UNIVERSITY OF CAPE TOWN

Conceptualising Improvisation in Information Security Risk Management Activities: A South African Case Study

Thesis Presented for the Degree of

DOCTOR OF PHILOSOPHY

in the Department of Information Systems

UNIVERSITY OF CAPE TOWN

February 2009

By

Name: Kennedy Nduati Njenga (Researcher)

Student Number: NJNKEN001

Dedication

TO MOM,
MARTHA AND NICOLE

FOR YOUR LOVE, GUIDANCE AND SUPPORT.
THIS THESIS IS DEDICATED TO YOU

Acknowledgments

Firstly, I would like to acknowledge **Professor Irwin J. Brown** of the University of Cape Town. His financial support, thoughts, ideas, and the lessons given to me on the research process and the structuring of this thesis were invaluable. His advice was always and continues to be useful.

I am indebted as well to **Professor Dewald Roode** of the University of Pretoria for his confidence in me and the advice he provided me during the first stages of this research study. I'm also very grateful for his comments and suggestions up to the completion of this thesis.

In addition, I am grateful for the comments and suggestions provided by **Dr Cathy Urquhart** of the University of Auckland, New Zealand and the rest of the anonymous reviewers of the PACIS Doctoral Consortium held in Auckland, New Zealand on the paper upon which many of the thesis chapters are built.

I would like to thank all my friends and colleagues at the **University of Cape Town** for the support and encouragement they showed me. I am indebted as well to the **Post Graduate Funding Office - UCT** for the scholarship given towards this study. This thesis would not have been possible without the support of these people mentioned.

I must not forget the IS executives and the rest of the Information Security Practitioners who gave of up their valuable time to participate in this research and for allowing me to collect data in their organisation. I'd like to say thank you.

Finally, I would like to thank my **family and friends**. I could not have completed this thesis without their understanding, patience, encouragement and support.

Preface

Parts of this thesis have already appeared in publications. These include the proceedings of *the 3rd IT Governance International Conference 2006*, Auckland, New Zealand, proceedings of *the 6th Conference on Information Security 2006*, Sandton, South Africa, proceedings of *the 11th Pacific Asia Conference on Information Systems–PACIS 2007 (Doctoral Consortium)* Auckland, New Zealand, and the proceedings of *the 7th Conference on Information Security, 2008. Auckland Park, South Africa*

This acceptance by the scholarly community has given direction, encouragement and impetus to the production of this thesis. In all cases, the published works have been re-formatted, updated and synthesized into this thesis.

Statement of Authentication

The work presented in this thesis is my own unaided work and is, to the best of my knowledge and belief, original, except as acknowledged in the text. I hereby declare that I have not submitted this material, either in whole or in part, for a degree at this or any other institution.

…….

(Signature)

…….

Abstract

The research gives a detailed overview of Information Security Risk Management (ISRM), a phenomenon ranked as a top issue of concern to Information Systems Management. The research was an in-depth conceptualisation of ISRM activities and the approaches towards these activities. The research identified two main approaches to ISRM; the functionalist rational approach and the incremental approach. The aim of this research was to understand how functionalist approaches and the incremental approaches are manifested in ISRM activities. New insights and meaning to the ISRM activities were presented when the incrementalist approaches to ISRM and the functionalist approaches to ISRM were examined holistically. *Improvisation,* for the purpose of this research, was used to explain this holistic understanding. Finding the manifestation of *improvisation* in ISRM activities as the holistic approach was therefore the main purpose for this research. The analogy of musical *improvisation* and jazz was the foundation for the insights about *improvisation.* The research problem posed in this research was that there was little evidence in literature to suggest that *improvisation* had been considered in ISRM activities. The research adopted a single case study strategy (of a multinational organisation). The research data collected was qualitative data, obtained through in-depth interviews, observations and review of the organisation's internal documents. The researcher also formulated an *a priori* theoretical framework, termed a *Sensitising Device* that was used as a lens for qualitative data analysis. The data obtained was analysed, interpreted and conceptualised using qualitative grounded theory techniques. The key knowledge claim (the key contribution to ISRM literature) for this research was that '*generally improvisation is manifested in ISRM activities and these manifestations occur in a variety of ways'.* One of the findings that support this claim was that there was a general trend toward *process improvisation,* being a more conceptually dense form of *improvisation* than any other *improvisation* type in ISRM activities. This research concluded by identifying implications of these findings for the scholarly community and for practical use.

