OPERATIONAL RISK MODEL FOR MSES: IMPACT ON ORGANISATIONAL INFORMATION COMMUNICATION TECHNOLOGY

By

Anass Bayaga

Dissertation

Submitted in fulfillment of the requirements for the degree

Masters of Commerce

in

Information Systems

in the

Faculty of Management and Commerce

of the

UNIVERSITY OF FORT HARE

Promoter: Prof. S. Flowerday

November 2011

DECLARATION

I hereby declare that this thesis is my own unaided work and that any assistance obtained has been fully acknowledged in the text. No part of this thesis has been previously submitted to any other University.

…………………………..

Anass Bayaga

November 2011

ABSTRACT

The aim of the study was to investigate the impact of Information Communication Technology Operational Risk Management (ICT ORM) on the performance of a Medium Small Enterprise (MSE). The study was based upon a survey design to collect the primary data from 107 respondents using simple random sampling. The research instrument was administered online. A one stage normative model, associative in nature, was developed based upon reviewing previous research and in line with the research findings. The model elicited five factors based upon the multiple regression analysis of the data: principal causes of ORM failure related to ICT; change management requirements and ICT risk; characteristic(s) of information; challenges posed by ORM solutions and evaluation models affecting ICT adoption within MSEs. Based on the methodologies used in this study including factor analysis and multivariate regression analysis, it is recommended that this model be applied to monitor these changes more closely and to measure the changing strategies and the associated factors such as insufficient or improper user participation in systems development process, identified as potential barriers to the effective adoption and implementation of ICT within an MSE.

Key words: Operational Risk Management; Risks Measures; Information Communication Technology; Medium Small Enterprise

ACKNOWLEDGEMENTS

Firstly, I would like to praise ALLAH for the gift of ability, for His love and all He has done for me. Secondly, I would like to thank my family for all their love.

Prof. S. Flowerday, my supervisor, thank you for all the work, encouragement and patience. Thanks to my dear Liile, Afrika and Reita. Appreciations to my parents and all family members for their continuous prayers.

DEDICATION

To

JAWAD BAYAGA & AFRIKA BAYAGA

TABLE OF CONTENTS

CHAPTER 1: BACKGROUND OF THE STUDY

CHAPTER 2: REVIEW OF LITERATURE: MEDIUM AND SMALL ENTERPRISES (MSEs) AND INFORMATION TECHNOLOGY (IT) OPERATIONAL RISK MANAGEMENT (ORM)

CHAPTER 3: RESEARCH PARADIGM AND METHODOLOGY

CHAPTER 4: PRESENTATION OF RESEARCH FINDINGS

CHAPTER 5: DISCUSSION OF RESEARCH FINDINGS

CHAPTER 6: SUMMARY CONCLUSIONS AND RECOMMENDATIONS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

BACKGROUND OF THE STUDY

1.1 INTRODUCTION

Chapter 1 of this study begins with Medium Small Enterprises (MSEs) and Information Communication Technology Operational Risk Management (ICT ORM) in South Africa. This is followed by MSE and ICT performance as well as motivation for the research statement and development of the hypotheses**.** The other sections include research objectives and delimitation of the study. Attention is also given to methodology and ethical considerations, as well as the outline of the study.

1.2 MSES AND ICT OPERATIONAL RISK MANAGEMENT (ORM) IN SOUTH AFRICA

A large portion of past empirical studies have focused on ORM use in the context of large organisations, and little effort has been made to understand how ORM is used by small organisations that lack information technology (IT) sophistication. A collection of such studies suggests there are generally three sources of risk (Anderson and Choobineh, 2008; Calder, 2006; Lee and Jang, n.d).

One study suggests that “medium and small enterprises recognise the need for information security” (Lee and Jang, n.d: 84). Further research points out that sources of risk include “market risk”, risk associated with fluctuations in value of traded assets. It adds that, “credit risk” is associated with the uncertainty that debtors will honour their financial obligations while, “operational risk” is associated with human error, IT failure, dishonesty and natural disaster (McNeil, Frey and Embrechts, 2005: 3).

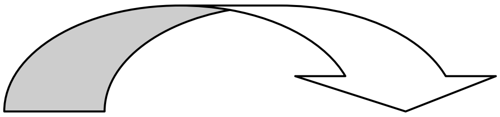
In fact, it has been suggested that "...because of the lack of resources and capabilities for building an Information Security Management System (ISMS), which include security policy, incident response and disaster recovery, businesses are vulnerable" (Lee and Jang, n.d: 84). Other authors also argue that all of these sources need some form of modelling (Balbas, 2007; McNeil *et al*, 2005).

A group of authors suggest that to model operational risk, risk analysts use language of probability theory (Balbas, 2007). The authors suggest that risks are represented by random variables mapping unforeseen future states of the world into values representing profits and losses (McNeil *et al*, 2005: 4).

Notwithstanding the listed sources of risk, the authors cautioned that "this is a non-exhaustive list" (McNeil *et al*, 2005: 3). However, in mid 2000, a study by the Basel Committee on Banking Supervision (2004: 18) suggested that:

> …quantification of operational risk is, for most institutions, at an early stage although progress is envisaged at many financial institutions. Many financial institutions did, however, provide some indication of the relative significance of operational risk within the institution. The data (based on a range of allocation methods) suggests that economic capital allocation for operational risk ranges between 15-25% for the majority of financial institutions.

In essence this trend has not changed in recent years, suggesting that traditionally, IT sophistication of small organisations is relatively low compared to that of large organisations. Several reasons have been attributed to this, as depicted in Figure 1.1.



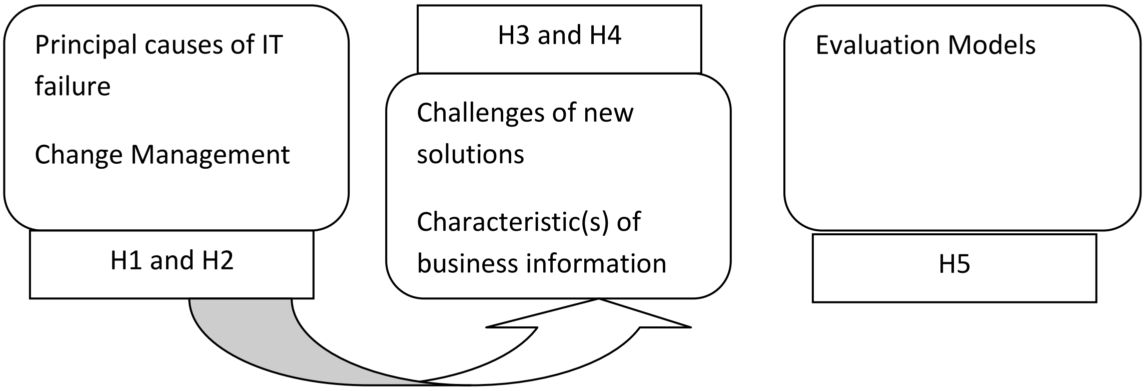

Principal causes of IT failure
Change Management
H1 and H2
H3 and H4
Challenges of new solutions
Characteristic(s) of business information
Evaluation Models
H5

Figure 1.1: Necessary and Sufficient Condition for Propositions

The first reason is principal causes of IT failure which has established that the setup and running costs of implementing IT with direct connection to financial partners can be high, especially for small organisations (King III Report, 2009; Ericsson, 2007). The transactions in small organisations are typically not voluminous and therefore do not involve extensive change management or evaluation models. Thus, the use of IT in small organisations is less than anticipated. As such, it is therefore necessary to examine the extent of IT ORM use and factors affecting ORM use. Findings of ORM studies in large organisations are likely to differ from those of small organisations by their very nature.

Secondly, with reference to the different dimensions, a dominant proportion of past IT empirical literature has concentrated on ORM adoption in large organisations in relation to characteristic(s) of business information. The work of the IT Governance Institute (ITGI) (2007), the Basel Committee on Banking Supervision (2004) and Committee of Sponsoring Organizations (COSO) (2004) fall in this group. The study done by Liebenberg and Hoyt (2003) is the only reported work focusing exclusively on small organisations.

Thirdly, a close look at these studies revealed that regardless of organisational context, survey studies and survey design methods were employed to identify the case institution and to explain how ORM was used within MSEs. The idea here is not to discount the method, but to investigate from a single standpoint, that is, a case study, in order to unearth the internal dynamics of such cases.

Fourthly, a review of IT literature indicated that most of the empirical studies on ORM attempted to identify a set of factors to help researchers distinguish ORM adopters from non-adopters. These factors were drawn from diverse disciplines including IT diffusion and economics. The commonly reported factors were grouped into three broad categories:

- Business Characteristic(s) Information;
- Evaluation Models and
- Innovation.

However, no established pattern of results emerged from these studies due to contradictory findings. It was evident that initially most studies conducted on IT ORM were confined to large businesses and produced mixed results.

However, in the mid-2000s, researchers began to question how the results of these studies could support MSEs (Lam, 2006; Liebenberg and Hoyt, 2003). Results also indicated that:

> “Though MSEs are at an earlier adopter stage, the evidence from larger organisations taken into consideration with the rapid pace of technology development suggests that MSE managers must engage with the concept of the amorphous supply chain model. By recognising the opportunities presented by such a supply chain model, there is potential for MSEs to increase their customer base and engage in international markets“(Ritchie and Brindley, 2000: 575).

The ITGI (2009) work is considered as a pioneering effort. In this process, the three ITGI frameworks—Control Objectives for Information and Related Technology (COBIT), Value Information Technology (Val IT) and Risk IT— complement each other and provide practical guidance as seen in Figure 1.2

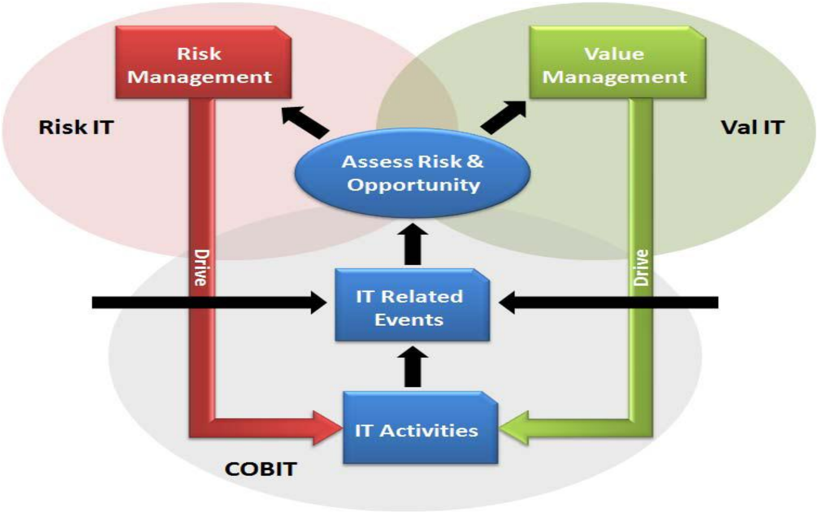


Figure 1.2: ITGI frameworks: COBIT, Val IT and Risk IT (Source: ITGI, 2009: 24)

The risk dimension, and how to best deal with it, is the main subject of the Risk IT framework (Figure 1.2). Once opportunities are identified, the Val IT framework describes how best to progress and maximise the opportunity. Both Risk IT and Val IT, after having addressed the details of risk and value management, will trigger specific (improved) IT activities, for instance project development activities, information security activities or service level management activities (ITGI, 2009: 24).

In summary, the ORM adoption has been studied within the context of MSEs using several approaches. From the review of the existing literature, it is evident that there is a number of overlapping divergent models that potentially explain an ORM adoption decision, but these are not applicable to MSEs. Most of the studies within their domain have added to existing knowledge, but are fairly skewed (ITGI, 2009).

Most of the studies on ORM are based on the survey method which is a good way of developing a hypothesis, but this method makes it difficult to study the effects of a single case (ITGI, 2009). So there is a need to conduct more empirical studies to provide statistical validity with respect to a single case. Additionally, researchers across the globe have selected different factors that may not necessarily be suitable to the South African MSE context (King III Report, 2009). For this reason, the research problem and the development of hypotheses were based on existing South African literature and ORM MSE model measurements (Risk Measure). In the current study, adoption of ORM was the dependent variable but there are several independent variables (cf. Methodology, for details).

1.2.1 MSE AND ICT Performance

In most African countries, medium and small enterprises (MSE) account for a significant share of production and employment and are therefore directly connected to poverty alleviation (King III Report, 2009).

Consequently, one can ask whether the use of ICT (as production technology, information processing technology or information communication technology) can help MSEs cope with new and existing challenges (King III Report, 2009). The spread of ICT has led several commentators to argue that these technologies create a new economy – an information economy – in which information is the critical resource and the basis for competition in all sectors (King III Report, 2009). Thus ICTs can improve efficiency and increase productivity in different ways including improving efficiency in resource allocation, reducing transaction costs, technical improvement and ultimately leading to the outward shifting of the production function.

It is argued that in remote regions, the disadvantages that arise from isolation can be significantly lessened through access to rapid and inexpensive ICT (King III Report, 2009). However, a more pessimistic view assumes that the digital divide will increase and therefore producers in developing countries, especially in rural areas, will face even greater disadvantages relative to their competitors in developed countries (King III Report, 2009). Although South Africa is much more developed and its ICT infrastructure is far more advanced than most Sub-Saharan African countries, in remote areas of South Africa with a poor population, similar difficulties as in other African countries exist with respect to ICT infrastructure and the role of the MSE sector (King III Report, 2009).

So far there is little empirical evidence on how the diffusion and application of ICTs can be a catalyst for economic competitiveness and growth in MSE.

Arguably, large organisations have higher profitability in terms of fixed assets employed than MSEs (ITGI, 2009). The King III Report (2009) mentions that the focus on production processes may be too narrow and that ICTs may need to exert their influence through product quality improvements and improved services. ICTs might additionally help MSEs in the administration of their businesses and enhance procurement and marketing processes. This study therefore focuses on an MSE rather than on a large business.

1.3 MOTIVATION FOR RESEARCH STATEMENT AND DEVELOPMENT OF HYPOTHESES

“The key issue for most companies, especially smaller ones, is the resources available for establishing and maintaining risk management procedures” (King III Report, 2009: 75). For this reason, research suggests the avoidance of unnecessary complexity so that risk management procedures can be understood and operationalised with minimum cost and disruption (King III Report, 2009). This current study is situated within the above context, that is, a model to manage ICT operational risk. The focus of the case study is a financial service provider (cf. Methodology for details). In support of the objectives of the study and to justify the research problem the study proposes *what* needs to be done, thus:

> "An approach that places the primary focus on, and concentrates training around, risks that are significant, ensures objectives are prioritised and clearly allocates responsibility within the company for the procedures" (King III Report, 2009: 75).

However, the justification in this current study is *how* this should be done, hence ICT operational risk. The objective is consistent with another study which suggested that:

> "For IT to be successful in delivering against business requirements, management should put an internal control system or framework in place. The Control Objectives for Information and Related Technology (COBIT) control framework contributes to these needs by (1) making a link to the business requirements (2) organising IT activities into a generally accepted process model (3) identifying the major IT resources to be leveraged (4) defining the management control objectives to be considered" (ITGI, 2007: 5).

On the basis of the institute's assertion and previous IT-based studies on the usage of ORM, a normative model was developed. This model is a one-stage model that relates independent and dependent variables without any intervening variables (cf. Methodology[1] and Results of Study for details). Thus, the relationship will intend to show a model that is associative rather than causal in nature due to the research methodology[2] used. In this study, adoption of ORM is the dependent variable while there are a number of independent variables (IVs) generated from the hypotheses and research objectives (cf. Methodology). Detailed

[1] The use of Analysis of Co-variance (ANCOVA), logistic regression/multivariate analysis due to scale of measurement and research hypotheses.

[2] Methodology used in this current study refers to research methodology and not IT methodology(ies); same should be applied in chapter 3; research methodology.

justification for the inclusion of each independent variable in the model is further elaborated in the literature review chapter (cf. Chapter 2).

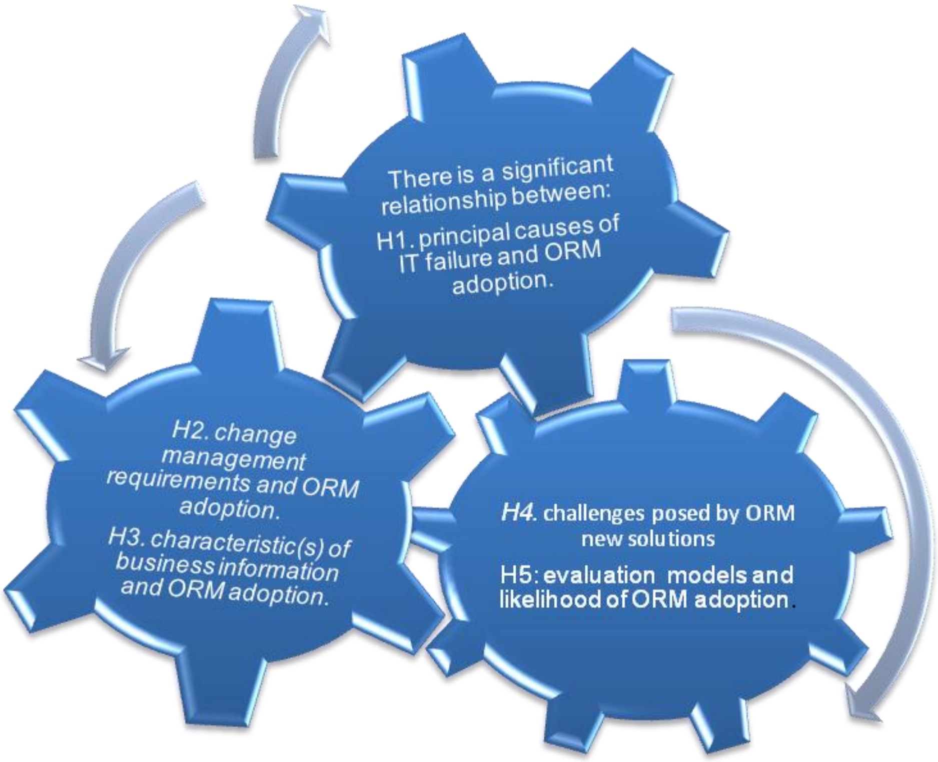

There is a significant relationship between:
H1. principal causes of IT failure and ORM adoption.
H2. change management requirements and ORM adoption.
H3. characteristic(s) of business information and ORM adoption.
H4. challenges posed by ORM new solutions
H5: evaluation models and likelihood of ORM adoption.

Figure 1.3: Hypothetical Factors

1.4 RESEARCH OBJECTIVES

The objectives of the research are to:

- Analyse the principal causes of IT ORM failure in an MSE.
- Assess the change management requirements for building successful systems-risk monitoring and reporting of ORM in an MSE.
- Identify which characteristic(s) of business information play a major role in supporting an organisation’s business operations.
- Identify the challenges posed by IT ORM new solutions.
- Evaluate models for understanding the value of IT ORM in an MSE.

1.4.1 RESEARCH PROBLEM STATEMENT

Key issue for most companies, especially smaller ones (MSE), is the shortage of resources for establishing and maintaining risk management procedures (King III report, 2009: 75). For this reason, King III Report (2009) suggests the avoidance of unnecessary complexity so that risk management procedures can be understood and operationalised with minimum cost and disruption. However, literature indicates that one of the problems for MSE is putting an internal control system or framework in place. There is also the problem of linking business requirements with the objectives of MSEs. Additionally, there luck organised IT activities into a generally accepted process model.

On the basis of the problems and ITRM-based studies on the usage of ORM, a normative model will be developed. This model is intended to show a one-stage model that relates the performance of MSE and the problems identified. Thus, the relationship will intend to show a model that is associative rather than causal in nature due to methodology used.

1.5 DELIMITATION OF THE STUDY

The study mainly focused on one MSE financial service company, since the research design was a case study in the province of Eastern Cape, South Africa. A survey design was used in selecting the unit of analysis (cf. Research Methodology). Although there are several MSEs, the study adopted only one consisting of about 107 units of analysis (cf. Research Methodology). It is important to note that the study relates where appropriate to other MSEs within the same industry. Thus suggesting that contrary to the general notion of adopting several MSEs, the study rather addressed only one MSE and its underlining variables (cf. Objectives and Hypotheses). ORM is a discipline that calls for firms to identify all the risks they face, to decide which risks to manage actively, and to then make that plan of action available to all stakeholders (not simply shareholders) as part of their annual report (King III Report, 2009). In this particular study the focus is on ICT operational risk in MSEs (cf. Chapter 2 section 2.2.1-2.2.4).

1.6 RESEARCH METHODOLOGY

The view taken in this study was dualistic. Adopting a dual view of the research design allowed for constructing a model which promoted a common understanding (descriptive and inferential). Thus, based on the research objectives and data collected, the research used a positivist perspective.

Additionally, a combined-mixed design (CMD) facilitated a holistic view and strengthened the reliability of the instrument (Creswell, 2007). Thus, CMD is built around testing the relationships between factors influencing ORM (Creswell, 2007). The study was conducted in a South African based micro finance company which has 90 branches nationally. The company's product range included unsecured loans, secured loans, insurance, cellular and educational products. The products are sold through its various channels: branches, telesales call centres and agents.

1.6.1 DATA ANALYSIS AND INTERPRETATION

The questionnaires received were analysed using the Statistical Package for the Social Sciences (SPSS) for correlation and multiple regression analysis to predict ORM adoption based on the hypotheses. In line with the principles of multivariate data analysis, the researcher conducted a zero-order correlation of the independent and dependent variables. The correlation provided support for predicted relationships and showed that co linearity among the independent variables was sufficient, such that it did not affect the stability of regression analysis. Other tests of various assumptions[3] such as, normality and multi co linearity were conducted (cf. Chapter 3 section 3.4: Research Methodology).

The researcher ensured that the validity and reliability aspects of the instrument were carefully developed. The face and construct validity were ensured developing a thorough analysis of the literature. Collegial validity was ensured giving the instrument to specialists in the field of risk management to check whether the constructs were represented correctly.

1.7 ETHICAL CONSIDERATIONS

Researchers define ethics as moral principles or rules and behavioral expectations of the one conducting the research (Creswell, 2007).The following were considered.

Informed consent: Operational, middle and senior managers were used in the research as the unit of analysis. Permission was sought in this regard (cf. Appendix A and Chapter 3 Methodology).

Voluntary participation: Participation in the study was voluntary. Respondents were informed about the nature of the study and given the choice to take part or not. Only individuals who volunteered were allowed to participate.

Anonymity and confidentiality: Privacy and confidentiality of participants were guaranteed. As a result, the identity of respondents and the research sites were not revealed in the reporting of the findings or even in subsequent reports. To identify respondents, the researcher gave each individual a pseudonym, which only the researcher understood. Thus, personal details remained anonymous**.**

[3] For details see Tabachnick and Fidel (2007).

1.8 OUTLINE AND MILESTONE

Chapter 1 of this study begins with the context of the study. This was followed by the motivation for the research statement and development of the hypotheses**.** The other sections included research objectives and delimitation of the study. Attention was also given to the research methodology and ethical considerations.

Chapter 2 concentrates on the reviewed literature. In so doing it addressed MSEs and ORM development in South Africa together with risk measures. The chapter also addressed evolution of operation risk management. It also included a section on models for understanding the value of IT ORM in a MSE, change management requirements for building successful IT/IS systems, characteristics of business information and lastly the theoretical framework of the study, which focused on chaos and complex theory.

Chapter 3 addresses the research methodology and its design**.** This is followed by the description of the selected designs, case study and survey design. The sample, sampling technique and instrumentation are also addressed. The last section focuses on the detailed data analysis technique used (that is multivariate regression and its assumptions).

Chapter 4 presents the findings/results of the research.

Chapter 5 reflects on the data and draws salient issues and meaning from them.

Chapter 6 provide a summary, conclusion and recommendations for further study.

