.2
Respondent	1	4	4	4	4	4	0	4	4
Respondent	2	4	3	5	5	4	0	2	4
Respondent	3	5	5	5	5	5	0	4	5
Respondent	4	4	4	4	4	4	0	4	4
Respondent	5	4	4	4	4	4	0	5	5
Respondent	6	4	4	4	4	4	0	4	5
Respondent	7	4	4	4	4	4	0	4	4
Respondent	8	4	5	4	4	4	0	4	4
Respondent	9	4	4	4	4	4	0	4	5
Respondent	10	4	4	4	4	4	0	5	5
Respondent	11	5	4	5	4	5	0	5	5
Respondent	12	4	4	4	4	4	0	4	4
Respondent	13	5	4	5	4	4	0	4	4
Respondent	14	4	4	4	4	4	0	5	5
Respondent	15	5	4	5	4	5	0	4	5
Respondent	16	4	4	4	4	4	0	4	5
Respondent	17	4	4	4	4	4	0	4	5
Respondent	18	4	4	4	4	4	0	4	4
Respondent	19	4	4	4	4	4	0	5	5
Respondent	20	5	5	5	4	5	0	5	5
Respondent	21	4	4	4	4	4	0	4	4
Respondent	22	4	4	4	4	4	0	4	4
Respondent	23	4	4	4	4	4	0	4	5
Respondent	24	4	4	4	4	4	0	4	5
Respondent	25	4	4	4	4	4	0	5	5
Respondent	26	4	4	4	4	4	0	4	4
Respondent	27	4	4	4	4	4	0	4	5
Count		27	27	27	27	27	27	27	27
Response	1	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	2	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	3.70%	0.00%
Response	3	0.00%	3.70%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	4	81.48%	85.19%	77.78%	92.59%	85.19%	0.00%	70.37%	40.74%
Response	5	18.52%	11.11%	22.22%	7.41%	14.81%	0.00%	25.93%	59.26%
Response	6	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	7	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	8	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Mean		4.19	4.07	4.22	4.07	4.15	0.00	4.19	4.59
Validate		100.00%	100.00%	100.00%	100.00%	100.00%	0.00%	100.00%	100.00%
t-value									
df=26									
p = 0.05									
p = 0.10									
Sig. 0.05									
Sig. 0.10									

		Q	Q	Q	Q	Q	Q	Q	Q
		46.3	**46.4**	**46.5**	**46.6**	**47**	**48**	**49.1**	**49.2**
Respondent	1	5	4	5	0	5	5	5	5
Respondent	2	5	4	5	0	5	5	5	5
Respondent	3	5	4	5	0	5	5	5	5
Respondent	4	5	4	5	0	5	5	5	5
Respondent	5	5	4	4	0	5	5	5	5
Respondent	6	4	4	4	0	5	5	5	5
Respondent	7	4	5	4	0	5	5	5	5
Respondent	8	5	5	5	0	5	5	5	5
Respondent	9	5	4	5	0	5	5	5	5
Respondent	10	4	4	4	0	5	5	5	5
Respondent	11	4	5	5	0	5	5	5	5
Respondent	12	5	5	4	0	5	5	5	5
Respondent	13	5	4	4	0	5	5	5	5
Respondent	14	4	4	4	0	5	5	5	5
Respondent	15	4	4	4	0	5	5	5	5
Respondent	16	5	4	4	0	5	5	5	5
Respondent	17	5	4	5	0	5	5	5	5
Respondent	18	5	4	4	0	5	5	5	5
Respondent	19	5	4	5	0	5	5	5	5
Respondent	20	4	4	5	0	5	5	5	5
Respondent	21	4	4	4	0	5	5	5	5
Respondent	22	5	4	5	0	5	5	5	5
Respondent	23	5	4	4	0	5	5	5	5
Respondent	24	4	4	4	0	5	5	5	5
Respondent	25	5	4	4	0	5	5	5	5
Respondent	26	4	4	5	0	5	5	5	5
Respondent	27	4	4	4	0	5	5	5	5
Count		27	27	27	27	27	27	27	27
Response	1	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	2	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	3	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	4	40.74%	85.19%	55.56%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	5	59.26%	14.81%	44.44%	0.00%	100.00%	100.00%	100.00%	100.00%