TABLE OF CONTENTS

List of Tables

List of Figures

CHAPTER ONE

This chapter introduces important issues that relate to Information Security Risk Management. The chapter presents and justifies a need for research into this area. A distinction is drawn from the many approaches that aim at optimal allocation of information security resources, (including cognitive resources) in protecting systems in an organization. The chapter briefly introduces *improvisation* as one of the approaches. A problem statement is formulated to give direction into the research.

Table of Content

Chapter One

CHAPTER ONE: INTRODUCTION

1.0 BACKGROUND TO INFORMATION SECURITY RISK MANAGEMENT (ISRM)

Modern organizations have become dependent on information technology (IT) and IT has come to be seen as increasingly vulnerable. It has been noted that while the spending on IT infrastructures has increased proportionately with time, so has the level of spending on information security (Middleton 2006). Studies that focus on how organisations deal with information security show that information security management is really about risk management of IT and processes (Smith *et al.* 2003).

Information security management and therefore risk management has increasingly been placed on a high priority scale. Organisations that understand the importance of information security management and risk management, have taken proactive steps to place these two management structures at par. This has resulted to these organisations having to spend less on information security and risk management.

Information Security Risk Management (ISRM) is seen as *the process of administering people, policies, and programs with the objective of assuring safety, protection and continuity of operations.* ISRM has moved from a situation whereby it was completely ignored, (Straub and Welke 1998) to one where it is now ranked as one of the top concerns by IS management (Luftman and McLean 2004). The relevance of ISRM, its knowledge, understanding and awareness by organizations have attracted interest among information security researchers (e.g. Thompson and Von Solms 1997; Straub and Welke 1998; Siponen 2000; Von Solms and Von Solms 2005;Vorster and Labuschagne 2006).

Chambers *et al*. (2005) list examples where organizations around the world have created security risk awareness through training programs that help boost their strategic security needs. Many large organisations continue to develop comprehensive approaches to information security which incorporate enterprise complexities (Chambers *et al.* 2005). The comprehensiveness of approaches to security is deficient if awareness of security issues is not prioritised. That is why it has been imperative for organisations to create security awareness programs that help users

understand how to value their assets, how to examine threats to these assets and finally how to safeguard the assets (Smith *et al*. 2003).

In the United States, the level of importance placed on ISRM is clear. The federal government has initiated an innovative program that addresses security risks and awareness by assisting its federal agencies in conforming to requirements stipulated by the Federal Information Security Management Act (FISMA) (Schultz 2005). The FISMA initiative is considered essential in providing assurances to its users of "*confidentiality*, *integrity*, and *validity* of federal systems" (Schultz 2005). Similarly, in Singapore, the government has initiated its InfoComm Security Master Plan "to provide momentum for developing the manpower needs to manage the growing number of cyber threats". The National InfoComm Security Committee and the InfoComm Development Authority (IDA) have set up a program that focuses on organisations, that seeks to enhance training and to augment skills of security professionals (Schultz 2005).

In South Africa, ISRM processes and methodologies have been driven by compliance requirements brought about by regulatory acts such as the Sarbanes-Oxley (SOX) Act (for US companies with branches/subsidiaries or close ties within South Africa), the Health Insurance Portability and Accountability Act (HIPAA) and the Electronics and Communication Transactions Act (ECT Act) (Middleton 2006; Vorster and Labuschagne 2006). The Regulation of Interception of Communications Act (RICA), the Provision of Communications Related Information Act and King II have also featured on a lesser scale within the South African information security landscape. Many South African organisations have been slow in taking account of these new trends in legislation. This has had an adverse impact on the South African information security landscape. Nonetheless, for matters pertaining to information security, South African organisations have been keen to follow the limited legislation available, including the ECT Act, RICA and King II amongst others (Middleton 2006).