CHAPTER 2: REVIEW OF LITERATURE

MEDIUM AND SMALL ENTERPRISES (MSEs) AND INFORMATION COMMUNICATION TECHNOLOGY OPERATIONAL RISK MANAGEMENT (ICT ORM)

2.7 INTRODUCTION

Chapter 2 concentrates on the reviewed literature. It addresses MSE ICT concepts, and IT ORM. The chapter also addresses the evolution of ORM. Included is a section on hypothetical models for understanding the value of ITRM in an MSE, risk measures and the theoretical framework of Chaos Theory and how it underpins this current study.

2.8 CONCEPT OF A MSE

MSE definitions vary from country to country and are ideally defined specifically according to a sector. The cut off point in terms of size for this study was based on a recommendation from the African Development Bank, which defines MSEs as having less than 200 employees. This study deals with businesses[4] where the primary aim is to generate sustainable income streams (King III Report, 2009).

In the information society environment, successful enterprises produce high technology goods and services and transform human effort materials and other economic resources into products and services that meet customers' needs (King III Report, 2009). In such a society, in order to be successful, an MSE would need high quality information and must always provide superior value to that of competitors when it comes to quality, price and services (King III Report, 2009).

[4] In this study 'business', 'firm', 'organisation' and 'institutions' are used interchangeably.

There is no acknowledged universal definition for a MSE. For this reason the researcher restricted the motive of the study to the common definition of the aforementioned, based on employment figures (King III Report, 2009). The widely accepted definition points to Medium Sized Enterprises with between 100 to 200 employees.

2.3 CONCEPT OF ICT

For the last two hundred years, economics has recognised only two factors of production: labour and capital. This is changing as Information and Knowledge are replacing capital and energy as primary wealth creating assets (King III Report, 2009). Information has become a critical resource, a priceless product and basic input to progress and development. Information has become synonymous with power. Therefore, accurate, rapid and relevant information is considered essential for an MSE (ITGI, 2007).

An MSE needs effective information systems to support and deliver information to different users. Such information systems would include technology that supports decision making, provides an effective interface between users and computer technology and provides information for managers on the day-to-day operations of the enterprise. Information is needed for various purposes and serves as an invaluable commodity or product. Information is a highly important aspect of decision making in all levels of management in an enterprise (ITGI, 2007). The ability of MSEs to realise their goals depends on how well the organisation acquires, interprets, synthesises, evaluates and understands information and how well its information channels support organisational processes.

2.4 IT OPERATIONAL RISK MANAGEMENT (ORM)

Several texts and periodicals (Quinn, 2008**;** ITGI, 2007) have introduced or discussed concepts such as ‘strategic risk management,’ ‘integrated risk management’, ‘holistic risk management’ and ‘organisational risk management.’ While Stoney (2007) explains that strategic risk management is about managing unpredictability of risk in corporate outcomes; the King III Report (2009) suggests that integrated risk management refers to acknowledgement that risks are not only financial or fraud related, but include the ability of a series of planned activities to accomplish relevant political and social objectives. Meanwhile, Stoney (2007) notes that holistic risk management, which is sometimes referred to as enterprise or organisational risk management, combines financial, strategic and operational risk in a holistic approach to identify and mitigating those risks that are the greatest threat.

These concepts are similar to, even synonymous with, Institution-wide Risk Management (IRM), in that they both emphasise a comprehensive view of risk, a movement away from the silo[5] approach of managing different risks within an organisation separately and distinctly (Stoney, 2007). For the purpose of this chapter IRM and organisational-wide risk management (ORM) will interchangeably be used. Quinn (2008:1) offers the following definition of ORM:

> “It is a relatively new (less than a decade old) management discipline that calls for corporations to identify all the risks they face, to decide which risks to manage actively, and then to make that plan of action available to all stakeholders (not simply shareholders) as part of their annual reports.”

[5] Silos traditionally concentrate on how individual business units operate and perform. Each department within a financial institution is responsible for managing its respective channels (Stoney, 2007)

Several parts of this definition are relevant and merit individual attention. Firstly, ORM is a discipline. This includes IT operational risk management (IT ORM) and reputational risk management. But the focus of this study is IT ORM. The motive is that IT ORM is an orderly or prescribed conduct or pattern of behaviour for an organisation that has the full support and commitment of the management of the organisation. That it influences corporate decision-making, and that it ultimately becomes part of the culture of that organisation. Secondly, IT ORM, even as defined by the King III Report (2009)**,** applies to all industries including ICT. Thirdly, the specific mention of exploiting risk as part of the risk management process (along with the stated objective of increasing short and long term value) demonstrates that the intention of IT ORM is to create value as well as risk mitigating. Fourthly, all sources of risk are considered, not only hazard risk or those traditionally managed within an organisation. Finally, implicit in this definition is the recognition of IT ORM as a strategic decision support model for management. Thus, it improves decision-making at all levels of the organisation in a defined conceptual model.

2.4.1 ICT EFFICIENCY WITHIN MSEs

There are a few suggestions in literature that demonstrate the need for IT operational risk in MSEs (ITGI, 2003). A few empirical studies show the association between ICT operational risk in MSEs and efficiency in an MSE (ITGI, 2003). Those studies found that good ICT operational risk in MSEs can generally improve efficiency. However, there are others which empirically suggest the existence of indirect relationships between ICT operational risk management in MSEs and efficiency (Anderson, 2005).

The National Credit Regulator (2008) states that for competition and merger analysis of financial institutions, it is important to know the effects of market concentration and past mergers on institution efficiency.

Additionally, Anderson (2005) found that ICT operational risk activities contribute significantly to enhancing the efficiency of MSEs. Here, the author argues that ICT operation in MSEs is activity used by insurers to improve efficiency. Anderson (2005) found that efficiency has positive effects on ICT Operational Risk in MSEs, interest rate risk and capitalisation. COSO (2004) shows that profit efficiency is sensitive to ICT operational and insolvency risks in MSEs but not to liquidity risk or to a mix of loan products in large firms.

Hence, by managing these risks, an institution’s efficiency is expected to improve. From the literature, IT operational risk in MSEs’ practices is associated with the level of efficiency and performance of MSEs.

2.4.2 ICT EFFICIENCY WITHIN LARGE FIRMS

The King III Report (2009) states that institution efficiency would imply improved profitability, greater amounts of funds for ICT operational risk in large firms, better prices and service quality for consumers, and greater safety and soundness if some of the efficiency savings are applied towards improving capital buffers that absorb risk. Curley (2004) adds that one reason for studying the efficiency of large firms includes an improvement in cost efficiency as a means of achieving higher profits and increasing the chance of survival in deregulated and competitive markets.

However, there are few studies in ICT that investigate the relationship between efficiency and an MSE firm’s performances (Curley, 2004). Most studies concentrate on large institutions. Froot and Stein (1998) found profitability is significantly related to measuring pure technical efficiency (PTE). Basel II (2004) investigated the performance of financial institutions in terms of efficiency, and found a significant positive relationship between ICT of financial institutions and all types of efficiency, supporting the notion that financial institutions become more efficient as a by-product of enhancing their profitability.

The findings on the relationship between ICT and efficiency could be explained by the perception that financial institutions become more efficient as a result of enhancing their ICT (Basel II, 2004). Moreover, Basel II (2004) suggests a positive relationship between profitability and performance due to the ability to raise more capital.

Recently, Layton (2007) found that the relationship between the effect of ICT and efficiency is positive. The coefficient of return on asset is positive, suggesting that more profitable financial institutions tend to be more efficient. However, Curley (2004) found that profitability is significantly negative associated to scale efficiency. Finally, from the literature, it is proven that there is an association between efficiency and financial performances especially when using ICT. However, there is also an association between efficiency and the likelihood of financial distress.

As stated by Artzner, Delbaen, Eber, Heath and Ku (2007), most financial institution failures are directly related to factors such as a large number of problem loans, low capital position, weak or negative cash flow, and poor management quality. Also, it is expected that institutions would display low efficiency prior to failure and these institutions would probably then have a high likelihood of financial distress.

Additionally, a few empirical studies have been conducted to show the relationship between capital adequacies and ICT (Artzner *et al*, 2007). Other studies at financial institutions also found an association between capital and ICT (Burget and Ruschendorf, 2006).

The foregoing suggests that there is some relationship between ICT and MSE performance; for this reason, this current study intent to establish the factors and their co-relationships.

2.4.3 ICT TRENDS IN FINANCIAL RELATED MSEs

Although ICT operational risk in MSEs is one of the key functions of financial institutions, very little has been done to date to link ICT operational risk in MSEs with performance (Basel II, 2004). However, conceptually, many discussions focus on the objectives of ICT operational risk in MSEs that provide relationships between ICT operations and MSE performance (Calder, 2006; Basel II, 2004).

Basel II (2004) states that while directors see ICT operational risk in MSEs as critical, there is a real concern that ICT operational risk in MSEs practices is less focused, which may detract from improving business performance. On other aspects, Liebenberg and Hoyt (2003) researched a sample of firms that had signalled their use of ICT operational risk by appointing a Chief Information Officer (CIO) and found that firms with greater ICT leverage were more likely to appoint a CIO.

The findings are consistent with the hypothesis that firms appoint CIOs in order to reduce information asymmetry with regard to the firm's current and expected risk profile, noting that this is particularly true for large firms. Liebenberg and Hoyt (2003) provide further evidence that financial institutional investment in ICT operational risk in MSEs during the 1990s helped increase earnings and were less volatility during the 2001 recession.

A recent study by Sholes (2007) used a hazard model to examine the factors that influence the MSE level of ICT. They found that firms which are more levered with volatile earnings together with poorer stock performances are more likely to initiate an ICT program (Sholes, 2007). According to the author, firms that face greater risk of financial distress may benefit from ICT when it reduces the chance of costly outcomes (Sholes, 2007). Also, it was revealed that firms that have greater risk of financial distress, that is those with more leverage and less financial slack, are more likely to adopt ICT (Layton, 2007). In addition, there are many studies looking at profitability and its various determinants including operational risk factors (Layton, 2007; Sholes, 2007).

A number of empirical studies show that ICT operational risk in MSEs is one of the determinants of profitability (King III Report, 2009). Hence, by managing ICT risks well, the financial institutions can expect to be more profitable. As the survival and success of an MSE depend on the efficiency with which they manage risks, ICT operational risk in an MSE is one of the critical factors in providing better returns to shareholders (Yeo, 2002).

2.5 INFORMATION TECHNOLOGY RISK MANAGEMENT

Recent studies on Information Communication Technology Risk Management (ICT RM) in large organisations have revealed the following benefits. Research suggests that ICT RM can be used to understand organisational operations and change management (Smith and Kruger, 2010; ITGI, 2009; Gerber and Von Solms, 2005). One study suggests that Information Communication Technology risk is a business risk, which is defined and operationalised as follows:

> " … Business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise. It consists of IT-related events that can potentially impact the business. It includes both uncertain frequency and magnitude, and it creates challenges in meeting strategic goals and objectives as well as uncertainty in the pursuit of opportunities" (ITGI, 2009: 11).

In contrast, the success of ICT RM models and theories in large organisations has shifted focus towards MSEs (King III Report, 2009; Allen, 2005; Basel Committee on Banking Supervision, 2004; ITGI, 2007; Kim, Kim and Lee, 2006).

> “However, despite these theoretical explanations there is still a shortage of reliable quantitative models that can provide enough information to analyze IT security investments, particularly in MSEs” (Smith and Kruger 2010: 1).

The factors that have necessitated this shift is depicted in Figure 1.1, which is shortly elaborated on.

One of the reasons attributable to the shift in paradigm as suggested by researchers and practitioners of ICT RM is that it serves as a new venue of improved services and potential benefits for MSEs (Smith and Kruger, 2010; King III Report, 2009; ITGI, 2007; Curley, 2004).

Additionally, the study of Standing, Guilfoyle, Lin and Love (2007; 1156) identified no main effects “…using project outcome (success and failure) as the repeated measure and job responsibility (IT support, line and executive managers) as the independent factor…” However, a significant interaction effect for outcome by responsibility, $F(2,102) = 4.45$, $p < .05$ was determined. When a post hoc analysis (Tukeys HSD and single degree of freedom *F* ANOVA) was conducted, it revealed that “… IT support workers attributed their self significantly more to IT project success (mean=0.34) than to IT project failure (mean = 0.33), $F(1, 28) = 5.10$, $p < .05$)” (Standing *et al*, 2007: 1156). The reverse was true for executive managers, who took more responsibility for their project failure than their project successes ($p = .08$) (Standing *et al*, 2007: 1156).

Yet, a number of studies have suggested that small businesses have not shown great interest in ICT RM, particularly Operational Risk Management (ORM) (King III Report, 2009; ITGI, 2007; Basel Committee on Banking Supervision, 2004).

Review of several literature texts indicates that ORM, a variation of ICT RM, provides a structural form of activity and has become a popular vehicle for risk management of information in industries such as financial and manufacturing (King III Report, 2009; Kritzinger and Smith, 2008; Lutchen, 2004; ITGI 2009). In addition to the aforementioned studies, Bayaga (2010: 77) highlighted that “as a rising management discipline, interest and current development of Institutional Risk Management (IRM) varies across industries and institutions.” This suggests that ORM is a tool that can be used to evaluate models for understanding the value of IT and for streamlining a company’s operations.

Operational risk management emerged in the late 1960s when manufacturing companies started looking for ways to alleviate delivery delays resulting from large volumes of products and services. The use of ORM however, only became popular in late 1980s and early 1990s (Nicholas and Steyn, 2008; Turban and Meredith, 1994). Currently, many large organisations in the United States of America, Canada, and Europe use ORM to support their IT financial and trading activities. The adoption of ORM has also progressed rapidly in Australia (Lam, 2006).

There is an indication that the growing use of ORM has drawn the attention of several academic studies. A number of success stories published in recent years have claimed a variety of benefits from ORM adoption, while several studies have also confirmed the ORM benefits to a varying extent (King III Report, 2009; ITGI 2007; Basel Committee on Banking Supervision, 2004).

In the past, considerable research on ORM was conducted for large businesses where as studies on MSEs towards the adoption of ORM are a recent phenomenon (King III Report, 2009; Lam, 2006). Additionally, the majority of these studies are confined to the USA, Canada and Europe. Comparatively less studies has been done in Africa and therefore the number of studies on ORM adoption in South Africa remains marginal. Regrettably, a limited number of empirical studies on ORM adoption in MSEs have been undertaken in the Eastern Cape. Yet, recently, some studies reflect the use of information technology (IT) among MSEs.

Therefore, this pioneering study investigates the ORM adoption in an Eastern Cape MSE. The objective is to examine one Eastern Cape business to study the ORM impact on an MSE. It is important to note that the study adopted a common industry definition of operational risk, namely “the risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events” (Basel Committee on Banking Supervision, 2004: 2). Noting that several categorisations of IT risk have been proposed for the purpose of this study, the researcher adopts and adapts that of the ICT Governance Institute (ITGI, 2009).

IT risk has been described as the solution delivery/benefit realisation risk, associated with the contribution of IT to new or improved business solutions, usually in the form of projects and programmes (ITGI, 2009: 11). It is important to note that this categorisation “focuses on the causes of operational risk which is appropriate for both risk management and, ultimately measurement” (Basel Committee on Banking Supervision, 2004: 2). Consequently, this study sets out further details on the effects of operational related IT risk.

2.6 EVOLUTION OF OPERATIONS RISK MANAGEMENT

IT Operation Risk Management (IT ORM) in financial institutions is not a new phenomenon (Basel Committee on Banking Supervision, 2004). In framing the current study, the author has adopted a common industry definition of operational risk and classification of risks in general from other authors who suggest that;

> “…strategic and reputational risk is not included in this definition for the purpose of a minimum regulatory operational risk capital charge. This definition focuses on the causes of operational risk and the Committee believes that this is appropriate

> for both risk management and, ultimately, measurement" (Basel Committee on Banking Supervision, 2004: 4).

However, in reviewing the progress of the industry in the measurement of operational risk:

> "...the Committee is aware that causal measurement and modelling of operational risk remains at the earliest stages. For this reason, the Committee sets out further details[6] on the effects of operational losses, in terms of loss types, to allow data collection and measurement to commence" (Basel Committee on Banking Supervision, 2004: 4).

The position of the Basel Committee on Banking Supervision gives an indication that dealing with risk has always been the raison d'être of financial intermediation and its underlying principle (King III Report, 2009; Lee and Jang, n.d). There have been other arguments that imply that an integrated, holistic approach to IT operation risk management can create shareholder value (King III Report, 2009; Lee and Jang, n.d). The effective management of IT ORM is crucial to any financial institution's performance. Researchers describe IT risk management as the performance of activities designed to minimise possible negative losses (King III Report, 2009; Lee and Jang, n.d). Yet others reveal that the purpose of the financial institution is to maximise revenue and offer the most value to shareholders by offering a variety of financial services, and especially by administering IT risks (King III Report, 2009; Lee and Jang, n.d).

[6] For details, readers may refer to Basel Committee on Banking Supervision (2004)

IT ORM is crucial in all industries. Accordingly, survival and success of financial organisations depend on the efficiency with which they are managed. Hence, ORM is one of the critical factors in providing better returns to shareholders (King III Report, 2009). This view has been shared by risk practitioners (Basel Committee on Banking Supervision, 2004). In fact, the author suggest that the Committee wants to enhance operational risk assesMSEnt efforts by encouraging the industry to develop methodologies and collect data related to managing operational risk (Basel Committee on Banking Supervision, 2004). Also, it will depend to a large extent on how these institutions manage different risks arising from their operations (Basel Committee on Banking Supervision, 2004; Lee and Jang, n.d). In addition, prudential standards on capital adequacy and risk management set out by Financial Services Boards around the world show the importance of operation risk management.

Finally, the efficacy of risk management in financial institutions is of particular importance in an endeavour to cope with the challenges of globalisation (Lee and Jang, n.d). For the aforementioned contestations, the objective of the current study is to investigate the relationship of ICT RM and MSE performance.

2.6.1 PRINCIPAL CAUSES OF ORM FAILURE IN AN MSE

Recent debate on failures of IT/IS projects suggests that many information systems fail to deliver benefits or solve the problems for which they were intended. This is often caused by the process of organizational change surrounding system building not being properly addressed by large organisations (ITGI, 2009).

For the same reason, the majority of organisations "…recognise the need for data protection measures, but at least the reasons are not lack of knowledge, lack of information, or financial problems” (Lee and Jang, n.d: 84).

Notwithstanding, in South Africa “there is a lack of the perception of information security for MSEs and necessary policy” (Lee and Jang, n.d: 84). One such lack of perception is the principal causes of IS/IT (King III Report, 2009). The principal causes of information system failure as suggested by researchers are (1) insufficient or improper user participation in the systems development process (2) lack of management support (3) high levels of complexity and risk in the systems development process and (4) poor management of the implementation process (ITGI, 2009; Lee and Jang, n.d).

However, it is important to keep this risk/reward duality in mind during all risk-related decisions (ITGI, 2009). Figure 2.1 shows that for all categories of IT risk there is an equivalent upside. For example:

- Service delivery—If service delivery practices are strengthened, the enterprise can benefit, e.g., by being ready to absorb additional transaction volumes or market share.
- Project delivery—Successful project delivery brings new business functionality (ITGI, 2009: 8).

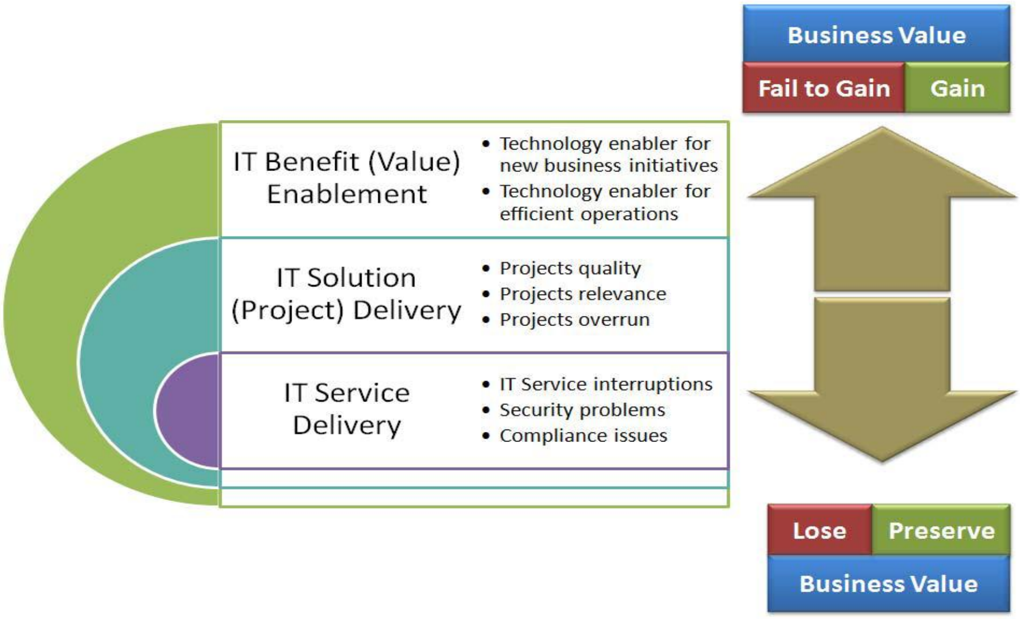


Figure 2.1: Categories of IT Risk (Source: ITGI, 2009: 8)

The Risk IT framework is aimed at a wide audience, as risk management is a pervasive and strategic requirement in any enterprise (ITGI, 2009: 8). However, there is a high failure rate among business process reengineering and enterprise application projects, because they require extensive organisational changes that are often resisted by members of the organisation (ITGI, 2009). In the case of MSEs, which operate under limited resources and capabilities, the characteristic of the information security has to be perceived in a different way and countermeasures should be differentiated from those of large enterprises (Lee and Jang, n.d). For instance, what is not known in South African MSEs is the extent to which enterprise application changes require ICT processes.

There are a few suggestions in literature that show the need for ITRM improvement of MSEs (Lee and Jang, n.d). A few empirical studies show the association between risk management and efficiency in the insurance industry and in the banking industries (ITGI, 2009; Lee and Jang, n.d). These studies found that good risk management generally improves efficiency. However, there are many studies which empirically prove indirect relationships between risk management and efficiency as well as other characteristics which include problem loans, weak or negative cash flows, and poor management quality all of which influence the efficiency of the financial institutions (ITGI, 2009; Lee and Jang, n.d).

Apart from evaluation models, works of the Committee of Sponsoring Organisations (COSO) (2004); Casualty Actuarial Society (CAS) (2003), and the King III Report (2009), further advocated that success of IT within an organisation can be determined by considering (1) principal causes of IS failure and (2) change management requirements to IT by allocating necessary resources, suggesting that parameters can be important for the success of IT risk within MSEs. In this study the intent is to measure parameters and find a significant predictor of ORM adoption (cf. Chapter 3 and 4).

Despite advances in IT and the acceptance of such technologies by large organisations, the same level of adoption is not evident among MSEs (ITGI, 2009). This suggests that MSEs face significant and unique challenges. This low level of adoption particularly impedes MSEs in developing countries. Literature reveals that many studies have been carried out in developed countries to investigate the factors inhibiting adoption of ICT (ITGI, 2009; Lee and Jang, n.d). These studies have looked at organisational perspectives, owner/manager perspectives and environmental perspectives. Among the few research studies carried out in developing countries are studies that investigate the facilitators/inhibitors affecting adoption (King III Report, 2009; Lee and Jang, n.d).

Predominantly these studies investigate the technological, organisational, physical and socio-economical environmental factors that hinder the adoption of ICT (ITGI, 2009). The differences between developed and developing countries (such as available infrastructure, social and cultural issues) do not support generalising the findings for developed countries to developing countries. MSEs in developing countries are faced with barriers specific to them, some more pronounced than would be in the case for MSEs in developed countries (ITGI, 2009). To understand the lack, or slow uptake of ICT technologies, it is appropriate to look into the environment in which they operate. Due to the many constrains inherent to developing countries, MSEs are faced with both internal and external barriers. To gain a better understanding and assist them, it is imperative to examine these barriers in depth (CAS, 2003).