Response	6	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	7	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	8	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Mean		4.59	4.15	4.44	0.00	5.00	5.00	5.00	5.00
Validate		100.00%	100.00%	100.00%	0.00%	100.00%	100.00%	100.00%	100.00%
t-value									
df=26									
p = 0.05									
p = 0.10									
Sig. 0.05									
Sig. 0.10									

		Q	Q	Q	Q	Q	Q	Q	Q
		49.3	**49.4**	**50**	**51**	**52**	**53**	**54**	**55**
Respondent	1	5	0	5	5	5	5	5	5
Respondent	2	5	0	5	5	5	5	5	5
Respondent	3	5	0	5	5	5	5	5	5
Respondent	4	5	0	5	5	5	5	5	5
Respondent	5	5	0	5	5	5	5	5	5
Respondent	6	5	0	5	5	5	5	5	5
Respondent	7	5	0	5	5	5	5	5	5
Respondent	8	5	0	5	5	5	5	5	5
Respondent	9	5	0	5	5	5	5	5	5
Respondent	10	5	0	5	5	5	5	5	5
Respondent	11	5	0	5	5	5	5	5	5
Respondent	12	5	0	5	5	5	5	5	5
Respondent	13	5	0	5	5	5	5	5	5
Respondent	14	5	0	5	5	5	5	5	5
Respondent	15	5	0	5	5	5	5	5	5
Respondent	16	5	0	5	5	5	5	5	5
Respondent	17	5	0	5	5	5	5	5	5
Respondent	18	5	0	5	5	5	5	5	5
Respondent	19	5	0	5	5	5	5	5	5
Respondent	20	5	0	5	5	5	5	5	5
Respondent	21	5	0	5	5	5	5	5	5
Respondent	22	5	0	5	5	5	5	5	5
Respondent	23	5	0	5	5	5	5	5	5
Respondent	24	5	0	5	5	5	5	5	5
Respondent	25	5	0	5	5	5	5	5	5
Respondent	26	5	0	5	5	5	5	5	5
Respondent	27	5	0	5	5	5	5	5	5
Count		27	27	27	27	27	27	27	27
Response	1	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	2	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	3	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	4	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	5	100.00%	0.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%
Response	6	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	7	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	8	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Mean		5.00	0.00	5.00	5.00	5.00	5.00	5.00	5.00
Validate		100.00%	0.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%
t-value									
df=26									
p = 0.05									
p = 0.10									
Sig. 0.05									
Sig. 0.10									

		Q	Q	Q	Q	Q	Q	Q	Q
		56	57	58	59	60.1	60.2	60.3	60.4
Respondent	1	5	5	5	4	5	5	5	0
Respondent	2	5	5	5	4	5	5	5	0
Respondent	3	5	5	5	4	5	5	5	0
Respondent	4	5	5	5	4	5	5	5	0
Respondent	5	5	5	5	5	5	5	5	0
Respondent	6	5	5	5	4	5	5	5	0
Respondent	7	5	5	5	4	5	5	5	0
Respondent	8	5	5	5	5	5	5	5	0
Respondent	9	5	5	5	4	5	5	5	0
Respondent	10	5	5	5	4	5	5	5	0
Respondent	11	5	5	5	5	5	5	5	0
Respondent	12	5	5	5	5	5	5	5	0
Respondent	13	5	5	5	5	5	5	5	0
Respondent	14	5	5	5	4	5	5	5	0
Respondent	15	5	5	5	5	5	5	5	0
Respondent	16	5	5	5	5	5	5	5	0
Respondent	17	5	5	5	4	5	5	5	0
Respondent	18	5	5	5	4	5	5	5	0
Respondent	19	5	5	5	5	5	5	5	0
Respondent	20	5	5	5	5	5	5	5	0
Respondent	21	5	5	5	5	5	5	5	0
Respondent	22	5	5	5	4	5	5	5	0
Respondent	23	5	5	5	5	5	5	5	0
Respondent	24	5	5	5	4	5	5	5	0
Respondent	25	5	5	5	4	5	5	5	0
Respondent	26	5	5	5	4	5	5	5	0
Respondent	27	5	5	5	4	5	5	5	0
Count		27	27	27	27	27	27	27	27