Ernst and Young (2004) found that 67% of South African organisations sampled rated information security as critical to achieving overall business objectives compared to 26% who rated information security as 'somewhat important'. It can be concluded that South African organisations are "giving information security top-level priority compared to their global counterparts" (Ernst and Young 2004).

1.1 NEED FOR RESEARCH INTO INFORMATION SECURITY RISK MANAGEMENT ACTIVITIES

The importance of understanding Information Security Risk Management (ISRM) is great when consideration is given to the many risks and vulnerabilities associated with information systems and technologies. The importance of also understanding **how** ISRM is carried out in an organisation is equally great and has a profound impact on the quality of information to be relied upon to efficiently run organisations (Straub and Welke 1998). This research begins with understanding what constitutes the entire spectrum of ISRM activities and how these activities are carried out. It is generally agreed among information security practitioners that research that draws our attention to ISRM activities has become increasingly important. This is especially so when research on ISRM helps information security practitioners understand how to contextually cope with uncertainties, vulnerabilities and risks caused by increased usage of computers and the internet (Siponen and Kukkonen 2007).

Anecdotal evidence from information security practitioners suggests that during times of heightened uncertainty, structured managerial activities focused on imposing control and order are usually required. There has not yet been conclusive research which suggests that these control and order measures are sufficient. Furthermore, there are some researchers who have suggested clear structured policies as being the only way to deal with risks and uncertainties. These clear structured policies are, for the purpose of this research, classified as **functionalist approaches**. Noting the functionalist approach to Information Security, Hu *et al.* (2007) considered how modern organisations have established routines and order to cope with internal and external influences of information security risk. Not surprisingly, the functionalist approach to order is evidenced by numerous publications that offer normative guidelines for designing, implementing and managing secure information systems (Baskerville 1988; Straub and Welke 1998). In their studies in Information Security, Dhillon and Backhouse (2001) have noted the dominance of the functionalist paradigm that emphasizes formalized rule structures in designing and managing security.

There are some researchers that have countered functionalist claims to ISRM and have called for the need for broader responsibilities by management regarding information security issues (Von Solms and Von Solms 2004). These researchers have become aware of an increasing number of

'new' approaches that explore alternative perspectives related to the interpretive, radical humanist and radical structuralist paradigms. These latter paradigms are based on sociological and philosophical theories (Hu *et al.* 2007). Researchers using these latter approaches which call for alternative ways of understanding ISRM have been classified as **incrementalists**. South African organisations have started to develop comprehensive approaches to ISRM that incorporate the complexities of their enterprises (Chambers et al 2005), the people and resources in an attempt to adhere to local compliance requirements. It is how South African organisations approach ISRM from a functionalist, incrementalist or both approaches that is of interest to this research. The research concerns itself with understanding how the information security practitioners attempt to mirror best practices by setting local baselines. This contextual understanding has justifiably generated great interest amongst quite a few South African information security researchers and many others across the globe (e.g. Thompson and Von Solms 1997; Straub and Welke 1998; Siponen 2000; Von Solms and Von Solms 2005).

1.2 NEED FOR RESEARCH INTO IMPROVISATION

Individual role *improvisation* is a phenomenon researched by social scientists due to its perceived importance in emergency response and planning (Webb 2006). However, there is little indication by way of publication that this phenomenon has been researched in ISRM and more specifically in the management and planning of information security risk. Webb (2006) appreciates the magnitude of problems faced by planners who have attempted to embrace approaches that emphasise centralised command and control (functionalist approach), a by-product of which discourages creativity. By extension, planning and managing information security risk from these centralised forms impedes reflexivity. A myriad of written rules, policies, guidelines, frameworks and standards that spell out exactly how security risk practitioners should perform their activities is an example of such an impediment. Webb (2006) depicts the strength of effective planning and management as means to encourage creativity and reflexivity as opposed to the rigid approach characterised by centralised control. The focus of the research has been geared towards exploring and conceptualising the presence of or impediments to reflexivity and *improvisation* in ISRM activities outside of functionalist approaches.