Internal Barriers: An MSE has control over and the ability to change the internal factors within the organisation. For example, lack of time or resources, and lack of awareness on the part of the owner/manager. Internal Barriers could be further categorised into Individual (owner/manager), organisational barriers and cost and return on investment (Lee and Jang, n.d). Another inhibiting set of impediments may arise due to infrastructure (technological, economic), political, legal, social and cultural barriers that exist within the country (Lee and Jang, n.d).

External Barriers: These are barriers that cannot be resolved by the MSE as they have no control over these factors. They are compelled to work within these external constraints, for example, inadequate telecommunication infrastructure. Some of the barriers could be addressed by MSEs working together, coming together irrespective of the industry sector to form clusters to share expenses, resources and facilities (King III Report, 2009). Alternatively, MSEs from the same industry sector could work together to address other external barriers where governmental intervention may be required.

For an MSE to successfully adopt the technologies, the above two sets of barriers need to be addressed (King III Report, 2009). The internal barriers may be resolved within the organisation, but it may have to work within the constraints of the external barriers, which are beyond the organisation's control and therefore may require government intervention (Lee and Jang, n.d). Hence, it is vital to understand the barriers that inhibit MSEs in developing countries and how they should overcome these barriers if they are to take advantage of the benefits of ICT (King III Report, 2009).

Even though there are now an interesting and growing number of studies addressing ICT Risk Management adoption within the specific context of MSEs, little research has been conducted in developing countries, especially South Africa (King III report, 2009; ITGI, 2007). This study seeks to fill this gap to help understand the factors that hinder the adoption of ICT Risk Management by MSEs in developing countries, and to explore how best they can be overcome. South Africa was chosen as it is a developing country struggling with its economy, but on its way to an ICT society.

2.6.2 CHANGE MANAGEMENT REQUIREMENTS FOR BUILDING A SUCCESSFUL INFORMATION TECHNOLOGY/SYSTEM

The management side of information system governance is concerned with how the stipulations for information security by executive management are implemented in an organisation (Posthumus and Von Solms, 2004). Many surveys have identified strategic alignment, value delivery, risk management, resource management and performance management as some of the most important drivers of IT Governance as seen in figure 2.2 (ITGI, 2007).

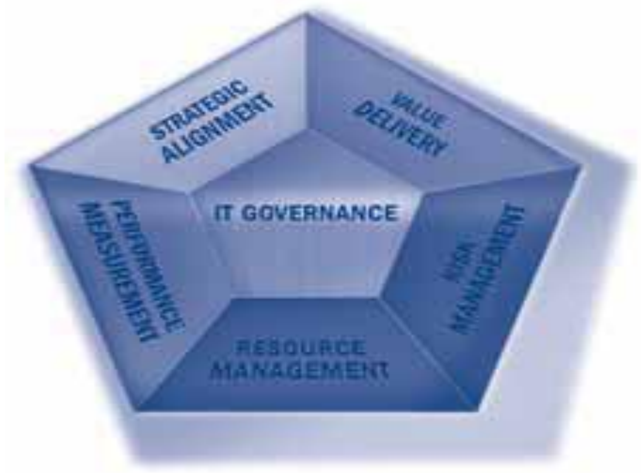


Figure 2.2: Drivers for IT Governance (Source: ITGI, 2007: 6)

• **Strategic alignment** focuses on ensuring the linkage of business and IT plans; defining, maintaining and validating the IT value proposition; and aligning IT operations with enterprise operations (ITGI, 2007: 6). A key step in the process of developing IT strategy is (1) the association of each initiative back to one or more of the organisational objectives and (2) being able to attribute a degree of influence in achieving that objective (ITGI, 2007). The building blocks of developing a good IT strategy demand that the organisation has a sound, and clear strategic plan. The plan should be structured in such a way that the strategies, and more importantly the objectives of the organisation, are spelt out in a clear and concise way. It is difficult to connect IT strategy to a broad and far reaching business strategy unless the intent is distilled down to core salient points. This aspect becomes vital as projects and initiatives need to be associative (ITGI, 2007).

- **Value delivery** is about executing the value proposition throughout the delivery cycle, ensuring that IT delivers the promised benefits against the strategy, concentrating on optimising costs and proving the intrinsic value of IT (ITGI, 2007: 6).

Literature investigating the barriers that affect MSEs adoption of IT and value delivery have identified a variety of factors which can be grouped into several categories. A number of authors identify factors relating to three major categories: owner/manager characteristics, firm characteristics, and costs and return on investment (ITGI, 2007; King III Report, 2009).

The owner/manager play an important role in decision making in MSEs. Hence it can be concluded that a number of factors that affect the adoption of value delivery relate to owner/manager characteristics. The King III Report (2009) found that the owner's lack of awareness of the appropriate technology and perceived benefits is a major barrier to incorporation of IT. Lack of knowledge on how to use the technology and low computer literacy are other contributory factors. Mistrust of the IT industry and lack of time are two other factors that affect the value delivery of MSEs (King III Report, 2009). Owners are concerned about return on their investments and are reluctant to make substantial investments particularly when short-term returns are not guaranteed.

The King III Report suggests that the current level of technology usage within organisations affects the process of adoption. In another study by the ITGI (2007), it was identified in addition that lack of awareness, uncertainty about the benefits of electronic commerce, concerns about lack of human resources and skills, set-up costs and pricing issues and concerns about security are the most significant barriers to value delivery for MSEs (King III Report, 2009). Low use of IT by customers and suppliers, concerns about security, concerns about legal and liability aspects, high costs of development, computer and networking technologies for IT, limited knowledge of models and methodologies, and unconvincing benefits to the company are other factors (ITGI, 2007). MSEs definitely have limited resources (financial, time, personnel). This poverty resource has an effect on the adoption of IT, as these small businesses cannot afford to experiment with technologies to incur expensive value delivery.

- **Resource management** is about the optimal investment in, and the proper management of, critical IT resources: applications, information, infrastructure and people. Key issues relate to the optimisation of knowledge and infrastructure (ITGI, 2007).

- **Risk management** requires risk awareness by senior corporate officers, a clear understanding of the enterprise's appetite for risk, understanding of compliance requirements, and transparency about the significant risks to the enterprise and the embedding of risk management responsibilities into the organisation (ITGI, 2007).

IT risk management identifies the threats to information technology, data, critical systems and business processes (King III Report, 2009). Management has a responsibility to identify areas of control weaknesses and respond in a timely fashion to these by improving processes, augmenting controls and even reducing the cycle time between control testing to ensure the organization identifies and responds properly to IT risks (King III Report, 2009). However, labour and cost constraints mean organisations cannot mitigate all these risk. There is always some degree of residual risk, either unidentified or known but unmitigated. The problem is that many organisations do not understand that managing their IT risk, from the shop floor to the boardroom, is critical to business success. The inherent risks of IT becomes apparent in complex and subtle ways, making IT risk management a difficult concept to communicate and manage effectively (King III Report, 2009; ITGI, 2007). By aggregating and reporting on the impact of security risks within IT and understanding how these risks impact the business, security professionals can become an integral part of the business decision-making process and help guide the organisation to a more risk-aware culture.

- **Performance measurements** track and monitor strategy implementation, project completion, resource usage, process performance and service delivery, using, for example, balanced scorecards that translate strategy into action to achieve goals measurable beyond conventional accounting (ITGI, 2007).

The aim of the performance measurement phase is to make sure there is a common goal of operational and strategic visibility in compliance, IT risk and control environments.

All businesses run on numbers; to make sound IT risk decisions is no different. The first step is to find useful numbers that can be gathered (ideally in an automated fashion); the second is effective measurement, and the third is to communicate those numbers to the business (King III Report, 2009).

For IT risk, it may seem logical to start with metrics generated by IT or information security for performance measurement (King III Report, 2009). However, the King III Report (2009) suggests that organisations should look elsewhere in the business to see the impact of IT operations, effective security and compliance activities. Using the numbers generated by those business units ensures that organisational success is aligned. This way metrics for compliance, performance measurement and risk management are received in a language stakeholders can understand.

By frequently monitoring these numbers, organisations will have real-time situational awareness of compliance and IT risk processes (ITGI, 2007). Long gaps in measurement can potentially undermine both the numbers' validity and the security department's credibility. That is why it is important to automate wherever possible to ensure good quality data without overburdening staff or inefficiently using limited resources.

Frequent measuring of IT risk indicators allows the organisation to spot trends and highlights under- or over-performing areas of the enterprise. The organisation can then target underperforming areas and remediate well in advance so that management can exercise due care (ITGI, 2007).

Once the data is available, it is important to engage those parts of the business that have been tapped for that data (ITGI, 2007). This show cases the value of high-quality IT risk management and provides a platform from which to grow the organisation's influence and involvement in guiding IT risk decisions and improving its overall risk posture.

By assigning a value to the tracking metrics, organisations can build confidence within the business for IT risk decisions.

2.6.3 CHARACTERISTICS OF BUSINESS INFORMATION

The developments in information, computing and communication technologies represent factors which are likely to alter the supply of information (Ritchie and Brindley, 2000: 575). The impact of these characteristic(s) of business information has been shown to have a direct effect on the supply of information (Posthumus and Von Solms, 2004). To address current difficulties of MSEs, which are reluctant to invest in information security, due to cost and security, an international study suggests that MSEs follow a formal approach or model to help protect their information assets (Lee and Jang, n.d: 87).

This may form part of their ICT operational risk governance, which is aimed at assisting the institution (MSE) in managing IT-related risk. In the process of IT governance, it will seek to interrogate (1) confidentiality (2) integrity (3) availability of the IT/IS operation of the institution (4) quality of information and (5) relevance of information, which may include concerns such as unauthorised use, access, disclosure, disruption or changes to the information system. It is information security that ensures on-going confidentiality, integrity and availability of the institutions information (ITGI, 2007). These concepts are discussed in the following section:

- ***Confidentiality***: "Is protection of information, in any form, while in storage, processing or transport from being available to any organisation or person who is not authorized by its owner to have it" (Lee and Jang, n.d:85).

  There is a risk that confidential or sensitive information may be mishandled or made available to those who should not have access to it. In many cases, protection of sensitive information is required by law.

- ***Integrity***: "Ensures that information is accurate and complete in storage and transport; that it is correctly processed and has not been modified in any unauthorized way" (Lee and Jang, n.d:85).

  This is incurred when the underlying data is unreliable because it is incomplete, inaccurate or otherwise suspect. The cause could be deliberate tampering or simple human error.

  Regardless of the cause, the impact to the business can be considerable, especially if the erroneous data is not discovered for some time.

- ***Availability***: "Ensuring that information is available to those who are authorized to have it, when and where they should have it." (Lee and Jang, n.d:85).

- **Relevance:** This type of risk is rarely considered, but is one of the most common types of risks the organisations face. Relevance means that the institution is failing to communicate the right information to the right people, processes or systems at the right time. This often means that the appropriate action is not taken or is taken too late (Ritchie and Brindley, 2000).

- **Quality of information:** Companies must ensure that information is of the highest quality possible. As noted, information quality in part is based on data quality. By studying the research of Stoney (2007) who appears to be one of the foremost researchers in IS data and information quality fields, it became evident that there was no consensus on "…data and/or information *quality…*" (Flowerday and Von Solms, 2005: 4).

For many organisations, characteristic(s) of business information have been a source of funding (Williams, 2005; Posthumus and Von Solms, 2004; Weill and Ross, 2004). This study investigates characteristic(s) of business information involvement and support in ORM adoption in MSEs. Consistent with other studies the Val IT Framework (2006: 18) suggests that: The goal of value governance is to optimise the value of an organisation's IT-enabled investments by: (1) establishing the governance, monitoring and control Framework (2) providing strategic direction for the investments and (3) defining the investment portfolio characteristics.

Similarly, several researchers in recent years have studied the role of the characteristic(s) of business information. Posthumus and Von Solms (2004) found that direct intervention of the characteristic(s) of business information can be considered important in promoting ORM, although the degree of influence on firms may vary from one organisation to another. Posthumus and Von Solms (2004) emphasise that characteristic(s) of business information play a vital role in supporting the pillars of ORM framework. In support of this view, Flowerday and Von Solms (2005: 611) argue that:

> "Based on quality information, a system of internal controls needs to be in place to provide, amongst others, integrity to the information. For these

> controls to be continuously effective, the controls need to be audited to ensure operational efficiency and effectiveness.”

The above studies suggest that an understanding of the roles of the characteristic(s) of business information as facilitator for ORM would flourish and mature the strategic framework for MSEs. Clearly, more evidence is needed to show that characteristic(s) of business information would support ORM adoption.

2.6.4 CHALLENGES POSED BY IT ORM SOLUTIONS

These IT governance focus areas describe the topics that executive management needs to address to govern IT within their enterprises. Operational management uses processes to organise and manage ongoing IT activities (ITGI, 2007). In consequence, building an information system is a process of planned organisational change that must be carefully managed. Therefore, one can better understand system success and failure by examining different patterns of implementation. Yet, other authors maintain that:

> “A temporary construction of an information security management system needs a constant investment whenever new vulnerabilities are discovered. Therefore to achieve objectives of information security investment efficiently and effectively, it is critical to build ISMS which retains consistency in terms of managerial level. In accordance with MSEs and characteristics of MSEs’ informatisation, a development of ISMS which is differentiated from security system for large enterprises possessing enough resources is essential” (Lee and Jang, n.d: 85).

Especially important is the relationship between participants in the implementation process, notably the interactions between system designers and users (Ritchie and Brindley, 2000). Additionally, it is important to note that conflicts between the technical orientation of system designers and the business orientation of end users must be solved (Ritchie and Brindley, 2000). This implies that the success of organisational change can be determined by how well information system specialists, end users, and decision makers deal with key issues at various stages of implementation.

Literature suggests that professionals in the IT field do not view success and failure the same way (Standing *et al*, 2007). This is especially true for IT support workers and executive IT managers (Kritzinger and Smith, 2008; Standing *et al*, 2007). The other significant feature that may be drawn from the study is the change in the adoption and application of ICTs.

Reasons for MSEs not establishing IT facilities are the IT illiteracy of customers or the prohibitive costs quoted by consultants (Kritzinger and Smith, 2008). However, it was evident from qualitative responses that ICT and Internet development were significant features in the thinking of most businesses in terms of future innovations (Standing *et al*, 2007). A result that perhaps indicates that such developments for MSEs are still viewed as an innovative product yet to be fully exploited. It is also evident that wider marketing applications involving database management and relationship marketing strategies have not been fully exploited by the MSEs (Ritchie and Brindley, 2000). Certainly, further exploration of the usage of the ICT by MSEs is necessary.

Yet, post hoc analysis of the interaction effect showed that while there were trends towards IT support and line managers, there was however a significant reversal effect from executive managers who attributed success to global and stable factors (mean = 0.18) more than project failure (mean=0.17), *F*(1, 39) = 3.99, *p*< .05 (Ritchie and Brindley, 2000: 575; Standing *et al*, 2007).

The results and insights from these studies indicate there is a need for the improvement of MSEs performance (Ritchie and Brindley, 2000: 575; Standing *et al*, 2007). IT professionals therefore need to be aware of how they attribute success and failure within IT projects and reflect on their contribution to projects.

2.6.5 EVALUATION MODELS FOR UNDERTANDING THE VALUE OF INFORMATION TECHNOGY RISK MANAGEMENT (ITRM) IN MSEs

An information system can provide business value for a firm in many different ways, including increased profitability and productivity. Some, but not all, of these business benefits can be quantified and measured (cf. Chapter 1: section 2.2) (Balbas, 2007; Froot and Stein, 1998). It has been pointed out that "one of the fundamental roles of banks and other[7] financial intermediaries is to invest in assets which, because of their information-intensive nature, cannot be frictionlessly traded in the capital markets" (Froot and Stein, 1998: 55). The authors indicate that "the standard example of such an illiquid asset is a loan to a small or medium-sized company" (Froot and Stein, 1998: 55). It is imperative to also note that:

> "At the same time that they are investing in illiquid assets, most banks also appear to engage in active risk management programs. Given a fixed capital structure, there are two broad ways in which a bank can control its exposure to risk. First, some risks can be offset by hedging transactions in the capital market. Second, for those risks where direct hedging transactions are

[7] Although financial risk is an entity on its own in terms of risk management in this study it is incorporated part in operational risks due to its implication in ICT risk management.

> not feasible, another way for the bank to control its exposure is by altering its investment policies. Therefore, with illiquid risks, the bank's capital budgeting and risk management functions become linked” (Froot and Stein, 1998: 56).

This reasoning suggests that capital budgeting models are used to determine whether an investment in information technology produces sufficient returns to justify its cost. Arguably, the principal capital budgeting models are the payback method, accounting rate of return on investment, net present value cost, cost benefits ratio, profitability index, and internal rate of return.

“Perhaps because the classical finance approach does not speak to their concerns with risk management, practitioners have developed alternative techniques for capital budgeting” (Froot and Stein, 1998: 57). Other models for evaluating information system investments involve non-financial considerations (Sholes, 2007; Balbas, 2007). It has been argued that another important contribution is the Portfolio Theory (Balbas, 2007). It was suggested that it is possible to maximise the expected return of a portfolio of stocks but the risk level [is] measured by the probability of losing money (Balbas, 2007). Nevertheless, since this probability is bounded from above by using variances and the Tchebycheff inequality, in practical situations, the variance becomes the risk measure once more (Balbas, 2007: 207).

Additionally, portfolio analysis and scoring models can be used to evaluate alternative information system projects. Real option pricing models, which apply the same techniques for valuing financial options to system investments, can also be useful when considering highly uncertain IT investments. Thus, these evaluating models (capital budgeting models) are applicable in large organisations (Froot and Stein, 1998). Although information technology has increased productivity in manufacturing, the extent to which computers have enhanced the productivity of the MSEs remains debatable (Balbas, 2007; Froot and Stein, 1998). In addition to reducing costs, evaluation models may increase the quality of products and services for the consumer or may create an entirely new product(s) and revenue stream. These intangible benefits are difficult to measure and consequently are not addressed by conventional productivity measures (Balbas, 2007).

Consequently, an evaluation model is one of the most important aspects of operation risk management, and financial institution supervisors regard evaluation models as a key element in the regulatory framework (ITGI, 2007; Froot and Stein, 1998).

Recent studies define two major concepts that constitute the critical role of evaluation models in the management of financial institution portfolios (Balbas, 2007; South Africa, 2006).

Firstly, to assess and manage risks, an institution must effectively determine the appropriate evaluation model necessary to absorb unexpected losses arising from its market, credit and operational risk exposures (Froot and Stein, 1998). Secondly, profits that arise from various business activities need to be evaluated relative to capital necessary to cover the associated risks. There are few conceptual explanations on the association between risk management and capital adequacy and even fewer on empirical studies that show the relationship between an evaluation model and ITRM that affects the performance of MSEs (Balbas, 2007; Froot and Stein, 1998).

Yet, others investigated how active management of financial institution exposure through loan sales market (such as the ‘case study’ used in this study) affects capital structure, lending, profits, and risks (Balbas, 2007; Froot and Stein, 1998). Finally, effective risk management strategies should contribute to the financial institution’s ability to assess not only the level of capital it would need in relation to assets and deposits, but also, in principle, mitigate the risk of financial institution failure (Froot and Stein, 1998).

From the literature, it is expected that there will be a relationship between risk management practices and evaluation models. Hence, it is expected that good risk management involves good IT operational risk management.

In the last six years, the Basel Committee on Banking Supervision Theory (2004) of specific models in the values and beliefs that constitute ORM, has gained significant prominence. One of the most important aspects of the Basel Committee on Banking Supervision's (2004) work is that they successfully linked the dimension of ORM to management practice. Other studies support the above study by arguing that:

> "Performance measurement is essential for IT governance. It is supported by COBIT and includes setting and monitoring measurable objectives of what the IT processes need to deliver (process outcome) and how to deliver it (process capability and performance). Many surveys have identified that the lack of transparency of IT's cost, value and risks is one of the most important drivers for IT governance" (ITGI, 2007: 6).

Inferring from the above quote, the IT Governance Institute describe the central concept of IT as having a coherent set of activities with a set of shared core values. ITGI (2007: 17) arguing that "modelling for management and control over IT processes is based on a method of evaluating the organisation, so it can be rated from a maturity level of non-existent (0) to optimised (5)." However, literature notes that in reviewing the progress of the industry in the measurement of operational risk "…causal measurement and modelling of operational risk remains at the earliest stages" (Basel Committee on Banking Supervision, 2004: 2).

Inferring from the above, 'evaluation models' affect the way an organisation operates from its values and its basic underlying assumption to technology diffusion. It is evident that evaluation models of an organisation either facilitate or impede the process of technology diffusion. However, the relevance of this variable in inter-organisational decision making has led the researcher of the current study to include this in the study of ORM adoption.

2.7 THEORETICAL FRAMEWORK: CHAOS AND COMPLEX THEORY

The literature review for this study was conducted for a number of reasons, first being the research objectives and secondly the dominant inferential analysis to reduce the degree of subjectivity to a minimum in the organisational context (cf. Chapter 3 Research Methodology). As Figure 2.3 suggests, when in a chaotic state, the impact of a variable change can be:

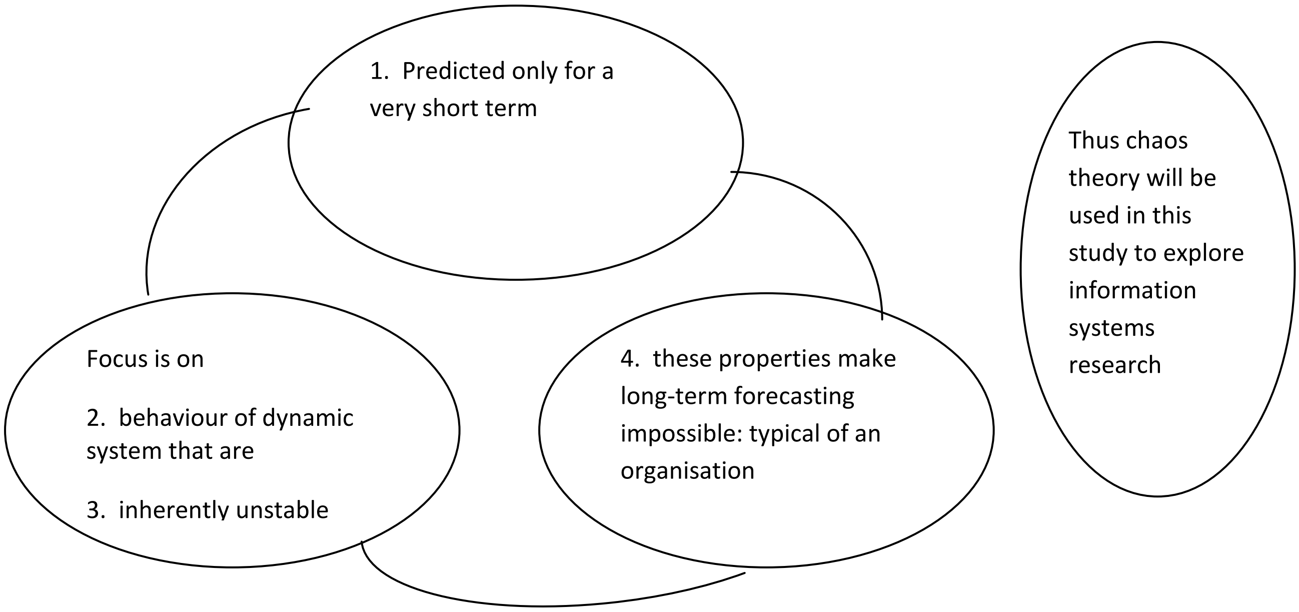

1. Predicted only for a very short term
Focus is on
2. behaviour of dynamic system that are
3. inherently unstable
4. these properties make long-term forecasting impossible: typical of an organisation
Thus chaos theory will be used in this study to explore information systems research

Figure 2.3: Properties of a Chaotic System

This approach depicted by Figure 2.3 is consistent with Thiétart and Forgues' (1995) work on Chaos Theory and information systems. In simple terms, chaos is order without predictability. There are systems (dynamical systems), physical and social, that are well understood (in the sense that they can be fully described by means of a finite set of conditions or rules) and yet are fundamentally unpredictable. Thus, chaos is not anarchy or randomness.