Response	1	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	2	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	3	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	4	0.00%	0.00%	0.00%	59.26%	0.00%	0.00%	0.00%	0.00%
Response	5	100.00%	100.00%	100.00%	40.74%	100.00%	100.00%	100.00%	0.00%
Response	6	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	7	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	8	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Mean		5.00	5.00	5.00	4.41	5.00	5.00	5.00	0.00
Validate		100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	0.00%
t-value									
df=26									
p = 0.05									
p = 0.10									
Sig. 0.05									
Sig. 0.10									

		Q	Q	Q	Q	Q	Q	Q	Q
		61.1	61.2	61.3	61.4	61.5	61.6	61.7	61.8
Respondent	1	4	4	4	4	4	4	3	0
Respondent	2	3	4	4	4	4	5	4	0
Respondent	3	3	4	3	4	4	5	5	0
Respondent	4	4	4	4	5	5	5	4	0
Respondent	5	3	4	4	4	4	4	4	0
Respondent	6	3	3	3	4	5	5	5	0
Respondent	7	3	3	3	4	5	4	4	0
Respondent	8	3	4	3	4	4	4	4	0
Respondent	9	3	4	3	5	5	5	5	0
Respondent	10	3	3	3	4	4	5	4	0
Respondent	11	3	4	3	5	5	5	4	0
Respondent	12	3	3	3	5	5	5	5	0
Respondent	13	3	3	3	5	5	5	5	0
Respondent	14	4	4	3	4	4	4	4	0
Respondent	15	3	3	3	5	5	5	5	0
Respondent	16	3	4	3	4	4	5	4	0
Respondent	17	4	4	3	4	4	5	4	0
Respondent	18	3	3	3	4	4	5	5	0
Respondent	19	3	4	3	5	5	4	4	0
Respondent	20	3	4	3	5	5	5	5	0
Respondent	21	3	4	3	4	4	5	4	0
Respondent	22	3	3	4	4	4	5	5	0
Respondent	23	3	3	3	4	4	4	4	0
Respondent	24	3	3	3	5	5	5	4	0
Respondent	25	3	3	3	4	4	5	4	0
Respondent	26	3	3	3	4	5	5	4	0
Respondent	27	3	3	3	4	5	5	4	0
Count		27	27	27	27	27	27	27	27
Response	1	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	2	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	3	85.19%	48.15%	81.48%	0.00%	0.00%	0.00%	3.70%	0.00%
Response	4	14.81%	51.85%	18.52%	66.67%	51.85%	25.93%	62.96%	0.00%
Response	5	0.00%	0.00%	0.00%	33.33%	48.15%	74.07%	33.33%	0.00%
Response	6	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	7	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	8	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Mean		3.15	3.52	3.19	4.33	4.48	4.74	4.30	0.00
Validate		100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	0.00%
t-value									
df=26									
p = 0.05									
p = 0.10									
Sig. 0.05									
Sig. 0.10									

		Q	Q	Q	Q	Q	Q	Q	Q
		62	63	64.1	64.2	64.3	64.4	64.5	64.6
Respondent	1	5	5	4	4	3	3	3	4
Respondent	2	5	5	5	4	5	4	4	4
Respondent	3	5	5	4	4	3	2	3	4
Respondent	4	5	5	3	4	2	2	3	4
Respondent	5	5	5	3	4	3	3	3	4
Respondent	6	5	5	4	3	2	3	4	5
Respondent	7	5	5	4	3	3	3	3	4
Respondent	8	5	5	4	3	3	3	4	5
Respondent	9	5	5	4	4	2	2	3	5
Respondent	10	5	5	4	4	3	3	3	4
Respondent	11	5	5	3	3	2	3	3	4
Respondent	12	5	5	3	3	3	3	4	3
Respondent	13	5	5	3	3	2	3	3	5
Respondent	14	5	5	3	3	3	2	4	4
Respondent	15	5	5	3	3	3	3	3	4
Respondent	16	5	5	4	4	2	3	3	5
Respondent	17	5	5	3	3	2	2	3	4
Respondent	18	5	5	4	4	3	3	3	4
Respondent	19	5	5	3	3	3	3	3	4