1.3 RESEARCH QUESTION AND PROBLEM STATEMENT

ISRM is embedded with characteristics that transcend ordinary risk management areas. There are functionalist rational approaches that characterize ISRM (Von Solms and Von Solms 2005; Schultz 2005) as well as creative reflexive approaches present in organisations (Suchman 1987; Zuboff 1988). New meaning to the ISRM process is presented when the incrementalist approaches to ISRM (reflexive and creative) and the functionalist structured approaches to ISRM are examined holistically. *Improvisation* for the purpose of this research is used to explain this holistic examination. (Improvisation is explained in depth in the subsequent chapters). The following problem statement therefore defines this research:

> ***How is improvisation manifested in Information Security Risk Management (ISRM) activities and how can improvisation in ISRM be conceptualised?***

This research therefore focused on how practitioners managed information security risks and incidents. ***Finding meaning*** attributed to the management and intervention processes in ISRM remained the focus of this research. The goal of the research was to provide insightful new awareness of the contrasts between *de-facto* routinised interventions to ISRM and those that were identified to be creative, spontaneous and improvised actions. Flowing from this main research problem are the following sub-questions:

- *What ISRM activities are in an organisation and how are they carried out?*
- *How is improvisation manifested in these ISRM activities in the organisation?*
- *How can improvisation in ISRM be conceptualised**?***
- *How can improvisation be used as a foundation for Positive ISRM?*

The research problem presented by these questions opens up understanding of conceptual issues and approaches to ISRM activities that have not been given much research attention. In a general sense, **Chapter 2** starts by explaining the general ISRM activities in an organisation. **Chapter 3** and **Chapter 4** give an indication as to the manifestations of *improvisation* in organisations, specifically extending these to ISRM activities. **Chapter 6** explains the outcomes of *improvisation* in ISRM activities, while **Chapter 7** conceptualises *improvisation* in ISRM. It is

by conceptualising the above questions and issues that a sharper focus of the ISRM process is brought to bear.

1.4 RESEARCH PURPOSE

Literature on ISRM is heavily functionalist and does not consider the soft approach of *improvisation*. Therefore this research is an attempt to address this gap in the literature. It follows then that the nature of the research targeted those specific and improvised interventions that mitigated risk. Studies that go a step further in the review of the meaning assigned to human behaviour with Information Systems use are encapsulated in the works of Boland (1991); Deetz (1996); Orlikowski and Baroudi (1991). These studies have revealed that understanding human behaviour is gained only through understanding meaning assigned to phenomena. Understanding meaning is achieved through social constructions such as language, consciousness, shared meanings, documents, tools, and other artefacts. This research looks at understanding the meaning of *improvisation* in ISRM by significantly considering previous research on situated action constrained by time (Suchman 1987; Zuboff 1988). This consideration aims to offer convincing reasons as to the meaning behind certain ISRM actions and is demonstrated in the latter sections of this thesis.

1.4.1 Research Value

It was anticipated that a detailed in-depth case study would be appropriate to research *improvisation*. The case would demonstrate rich cognitive insights from information security risk practitioners. The research is characterised by the appropriate use of information security risk terminology that captures ISRM cognitive aspects. The themes and cognitive aspects inductively and deductively provide a substantive theory that recognises *improvisation* in ISRM. The value of the research after conceptualisation is explained in the following section.

This research was undertaken to provide deeper insights into ISRM and enrich the literature in Information Systems and Security, by revealing the softer areas that have so far received little research attention in ISRM. The assigning of meaning to the role that reflexive activities (including *improvisation*) play adds value by providing deeper insights into the phenomenon of *improvisation* in organisations. The underlying motivation for the research and the intended

beneficiaries (academics and information security practitioners alike) has been discussed in this chapter. The chapter has also raised awareness of issues and that may be deemed important in ISRM generally. The following section describes how this awareness is developed and gives an outline of the thesis.