A dynamic system is a recent theoretical approach to the study of development (Hubbard, 2007). In its contemporary formulation, the theory grows directly from advances in understanding complex and non-linear systems in physics and mathematics, but it also follows a long tradition of systems thinking in biology and psychology (Hubbard, 2007). The term dynamic systems, in its most generic form, mean systems with elements that change over time. The more technical use, dynamical systems, refers to a class of mathematical equations that describe time-based systems with particular properties. The value of dynamic systems is that it provides theoretical principles for conceptualising, operationalising, and formalising these complex interrelations of time, substance, and process (Hubbard, 2007). It is a meta theory in the sense that it may be (and has been) applied to different species, ages, domains, and grains of analysis. But it is also a specific theory of how humans gain knowledge from their every day actions.

Although the terms are used in various ways among the general public, many specialists in risk analysis and other quantitative fields have modelled uncertainty and risk more specifically. Hubbard (2007) explains that uncertainty and risk are seen as:

1. **Uncertainty**: The lack of certainty, a state of having limited knowledge where it is impossible to exactly describe an existing state or future outcome, or more than one possible outcome.
2. **Measurement of Uncertainty**: A set of possible states or outcomes where probabilities are assigned to each possible state or outcome.

This also includes the application of a probability density function to continuous variables.

3. **Risk**: A state of uncertainty where some possible outcomes have an undesired effect or significant loss.
4. **Measurement of Risk**: A set of measured uncertainties.

All these models can be unified conceptually in the mathematical notion of a dynamical system, which consists of two parts: the phase space and the dynamics (Hubbard, 2007). The phase space of a dynamical system is the collection of all possible world-states of the system in question. Each world state represents a complete snapshot of the system at some moment in time (Hubbard, 2007). The dynamics is a rule that transforms one point in the phase space (that is, a world state), representing the state of the system now, into another point (= world state), representing the state of the system one time unit later. In mathematical language, the dynamics is a function mapping world states into world states (Hubbard, 2007).

Chaos is order, but it is order that is invisible. What chaos implies is a kind of inherent "uncertainty principle[8]" not just in how we perceive the world but in how the world actually works. While the prediction of chaotic behaviour may be impossible, understanding the order that gives rise to it may not be as difficult as first thought. In other words, highly complex and unpredictable behaviour can be the product of quite simple and accessible rules.

Thiétart and Forgues (1995: 1) argue that "Chaos Theory and properties of chaotic systems are used to suggest a new approach to understand how organisations work." Thiétart and Forgues (1995: 1) maintain that an "organisation is presented as an open, dynamic, nonlinear system subject to internal and external forces which might be sources of chaos." They further argue that Chaos Theory, which has received a great deal of

[8] Readers are advised to read uncertainty principle (Thiétart and Forgues, 1995).

attention from researchers in the natural sciences, is probably difficult to apply to less structured areas such as management.

However, it seems that the qualitative properties of Chaos Theory have an explanatory and integrative power that organisation theories can use to their advantage. Supporting the theoretical framework of this study, Thiétart and Forgues (1995: 22) argue that "the qualitative properties[9] evoked by Chaos Theory, sensitivity to initial conditions, strange attractors, scale invariance, time irreversibility, and bifurcation processes are powerful enough to offer another perspective from which to view the way organisations work."

Thus, the use of this theory in this study explores the relevance of Chaos Theory to information systems research. Chaos Theory focuses on the behaviour of dynamic systems that are inherently unstable and typical of an organisation. Thiétart and Forgues (1995: 21) suggest that:

> "When in a chaotic state, the impact of a variable change can be predicted only for the very short term. This property makes long-term forecasting impossible. In fact, a small initial change, the effect of which multiplies as time passes, can lead to a dramatically different evolution."

McBride (1999) adds that the concept of chaos suggests an absence of organisation, a disorder in which uncertainty and unpredictability predominate. This, as McBride (1999) elucidates, would seem a strange field of study to unite with information systems which is predominately concerned with order. However, McBride (1999) maintains that chaos refers to what might be called ordered disorder, which is a complex

[9] This master's dissertation cannot exhaust the application and relevance of the qualitative properties of Chaos Theory. For further understanding of the theory and related theories, details are provided in Thiétart and Forgues (1995) and McBride (1999).

system. McBride (1999: 2) has this to say about complex systems indicative of chaotic behaviour:

> "… which is not a lack of order, but order of a complexity that is difficult or impossible to describe in simple terms…. The patterns in chaotic behaviour are present, but not regular or easily predictable. While we are considering chaos in the context of organisations, which hold a complexity of human behaviour and action which will give rise to chaotic phenomena, it should be noted that some of the simplest phenomena, can give rise to chaotic behaviour in which changes are chaotic and unpredictable. The concepts of chaos may support a better explanation of organisational behaviour than the more traditional explanations of scientific management because organisations are complex and dynamic phenomenon."

With reference to the works of Tsoukas (1998), Thiétart and Forgues (1995) and McBride (1999), it can be established that organisations do not manifest fixed, predictable behaviour. Rather, their behaviour is non-linear and periodic.

Therefore, Chaos Theory has application in information systems where the effects of an information system within an organisation are often unpredictable and unintentional. This forms the first basis for using Chaos Theory as the theoretical framework of the thesis statement for this study (Thiétart and Forgues, 1995).

In this research, Chaos Theory provides a means of extending the descriptions of information systems and sensitising practitioners and theorists to some of the problems in information systems (cf. Research

Objectives and Research Methodology).

Inferring from Thiétart and Forgues (1995), the term Chaos Theory is widely used to describe an emerging scientific discipline whose boundaries are not yet clearly defined. The terms, complexity theory and complex systems theory as used by McBride (1999), provide a better description of the subject matter, but the term Chaos Theory will be used throughout this study as it is more widely accepted. To understand Chaos Theory in relation to this study, it is imperative to first have a grasp of the terms *system* and *nonlinear*.

The first term, *system*, can be defined as the understanding of the relationship between things that interact. To better understand this idea in relation to the current study, the researcher will examine the case (i.e. the organisation) (McBride, 1999).

2.7.1 ORGANISED CHAOS

An organisation is a system which interacts based upon how it operates. If the initial organisation is not in balance then it faces risk; the interaction results in movement until it find a condition under which it is in balance (McBride, 1999).

This suggests that systems can be modelled. In other words, systems can be created which will theoretically replicate the behaviour of the original system (Thiétart and Forgues, 1995). Following the case for this study, one can take a second group of organisation(s) identical to the first, model them in exactly the same way as the first, and predict that they will operate in the exact same configuration as the first. The question then is how can this be done? This is where Chaos Theory are applied and demonstrated via mathematical modelling. Generally speaking mathematical modelling is the key to modelling systems, although it is not the only way (cf. Chapter 3 Research Methodology and Chapter 4 Findings).

The second term, *nonlinear*[10], has to do with the type of mathematical model used to describe a system. Thiétart and Forgues (1995:20) argue that "nonlinear dynamic system is a system where relationships between time-dependent variables are nonlinear."

Differential calculus[11] (especially stochastic differential calculus) is a mathematical method for showing change in systems within the context of a straight line as a function of time. In this study, statistical multivariate analysis (multivariate regression analysis) in particular, was used (cf. Chapter 3 Research Methodology), in order to convert nonlinear data into a linear format for further analysis and prediction using Chaos Theory (Thiétart and Forgues, 1995). Linear systems are easy to generate and simple to work with since they are predictable. For example, in the current study, the organisation under investigation was thought of as a linear system. It was predicted that if the researcher added a certain number of variables (for instance business characteristics of information) then the researcher would increase the effectiveness produced by the organisation by a comparable amount (cf. Hypotheses and Objectives; Multivariate Analysis).

As cautioned by Thiétart and Forgues (1995) organisations do not operate this way in practice. By changing any variable in the organisation such as the number of people or inventory, one receives widely differing results on a daily basis from what would be predicted using a linear model. This is true because an organisation is actually a nonlinear system, as are most systems found in life. When systems in nature are modelled mathematically, a researcher finds that their graphical representations are not straight lines and that the system's behaviour therefore is not so easy

[10] This system has three types of equilibrium. For further details cf. Thiétart and Forgues (1995: 20); this is out of the scope of this study.

[11] There are various forms: ordinary differential equations, partial differential equations, delay differential equations, stochastic differential equations and differential algebraic equations.

to predict. This anomaly is explained by the qualitative properties of Chaos Theory.

2.7.2 SENSITIVE: DEPENDANCE ON INITIAL CONDITIONS

One of the most essential elements in a complex system, in this case chaos system, is unpredictability. The generator of this unpredictability is what Lorenz (1969) calls *sensitivity to initial conditions*[12], otherwise known as the *butterfly effect*. This concept means that with a complex, nonlinear system, (infinitely) small changes in the starting conditions of a system will result in dramatically different outputs for that system. This phenomenon is commonly known as the butterfly effect. Due to extreme dependence on initial conditions, the general rule for complex systems is that one cannot create a model that will accurately predict outcomes. However, one can create models which simulate the processes that the system will go through to create the models, noting that the concept of sensitive dependence on initial conditions has strong mathematical roots (Casdagli, 1992).

This realisation impacts on many activities in business. For example, it raises considerable questions relating to the value of creating organisational visions and mission statements.

McBride (1998) suggests that no matter how close two conditions start out, after only a few iterations, minor differences will be blown out of proportion. This means that even if initial numbers are entered into the computer with precision, there will still be a certain amount of decimal error. After iterating, McBride (1998) maintains that one quickly notices that a minute error is magnified so that the computed result is actually very far away from the actual results. Thus, a minor error in the initial conditions makes an extremely large difference to the outcome.

[12] cf. Lorenz E. (1969). how much better can weather prediction become? *Technology Rev.,* 39-49. And related work on prediction of weather as chaos theory originated from the study of weather patterns using a mathematical model.

Inferring from the works of Thiétart and Forgues (1995) and McBride (1999), this study summarises the qualities of a chaotic system to be used in the research, which is also consistent with that of Casdagli (1992). A chaotic system has these simple defining features:

- Chaotic systems are deterministic. This means they have some determining equation ruling their behaviour.
- Chaotic systems are sensitive to initial conditions. Even a very slight change in the starting point can lead to significant different outcomes.
- Chaotic systems are not random, nor disorderly. Truly random systems are not chaotic; chaos has a sense of order and pattern; hence organisations equally have predictable behaviour that can be modelled.

In summary, these properties together with the literature reviewed shall be used to further explore ORM in the MSE context (cf. Chapter 4 Discussion). Other studies related to Basel II (2004) suggest that at present several kinds of measurement methods are being developed but no industry standard has yet emerged. In this circumstance, basing MSEs performance on a large financial institution methodology could cause comparability problems because the outcome may differ depending on the method and size of the organisation used. Further, it is not clear if many MSEs in South Africa have the data or methodology yet to perform the necessary estimations. However, by researching the measurement methods that attain a certain level of robustness, it may be possible to establish a set of standards on the basis of which MSEs can secure the overall prudence of the capital framework.

Thus, further work is needed by MSEs to develop a better understanding of the key assumptions of internal measurement techniques (e.g. goodness-of-fit tests) that can be used by MSEs.

2.8 RISK MEASURES

Risk measures attempt to quantify the riskiness of a portfolio. The most popular risk measures such as value at risk describe the right tail of the loss distribution of L_{t+1} (or the left tail). To address this question the researcher investigates whether to look at conditional or unconditional loss distribution and assumes that this has been decided (Balbas, 2007; Rockafellar, Uryasev, and Zabarankin, 2006; Pflug, 2006). For instance, a recent study indicates that:

> "In the European Union the set of rules that the industry must respect are mainly contained in Basle II (banking) and Solvency II (insurance). They provide the way that any corporation must follow in order to compute its "capital reserves", i.e., additional capital that will be devoted to overcome those periods characterized by losses of the economic activity. The size of the appropriate reserve may be considered as the risk level associated with the firm (or its activity)" (Balbas, 2007: 206).

In the same regard, risk measurement is a critical point affecting all major topics such as pricing, hedging, portfolio optimisation and risk management (Balbas, 2007). However, there is no general method to measure the degree of risk of every financial strategy (Balbas, 2007: 205). On the contrary, there are alternative approaches and the use of a concrete method mainly depends on the specific problem (Balbas, 2007).

The Coherent, Expectation Bounded, Convex, Consistent and Multivariate Analyses of risk measures are but a few that have been introduced and studied. There are however many open problems that will have to be addressed in a forthcoming research project. The works of Balbas (2007), and McNeil *et al* (2005) attempt to summarise the achieved findings[13] of their relationships with other mathematical fields with special focus on other usual topics of mathematical finance. Particular attention has been given to: (1) Variance-Covariance Method (2) Historical Simulation Method (3) Monte Carlo Simulation Method (McNeil *et al*, 2005).

Amongst the aforementioned, it is important to acknowledge that it is multivariate risk that is of interest to the current study, the motive being in relation to the research question posed (cf. Research Hypotheses). These might be daily (log) returns in the context of market risk or longer interval returns in credit risk (that is monthly/yearly asset value returns) (McNeil *et al*, 2005).

Burget and Ruschendorf (2006) and McNeil *et al* (2005) recommend testing for multivariate normality, noting that this shall be dealt with in the research methodology chapter. However, it has been cautioned that if data turns out to be multivariate normal then margins must be univariate normal (McNeil *et al*, 2005). This can be assessed graphically with QQplots or tested formally with tests like Jarque-Bera or Anderson-Darling. Nevertheless, the authors suggest that normality of the margins is not sufficient – the researcher must test joint normality[14] (Artzner *et al*, 2007; McNeil *et al*, 2005). Additionally, these should form (approximately) a sample from a distribution, and this can be assessed with a QQplot or tested numerically with, for example, Kolmogorov-Smirnov (also cf. Chapter 3 Research Methodology for detail).

Notwithstanding the aforementioned, there exist deficiencies of multivariate normal for risk factors as authors cautiously indicate (Balbas, 2007; McNeil *et al*, 2004). One author groups them as: (1) tails of univariate margins are thin (thus few extreme values) (2) simultaneous large values in several margins relatively infrequent (3) model cannot

[13] Interested readers are recommended to scan the works of Balbas (2007) and McNeil et al. (2005); noting that this Master's thesis cannot provide entire synopsis on measures of risks.
[14] There is quite extensive application for such suggestions see Balbas (2007), McNeil et al. (2005): Deutsch (2004).

capture phenomenon of joint extreme moves in several risk factors, and lastly (4) very strong symmetry (known as elliptical symmetry) (McNeil *et al*, 2004). To rectify this anomaly for operational reasons, various multivariate tests of assumptions are conducted (cf. Chapter 3 Data Analysis).

2.9 CONCLUSION

Chapter 2 concentrated on a review of relevant literature. In so doing, it addressed MSEs ICT concepts and ORM. What was prominent in this section was that MSEs recognise the need for information security via ORM, but lack a viable model(s) for such processes. The chapter also addressed the evolution of ORM. Other sections include a synopsis on models for understanding the value of ITRM in an MSE, change management requirements for building successful IS, characteristics of business information, risk measures and lastly the theoretical Framework of the study, which focused on chaos and complex theory. Here the writer argued that Chaos Theory, which has received a great deal of attention from researchers in the natural sciences, is probably applicable also to less structured areas such as management.

CHAPTER 3

RESEARCH PARADIGM AND METHODOLOGY

3.1 INTRODUCTION

Chapter 3 looks at the research paradigm[15] and its design. This is followed by a description of the selected designs for this study, namely case study and survey design. The sample, sampling technique and instrumentation as well as the data analysis and interpretation section are addressed. The last section focuses on a summary of multivariate regression of assumptions in data analysis.

3.2 RESEARCH PARADIGM

Due to the research objectives (cf. Chapter 1 section 1.4) and problem statement, this research adopts a positivist paradigm which enables the researcher to adopt a survey design for unit analysis, using a case study as the site. The research paradigm refers to the philosophy of the research process (Creswell, 2007). This includes the assumption and values that serve as a rationale for research and the criteria the researcher uses for interpreting data and reaching conclusions (De Vos, Strydom, Fouché and Delport, 2005). According to De Vos *et al* (2005) the research paradigm must suit the objective or purpose of the study. Bearing this in mind, the researcher deems a post-positivist paradigm suitable for this research. This is necessary as the central knowledge objective is to understand the complex nature of the management of ORM in the Eastern Cape Province and possible strategies that might improve this management. These two objectives demand a post-positivist approach.

[15] In this study paradigm refers to research philosophy.

3.3 RESEARCH DESIGN

This research adopted a case study as well a survey design for different purposes.

3.3.1 CASE STUDY DESIGN

The study was conducted in two phases; one phase followed a case study design, the other, a survey making use of a questionnaire. The ‘case’ in this study was a financial company in the Eastern Cape (cf. Chapter 1 Background of the study). All units within this case form part of the case (managers, implementers, directors, etc) (cf. Appendix A – questionnaire). Building on prior research related to the impact of information technology (IT) and operational risk management (ORM) in the context of MSEs, the current research proposes that there is a relationship between IT operational risk management and performances of MSEs.

The motive for using a case study was to understand the complexity of one organisation. It extends experience or adds strength to what is already known through previous research. Case studies emphasise detailed contextual analysis of a limited number of events or conditions and their relationships (Creswell, 2007). Creswell (2007) notes that case studies are complex because they generally involve multiple sources of data, may include multiple cases within a study, and produce large amounts of data for analysis. Researchers from many disciplines use the case study to build upon theory, to produce new theory, to dispute or challenge theory, to explain a situation, to provide a basis to apply solutions to situations, to explore, or to describe an object or phenomenon. The advantages of the case study method are its applicability to real-life, contemporary human situations and its public accessibility through written reports. Case study results relate directly to the common reader’s everyday experience and facilitate an understanding of complex real-life situations.

3.3.2 SURVEY DESIGN

A survey is used to gather large scale data from a sample of the population (Creswell, 2007). The second phase of the study followed a survey of the units to get their opinions on the operation of IT risk management strategies as per the objectives. The survey allowed the researcher to identify trends in the way certain aspects of IT operation risk management strategies were implemented and how to improve on these. Some of the advantages considered included the virtual elimination of data entry and editing costs (Creswell, 2007). It also adds more accurate answers to sensitive questions. In addition, Creswell (2007) notes those different interviewers can ask questions in different ways, leading to different results. This method overcomes the problem and also ensures that skip patterns are accurately followed, so that participants are not asked questions they should skip based on earlier answers. For that reason response rates are usually higher.

3.3.2.1 SAMPLE SIZE AND SAMPLE TECHNIQUE

The study was conducted at a South African based micro finance company with 90 branches nationally. The company’s product range includes unsecured loans, secured loans, insurance, cellular and educational products. The products are sold through its various channels: branches, telesales call centres and agents.

From the review of literature, an instrument (closed -ended questionnaire) was developed with the aim of covering the research objectives (cf. Chapter 1 section 1.4). In terms of sample size calculation, Tabachnick and Fidel (2001) recommend a formula for calculating sample size requirements, taking into account the number of independent variables that a researcher wishes to use; $n \geq 50 + 8m$ ($m =$ number of independent variables). Due to the hypotheses posed (cf. Chapter 1 section 1.3 and

Fig 1.1, Hypotheses), questionnaires were sent to a minimum of n=90 respondents[16] of the MSE according to a simple random sampling plan.

3.3.2.2 INSTRUMENTATION

The questionnaire was adapted and administered online electronically based on the hypotheses, objectives and contestations from literature (cf. Chapter 2 Literature Review). First, the research instrument sought information about basic demographics (Creswell, 2007). In order to address the hypotheses, one of the parts addressed the principal causes of ORM failure in MSEs. It also addressed the change management requirements for building successful systems-risk monitoring and reporting of ORM in an MSE (Creswell, 2007). Next were characteristic(s) of business information and this was followed by the challenges posed by new ORM solutions and evaluating models for understanding the value of IS in an MSE. This was done by identifying the traditional and modern capital budgeting models and their drivers/impact on business processes (risky elements).

Creswell (2007) argues that the motive for using a questionnaire is that often it is the only feasible way to reach enough respondents to allow statistical analysis of results. A well-designed questionnaire can gather information on the overall performance of the test system as well as information on specific components of the system (Creswell, 2007). If the questionnaire includes demographic questions on the participants, the resultant data may be used to correlate performance and satisfaction with the test system among different groups of users.

There is no all-encompassing rule for using a questionnaire. The choice will be made based on a variety of factors including the type of information to be gathered and the available resources for the experiment. According

[16] N>50 + 8m (m=5 number of independent variables) = 90: Note that it was anticipated that more cases were used to cater for any possible skewness for dependent variable such that the distribution of data satisfies the assumptions of multiple regression related to sample size.

to Creswell (2007) a questionnaire should be considered in three main parts:

When resources and money are limited: A Questionnaire can be inexpensive to administer. Although preparation may be costly, any data collection scheme will have similar preparation expenses. The administration cost per person of a questionnaire can be as low as postage and a few photocopies. Time is also an important resource that questionnaires can maximize. If a questionnaire is self-administered, such as an e-mail questionnaire, potentially several thousand people could respond in a few days. It would be impossible to get a similar number of usability tests completed in the same short time.

When it is necessary to protect the privacy of the participants: Questionnaires are easy to administer confidentially. Often confidentiality is necessary to ensure participants will respond honestly if at all. Examples of such cases would include studies that need to ask embarrassing questions about private or personal behavior.

When corroborating other findings: In studies that have resources to pursue other data collection strategies, questionnaires can be a useful confirmation tool. More costly schemes may turn up interesting trends, but occasionally there will be no resources to run these other tests on large enough participant groups to make the results statistically significant. A follow-up large scale questionnaire may be necessary to corroborate earlier results.

3.4 DATA ANALYSIS AND INTERPRETATION

The questionnaires received were analysed using SPSS for correlation and multiple regression analysis to predict ORM adoption based on the parts mentioned. In line with the principles of multivariate data analysis, the researcher conducted a zero-order correlation of the independent and dependent variables. The correlation provided directional support for predicted relationship and showed that co linearity among the independent variables was sufficiently low so as not to affect the stability of regression analysis. This also included the test of various assumptions[17] such as normality and multi co linearity (cf. Chapter 4 Table 4.5: Analyses of Hypothesis 3)**.**

During the analysis, operational risk divided into a number of sub risks using business lines and risk categories defined by the institution. In each subsection ORM data was collected and robust estimation techniques as indicated were used (cf. Chapter 4 Presentation of data).

3.4.1 MULTIVARIATE REGRESSION

Generally, multivariate regression explains the relationship between multiple independent or multiple predictor variables and one dependent or criterion variable (cf. Chapter 1 section 1.4: Hypotheses). In multiple regressions, a dependent variable is modeled as a function of several independent variables with corresponding multiple regression coefficients, along with the constant term (Tabachnick and Fidell, 2007). Multiple regressions require two or more predictor variables, and this is why it is called multiple regression (Tabachnick and Fidell, 2007). The multiple regression equation explained above takes the following form:

$$y = b_1x_1 + b_2x_2 + \ldots + b_nx_n + c.$$

In the multivariate case, when there is more than one independent variable, the regression line cannot be visualised in the two dimensional space, but can be computed just as easily. It could construct a linear equation containing all those variables.

Here, b_i's (i=1, 2…n) are the regression coefficients, which in multiple regression represents the value at which the criterion variable changes when the predictor variable changes (Tabachnick and Fidell, 2007) (cf. Chapter 2 section 2.7: Theoretical framework: Chaos Theory). For the purpose of the current study, there are certain terminologies that help in

[17] For details see Tabachnick and Fidel (2007).

understanding multiple regression (Tabachnick and Fidell, 2007). These terminologies are as follows.

The beta value in multiple regression was used in measuring how effectively the predictor variable influenced the criterion variable (cf. Chapter 4 Table 4.6: Analyses of Hypothesis 4) (Tabachnick and Fidell, 2007). In multiple regression (cf. Chapter 4), it is measured in terms of standard deviation (Tabachnick and Fidell, 2007).