Respondent	20	5	5	4	4	2	3	3	4
Respondent	21	5	5	3	3	3	3	3	4
Respondent	22	5	5	4	4	2	2	3	5
Respondent	23	5	5	4	4	3	3	4	4
Respondent	24	5	5	4	4	2	2	3	5
Respondent	25	5	5	3	3	3	2	4	5
Respondent	26	5	5	4	4	2	3	4	4
Respondent	27	5	5	3	3	2	2	3	4
Count		27	27	27	27	27	27	27	27
Response	1	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	2	0.00%	0.00%	0.00%	0.00%	44.44%	33.33%	0.00%	0.00%
Response	3	0.00%	0.00%	44.44%	48.15%	51.85%	62.96%	70.37%	3.70%
Response	4	0.00%	0.00%	51.85%	51.85%	0.00%	3.70%	29.63%	66.67%
Response	5	100.00%	100.00%	3.70%	0.00%	3.70%	0.00%	0.00%	29.63%
Response	6	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	7	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	8	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Mean		5.00	5.00	3.59	3.52	2.63	2.70	3.30	4.26
Validate		100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%
t-value									
df=26									
p = 0.05									
p = 0.10									
Sig. 0.05									
Sig. 0.10									

		Q	Q	Q	Q	Q	Q	Q	Q
		64.7	65	66	67	68	69	70.1	70.2
Respondent	1	0	4	5	4	5	5	5	4
Respondent	2	0	3	5	4	5	3	5	4
Respondent	3	0	5	5	5	5	5	5	5
Respondent	4	0	5	5	4	5	5	5	5
Respondent	5	0	4	5	5	5	5	5	5
Respondent	6	0	5	5	4	5	5	5	4
Respondent	7	0	5	5	4	5	5	5	4
Respondent	8	0	4	5	5	5	5	5	5
Respondent	9	0	5	5	5	5	5	5	4
Respondent	10	0	4	5	4	5	5	5	4
Respondent	11	0	4	5	5	5	5	5	5
Respondent	12	0	5	5	5	5	5	5	4
Respondent	13	0	5	5	5	5	5	5	5
Respondent	14	0	4	5	4	5	5	5	4
Respondent	15	0	5	5	5	5	5	5	4
Respondent	16	0	4	5	4	5	5	5	5
Respondent	17	0	4	5	5	5	5	5	5
Respondent	18	0	4	5	5	5	5	5	4
Respondent	19	0	4	5	4	5	5	5	4
Respondent	20	0	5	5	5	5	5	5	4
Respondent	21	0	4	5	4	5	5	5	5
Respondent	22	0	5	5	4	5	5	5	5
Respondent	23	0	4	5	4	5	5	5	4
Respondent	24	0	5	5	5	5	5	5	5
Respondent	25	0	5	5	5	5	5	5	4
Respondent	26	0	4	5	4	5	5	5	4
Respondent	27	0	5	5	5	5	5	5	5
Count		27	27	27	27	27	27	27	27
Response	1	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	2	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	3	0.00%	3.70%	0.00%	0.00%	0.00%	3.70%	0.00%	0.00%
Response	4	0.00%	48.15%	0.00%	48.15%	0.00%	0.00%	0.00%	55.56%
Response	5	0.00%	48.15%	100.00%	51.85%	100.00%	96.30%	100.00%	44.44%
Response	6	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	7	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	8	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Mean		0.00	4.44	5.00	4.52	5.00	4.93	5.00	4.44
Validate		0.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%
t-value									
df=26									
p = 0.05									
p = 0.10									
Sig. 0.05									
Sig. 0.10									

		Q	Q	Q	Q	Q	Q	Q	Q
		70.3	70.4	70.5	70.6	70.7	70.8	71	72
Respondent	1	4	4	5	4	4	0	4	4
Respondent	2	4	5	4	3	4	0	5	4
Respondent	3	4	4	4	3	4	0	4	4
Respondent	4	5	4	5	3	3	0	5	4
Respondent	5	4	5	4	3	4	0	4	4
Respondent	6	4	4	4	3	4	0	5	5
Respondent	7	4	4	4	4	4	0	4	4
Respondent	8	4	4	4	3	4	0	5	5
Respondent	9	4	5	5	4	4	0	4	4