1.5 THESIS OUTLINE

This thesis consists of eight (8) chapters. **Chapter I** started by introducing ISRM and why it was necessary to carry out this research. **Chapter 2** discusses the general approach towards ISRM activities by giving a detailed explanation of what these ISRM activities are. This was achieved by carrying out a detailed literature review on ISRM. This chapter unpacks terminology common to information security risk practitioners. **Chapter 3** discusses how these ISRM activities are carried out in organisations. The chapter introduces two main approaches to ISRM and discusses the first approach (structured functionalist approach) in greater detail. **Chapter 4** explains the incremental approach (reflexive approach) to ISRM. **Chapter 4** also provides a holistic synergy between the functionalist and incrementalist approaches by presenting a fusion framework: the holistic approach. This chapter concludes by explaining how *improvisation* is manifested as a fusion of these two approaches. **Chapter 5** discusses the research methodology and the methods used to carry out this research. This chapter outlines how knowledge about *improvisation* in ISRM was scientifically generated. **Chapter 6** discusses the outcomes of *improvisation* in ISRM activities using an in-depth qualitative data analysis technique. **Chapter 7** interprets and conceptualises *improvisation* in ISRM through a combination of primary interview data and document analysis. **Chapter 8** gives an overall conclusion on the research findings. **Figure 1** (next page) illustrates the research outline.