R in multiple regression is the measure of association between the observed value and the predicted value of the criterion variable (Tabachnick and Fidell, 2007). It also makes provision for degree of freedom. R Square, or R^2, in multiple regression is the square of the measure of association which indicates the percentage overlap between the predictor variables and the criterion variable (cf. Chapter 4 Table 4.6: Analyses of Hypothesis 4) (Tabachnick and Fidell, 2007). Adjusted R^2 in multiple regression is an estimate of the R^2 if one uses this model with a new data set (Tabachnick and Fidell, 2007).

3.4.1 ASSUMPTIONS OF MULTIPLE REGRESSION

There should be proper specification of the model in multiple regression (Tabachnick and Fidell, 2007). This means that only relevant variables must be included in the multiple regression model (Tabachnick and Fidell, 2007). This means that in multiple regression the model should be reliable (Tabachnick and Fidell, 2007).

Assumption of Linearity

First of all, as is evident in the name multiple regression, it is assumed that the relationship between variables is linear. In practice this assumption can virtually never be confirmed; fortunately, multiple regression procedures are not greatly affected by minor deviations from this assumption (Tabachnick and Fidell, 2007). Linearity must be assumed in multiple regression (Tabachnick and Fidell, 2007).

Normality Assumption

Normality is assumed in multiple regression (cf. Chapter 2, section 2.2: Risk Measures). This means that in multiple regression, variables must have normal distribution. It was assumed in multiple regression that the residuals (predicted minus observed values) were distributed normally (i.e., follow the normal distribution) (Tabachnick and Fidell, 2007) (cf. Chapter 2 section 2.3: Risk measures). Again, even though most tests (specifically the F-test) are quite robust with regard to violations of this assumption, it is always prudent, before drawing final conclusions, to review the distributions of the major variables of interest. In this case the researcher produced the Kolmogorov-Smirnov (KS) test (use KS test-cf.ch 2 section 2.3 Risk measures) in order to inspect the distribution of the residual values (Tabachnick and Fidell, 2007) (cf. Table 3.1: Tests of Normality).

Table 3.1: Tests of Normality

Tests of Normality

Position	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Stats	df	Sig.	Stats	df	Sig.
Middle Mgt	.392	13	.000	.628	13	.000
Senior Mgt	.397	38	.000	.678	38	.000
Operations	.313	56	.000	.771	56	.000

a. Lilliefors Significance Correction

The test for the KS test is denoted by D and Middle Mgt, D(13) = 0.39, *p= 0.*000*;* Senior Mgt D(38) = .40, *p= 0.*000 and Operations D(56) = 0.313, p= 0.000, were all significantly normal. Although this is so, Fidell (2009) suggests that it is common in large sample size.

Homoscedasticity

Homoscedasticity must be assumed in multiple regression. This means that in multiple regression, the variance is constant across all levels of the predicted variable (Tabachnick and Fidell, 2007).

Multicollinearity and Matrix Ill-Conditioning

This is a common problem in many correlation analyses. This results from having two predictors and then having to decide which one of the two measures is the better predictor (Tabachnick and Fidell, 2007) (cf. Chapter 2 section 2.7: Theoretical Framework: Chaos Theory). This is exactly what would be done when performing a multiple regression analysis, a dependent (Y) variable (performance of MSEs) and the two (or more) measures of independent (X) variables. When there are many variables involved, it is often not immediately apparent that this problem exists, and it may only manifest itself after several variables have already been entered into the regression equation (Tabachnick and Fidell, 2007).

Nevertheless, when this problem occurs it meant that at least one of the predictor variables is completely redundant (Tabachnick and Fidell, 2007). There are many statistical indicators of this type of redundancy (tolerances, semi-partial R, etc.,) as well as some remedies (e.g. Ridge regression). In this case, Tolerance was used to test for multi co linearity and was seen as satisfactory (cf. Chapter 4 Table 4.5: Analyses of Hypothesis 3).

Stepwise Regression[18]

Forward stepwise selection begins with independent variables being entered into the regression equation one at a time, provided predictors meet the statistical significance criteria with the dependent variable (Tabachnick and Fidell, 2007). In this case the selection of independent variable entry was based on descending order of the largest significant

[18] Refer toTabachnick and Fidel, (2001) for details.

correlation coefficient. Independent variables were entered into the regression until an independent variable did not uniquely influence the dependent variable.

Tabachnick and Fidell (2001: 144) state that “stepwise regression is a model-building rather than a model-testing procedure. As an exploratory technique, it was useful for such purposes as eliminating variables that are clearly superfluous in order to tighten up future research.”

3.5 ENSURING RELIABILITY AND VALIDITY

The researcher used the Cronbach alpha technique to assess the reliability coefficient (cf. Chapter 4 Table 4.1c: Zero-order correlation between). In order to ascertain face validity, an initial questionnaire (research instrument) was passed through routine editing. It was given to experts (academics, practitioners and business managers) who were asked to respond to the questionnaire and, based upon their comments; the questionnaire was reworded to enhance clarity. Convergent validity was measured by the average variance extracted for each construct during the reliability analysis, 0.5 (50 percent) or better. To further analyse for convergent and discriminating validity of any constructs of ORM used, the principal component method with varimax rotation was used to assess the variance explained (cf. Chatper 4 Table 4.1c: Zero-order correlation between). This was to ensure that in general, results demonstrated that, both validities were satisfied.

Ethical Consideration

Ethical considerations such as voluntary participation, confidentiality and anonymity were deemed necessary at all times. Additionally, the questionnaire on which the model(s) was developed was cross approved by the institution’s chief information officer (CIO).

Measures to Ensure Trustworthiness

Creswell (2007) defines trustworthiness as the way in which the inquirer is able to persuade the audience that the findings are worth paying attention to and that the research is of a high quality. Creswell (2007) further states that trustworthiness is further divided into:

- credibility – which corresponds with the positivist concepts of internal validity and dependability, which relates more to reliability
- transferability – which is a form of external validity
- confirmability – which is largely an issue of presentation.

De Vos *et al* (2005) agree with Creswell (2007) and assert that the key criteria for trustworthiness are credibility, applicability, dependability and confirmability.

3.6 CONCLUSION

Chapter 3 looked at the research paradigm and its design. This was followed by a description of the selected designs, namely case study and survey design. The sample, sampling technique and instrumentation, as well as the data analysis and interpretation section were discussed. The last section focused on a synopsis on multivariate regression and its assumptions highlighting the data analysis method.

CHAPTER 4

PRESENTATION OF RESEARCH FINDINGS

4.1 INTRODUCTION

This chapter presents the findings of the empirical investigation carried out in this study. In consequence, it addresses findings related to the factors impacting on IT and operational risk management within MSEs. The chapter commences with an overview of the specific research questions, statistical techniques, demographics of respondents and data reduction technique, factor analysis. The chapter concludes with the analysis of each research finding based on the hypotheses/objectives posed in chapter 1.

4.2 SPECIFIC RESEARCH QUESTIONS

Building on prior research related to: (1) impact of information communication technology (ICT) and (2) operational risk management (ORM) in the context of MSEs, the focus of this study was to investigate the relationship between: (1) ICT ORM and (2) performances of MSEs. The research identified and determined five specific research objectives:

- Analysing the principal causes of IT ORM failure in MSE.
- Assessing the change management requirements for building successful ICT systems in an MSE.
- Identifying which characteristic(s) of business information plays a major role in supporting an organisation’s business operations.
- Identifying the challenges posed by new solutions in IT ORM.
- Evaluating models for understanding the value of IT ORM in MSE.

Consequently, an ICT operational risk model for MSEs was discussed and developed (cf. Chapter 5). Following the research objectives and the reviewed literature, the hypotheses that emerged included:

(H1) that there is a significant relationship between principal causes of ICT failure and ORM adoption

(H2) that there is a significant relationship between change management requirements and IC ORM adoption

(H3) that there is a significant relationship between characteristic(s) of business information and ORM adoption

(H4) that there is a significant relationship betweenchallenges posed by ORM and ICT solutions, and lastly

(H5) that there is a significant relationship between evaluation models and likelihood of IT ORM adoption within MSEs.

To analyse the hypotheses, various statistical techniques (multiple regression, factor analysis and multivariate analysis of variance) were deemed appropriate (cf. Chapter 3 section 4.3).

4.3 STATISTICAL TECHNIQUES

Simple descriptive and inferential statistical methods were incorporated into the SPSS programme for analysing the data. The variables were precoded for entry into the programme (Tabachnick, 2008; Tabachnick and Fidell, 2007).

Despite the fact that the variables were descriptive in nature, they were assigned numeric codes to facilitate different statistical analyses (Meyers, Gamst and Guarino, 2006). Some of the measurement levels (scale of measurement) were nominal and others ordinal (cf. Appendix A – questionnaire). After the data had been checked, the codes were entered into the programme and the process of data cleaning ensured.

Appropriate statistical procedures were then performed. Frequency counts and percentages were applied to the data relating to the demographic details of the respondents in order to determine the distribution of gender, age group, position, department and level of education. A bivariate analysis between the respondents demographic characteristics and the relationship between ICT operational risk management and performances of MSEs, was performed.

Factor Analysis was used to reduce a large number of related variables (cf. Questionnaire - Appendix A, and Table 4.2: KMO and Bartlett's Test and Table 4.3: Factor loadings after rotation: Component Matrix) to a more manageable number, prior to using them in other analyses such as multiple regression or multivariate analysis of variance (MANOVA) (Raykov and Marcoulides, 2008; Tabachnick and Fidell, 2007).

In order to understand the degree of association between the performances of MSEs and the independent variables, multiple regression, Repeated-Measures Analysis of Variance[19] (RM-ANOVA) and Repeated-Measures Multivariate Analysis of Variance (RM-MANOVA) were performed (Cody and Smith, 2005). Where a significant value was observed, either Betas of multiple regression or significant levels of RM-ANOVA or RM-MANOVA ascertained these differences (Tabachnick and Fidell, 2007). The outcomes of these analyses are described in subsequent sections.

One of the objectives of this study was to find the factors predicting ICT operational risk within MSEs. Multi-item constructs were used to capture the information about various types of variables to adopt ICT operational risk. Multi-items construct of the instrument were used. Table 4.1a and 4.1b included items with their descriptive statistics. To assess as seen in

[19] A four point Likert scale also cf. questionnaire

the questionnaire a construct was used to measure five main support items (cf. Chapter 1 section 1.4, Chapter 2 Table 4.1c).

The study was based upon a survey design to collect the primary data from 107 respondents using the simple random sampling technique. A one stage normative model associative in nature was developed based upon review of previous researches and in line with the research objectives (cf. Chapter 5 Figure 5.1). The model elicited five factors (cf. Table 4.1c and Chapter 1 section 1.3 and 1.4).

4.4 DEMOGRAPHICS OF RESPONDENTS

The demographics of the respondents are presented in Tables 4.1a and 41b. A total of 107 human resource (HR), IT, finance, operations and support staff participated in the study. This and other details are presented in Table 4.1a.

Well over half (62.6%) of the sample was male. IT personnel constituted 60.7%. Among three main levels of appointment, only 12.1% respondents were middle management. The majority (52.3%, n=56) constituted operations staff. The majority (36.4%) of participants were in the 26 to 30 years age range (*M* = 25.5, *SD* = 7.94), with 41 to 45 years constituting 2.7% of respondents.

Table 4.1a: Demographic characteristics of respondents

Demographics	Frequency	Percentage
Gender		
Male	67	**62.6**
Female	40	37.4
Total	107	100.0
Department		
IT	**65**	**60.7**
HR	6	5.6
Finance	25	23.4

Operations	11	10.3
Total	107	100.0
Position		
Middle Management	**13**	**12.1**
Senior Management	38	35.5
Operations	56	**52.3**
Total	107	100.0
Age (years)		
20-25	15	14.0
26-30	**39**	**36.4**
31-35	31	29.0
36-40	11	10.3
41-45	**3**	**2.7**
46 or more	8	7.5
Total	107	100.0

The sample as a whole was relatively old in terms of years of services (More than 5 years, 35.5%, n=38). The least years of service was n=5 respondents (Less than 1yr, 4.7%). Most (33.6%, n=36) had a Diploma as a level of educational qualification, noting that 19.6% (n=21) constituted postgraduate employees (cf. Table 4.1b: Demographic characteristics of respondents for other details).

Table 4.1b: Demographic characteristics of respondents

Years of services	**Frequency**	**Percent**
Less than 1yr	**5**	**4.7**
2yrs	17	15.9
3yrs	13	12.1
4yrs	22	20.6
5yrs	12	11.2

More than 5 years	**38**	**35.5**
Total	107	100.0
Education		
Less than	2	1.9
Matric	15	14.0
Matric	36	33.6
Diploma	33	30.8
Degree	21	19.6
Post graduate	107	100.0
Total		

In line with the principles of multivariate data analysis (cf. Chapter 3 multivariate data analysis assumptions), the researcher conducted a zero-order correlation between the independent and dependent variables (cf. Table 4.1c). The correlation provided directional support for the predicted relationship and showed that co linearity among the independent variables was sufficiently low (> or = .6) so as not to affect the stability of regression analysis (Tabachnick and Fidell, 2007).

Table 4.1c: Zero-order correlation

Constructs	**No of items**	**a value (0.60 or >)**	**Mean**	**Variance explained**
Principal causes of ORM failure related to ICT	5	0.82	3.04	0.59
	4	0.67	3.78	0.75
Change management requirements and ICT Risk				
	5	0.86	3.59	0.71

Characteristic(s) of information influences ICT Risk				
	4	0.84	3.04	0.57
Challenges posed by ORM solutions				
Evaluation models affecting ICT adoption within MSEs	6	0.60	3.52	0.57

4.4.1 INSTRUMENT RELIABILITY, VALIDIDTY AND MULTI-CO LINEARITY

Several techniques were used to assess (a) the reliability coefficient (cf. Table 4.1c) (Cronbach, 1951) and (b) face and construct validity.

In order to ascertain face validity, an initial questionnaire was passed through routine editing, after it was given to a panel of experts (some of whom included academics, practitioners or business managers and colleagues).

In general, validity refers to the degree to which an instrument truly measures the constructs it is intended to measure. There are several types of validity measures, including face validity and construct validity. Fidell (2009) proposed two types of validity: convergent and discriminating validity. Convergent validity is measured by average variance extracted for each construct during the reliability analysis that should be 0.5 or 50 percent or better (cf. Table 4.1c).

The results showed that all the constructs had considerable validity support (cf. Table 4.1c). To further analyse for convergent and discriminating validity of these five constructs, the principal component method with varimax rotation was used to assess the variance explained. In general, results show that both validities are satisfied.

All factors (within MSEs) are significantly correlated with ICT adoption. It was also found that none of the variables were highly inter-correlated, so the problem of multi-co linearity did not exist, thus fulfilling Fidell's (2009) criterion that for variables to qualify for multi co linearity they should have a coefficient of correlation of 0.6 or more (cf. Table 4.1c).

Prior to the regression analysis, data were screened for outliers and cases with a standard deviation greater than 2 were removed. The result of a stepwise regression analysis was presented in section 4.5. The current chapter confirmed the above result of multi co linearity (cf. Table 4.5: VIF and Tolerance). In conclusion, the data in Table 4.1c indicated that five independent variables significantly contributed towards regression equation.

For further analysis, the effect of multi-co linearity was studied by examining the VIF values for each of the regression coefficients (cf. Chapter 3: assumptions of multivariate regression and section 4.5). It was found that values for all the coefficients were less than 0.1 (cf. Table 4.5: Tolerance) and averages of VIF were close to 1 and as such multi-co linearity would not to distort the regression analysis (Fidell, 2009). Additionally, the models (i.e. regression coefficients) with a high and significant *F* ratio indicate a good fit of the model and are statistically significant in explaining the adoption of ICT operation by MSEs. The (beta) (standardised coefficient) indicates the relative importance of the independent variables in explaining the adoption of ICT operation by MSEs (for instance cf. Table 4.4 or 4.5).

4.4.2 DATA REDUCTION TECHNIQUE: FACTOR ANALYSIS (FA)

FA sought to answer the question: ‘What is the underlying factor structure of IT ORM measures that influence MSEs as proposed by the current study’s instrument? The items of IT ORM measuring the influence of MSE were subjected to FA - Principal Component Analysis (PCA) - using SPSS version 18.

Prior to performing PCA, the suitability of data for FA was assessed. Inspection of the correction matrix revealed the presence of many coefficients of .3 and above. The Kaiser-Meyer value was acceptable (cf. Table 4.2), exceeding the recommended value of .6 (Pallant, 2005) and the Barlett’s test of sphericity (Pallant, 2005) reached statistical significance, supporting the factorability of the correlation of the matrix.

A PCA was conducted on 24 items with orthogonal rotation (varimax). The Kaiser-Meyer-Olkin (KMO) measure verified the sampling adequacy for the analysis, KMO = .61 (Fidell, 2009), and all KMO values for individual items were > .70, which is well above the acceptable limit of .5 (cf. Table 4.2: KMO and Bartlett's Test). As mentioned, Barlett’s test of sphericity X^2 (276) = 783.39, *p* = .000, indicated that correlations between items were significantly large for PCA, which was satisfactory (cf. Table 4.2: KMO and Bartlett's Test).

Table 4.2: KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.612
Bartlett's Test of Sphericity	Approx. Chi-Square	783.393
	Df	276
	Sig.	.000

An initial analysis was run to obtain Eigenvalues of each component in the data. Five components had Eigenvalues over Kaiser’s criterion of 1 and in combination explained 65.97% of the variance. The scree plot showed inflexions that would justify retaining the five components. Given the large sample size, and the convergence of the scree plot on five components, this was the number of components retained in the final analysis (Fidell, 2009). Table 4.3 shows the factor loadings after rotation. The items that cluster on the same components[20] suggest that component 1 represents X, component 2 Y, component 3 Z, component 4 K and component 5 L (cf. Table 4.3: Factor loadings after rotation: Component Matrix).

[20] X- principal causes of ORM failure related to ICT

Y- change management requirements and ICT Risk

Z- characteristic(s) of information influences ICT Risk

K- challenges posed by ORM solutions

L-evaluation models affecting ICT adoption within SMEs

For details cross reference appendix A -questionnaire

Table 4.3: Factor loadings after rotation: Component Matrix

	Component				
	1	2	3	4	5
Q7	.718				
Q8	.711				
Q9	.701				
Q10	.655				
Q11	.584				
Q12		.583			
Q13		.514			
Q14		.499			
Q15		.427			
Q16			.640		
Q17			-.519		
Q18			.327		
Q19			301		
Q20			.333		
Q21				.454	
Q22				-.402	
Q23				-525	
Q24				.400	
Q25					.460
Q26					.425
Q27					.402
Q28					.602
Q29					.505
Q30					.331

Extraction Method: Principal Component Analysis

4.5 RESEARCH FINDINGS (HYPOTHESES/OBJECTIVES)

In this subsection the data is presented per research hypotheses, starting with research hypothesis 1.

4.5.1 RESEARCH HYPOTHESIS 1

There is a significant relationship between the principal causes of ICT failure and ORM adoption. To answer this hypothesis, the following questions are addressed: (1) how well do the measures of principal causes of ICT failure predict ORM adoption within MSEs and (2) which is the best predictor of principal causes of ICT failure? This section also sought to name and describes generally the principal causes of ICT failure in MSEs.

On analysing the principal causes of ICT failure and ORM adoption, the distribution reveals that 32.7% (n=35) of respondents strongly agree that one of the principal causes of information system failure is insufficient or improper user participation in the systems development process. Meanwhile, 60.7% (n=65) agree and 6.5% (n=7) disagree. While, 69.2% (n=74) agree with the statement that one of the principal causes of information system failure is lack of management support, 29.9% (n=32) disagree. Noting that 23.4% (n= 25) strongly agree that the principal causes of information system failure are high levels of complexity and risk in the systems development process. Meanwhile, 59.8% (n=64) agree. Very few (0.9%) strongly disagree, while, 15.9% (n=17) disagree.

The majority (48.6%, n=52) agree that one of the principal causes of information system failure is the process of organisational change surrounding the new system. However, 18.7% (n=20) strongly agree, while 31.8% (n=34) disagree and only 0.9% (n=1) strongly disagree.

Most respondents 76% (n=82) agree that one of the principal causes of information system failure is poor management of the implementation process, while 22.4% disagree.

Additionally, as evidenced in the distribution, different departments had varying levels of agreement regarding insufficiency or improper user participation in the systems development process. For instance, from IT 59 out of 65 agree; all (6 out of 6) of HR personnel agree; as do Operations personnel (11 out of 11). As evidenced in the distribution, different departments have varying levels of agreement regarding lack of management support. While 39 out of 64 agree with the statement, and 5 out of 6 agree for HR, nearly all Operations (10 out of 11) agree.

Further evidence suggests that different departments have varying levels of agreement regarding the statement about high levels of complexity and risk in the systems development process. Once more, 51 out of 65 IT personnel agree. While all HR and operations (6 out of 6; 11 out of 11 respectively) agree and 21 out of 25 personnel from finance agree.

By implication, there seems to be ample evidence that the principal causes of ICT failure and ORM adoption are insufficient/improper user participation in the systems development process, lack of management support, high levels of complexity and risk in the systems development process, process of organisational change surrounding new system and lastly poor management of the implementation process. The next section (Analyses of Hypothesis 1) addresses or tests for the significance of the decision made by respondents.

- **Analyses of Hypothesis 1: There is a significant relationship between principal causes of ICT failure and ORM adoption.**

To answer hypothesis 1, two questions were posed; (1) how well do the measures of principal causes of IT failure predict ORM adoption within MSEs and (2) which is the best predictor of principal causes of IT failure? Multiple regression analysis was used to test for the significant predictors of principal causes of ORM failure related to ICT. It was indicated that ' A[21]' significantly predicted ICT operations [β= -.38, *t*(210) = 6.03, *p*< .01]. 'A' also explained a significant proportion of variance [R^2 = .13 (13%), *F*(1, 210) = 41.04, *p*< .01]. This confirmed that 'A' in the first hypothesis was accepted. By implication ICT operation control would become more effective if efforts were targeted towards 'A'.

[21] cf. SECTION H1: Principal causes of ICT failure and ORM adoption in appendix A - Questionnaire; One of the principal causes: A = of information system failure is insufficient or improper user participation in the systems development process.

However, a mixed-design analysis of variance (ANOVA) with gender (male, female) as a within-subjects factor and ICT operation principal causes of ORM failure related to ICT and position as between-subjects factors, did not reveal the main effect of gender [*F*(1, 1250) = 1300, *p*>.05, ηp2 = .003]. This was qualified by interactions between gender and departments [*F*(2, 1250) = 6.50, *p*> .05, ηp2 = .021]. The predicted interaction among gender, ICT operation and position use was not significant [*F*(2, 1250) = 0.07, *p*> .05, ηp2 < .01]. All other main effects and interactions were non-significant and irrelevant to the hypothesis with all *F* ≤ 0.95, *p*≥ .40, ηp2 ≤ .001.

In conclusion, the results of the analysis presented above allowed the researcher to answer the two questions posed at the beginning of this subsection. The model, which includes five sub variables[22], explains 13% (R^2 = .13) of the variance in principal causes of ICT failure as predictor of ORM adoption within MSEs. Of the five sub variables, 'A' makes the largest unique contribution (β= -.38, *p*< *.05*); although, the rest made some contribution, these do not reach statistical significance in terms of contributions (*p*> *.05*).

4.5.2 RESEARCH HYPOTHESIS 2

There is a significant relationship between change management requirements and IT ORM adoption in MSEs. This subsection sought to interrogate the issue of organisational change surrounding a new information system in MSEs. Thus, the motive was to answer the questions, (1) how well do the measures of change management requirements predict ORM adoption within MSEs (2) Which is the best predictor of change management requirements?

Generally, amongst the participants who responded to levels of agreement with regards to factors influencing change management requirements and IT ORM adoption within MSEs, it was noted that while

[22] cf. sub variables on "principal causes of IT failure."

15.9% (n=17) strongly agree, 33.6% (n=36) agree, 46.7% (n=50) disagree while 2.7% (n=3) strongly disagree.