Respondent	10	4	5	4	3	4	0	4	4
Respondent	11	4	4	5	3	3	0	5	5
Respondent	12	4	4	4	3	3	0	4	4
Respondent	13	4	4	4	4	4	0	5	5
Respondent	14	4	5	4	4	3	0	4	4
Respondent	15	4	4	4	3	4	0	4	5
Respondent	16	4	4	5	3	3	0	5	4
Respondent	17	4	4	4	3	4	0	4	5
Respondent	18	4	4	4	3	4	0	4	4
Respondent	19	4	5	4	3	3	0	4	4
Respondent	20	4	4	4	4	4	0	4	4
Respondent	21	4	5	5	4	3	0	4	4
Respondent	22	4	5	4	3	4	0	4	4
Respondent	23	4	4	4	3	4	0	4	4
Respondent	24	4	4	5	4	3	0	4	4
Respondent	25	4	4	4	3	4	0	4	4
Respondent	26	4	4	4	3	4	0	4	4
Respondent	27	4	5	4	3	3	0	4	4
Count		27	27	27	27	27	27	27	27
Response	1	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	2	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	3	0.00%	0.00%	0.00%	70.37%	33.33%	0.00%	0.00%	0.00%
Response	4	96.30%	66.67%	74.07%	29.63%	66.67%	0.00%	74.07%	77.78%
Response	5	3.70%	33.33%	25.93%	0.00%	0.00%	0.00%	25.93%	22.22%
Response	6	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	7	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	8	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Mean		4.04	4.33	4.26	3.30	3.67	0.00	4.26	4.22
Validate		100.00%	100.00%	100.00%	100.00%	100.00%	0.00%	100.00%	100.00%
t-value									
df=26									
p = 0.05									
p = 0.10									
Sig. 0.05									
Sig. 0.10									

		Q	Q	Q	Q	Q	Q	Q	Q
		73	74	75	76	77	78	79	80
Respondent	1	4	4	5	4	5	4	4	5
Respondent	2	3	5	5	4	5	4	5	5
Respondent	3	1	5	5	5	5	4	5	5
Respondent	4	2	4	5	4	5	4	5	4
Respondent	5	2	4	5	5	5	5	5	5
Respondent	6	4	5	5	4	5	4	4	5
Respondent	7	2	4	5	5	5	3	4	4
Respondent	8	1	4	5	5	5	4	5	5
Respondent	9	1	3	5	4	5	4	4	5
Respondent	10	2	4	5	4	5	3	4	5
Respondent	11	1	4	5	4	5	4	5	5
Respondent	12	3	4	5	4	5	4	4	4
Respondent	13	3	5	5	4	5	4	5	5
Respondent	14	2	4	5	4	5	5	4	5
Respondent	15	3	4	5	5	5	4	5	5
Respondent	16	1	4	5	5	5	3	5	5
Respondent	17	1	4	5	5	5	4	4	5
Respondent	18	2	4	5	4	5	4	5	5
Respondent	19	1	4	5	4	5	4	4	5
Respondent	20	2	5	5	4	5	5	5	5
Respondent	21	3	4	5	4	5	4	4	5
Respondent	22	1	5	5	4	5	5	5	4
Respondent	23	2	4	5	5	5	4	4	5
Respondent	24	2	4	5	4	5	4	4	5
Respondent	25	1	5	5	4	5	4	4	5
Respondent	26	3	4	5	5	5	5	5	5
Respondent	27	2	4	5	4	5	4	4	4
Count		27	27	27	27	27	27	27	27
Response	1	33.33%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	2	37.04%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	3	22.22%	3.70%	0.00%	0.00%	0.00%	11.11%	0.00%	0.00%
Response	4	7.41%	70.37%	0.00%	66.67%	0.00%	70.37%	51.85%	18.52%
Response	5	0.00%	25.93%	100.00%	33.33%	100.00%	18.52%	48.15%	81.48%
Response	6	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	7	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Response	8	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Mean		2.04	4.22	5.00	4.33	5.00	4.07	4.48	4.81
Validate		100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%
t-value									
df=26									
p = 0.05									
p = 0.10									
Sig. 0.05									
Sig. 0.10									