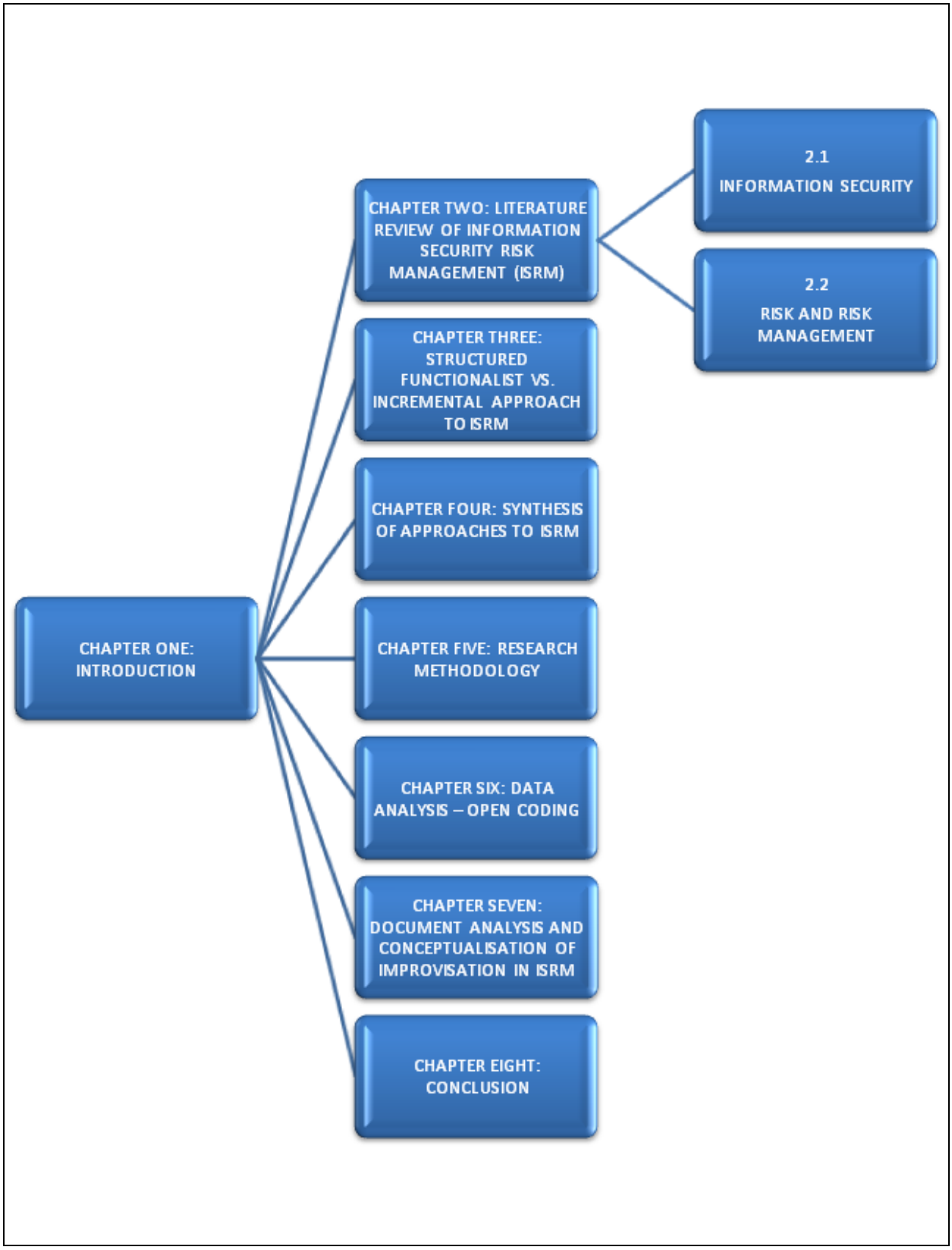


Figure 1. Thesis Layout

CHAPTER TWO

This chapter unpacks the concept of information security risk and how this is managed. The chapter is an attempt to better understand the nature of risk and how the technical and the social issues within an organization influences practitioners' actions for improving information systems security. The chapter places significance on the need for conceptualising information security risk.

Table of Content

Chapter Two

CHAPTER TWO: LITERATURE REVIEW OF INFORMATION SECURITY RISK MANAGEMENT

2.0 INTRODUCTION

The significance attached to the need for conceptualising information security risk management (ISRM) should be high when consideration is given to the following statistics. In 1998, the Computer Security Institute (CSI) and the Federal Bureau of Investigations (FBI) conducted a survey of information security managers. The survey generated responses from over 400 respondents. 64% of these respondents had reported computer security breaches, while 54% indicated that their organisations were attacked via internet connections. 70% of the respondents also reported unauthorised uses by insiders (Forno and Baklarz 1999). Given the above statistics, ISRM predicatively, is given much attention particularly in rapid environmental turbulence and unpredictability where breaches and vulnerabilities keep occurring. On account of turbulence and unpredictability, organisations have gone to great lengths to leverage their security postures. Some have performed exceptionally well while others have performed dismally.

Planning and structure (referred to as functionalism) in this research can have negative consequences to ISRM because they consume time and resources and provide counterproductive guides to action when the context changes faster than the planning cycle (Eisenhardt and Tabrizi 1995). This is particularly so in rapid environmental turbulence and unpredictability. There is constant frustration among unsuccessful organisations due to security incidents that have largely been unpredictable, making functionalist guidelines and standards less effective. The frustration is exacerbated by information security practitioners' inability to identify effective strategies in times of unpredictability, uncertainty and chaos.

This research conjectures that what makes a difference and is the key distinguishing element contributing to success in ISRM practices stems from significant contextual and cognitive differences in approach to ISRM by information security practitioners. This chapter aims to elaborate on how organisations currently manage information security risk. It will do this by focussing on typical functionalist structured implementing procedures and guidelines as contained in standard codes of practice such as ISO IEC 17799 (ISO 17799).

In order to understand cognitive and contextual differences that influence the approach to ISRM by information security practitioners, it becomes necessary to understand the science and practice of ISRM including the many associated activities at a deeper conceptual level. This chapter contributes to a deeper understanding of ISRM by examining the concept of information security risk and its importance. The chapter closely examines the main concepts of information risk as an important managerial issue and the value attributed to protecting organisational information. The chapter aims to give clarity about *risk* to information systems, *about information security in* organizations by examining threats and vulnerabilities to information and, finally, about the *management* process of these attributes.