About a quarter (25.2%, n=27) strongly agree that enterprise applications are difficult to implement successfully, because they usually require far-reaching changes to business processes. A little under two-thirds (70%, n= 65) agree. While, 11.2% (n=12) disagree and 1.9% (n=2) strongly disagree.

Nearly three-quarter (72.0%, n=77) agree that the success of organizational change can be determined by how well information system end users deal with various stages in the implementation of ICT projects. But 15.0% (n= 16) strongly agree and 13.1% (n= 14) disagree.

About one-fifth (20.6%, n=22) strongly agree that the success of organisational change can be determined by how well information systems decision makers deal with various stages in the implementation of ICT projects. Noting that 36.4% (n=39) agree, 38.3% (n=41) disagree and 3.7% (n=4) strongly disagree. In summary, it can be said that the majority agree that change management requirements and ICT ORM adoption are impacted by the above measures.

Meanwhile as evidenced in Table 4.4, nearly equal portions of respondents from ICT personnel had varying views. Thus, while 20 out of 65 agree, 33 out of 65 disagree.

Table 4.4: Analysis of Hypothesis 2

Count						
		There is a high failure rate among enterprise application projects because they require extensive organisational change that is often resisted by member of the organisation				
		Strongly Disagree	Disagree	Agree	Strongly Agree	Total
Department	IT	3	33	20	9	65
	HR	0	2	3	1	6
	Finance	0	13	8	3	24
	Operations	0	2	5	4	11
Total		3	50	36	17	106

- **Analysis of Hypothesis 2: There is a significant relationship between change management requirements and ICT ORM adoption.**

  In answering the hypothesis, (1) how well do the measures of change management requirements predict ORM adoption within MSEs and (2) which is the best predictor of change management requirements? Multiple regression analysis was utilised to determine the percentage contribution of some of the identified significant predictors of change management requirements and ICT risk management adoption in MSEs. The distribution revealed that only one variable made significant percentage contributions to the level of change management requirements and ICT Risk. This was; ‘A’[23] (β = 0.291, $p < 0.05$).

[23] cf SECTION H2: Assess change management requirements and ICT risk: appendix A

A = One of the principal causes of information system failure is insufficient or improper user participation in the systems development process

It may thus be inferred that ‘A’ is the only variable, prominent in explaining the variation in change management requirements and ICT Risk. The variable has a correlation of 0.85. The R^2 value also suggests that the variable contributed approximately 55.2 percent of the variations in level of change management requirements and ICT operation. The analysis of variance also revealed that the regression coefficients are real and did not occur by chance.

In conclusion, the results of the analysis presented above allow the researcher to answer the two questions posed at the beginning of this subsection. The model, which includes five [24] sub variables, explains 55.2 percent of the variance of ORM adoption within MSEs. Of the five sub variables, ‘A’ makes the largest unique contribution ($\beta = 0.291$, $p < 0.05$); although the rest made some contribution, these do not reach statistical significance in terms of contributions ($p > .05$).

It may therefore be inferred that relatively, ‘A’ actively impacts on change management requirements and ICT operation. By implication, there seems to be enough evidence to suggest that change management requirements and ICT risk in an MSE would become more effective if efforts were targeted towards ‘A’.

4.5.3 RESEARCH HYPOTHESIS 3

The object of this objective was to answer the question, (1) how well do the measures of Information characteristics predict ORM adoption within MSEs and (2) Which is the best predictor of information characteristics? Consequently, determine the significant relationship between information characteristics and ICT ORM adoption in an MSE.

About 51.4% (n=55) strongly agree that confidentiality of information has a direct relationship on their work performance. 40.2% (n=43) agree and 8.4% (n=9) disagree.

[24] cf. sub variables on “principal causes of IT failure”

About one-half (50.5%, n=54) strongly agree that integrity of information has a direct relationship with their work performance. Nearly one-half (46.7%, n=50) also agree and just 2.7% (n=3) disagree.

While 94.4% (n=101) agree that the impact of the availability of information has a direct relationship on their work. Just 4.7% (n=5) disagree.

About 84.1% (n=90) agree that the impact of the quality of information has a direct relationship on their work performance. 15.0% (n=16) disagree with 0.9% (n=1) not responding.

About 99% (n=106) agree that the impact of the relevance of information has a direct relationship with their work. About 0.9% (n=1) disagree.

Table 4.5: Analyses of Hypothesis 3

Model	Unstandardised Coefficients		Standardised Coefficients			95.0% Confidence Interval for B		Correlations			Collinearity Statistics	
	B	Std. Error	Beta	T	Sig.	Lower Bound	Upper Bound	Zero-order	Partial	Part	Tolerance	VIF
(Constant)	.974	.588		1.657	.101	-.192	2.140					
A	.484	.121	.416	3.993	.000	.244	.725	.396	.371	.358	.740	1.351
B	-.008	.112	-.008	-.074	.941	-.231	.214	.188	-.007	-.007	.777	1.286
C	-.018	.094	-.018	-.191	.849	-.204	.168	.128	-.019	-.017	.869	1.151
D	.242	.113	.194	2.148	.034	.019	.466	.171	.210	.193	.983	1.018

1. a. Dependent Variable: Identify which characteristic(s) of information influences ICT Risk

A- confidentiality of information has a direct relationship with my work performance

B- integrity of information has a direct relationship with my work performance

C- The availability of information has a direct relationship on work performance

D- The quality information has a direct relationship on work performance

- **Hypothesis 3: There is a significant relationship between Characteristic(s) of business information and ORM adoption**

  Once more to answer the initial two questions posed, multiple regression analysis was utilised to determine the percentage contribution of some of the identified significant predictors of characteristic(s) of information influences on ICT adoption in MSEs**.**

  The distribution revealed that only two variables made significant percentage contributions to the characteristic(s) of information (cf Table 4.5). These are; 'A' (β =0.416, *p <.000*) and 'D' (β = .194, *p =.000*). It may thus be inferred that 'A'[25] and 'D' are the two variables prominent in explaining the variation in level of characteristic(s) of information influences in ICT risk in MSEs.

  Altogether, according to the results, these two variables have a joint correlation of 0.85. The R^2 value also suggests that these two variables explained approximately 65 percent of the variations in characteristic(s) of information influences on ICT risk leaving the other 35% to the remaining factors and other factors not included in the equation.

  In conclusion, it may therefore be inferred that relatively, 'A' and 'D', actively impact on ICT risk. There seems to be enough evidence to suggest that information influences on ICT risk control would become more effective if efforts were targeted towards 'A' and 'D'. Thus, the third hypothesis was accepted.

4.5.4 RESEARCH HYPOTHESIS 4

This section aims at determining the significance of the relationship between actions taken by large organisations and IT ORM adoption in MSEs. This subsection sought to interrogate the issue of challenges posed by ORM solutions in terms of its predictors as other research questions.

[25] cf SECTION H2: Identify which characteristic(s) of information influence ICT Risk: appendix A

Generally, most respondents (97.2%, n=104) agree that maintaining an appropriate level of user involvement at all stages of the systems development lifecycle is essential. About 2.7% (n=3) disagree.

The majority (86.9%, n=93) agree that information system design should be managed as planned organisational change, while, 13.1% (n=14) disagree.

The majority (90.6%, n=97) agree that people and technology (sociotechnical design) aim for an optimal blend of achieving both excellent technology and work performance, while 9.3% (n=10) disagree.

- **Hypothesis 4: There is a significant relationship between**

  challenges posed by ORM new solutions

Multiple regression analysis was once more used to determine the percentage contribution of some of the identified significant predictors of challenges posed by ORM solutions as other research hypothesis (cf. Research questions 1.4).

The distribution revealed that only one variable made a statistically significant percentage contribution. This is 'C'[26] (β=0 .447, p< 0.01) (cf. Table 4.6). It may thus be inferred that 'C' is the variable prominent in explaining the variation in level of challenges posed by ORM solutions.

[26] cf. SECTION H4: Identify the challenges posed by ORM solutions: appendix A. Note that questions as appeared in table are 1-4 (used as A-D).

Table 4.6: Analyses of Hypothesis

Model	Unstandardised Coefficients		Standardized Coefficients			95.0% Confidence Interval for B		Correlations			Collinearity Statistics	
	B	Std. Error	Beta	T	Sig.	Lower Bound	Upper Bound	Zero-order	Partial	Part	Tolerance	VIF
Constant	2.206	.375		5.888	.000	1.463	2.949					
A	.063	.081	.071	.772	.442	-.099	.224	.103	.076	.067	.900	1.111
B	-.070	.086	-.074	-.812	.418	-.240	.101	-.072	-.080	-.071	.911	1.097
C	.368	.073	.447	5.070		.224	.512	.458	.447	.442	.979	1.021

A - Information system design should be managed as planned organizational change.

B - People, social and technology (sociotechnical design) aims for an optimal blend of achieving both excellent technology and people’s work performance.

C - Maintaining an appropriate level of user involvement at all stages of the systems development lifecycle is essential.

The results suggest that the variable contributed to approximately 88.4% of the variations in level of challenges posed by ORM solutions.

It may therefore be inferred that relatively, ‘C’ actively impacts on challenges posed by ORM solutions.

By implication there seems to be enough evidence to suggest that ORM solutions control would be more effective if efforts were targeted towards ‘C’. Thus, the fourth hypothesis was accepted.

4.5.5 RESEARCH HYPOTHESIS 5

Lastly, this section sought to determine the significance of the relationship between evaluation models and ICT adoption in MSEs. The object of this research question was to answer the question, (1) how well do the measures of evaluation models and ICT predict ICT adoption within MSEs and (2) Which is the best predictor of the use of evaluation models and ICT in MSEs?

About two-thirds (66.4%, n=71) agree that the payback method is used to evaluate and align objectives of executive management and information systems projects. About one-third (33.6%, n=36) disagree.

Well over half (59.8%, n=102) agree that the Net Present Value method is used to evaluate and align objectives of executive management and information systems projects. Meanwhile, 40.2% (n=43) disagree.

Nearly two-thirds (64.5%, n=69) agree that the Internal Rate of Return (IRR) method is used to evaluate and align objectives of executive management and information systems projects while 35.5% disagree.

A little over three-quarter (75.7%, n=81) agree that Portfolio analysis and scoring models are used to evaluate and align objectives of executive management and information systems projects which 24.3% disagree.

Nearly a half (49.6%, n=53) agree that the ValIT framework is used to evaluate and align objectives of executive management and information systems projects. More than half (57%, n=61) agree that the COBIT framework is used to evaluate and align objectives of executive management and information systems projects while 43.0% disagree.

Table 4.7:Analyses of Hypothesis

Model	Unstandardised Coefficients	StandardiseCoefficients		T	Sig.	95.0% Confidence Interval for B		Correlations		Collinearity Statistics		
	B	Std. Error	Beta			Lower Bound	Upper Bound	Zero-order	Partial	Part	Tolerance	VIF
Constant	1.651	.345		4.780	.000	.966	2.337					
A	.430	.164	.410	2.618	.010	.104	.756	.258	.252	.246	.359	2.787
B	-.164	.136	-.180	-1.205	.231	-.434	.106	.143	-.119	-.113	.395	2.533
C	.187	.103	.190	1.813	.073	-.018	.392	.207	.178	.170	.802	1.247
D-	-.114	.110	-.142	-1.034	.304	-.333	.105	.113	-.102	-.097	.468	2.136
E	.055	.113	.065	.487	.627	-.169	.279	.132	.048	.046	.501	1.996

A-Net Present Value method is used to evaluate and align objectives of executive management and information systems projects.

B- Internal Rate of Return (IRR) method is used to evaluate and align objectives of executive management and information systems projects.

C- Portfolio analysis and scoring models are used to evaluate and align objectives of executive management and information systems projects.

D- ValIT framework is used to evaluate and align objectives of executive management and information systems projects.

E- COBIT framework is used to evaluate and align objectives of executive management and information systems projects.

- **Analysis of Hypothesis 5: There is a significant relationship between evaluation models and likelihood of ORM adoption**

  Multiple regression analysis was utilised to determine the percentage contribution of some of the identified significant predictors of evaluation models affecting ICT adoption within MSEs.

  The distribution revealed that only one variable made a significant percentage contribution to the level of ICT operation in MSEs. This is 'A'[27] (β =0.410, *p<.000*). It may thus be inferred that 'A' is the variable, prominent in explaining the variation in level of evaluation models affecting ICT adoption within MSEs.

  In answering the two questions (1) degree of variability explained and (2) predictors, the results revealed that the variable contributed approximately 88.4% of the variations in evaluation models affecting ICT adoption within MSEs.

  It may therefore be inferred that, 'A' is the most common evaluation models which affects ICT adoption within MSEs.

  By implication there seems to be enough evidence to suggest that evaluation models in ICT operation would be more effective if efforts were targeted towards 'A'. Thus, the fifth hypothesis was accepted.

[27] cf. SECTION H5: Assess evaluation models affecting ICT adoption within SMEs : appendix A

Table 4.8: Multivariate Tests

Effect		Value	F	Hypothesis Df	Error df	Sig	Partial Eta Squared
Intercept	Pillai's Trace	.980	967.9	5.00	98.0	.000	.980
	Wilks' Lambda	.020	967.9	5.00	98.0	.000	.980
	Hotelling's Trace	49.38	967.9	5.00	98.0	.000	.980
	Roy's Largest Root	49.38	967.9	5.00	98.0	.000	.980
Dept's	Pillai's Trace	.184	1.306	15.000	300.00	.197	.061
	Wilks' Lambda	.825	1.302	15.000	270.9	.020	.062
	Hotelling's Trace	.201	1.295	15.000	290.0	.204	.063
	Roy's Largest Root	.124	2.474[b]	5.00	100.0	.037	.110

For further analysis using Wilk's statistics, there was no significant effect of department Λ=.825, (5, 15) = 1.30, *p*> *.05*. Additionally, a one-way repeated measure ANOVA was conducted to compare scores on the various departments. There was a significant effect for evaluation models (Wilks' lamda = 0.25, F(2, 28) = 41.17, p>.000, multivariate partial eta squared =

0.75), noting that this result suggests a small effect size and then is a significant relationship between departments and evaluation models used in ICT operations.

Additionally, data was analysed using a mixed-design ANOVA with a within-subjects factor of subscale (years of service) and a between-subject factor of gender (male, female).

Mauchly’s test indicated that the assumption of sphericity had been violated (χ^2 = 16.8, *p*< .001), therefore degrees of freedom were corrected using Greenhouse-Geisser estimates of sphericity (ε = 0.98).

The results revealed no main effects of sub scale, *F*(1.91, 1350.8) = 378, *p* >.05, ηp2 = .03, and gender, *F*(1, 709) = 78.8, *p* > .05, ηp2 = .10, were qualified by an interaction between subscale and gender, *F*(1.91, 1351) = 30.4, *p* > .05, ηp2 = .041.

Furthermore, an ANCOVA [between-subjects factor: gender (male, female); covariate: Education] revealed no main effects of gender, *F*(1, 732) = 2.00, *p*= .16, ηp2 = .003, or education, *F*(1, 732) = 3.25, *p*= .072, ηp2 = .004, and no interaction between gender and education, *F*(1, 732) = 0.016, *p*= .90, ηp2 < .001.

All other main effects and interactions were non-significant and irrelevant to the hypotheses, all *F* ≤ 0.94, *p*≥ .39, ηp2 ≤ .001

4.6 CONCLUSION

This chapter presented the findings of the empirical investigation carried out in this study. The chapter commenced with an overview of the specific research questions, statistical techniques, demographics of respondents and data reduction, data reduction technique: factor analysis, and finally analysis of each Research Findings (hypotheses/objectives).

The two main questions were (1) how well does each measure of the five variables predict ICT ORM adoption within MSEs and (2) which is the best predictor of the sub variables? Multiple regression analysis was used to test for the significant predictors. Thus, findings related to those factors impacting on ICT and operational risk management within MSEs.

CHAPTER 5

DISCUSSION OF RESEARCH FINDINGS

5.1 INTRODUCTION

This chapter discusses the research findings presented in chapter four. In addition it addresses factor analysis-data reduction, determining the factors for principal causes of ORM failure related to ICT, organisational factors related to change management requirements and ICT risk, characteristic(s) of information influence on ICT risk, challenges posed by ORM solutions, evaluation models affecting ICT adoption within MSEs, ICT operational risk and MSEs performance, chaos system and ICT operational risk, ICT development and Performance within MSEs, changes management model for MSEs and finally Chaos Theory, a guide to managing MSEs as well as the requirements of Chaos Theory in the management of MSEs.

5.2 FACTOR ANALYSIS - DATA REDUCTION

The 107 questionnaires received were analysed using SPSS version 18. The analysis included descriptive analysis, multiple regression, RM-ANOVA, RM-MANOVA and ANCOVA which were used to predict ICT operational risk adoption in MSE. The data showed that about 60.7 percent of the respondents were IT personnel, 23.4 percent finance and 10.3 percent operations personnel. The study identified various factors of ICT operational risk in MSEs adoption within the case organisation.

The findings support other similar studies and increased the generalisability of previous research conducted (Standing *et al*, 2007; Curley, 2004).

At the outset, the ICT adoption was measured on a four-point Likert scale.

All five operational risk variables of MSEs (cf. Figure 5.1) of the current study had evidence to support a significant relationship between: ICT operational risk management and performance of MSEs.

For the purpose of these five variables, a one stage normative model, associative in nature, was developed based upon review of previous research and in line with the research objectives and findings in chapter 4 (cf. Figure 5.1). Based upon the findings, regression analysis indicated that factors such as (1) the principal causes of ORM failure related to ICT (2) change management requirements and ICT risk (3) characteristic(s) of information that influences ICT risk (4) challenges posed by ORM solutions and (5) evaluation models affecting ICT adoption within MSEs were significant determinants of ICT operational risk in MSEs adoption.

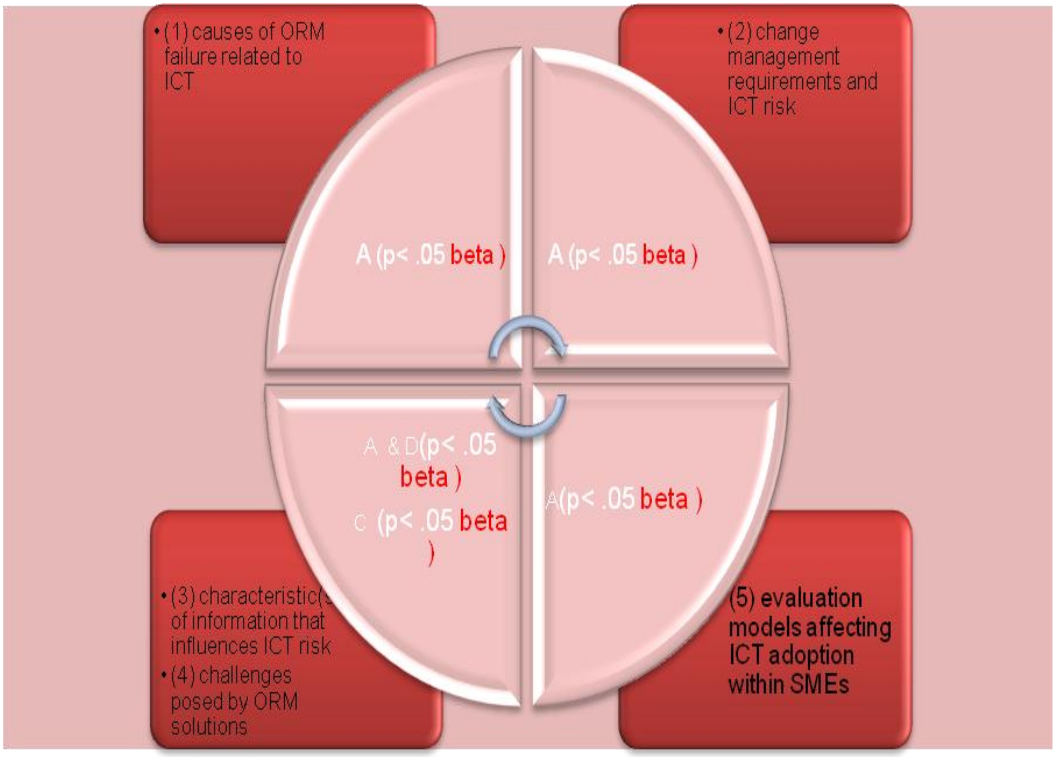

• (1) causes of ORM failure related to ICT
• (2) change management requirements and ICT risk
A (p< .05 beta)
A (p< .05 beta)
A & D(p< .05 beta)
C (p< .05 beta)
A(p< .05 beta)
• (3) characteristic(s of information that influences ICT risk
• (4) challenges posed by ORM solutions
(5) evaluation models affecting ICT adoption within SMEs

Figure 5.1: Factors impacting Performance of ICT adoption in MSE

Under principal causes of IT failure, the current study revealed that 'A'[28] was significant in determining the ICT operational risk in MSE adoption. Of the other factors studied 'A' was the only significant ICT operational risk that affected MSEs. Thus, MSEs need to adopt 'A' for ICT operation, since they would reap significant benefits.

Although the principal causes of ORM failure related to ICT are important, so too are change management requirements, challenges posed by ORM solutions and evaluation models, which also have a high beta coefficient obtained through regression analysis (cf. Chapter 4: section 4.5). Analysis of the relative importance of variables showed that 'A'[29] has a significant impact on change management requirements. This further indicates that

[28] One of the principal causes of information system failure is insufficient or improper user participation in the systems development process

[29] There is a high failure rate among enterprise application projects because they require extensive organizational change that is often resisted by members of the organization.

management of MSEs must focus on reducing resistance to gear up the adoption process.

Additionally, around half of the ICT operational risks in MSE adoption variance were explained (cf. Chapter 4: section 4.5). Based upon the results, the current study proposes that in order to obtain the full benefits from ICT operational risk, MSEs must adopt a pro-active approach and focus more on the potential benefits as aforementioned.

Building on prior research in ICT operational risk in MSEs and performances of financial institutions, this current study suggests there are relationships between ICT operational risk in MSEs and performance. Specifically, a developed model (cf. Figure 5.1) shows the relationship between ICT operation and performance of MSE practices.

ICT operational risk in MSEs, specifically financial institutions, is not a new phenomenon (Allen, 2005; Anderson, 2005). Dealing with risk has always been the raison d'être of some institutions (Weill and Ross, 2004). For instance, MSE financial institutions are exposed to risk (Williams, 2005). Yeo (2002) argues that an integrated, holistic approach to ICT operational risk in MSEs can create shareholder value. Therefore, the effective management of ICT risk in MSEs is crucial to any financial institution's performance. In support of this, Ritchie and Brindley (2000) describe ICT operational risk activities designed to minimise negative possible losses. Ritchie and Brindley (2000) reveal that the purpose of ICT operations are to maximise revenues and offer the most value to shareholders by offering a variety of financial services, and especially by administering risks. Accordingly, ICT operations are central to MSEs.

This suggests that effective and efficient ICT operational risk in MSE financial institutions is of particular importance as they endeavour to cope with the challenges of globalisation. The findings of this current study are thus consistent with previous studies (Rockafellar *et al*, 2006). The next section addresses individual factors of the five main objectives.

5.3 PRINCIPAL CAUSES OF ORM FAILURE RELATED TO ICT IN MSEs

One of the objectives of this study was to identify the principal causes of ORM failure related to ICT adoption within an MSE. On a four-point Likert scale the betas show an attractive picture of ICT operational risk in MSEs adoption. The results were consistent with similar research by ITGI (2009). In chapter 4, section 4.5.1, it was noted that 60.7% (n=65) agree that a principal cause of information system failure is insufficient or improper user participation in the system development process ($p < 0.05$). Most respondents 76% (n=82) agree that one of the principal causes of information system failure is poor management of the implementation process, while 22.4% disagree.

Conceptual studies (Standing *et al*, 2007; South Africa, 2006) agree that a MSE will consider making use of ICT either to avoid negative consequences (i.e. risk associated to negative outcomes) or to achieve positive consequences (i.e. risk associated to opportunity) (Standing *et al*, 2007). The current study’s findings are supported by previous study reviews that ICT operations in MSEs are increasingly recognised as being concerned with both positive and negative aspects of risk (Standing *et al*, 2007; South Africa, 2006). The present results resonate with the conceptual studies, thus emphasising the relationship between ICT operations and MSE performances.

There are a few other literature discussions on the relationships between ICT operational risk in financial related MSEs and their performance. This current study categorised the literature as follows:

1. ICT operational risk in MSEs and efficiency (Conner and Coviello, 2004)

2. ICT operational risk in MSEs and financial performances (Ericsson, 2007; Curley, 2004).

In support of the current study, the variables related to performance as determined in chapter 4 (cf. Section 4.5.1 - 4.5.5) not only revealed relationships between ICT operational risk in MSEs practices, but also indicated the relative percentage contributions (cf. Betas in section 4.5). The next variable addressed was change management requirements and ICT operation.

5.4 ORGANISATIONAL FACTORS RELATED TO CHANGE MANAGEMENT REQUIREMENTS AND ICT RISK

Change management was also found to be an important factor influencing ICT operations in MSEs. Most of the results showed significant relationships and percentage contribution (cf. Section 4.4.2 for example). The findings do not only provide empirical support to the previous findings of Froot and Stein (1998), but also support the argument for the influence of change management on ICT operational activation in a MSE. Additionally, the results of this study are in line with Gattiker and Goodhue (2004), because more MSEs are adopting ICTs and hence, change management is a significant factor in the influencing early adoption stages.

5.5 CHARACTERISTIC(S) OF INFORMATION INFLUENCES ON ICT RISK

The third MSE factor, characteristic(s) of information was found to be significant. The characteristics addressed were *confidentiality, integrity, availability, quality and relevance* of information and the relationship to work performance (cf. Chapter 4 section 4.5.3 and Appendix A).

The respondents agreed that characteristic(s) of information can impact on the strategic importance of ICT operations in MSEs, but, few of the variables reached statistical significance. The result is in line with the findings of Kim, Kim and Lee (2006).

The findings of this study further indicate that of five organisational factors only two were significant in influencing ICT operations in MSEs adoption.

However, respondents noted that characteristics of information control are an important aspect of ICT operations and they regard characteristics of information as a key element in the regulatory model. This resonates with the current work and previews on ICT operational issues by Kritzinger and Smith (2008).

Thus, to assess and manage risks, an MSE must effectively determine the confidentiality of information necessary to absorb unexpected losses arising from its market.

Many argue that the performance of MSEs commensurate with ICT operations and is sensible from both economic and regulatory point of views (Lam, 2006). Consequently, paying attention to characteristic(s) of information can be considered a factor influencing ICT operations in MSEs.

To date, much of the discussion on the benefits of ICT operations have been linked to the larger organisations. Liebenberg and Hoyt (2003) have begun to explore the use of the Internet by MSEs, though the literature and empirical research in this area is still very limited. Many studies argue that the potential impact of these developments on the smaller business is likely to be even more significant than their larger counterparts. This argument is consistent with the current study (cf. Chapter 4 section 4.5.3).

In summary, and from the findings in chapter 4 section 4.5, the results supported the hypothesis that there is a relationship between ICT operations and performance of MSEs. Hence, the current study concludes that MSEs that have effective ICT operations have a leveraged output.

5.6 CHALLENGES POSED BY IT ORM SOLUTIONS

Previous researchers have studied the relative importance of challenges posed by IT ORM solutions. Because of their importance, it was included in this study. Challenges posed by IT ORM solutions were found to be significant and to influence performance. It is mainly due to 'C'[30] which may be used to develop and promote ICT operations within MSEs (as evidenced by results in Chapter 4: section 4.5.4).

It was obvious from the results that MSEs consider 'C' as an important and fundamental factor for their operations. The current findings support prior studies by Layton (2007) and Olivier (2006). Findings further resonate with Stoney (2007) who argues that an understanding of 'C' improves the performance of small businesses.

A survey of ICT MSE operations of all issues by Pricewaterhouse Coopers (2007), found that 'C' is currently at 54 per cent for ICT operations in MSEs and 33 per cent for large companies. Similar studies by Lam (2006) indicate that smaller organizations are rapidly becoming aware of the potential for competitive advantage that IT ORM offers; though they are perhaps less aware of potential risks benefits, particularly in South Africa.

For instance, Lam's (2006) study reports that results into 'C' usage indicate that the nature of developments within the MSE sector is increasing exponentially.

[30] People, social and technology (sociotechnical design) aims for an optimal blend of achieving both excellent technology and people's work performance

PricewaterhouseCoopers (2007) emphasise this development, suggesting that it is not simply about new channels or even about new customers. Entirely new business models are appearing, where the ability to build flexible alliances at speed is a critical management skill for MSEs. Although these changes will have an impact on all organisations irrespective of size, the focus regarding the current study is directed towards PricewaterhouseCoopers (2007) assertion of the MSE sector.

It is thus anticipated that the outcomes from this current study and the associated empirical data will enhance awareness and understanding of the nature of MSE management and provide guidelines for developments in strategic management, and most importantly, ICT operations.

The other significant feature that may be drawn from the current study is the difference between the adoption and application of ICTs in large organisations in contrast to MSEs. In support of the current study's findings, relevant research literature maintains that almost every sector is experiencing a doubling of usage of ICT development.

5.7 EVALUATION MODELS AFFECTING ICT ADOPTION WITHIN MSEs

Evaluation models are found to be important for ICT operational risk in MSEs. The plausible reason for the relevant importance of this variable in MSEs is due to 'A'[31] and 'D'[32] (cf. Chapter 4 section 4.5.5). This might be because the evaluation model process in MSEs is almost always short-term (Conner and Coviello, 2004). For instance, the role of equity capital in MSEs is a substitute for transferring risk and hence, a buffer that protects the MSEs against unexpected shocks to its capital base (Lam, 2006).

[31] Payback method is used to evaluate and align objectives of executive management and information systems projects

[32] Portfolio analysis and scoring models are used to evaluate and align objectives of executive management and information systems projects

The findings of this study support the literature which suggests that evaluation models can act as motivators to encourage the adoption of an innovation because direct benefits are more viable and are easier to measure (CAS, 2003). So this study supports the prior study of CAS (2003), that evaluation models are influential determinants of technology usage in MSEs. A similar finding is reported by a previous study of ICT operations (Calder, 2006). The study found the relative advantage of evaluation models a significant factor of adoption within MSEs. The study however does not support the previous findings of Burget and Ruschendorf (2006), contrasting the view of evaluation mode usage in MSEs.

The existing models of information management recognise the potential impact of the revolution that is taking place within the global economy (Balbas, 2007). Such models particularly in MSEs have not fully articulated the changes that have occurred or are likely to occur, nor have they developed effective management strategies to handle these and the consequent ICT risks.

Once MSEs give attention to such development, it will, like the larger multinational organisations, be exposed to the consequences of these developments which will arguably provide competitive opportunities. Another likely result is that localised incidents and market developments will be experienced across the globe. A significant feature is that opportunities will no longer be restricted to the large organisations, which arguably possess the necessary resources, structures and processes to undertake global ICT operation.

In support of the current study’s position, Lam (2006) noted that even the smallest of businesses will now have the potential to trade in the global economy using ICT. Lam (2006) maintains that these changes in the nature of the competitive processes and commercial relationships provide significant strategic opportunities for the smaller organisation, arguably placing them on an equal footing with their larger competitors already established in the marketplace.

For example, it is likely that substantive changes in technology and other product/service innovations will be disseminated more rapidly and evenly across the globe. It will become increasingly difficult to segregate market segments in terms of design, technology, service levels and pricing (e.g. delaying implementation of new products to lesser developed market segments).

For this reason, managers in MSEs need to be equipped to identify, analyse and manage ICT operational issues from a more diverse range of sources and contexts. If this is not carefully considered, MSE managers, irrespective of whether they engage in business or not, may find it more difficult to avoid the risks resulting from increased ICT global competition in their home markets.

5.8 IT OPERATIONAL RISK AND MSE PERFORMANCE

The previous sections and reviewed literature have explained the relationships of the variables influencing ICT adoption in MSEs (cf. Chapter 1 Sections 1.3 and1.4). By testing the hypotheses, relationships and associations were found among the variables. Moreover, the factors that influence ICT operations in MSEs were cross validated with literature.

Nonetheless, further research is needed to prove the hypotheses suggested in MSEs. Hence, several contributions can be achieved especially by the various stakeholders of MSEs, namely the regulator, shareholders, management team, depositors, and the general public.

In academia, the empirical evidence of the relationships is important to add value to the literature by supporting the previous findings and theories. Ultimately, this current study will contribute to filling the gaps in the area of IT ORM related to MSEs.

Both the current findings and reviewed literature show that performance of MSEs holds significant importance to the variables studied. In fact, a previous study by Conner and Coviello (2004) examined the relationship between ICT and performance of financial institutions (MSEs) and found mixed results.

From the current study's results, there are particular sub variables of the five main categories that impact on performance of MSE (cf. Chapter 4 sections 4.5.1-4.5.5).

However, as suggested by literature (Lam, 2006) a major reason noted for not establishing such effective ICT systems is the prohibitive costs quoted by consultants for setting up an ICT site.

Indeed, most of the respondents surveyed in the study recognised the need for establishing an enterprise application project because they required extensive organisational change that was often resisted internally. Similarly, the study identified that the major orientation of MSEs' plans to exploit the success of organisational change could be determined by how well information system end users deal with various stages in the implementation of ICT projects.

Further analysis of the results suggested minimal impact of the confidentiality of information. Respondents were actively engaged in quality information technologies not only in terms of providing specialist services to their clients, but also in terms of their own business operations. The internal focus was towards maintaining an appropriate level of user involvement at all stages of the systems development lifecycle.

More radical developments as indicated by respondents in terms of people, social and technology (sociotechnical design) aimed for an optimal blend of achieving both excellent technology and performance. However, other respondents acknowledged they did not yet recognised the implications for future ICT operational relationships. Few respondents recognised the potential impact in terms of the developing metrics and processes as a whole.

Though there was unanimous recognition that the payback method would have a fundamental impact on decision making and business operations, most related this to information system design. The findings of the current empirical study confirm previous results of the study by Conner and Coviello (2004).

This current study also made a significant contribution to payback method (cf. Chapter 4 section 4.5.5). Most outcomes primarily revealed that the competitive advantage of an evaluation model in terms of payback method was increased recognition of the potential in terms of MSE performance.

The current study and comparative studies conducted by ITGI (2007) largely support the suggestion to adopt ICT operations within MSE business strategies.

However, key barriers to the pace and success of adopting ICT operations were identified as insufficient or improper user participation in the systems development process as well as and high levels of complexity and risk. The belief that ICT provides a potential transformational impact or a solution to key business issues and challenges gives some explanation for the overall level of strategic commitment by respondents.

5.9 CHAOS SYSTEM AND ICT OPERATIONAL RISK

As in the cases of Lorenz’s work a complex system such as an MSE will reacts to different variables (Lorenz, 1969). The results thus suggest that MSEs are sensitive to initial conditions. This is particularly true in ICT operational risk. Even starting with the same or slightly different variables in a model will result in significantly different outcomes, thus no same context in Chaos Theory terms is time irreversibility.

The definition of Time Irreversibility is that in a complex system such as MSEs, there is never the same context twice. Thus a business (MSEs), or team with essentially identical personnel and similar characteristics will never perform exactly the same as another (or itself), if the ICT operational factors are instituted (Theitart and Forgues, 1995). As applied to management, a strategy or decisions will never be made twice within the same context.

Chaos Theory is of the view that organisations such as MSEs are complex adaptive systems that have behaviours similar to those found in nature, that is, different stages of stability and chaos. Rather than trying to control an organisation, a manager, is prompted to take advantage of its complexity. Theorists in management and social organisation now believe that organisations are also non-linear dynamic systems, having the same characteristics as natural phenomena (Conner and Coviello, 2004).

The organisation is often seen as a complex adaptive system comprised of formal and shadow systems, and in this way the analogy is made between chaos in natural systems and social organisations. As discussed in Chapter 2 section 2.7, McBride (2005) addresses this issue by stating that managers learn how to manage the ICT failures that are on the edge of chaos. McBride (2005) ends with optimism, believing that although long term outcomes are possible for ICT operation in MSEs, dealing effectively with change and challenge on a daily basis will ultimately result in success. Chaos Theory is often used as a way to conceptualise management theory and other social systems. Therefore, the efficient manager will plan for and expect constant change in the environment. His or her goals become not a set of results but a series of contingency scenarios to which he or she can react in the short term at some later date.

The same principle applies to MSEs. Thus, tiny changes in one of the variables studied (cf. Chapter 4 sections 4.5.1-4.5.5) can, on occasion, lead to major changes.

5.10 ICT DEVELOPMENT AND PERFORMANCE WITHIN MSEs

The pattern of results reported within the current study reflects the patterns from earlier studies into ICT adoption (Theitart and Forgues, 1995). ICT adoption suggests a process of more rapid adoption of technologies as the global economy has developed (Theitart and Forgues, 1995). This also implies that MSEs should be prepared to migrate to the next technology more readily than previously. This may also be supported by the findings relating to ICTs and the changing ICT performance (Theitart and Forgues, 1995).

The view is that MSEs will adopt new technologies more readily and that the pace of development of say, e-business may become ever rapid as indicated by Curley (2004) and supported by the current study. Similarly, Gattiker and Goodhue (2004) suggest that the momentum for ICT development and innovation will become unstoppable and will accelerate.

Although the integration of the implications of ICT operations into the strategic planning of MSEs may only be partial at this stage, the empirical evidence available suggests that rapid changes are taking place in relation to smaller organisations.

However, further research is needed to monitor these changes more closely to measure the changing strategies and the associated factors such as insufficient or improper user participation in the systems development process, which have been identified as potential barriers to the effective adoption and implementation of e-business strategies (cf. Chapter 4 section 4.5.1-4.5.5). In fact, Balbas (2007) estimates that over a 25-year period that is 1970 –1995, the degree of complexity has doubled, with 78% of products being classified as complex in terms of the inherent technology or the processes employed, particularly in the manufacturing industry.

The more recent developments within ICT related to MSEs may lead to another dimension of complexity in addition to product and manufacturing process complexities, that is operational complexity. This will provide a further set of challenges and opportunities to harness and integrate all complexity dimensions to achieve an effective competitive advantage. Monitoring the strategic responses of organisations, particularly MSEs, will provide important insights for the future of operational structures and relationships.

5.11 CHANGE MANAGEMENT MODEL FOR MSEs

The foregoing sections articulated fundamental changes in decision making and processes associated with the present formulation and operations of MSEs. The evidence suggests that the primary impact is in terms of (1) analysing the principal causes of ORM failure related to ICT (2) assessing change management requirements and ICT operation (3) identifying which characteristics of information influence ICT risk (4) identifying the challenges posed by ORM solutions and lastly (5) assessing evaluation models affecting ICT adoption within MSEs.

The empirical evidence presented in chapter 4 (cf. Section 4.5.1-4.5.5) indicates that a significant number of the aforementioned variables impacts on the performance of an MSE. Therefore, the premise of the model in the current study is that there is potentially a far greater strategic impact in terms of ICT operations and MSE performance.

This is contrary to the evidence reported in relation to the larger organisations that have for a longer period engaged in the wider implications of ICT operations.

The evidence also available for the smaller organisation would indicate that MSEs may be advanced in their strategic thinking about the potential use of the ICT operations, though in most cases this is primarily focused on the marketing communications and sales strategies rather than procurement or other business-to-business relationships.

Additionally, there is evidence that the pace of adoption of ICTs and the associated competitive pressures are increasing rapidly (cf. Section 4.5.1). The evidence available for the MSE sector suggests an increased pace of change and competitive pressure, though most small businesses are still at a much earlier stage of ICT adoption and development (Lam, 2006).

Though MSEs are at an earlier adopter stage, the evidence from larger organisations, taken into consideration with the rapid pace of technology development, suggests that MSE managers must engage with the concept of the ICT operational models.

By recognising the opportunities presented by such an ICT operations model, there is potential for MSEs to increase their customer base and engage in larger markets. MSE managers who can respond to the changing nature of ICT operational relationships may have an opportunity to gain competitive advantage. Response will be a key management challenge, given the amount of change and the dynamism of ICT operations.

This suggests that there will be a need for MSE managers to manage a multitude of relationships. Thus, internal processes and procedures, such as production time, order processing, delivery methods, etc., will have to be geared to achieve different expectations driven by (1) the principal causes of ORM failure related to ICT (2) change management requirements and ICT risk (3) characteristics of information that influence ICT risk (4) challenges posed by ORM solutions and (5) evaluation models affecting ICT adoption within MSEs. Ignoring the challenges and opportunities presented by the ICT operational model could lead to the failure of some MSEs.

For example, geographical location may no longer guarantee preferred supplier status; there could be competition from a greater number of businesses, both domestic and international, and custom-built orders may increasingly become the norm.

5.12 CHAOS THEORY: A GUIDE TO MANAGE MSEs

Chaos Theory extends to both analysis and intervention in the way managers understand MSEs. Most managers assume that, given enough information, they can anticipate what is going to happen in a particular situation, and thus can determine how best to act so as to promote, defer, deflect, or divert it.

Chaos Theory suggests that, on the contrary, some systems are inherently risky in MSEs and can never be fully understood, no matter how much effort or expense is devoted to trying (McBride, 2005). Probable suggestions like, gathering more information or constructing more elaborate models explaining chaotic systems may be pointless. In fact, ‘research’ can even be counter-productive if it creates a false sense of security about planning and what it promises to achieve (McBride, 2005). Moreover, in such cases, planning strategies that depend on foresight are inappropriate and even misleading. Instead, managers must become accustomed to working not with single forecasts of the future, but rather with an ensemble of forecasts (Pflug, 2006).

5.13 REQUIREMENTS OF CHAOS THEORY IN THE MANAGEMENT OF MSEs

Managers seek understanding not as an end in itself, but as a means to an end as a basis for making informed judgments about the effects of intervention. Rather than looking for more detailed information on, and more accurate models of their systems, managers should instead look for (1) patterns of system behaviour and (2) points to which systems seem to return (which mathematicians call ‘attractors’), even if not in any ICT operation as presented in Figure 5.2.

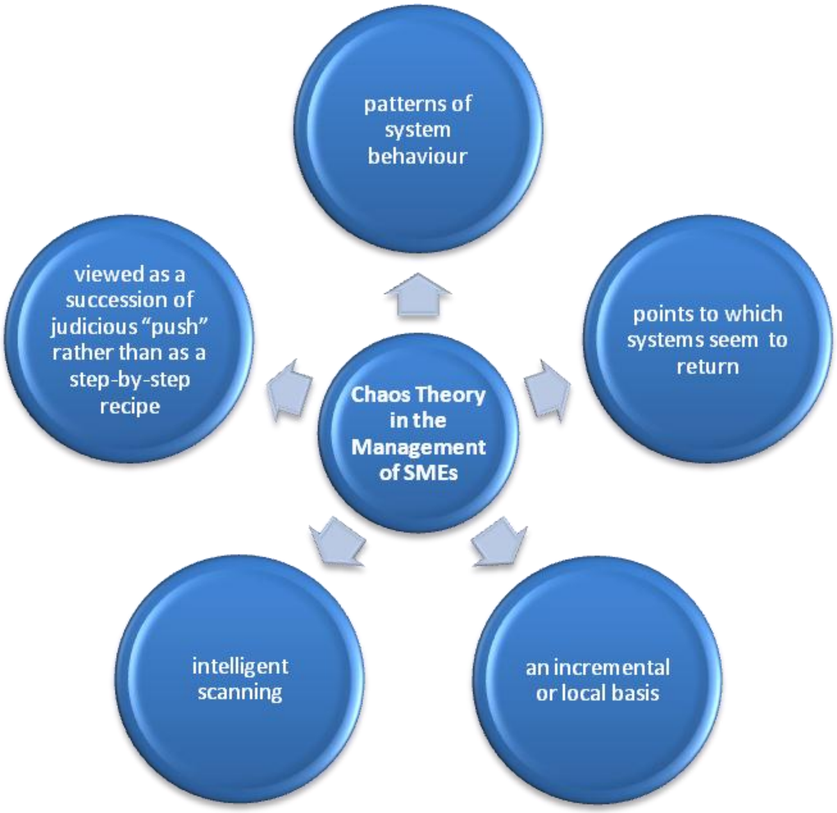

patterns of system behaviour
points to which systems seem to return
an incremental or local basis
intelligent scanning
viewed as a succession of judicious "push" rather than as a step-by-step recipe
Chaos Theory in the Management of SMEs

Figure 5.2: Requirements of Chaos Theory in Management of MSEs

Chaos reinforces the need for what literature called intelligent scanning (Thiétart and Forgues, 1995). The fundamental implication that can be drawn from Chaos Theory is that managers must learn to rethink some of the deep-rooted beliefs in the virtues of order, of chaos and disorder. In other words, managers must learn to accept the possibility that a chaotic operation, for instance, may be preferable to and 'healthier' than an orderly one. It may even be that managers need chaos in order to survive that chaos is an essential part of ICT operations in MSEs.

Most important of all for managers, is the fact that chaotic systems for ICT operations should be seen only as an incremental or local basis, meaning that operations of ICT in chaotic systems normally result in cumulative effects of various kinds of feedback. But, on an incremental or local basis, the effects of feedback from one time period to the next are often perfectly clear. This should be the dominant argument for planning strategies that are incremental rather than comprehensive in scope, and that rely on a capacity for adaptation rather than on blueprints of results (Thiétart and Forgues, 1995).

Related to this is that for chaotic systems, the shortest distance between two points is not always a straight line (Tsoukas, 1998). In other words, even when managers are satisfied that a particular goal is desirable, the best way of getting there may not always be the most direct one. Instead, it may be easier to plan for a chaotic system by deliberately 'over-shooting, or 'under-shooting' the goal, or even by a sequence of such steps, than by going straight towards it.

Planning for chaotic systems may be more successful when it is viewed as a succession of judicious 'pushes' rather than as a step-by-step recipe. In chaotic systems, as noted in Chapter 2, section 2.7, relatively small changes in inputs can have a dramatic effect on system behaviour. This was consistent with the result in Chapter 4, section 4.5.1-4.5.5. The findings in Chapter 4 also revealed that significant differences were accounted for from particularly variables (cf. Chapter 4, section 4.5.1 for example).

The implication is that different parts of a system communicate with one another. The system has an environment with which at least one of its parts communicates; thus the system is always changing. This is a beneficial reminder that, in managing, the details can be just as important as the broad strokes. For these reasons, Chaos Theory promises a revolution in managing at least as profound as that entailed in the current trend towards an information society (Tsoukas, 1998). As Lorenz (1969) notes the view that order emerges from an underlying formless chaos and that this order is recognised only by periodic patterns is the predominant view in the dynamics system.

5.14 CONCLUSION

This chapter discussed of the research findings given in Chapter 4. The chapter addressed factor analysis - data reduction, principal causes of ORM failure related to ICT, organisational factors related to change management requirements and ICT Risk, characteristics of information influences on ICT risk, challenges posed by ORM solutions, evaluation models affecting ICT adoption within MSEs, ICT operation and MSEs performance, Chaos system and ICT operation, ICT development and performance within MSEs, changes management model for MSEs, Chaos Theory as a guide to managing MSEs and requirements of Chaos Theory in the management of MSEs.

CHAPTER 6

SUMMARY CONCLUSIONS AND RECOMMENDATIONS

6.1 INTRODUCTION

Chapter 6 provides a summary of the main ideas. It continues with a summary of findings, conclusions and recommendations for further study.

6.2 SUMMARY OF MAIN IDEAS

Chapter 1 of this study provided the background of the study with its intent being to give the context of the study. This was followed by a motivation for the research statement and development of the hypotheses**.** The other sections included the research objectives and delimitation of the study. Attention was also given to the research methodology, ethical considerations and an outline of the study.

Chapter 2 concentrated on the reviewed literature. It addressed MSEs and operational risk management (ORM) development in South Africa. In doing so, it was noted that MSEs recognise the need for information security. However, it noted that because of the lack of resources and capabilities for building ICT, MSEs are vulnerable from the ICT standpoint.

The chapter also addressed evolution of operation risk management including a section on hypothetical models for understanding the value of ITRM in an MSE. It was noted through a review of ITRM literature that most of the empirical studies on ORM had attempted to identify a set of factors to help researchers distinguish ORM adopters from non-adopters. However, these results were inconclusive. It was suggested that Chaos Theory underpinned the management of MSEs in information systems. This formed the rationale for using Chaos Theory as the theoretical framework for the current study.

Chapter 3 looked at the research methodology and design, with reference to the philosophy of the research process. This was followed by a description of the selected designs used in this study which is a case study and survey design. The sample, sampling technique and instrumentation as well as the data analysis and interpretation section were addressed. The last section focused on a summary of multivariate regression of assumptions used in data analysis.

Chapter 4 presented the findings of the empirical investigation carried out in this study. In consequence, it addressed findings related to those factors impacting on ICT and operational risk management within MSEs. The chapter commenced with an overview of the specific research questions, statistical techniques, demographics of respondents and the data reduction technique: factor analysis. The chapter concluded with an analysis of the research findings based on the hypotheses/objectives posed in Chapter 1.

Chapter 5 addressed the research findings given in Chapter 4. The chapter addressed:

- Factor analysis - data reduction,
- Principal causes of ORM failure related to ICT,
  - Organisational factors related to change management requirements and ICT risk,
- Characteristic(s) of information influences ICT risk,
- Challenges posed by ORM solutions,
- Evaluation models affecting ICT adoption within MSEs,
- ICT operational risk and MSE performance,
- Chaos system and ICT operational risk,
- ICT development and performance within MSEs,
- Changes management model for MSEs,
- Chaos Theory; a guide to managing MSE and
- Requirements of chaos theory in the management of MSEs.

Chapter 6 summarised the main ideas of the study. It continues with a summary of findings, conclusions and recommendations for further study.

6.3 SUMMARY OF MAIN FINDINGS

Factor Analysis (FA) sought to answer the question ‘what is the underlying factor structure of IT ORM measures that influence an MSE as proposed by the current study’s instrument?’ This was conducted before a multivariate regression analysis. The items of IT ORM measuring the influence of MSE were subjected to FA - principal component analysis. Five components were eventually retained in the analysis. The items that cluster on the same components[33] suggest that component 1 represents X, component 2 Y, component 3 Z, component 4 K and component 5 L.

For hypothesis 1 the results of the analysis presented answered the two questions posed at the beginning of the subsection. The model included five sub variables which explained 13% (R^2 = .13) of the variance in principal causes of ICT failure as predictor of ORM adoption within MSEs. Of the five sub variables, insufficient or improper user participation in the systems development process made the largest unique contribution (β= -.38, *p*< *.05*); although the rest made some contribution, they did not reach statistical significance (*p*> *.05*).

For hypothesis 2 the results answered the two objectives posed. The model, which included four sub variables[34], explained 55.2% of the variance of ORM adoption within MSEs. Of the four sub variables, extensive organisational change that is often resisted by members of the organization made the largest unique contribution (β = 0.291, p< 0.05); although the rest made some contribution, however they did not reach statistical significance in terms of contributions (*p*> *.05*). It may therefore be inferred that relatively, resistance to change actively impacts on change management requirements and ICT Risk.

[33] X- principal causes of ORM failure related to ICT

Y- change management requirements and ICT Risk

Z- characteristic(s) of information influences ICT Risk

K- challenges posed by ORM solutions

L- evaluation models affecting ICT adoption within SMEs

For details cross reference appendix A -questionnaire

[34] cf. sub variables on **“**principal causes of IT failure.”

For hypothesis 3 it was inferred that relatively, ‘A’ and ‘D’ characteristics of information influence ICT operation. There was enough evidence to suggest that ICT operational risk control would be more effective if efforts were targeted towards ‘A’ and ‘D’.

For hypothesis 4 it was also inferred that relatively, ‘C’ actively impacted on challenges posed by ORM solutions. There was enough evidence to suggest that ORM solutions control would be more effective if efforts were targeted towards ‘C’.

For hypothesis 5, an impacted on evaluation models affecting ICT adoption within MSEs. By implication evaluation models in ICT operation would be more effective if efforts were targeted towards ‘A’.

6.4 CONCLUSION

The study was conducted by means of a survey to collect the primary data from 107 respondents in an MSE, based upon simple random sampling plan. A one stage normative model associative in nature was developed based upon review of previous research and in line with the research objectives (cf. Chapter 5, Figure 5.1). The model elicited five factors. Based upon the multiple regression analysis of the data, the findings indicated that the principal causes of ORM failure related to ICT, change management requirements and ICT risk, characteristics of information, challenges posed by ORM solutions and evaluation models affecting ICT adoption within MSEs, were significant determinants of ICT operational risk in MSEs.

The findings supported similar other studies and increased the generalisability of the previous research (Standing et al., 2007; Curley, 2004).

All five operational risk variables of MSEs (cf. Chapter 1, section 1.4) of the current study had evidence to support the notion that there was a relationship between IT operational risk management (ITRM) and MSE performance.

The empirical evidence presented in Chapter 4 indicated that a significant proportion of aforementioned variables impacted the performance of an MSE. The premise of the model in the current study is that there is a strategic impact in terms of ICT operation and MSE performance.

6.5 RECOMMENDATIONS

The recommendations are twofold: For the practice of ICT operations in MSEs, and further research on ICT within MSEs.

6.5.1 METHODOLGICAL USE

Further research is needed incorporating the methodology used in this study, that is, factor analysis and multivariate regression analysis, to monitor changes of the studied variables more closely and to measure the changing strategies and the associated factors such as insufficient or improper user participation in the systems development process, identified as a potential barrier to the effective adoption and implementation of e-business strategies. The methodology used in this study, can also be applied in different sectors of MSEs, either to study similar factors or emerging factors other than the current study's variables.

6.5.2 PRACTICE OF ICT OPERATIONS IN MSEs

One of the key barriers to the pace and success of adopting ICT operational risk management is insufficient or improper user participation in the systems. Managers need to take notice of this.

Thus ICT operations managers of MSEs should look instead for: principal causes of ORM failure related to ICT, change management requirements and ICT risk, characteristic(s) of information influences on ICT risk, challenges posed by ORM solutions and evaluation models affecting ICT adoption within MSEs to leverage the institution's performance.

6.5.3. FURTHER RESEARCH

However, further research is needed to monitor these changes more closely to measure the changing strategies and the associated issues of insufficient or improper user participation in the systems development process, lack of management support, high levels of complexity and risk in the systems development process and poor management of the implementation process, all identified as potential barriers to the effective adoption and implementation of ICT operations.

Additionally, further research is needed to prove the hypotheses in MSEs. Hence, several contributions can be achieved especially those of the various stakeholders of MSEs, namely the regulator, shareholders, management team, depositors and the general public.

Though MSEs are at an earlier adopter stage, the evidence from the current study taken into consideration along with the rapid pace of technology development, suggests that MSE managers must engage with the ICT operation model. By recognising the opportunities presented by such an ICT operations model, there is potential for MSEs to increase their customer base and engage in both local and international markets.

6.6 RESEARCH LIMITATIONS

Due to time and financial constraints, the current study did not consider the inclusion of MSEs from different sectors.

6.7 IMPLICATIONS OF THE STUDY

The study has a practical significance as it provides help to the management of MSEs concerning factors contributing to ICT usage in the event that they may wish to maximize its benefits.

REFERENCE LIST

Allen, J. (2005). *Governing for Enterprise Security.* Retrieved Feb 13 2010, http://www.sei.cmu.edu/publications/documents/05.reports

Anderson, A. (2005). *The business reporting model of the future. The American Institute of Certified Public Accountants*. Retrieved November 12, 2008, from http://www.aicpa.org/pubs/cpaltr/nov2002

Anderson, E.E., and Choobineh, J. (2008). Enterprise information security strategies. *Computers and Security, Corrected Proof.* 23(3), 56-69

Artzner, P., Delbaen, F., Eber, J.M., Heath, D. and Ku, H., (2007). Coherent multiperiod risk adjusted values and Bellman's principle. *Annals of Operations Research*, 15 (2) 5–22

Balbas, A. (2007). Mathematical Methods in Modern Risk Measurement: A Survey, *Applied Mathematics,*101(2) 205–219

Basel Committee on Banking Supervision. (2004). Consultative Document. *New Basel Capital Accord Operational Risk*

Basel II. (2004). *The new Basel capital accord*. Switzerland: Bank for International Settlements

Bayaga, A. (2010).Institutional risk management: Analysis of factors associated with the extent of monitoring and reporting of Risk. *The Journal of International Social Research,* (3)10, 77-89

Burget, C. and Ruschendorf, L. (2006). Consistent risk measures for portfolio vectors. *Insurance: Mathematics and Economics*, 38, 289–297

Calder, A. (2006). *Information security based on ISO 27001/ISO 17799.* Amersfoort - NL: Van Haren Publishing

Casdagli, M. (1992). Chaos and deterministic versus stochastic non-linear modelling, *Journal of the Royal Statistical Society,* 54(2), 303-328

Casualty Actuarial Society, CAS. (2003). *Overview of Enterprise Risk Management. CAS.*

Cody, R.P, and Smith, J.K. (2005). *Applied statistics and the SAS programming language*. Upper Saddle River, NJ: Prentice Hall

Committee of Sponsoring Organizations, COSO (2004). *Enterprise risk management—integrated framework.* COSO: New York

Conner F.W. and Coviello, A.W. (2004). Information security governance: A call to action. The Corporate Governance Task Force.

Creswell, J.W. (2007). *Qualitative inquiry and research design: Choosing* *among five traditions*. (2nd ed). Thousand Oaks: Sage

Cronbach, L.J. (1951). Coefficient alpha and the internal structure of tests. *Psychometrika*, 16(3), 297-334

Curley, M. (2004). *Managing information technology for business value.* Intel Press

De Vos, A.S., Strydom, H., Fouché, C.B. and Delport, C.S.L. (2005). *Research at grassroots: For the social sciences and human service professions* (3rd ed.) Pretoria: Van Schaik

Ericsson, M. (2007). *The governance landscape: Steering and measuring development organisations to align with business strategy*. Retrieved: November 12, 2008, from www.ibm.com/developerworks/rational/library

Fidell, A. (2009). *Discovering statistics with SPSS*. London: Sage

Flowerday, S., and Von Solms, R. (2005). Real-time information integrity = system integrity + data integrity + continuous assurances. *Computers and Security, 24* (8), 604-613 Retrieved November 7, 2008 from http://www.isaca.org/AMTemplate.cfm

Froot, K.A. and Stein, J.C. (1998). Risk management, capital budgeting, and capital structure policy for financial institutions: An integrated approach. *Journal of Financial Economics,* 47, 55 82

Gattiker, T.F. and Goodhue, D.L. (2004). Understanding the local-level costs and benefits of ERP through organizational information processing theory, *Information & Management,* 41(4), 431-443

Gerber, M. and Von Solms, R. (2005). Management of risk in the information age. *Computers & Security, 24* (1), 16-30

Hubbard, D. (2007). *How to measure anything: finding the value of intangibles in business.* John Wiley and Sons. US

IT Governance Institute, ITGI. (2009). *Enterprise risk: identify, govern and manage IT Risk,* The Risk

IT Governance Institute, ITGI. (2003). *Board briefing on IT governance*

IT Governance Institute, ITGI. (2007). *CobiT 4.., Executive Summary*

Kim, S., Kim, S. and Lee, G. (2006). Structure design and test of enterprise security management system with advanced internal security. *Future Generation Computer Systems, Article in press, Corrected proof*

King III Report. (2009). *King Committee on Governance: code of Governance Principles for South Africa*. South Africa

KPMG. (2008). *Understanding and articulating risk appetite*. Retrieved November7, 2008, fromhttp://www.kpmg.com.au/Portals/0/ias_erm-

Kritzinger, E. and Smith, E. (2008). Information security management: An information security retrieval and awareness model for industry. *Computers and Security*, 224-331

Lam, J. (2006). *Emerging best practices in developing key risk indicators and ERM reporting*. Japan: James Lam and Associates

Layton, T. (2007). *Information security: design, implementation, measurement and compliance.* BocaAuerbach:Raton

Lee, W.S., and Jang, S.S. (nd). *A Study on information securitymanagement system model for small and medium enterprises*. Sage: NY. USA

Liebenberg, A. and Hoyt, R. (2003). The determinants of enterprise risk management: Evidence from the appointment of chief risk officers. *Risk Management and Insurance Review*. 6(1), 37–52

Lorenz, E. (1969). How much better can weather prediction become? *Technology Review.* July/August**,** 39-49

Lutchen, M.D. (2004). *Managing IT as a business.* USA: John Wiley and Sons

McBride, N. (1999). *Chaos theory and information systems*. Unpublished working paper. retrieved Jan 20 2010http://www.cse.dmu.ac.uk/

McBride, N. (2005). Chaos theory as a model for interpreting information systems in organizations*. Information Systems,* 15, 233–254

McNeil, A.J., Frey, R., and Embrechts, P. (2005). *Quantitative Risk management; concepts, techniques, and tools*. Princeton: Princeton University

Meyers, L.S., Gamst, G., and Guarino, A.J. (2006). *Applied multivariate research*. Thousand Oaks, CA: Sage

National Credit Regulator. (2008). *About the NCR*. Retrieved February 21, 2009, from http://www.ncr.org.za/the_NCR.html

Nicholas, J.M. and Steyn, A. (2008). *Project management for business and engineering*: principles and practices:' (3rd ed). Burlington, MA: Butterworth Heineman

Olivier, M. (2006). *Information technology research.*Pretoria: Van Schaik

Pallant, J. (2005). *SPSS Survival Manual*. London: Open University

Pflug, G.C. (2006). Subdifferential representation of risk measures. *Mathematical Programming*, Ser B, 108

Posthumus, S. and Von Solms, R. (2004). A framework for the governance of information security, *Computers & Security*, 23, 638-646

PricewaterhouseCoopers. (2007). IT Risk—closing the gap: giving the board what it needs to understand. manage and challenge IT risk. Price water house Coopers. PWC

Quinn, L.R. (2008). *The evolution of enterprise risk management.* Retrieved 14 October 2008, http://www.investopedia.com/a

Raykov, T. and Marcoulides, G.A. (2008). *An introduction to applied multivariate analysis*. New York, NY: Routledge

Ritchie, B. and Brindley, C. (2000). Disintermediation, disintegration and risk in the MSE global supply chain. *Management Decision,* 38(8) 575-583

Rockafellar, R.T., Uryasev, S. and Zabarankin, M. (2006). Generalized deviations in risk analysis. *Finance & Stochastics,* 10, 51–74

Sholes, M. (2007). R*isking business value*. Retrieved February 3, 2009, from http://www.mhmonline.com/viewStory

Smith, E.H. and Kruger, H.A. (2010). *A framework for evaluating IT security investments in a banking environment.* Information Systems. South Africa (ISSA) 2010 Conference: ISSA 2010, Proceedings. published by the IEEE Online

South Africa. (2006). Department of Trade and Industry. *Micro Finance Regulatory Council (MFRC)*. Retrieved February 21, 2009, from The DTI: http://www.dti.gov.za/thedti/mfrc.htm

Standing, C., Guilfoyle, A., Lin, C. and Love, P.E.D. (2007). The attribution of success and failure in IT projects. *Industrial Management & Data Systems.106 (8),* 1148-1165

Stoney, C. (2007). *Risk management: a guide to its relevance and application in Quality management and enhancement.* Leeds Metropolitan University

Tabachnick, B.G. (2008). *Multivariate statistics: an introduction and some applications.* Invited workshop presented to the American Psychology - Law Society, Jacksonsville, FL

Tabachnick, B.G., and Fidell, L.S. (2007). *Using multivariate statistics,* (5th ed*).* Boston: Allyn and Bacon

Thiétart, R.A. and Forgues, B. (1995). Chaos theory and organization, *Organisation Science*, 6(1), 19-31

Tsoukas, H. (1998). Chaos, complexity and organization theory. *Organization*, 5, 291–313

Turban, E. and Meredith, J.R. (1998). *Fundamentals of management* *science,* McGraw-Hill College: Thomson South-Western. NY

Weill, P. and Ross, J.W. (2004). *IT governance: How top performers manage IT decision rights for superior results*, Harvard Business School

Williams, P. (2005). Optimising returns from IT-related business Investments. *Information Systems Control Journal*, 5, 23-38

Yeo, K.T. (2002). Critical failure factors in information system projects. *International Journal of Project Management*, 20(3), 241-246

ACRONYMS

Analysis of Co- Variance	ANCOVA
Casualty Actuarial Society	CAS
Chief Information Officer	CIO
Combined-Mixed Design	CMD
Committee of Sponsoring Organisations	COSO
Control Objectives for Information and related Technology	COBIT
Human Resource	HR
Independent Variables	IVs
Information Communication Technology	ICT
Information Security Management System	ISMS

Information Technology	IT
Information Technology Risk Management	ITRM
Institutional Risk Management	IRM
IT Governance Institute	ITGI
Kaiser-Meyer-Olkin	KMO
Kolmogorov-Smirnov	KS
Multivariate Analysis Of Variance	MANOVA
Operational Risk Management	ORM
Pure Technical Efficiency	PTE
Repeated-Measures Analysis of Variance	RM-ANOVA
Repeated-Measures Multivariate Analysis of Variance	RM-MANOVA
Small And Medium Enterprises	MSEs
South Africa	SA
Statistical Package for the Social Sciences	SPSS
Value Information Technology	ValIT

GLOSSARY

Information Technology

IT is hardware and software. IT automates an information system which is independent on IT. The term IT used within this study refers to both IT and IS interchangeably, as the two in effect operate together within an organisation to enable business objectives to be met.

Risk

The potential of loss and/or damage to assets through vulnerabilities. It is usually measured by a combination of impact and probability of occurrence (ITGI, 2005).

Model

A basic conceptual structure, used to solve a complex issue.

Information technology (IT) risk

Business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise. It consists of IT-related events that can potentially impact the business. It includes both uncertain frequency and magnitude, and it creates challenges in meeting strategic goals and objectives as well as uncertainty in the pursuit of opportunities(ITGI, 2009).

A nonlinear dynamic system

Is a system where relationships between time-dependent variables are nonlinear.

Chaotic behaviour

Is not a lack of order, but order of a complexity that is difficult or impossible to describe in simple terms and cannot be broken down into simple equations but require a complex narrative to describe it. The patterns in chaotic behaviour are present, but not regular or easily predictable.

Chaos

Is ordered disorder.

Homoscedasticity

This means that in multiple regression, the variance is constant across all levels of the predicted variable.

Risk

The potential of loss and/or damage to assets through vulnerabilities. It is usually measured by a combination of impact and probability of occurrence (ITGI, 2005).

APPENDIX A: QUESTIONNAIRE

30th October 2010

Real People
East London

Re: Request to conduct research in conjunction with Real People

The purpose of this research project is to investigate ICT Risk as a component of Operational Risk Management (ORM). This study will benefit Real People by highlighting the impact of ICT on ORM within MSEs by means of testing a number of formulated propositions. An anonymous questionnaire will be distributed electronically to 90 Real People employees taking no more than 15 minutes to complete. The information will be kept confidential.

The objectives of the study are to:

- Analyse the principal causes of ORM failure related to ICT
- Assess change management requirements and ICT Risk
- Identify which characteristic(s) of information influences ICT Risk
- Identify the challenges posed by ORM solutions
- Assess evaluation models affecting ICT adoption within MSEs

Sincerely yours,

Mr. A. Bayaga and Prof. S. Flowerday

QUESTIONNAIRE

Impact of ICT and Operational Risk Management within MSEs

In recent years many factors have fuelled a heightened interest in Information Communication Technology (ICT) and Operational Risk Management (ORM). This questionnaire aims to investigate ICT within the context of Operational Risk. Please indicate the extent to which you agree/disagree with the following statements.

Please **tick** the number which characterises the situation in your institution.

Background

1. **Gender**

(a) Male (b) Female

2. **Department**

(a) IT (b) HR (c) Finance (d) Operations (e) Support

(f) Other……………………

3. **Position**

(a) Middle Management (b) Senior Management (c) Operations

(f) Other……………………

4. **Age (in years)**

(a) Less than 20 (b) 20-25 (c) 26-30 (d) 31-35

(e) 36-40 (f) 41-45 (g) 46 or more

5. Years of Service

Less than 1, 2 , 3, 4, 5, More than 5 years

6. Education

(a) Less than Matric (b) Matric (c) Diploma (d) Degree (e) Post graduate
(f) Other……………………

SECTION H1: Principal causes of ICT failure and ORM adoption

This section seeks to name and describe the principal causes of ICT failure by information systems in MSEs.

1 – Strongly Disagree 3 - Agree

2 – Disagree 4 – Strongly Agree

1. One of the principal causes of information system failure is insufficient or improper user participation in the systems development process.	1	2	3	4
2. One of the principal causes of information system failure is lack of management support.	1	2	3	4

3. One of the principal causes of information system failure is high levels of complexity and risk in the systems development process.	1	2	3	4
4. One of the principal causes of information system failure is the process of organizational change surrounding the new system.	1	2	3	4
5. One of the principal causes of information system failure is poor management of the implementation process.	1	2	3	4

SECTION H2: Change management requirements and ICT ORM adoption

This section seeks to interrogate the issue of organisational change surrounding a new information system in MSEs.

1 – Strongly Disagree

2 – Disagree

3 - Agree

4 – Strongly Agree

1. There is a high failure rate among enterprise application projects because they require extensive organizational change that is often resisted by members of the organization.	1	2	3	4
2. Enterprise applications are difficult to implement successfully because they usually require far-reaching changes to business processes.	1	2	3	4
3. The success of organizational change can be determined by how well information system **end users** deal with various stages in the implementation of ICT projects.	1	2	3	4
4. The success of organizational change can be determined by how well information systems **decision makers** deal with various stages in the implementation of ICT projects.	1	2	3	4

SECTION H3: Information characteristics and ICT ORM adoption

This section seeks to interrogate **information characteristics.**

1 – Strongly Disagree
3 - Agree

2 – Disagree
4 – Strongly Agree

1. The impact of the **confidentiality** of information has a direct relationship with my work performance.	1	2	3	4
2. The impact of the **integrity** of information has a direct relationship with my work performance.	1	2	3	4
3. The impact of the **availability** of information has a direct relationship with my work performance.	1	2	3	4
4. The impact of the **quality** information has a direct relationship with my work performance.	1	2	3	4
5. The impact of the **relevance** of information has a direct relationship with my work performance.	1	2	3	4

SECTION H4: Similar actions taken by organisations and ICT ORM adoption.

Identify the challenges posed by ORM solutions.

1 – Strongly Disagree
3 - Agree

2 – Disagree
4 – Strongly Agree

1. Maintaining an appropriate level of user involvement at all stages of the systems development lifecycle is essential.	1	2	3	4

2. Information system design should be managed as planned organizational change.	1	2	3	4
3. People, social and technology (sociotechnical design) aims for an optimal blend of achieving both excellent technology and people’s work performance.	1	2	3	4
4. Developing metrics and processes provide business value to ICT project management.	1	2	3	4

SECTION H5: Evaluation models and ICT adoption

This section seeks to evaluate and align objectives of executive management and information systems projects.

1 – Strongly Disagree 3 - Agree

2 – Disagree 4 – Strongly Agree

1. Payback method is used to evaluate and align objectives of executive management and information systems projects.	1	2	3	4
2. Net Present Value (NPV) method is used to evaluate and align objectives of executive management and information systems projects.	1	2	3	4
3. Internal Rate of Return (IRR) method is used to evaluate and align objectives of executive management and information systems projects.	1	2	3	4

4. Portfolio analysis and scoring models are used to evaluate and align objectives of executive management and information systems projects.	1	2	3	4
5. ValIT framework is used to evaluate and align objectives of executive management and information systems projects.	1	2	3	4
6. COBIT framework is used to evaluate and align objectives of executive management and information systems projects.	1	2	3	4

End: Thank you

APPENDIX B: PUBLISHED ARTICLE