The next sections of this chapter are divided into five sections. The first section looks at concepts associated with information security. The second section examines in detail concepts of risk. The third section draws a distinction between the use of various concepts and terminologies associated with information security risk. This section clarifies the use of these terminologies. The fourth section talks of the process of managing information security risk in organisations and contextualises the South Africa perspective. The last section gives an overall summary of this chapter.

2.1 INFORMATION SECURITY

There are concerns that deal with information systems (IS) that tend to revolve around information security. Information systems as a discipline refers to a system of people, data records and activities that process the data and information in an organization, and it includes the organization's manual and automated processes (Trcek *et al.* 2007). ***Information security*** on the other hand means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction.

At a meta level, the science of the main components of the Information Security process considers three components: *confidentiality*, *availability* and *integrity* of information (Tudor 2001). The understanding of these three concepts should be placed in the following perspective:

1) that many organisations have increasingly placed a high value on information and classified certain sections of it as assets to be treated confidentially and accessed by only those who are designated to do so;

2) that organisations have placed security on information systems making information available to only those authorised to do so;
3) that the information to be accessed and used for managerial activities passes integrity checks by way of accuracy checks, completeness and freedom from unauthorised manipulation.

Parker (2002) extended the components explained by Tudor (2001) with the incorporation of additional concepts such as; *utility*, *deterrence*, *possession*, *prevention*, *detection*, *mitigation*, *transference*, *sanctions and rewards*, *recovery* and *correction of loss*.

2.1.1 Information as a Valued Asset

When organizations speak of information as being assets they consider a resource that should be controlled. Peltier (2001) extended the idea of the intangible nature of the information asset being the intellectual property of organizations, characterized by the skills and knowledge of employees.

2.1.2 Importance of Information Security

Forno and Baklarz (1999) saw the need for information security to be considered a management issue primarily because they understood the nature of the information security program as being dependent upon those they managed, namely people. They argued for active management support and engagement with information security risk programs. They also argued the need for the people who administered these programs to be exceptionally skilled and knowledgeable. Forno and Baklarz (1999) acknowledged the relevance of addressing management and people first before technology and postulated the following pillars of Information Security:

a) the pillar of protection that enables managerial activities to be focused on understanding the value of information being protected, and how the planning for protection would occur;
b) the pillar of detection which places managerial emphasis on activities that attempt to recognize the unknown information system vulnerabilities;
c) the pillar of reaction which places managerial concerns in the quantification of information security activities already planned for and put into place to address system breaches;

d) the pillar of documentation which aids information security managers establish trends that could influence an organisation's risk rating, and finally;

e) the pillar of prevention which emphasises the way managers understand the multifaceted nature of security risks when they initiate programs for risk assessments and risk mitigation.

2.2 RISK AND RISK MANAGEMENT

Much research done on risk in terms of risk attitudes and risk perceptions has focused on a value/positive approach (Dyer and Sarin 1982; Weber and Milliman 1997). These researchers have denoted risk to have an associated positive appeal. This means they have seen risk as having some intrinsic benefit or value. Researchers such as Sarin and Weber (1993) described the 'intuitive appeal' to risk value. They saw risk as an open choice dependent on the 'riskiness of the gamble' and its value. There has also been research that associates risk with organisational success as demonstrated by Weber and Milliman (1997) which primarily deals with attitudes towards risk derived from choice.

In this research, the concept of risk should not be seen as an association in the positive. The association of risk in the negative contrasts this research in ways that are significantly different from research done on risk attitudes and risk preference particularly in the theoretical frameworks for decision making under risk, namely risk return also known as **risk-value.** This research considers the negative value associated with risk. In this research, risk is seen as contrary to value or benefit to information systems. Conversely, the negative impact risk has on information system introduces this research to successful ways and activities that would manage risk in ways that reduce or mitigate the negative impact of risk.

2.2.1 Concept of Risk- Negative Association

The National Institute of Standards and Technology (NIST**)** Special Publication 800-30, indicates a negative association with the word **risk**. This standards publication considers risk as a net negative impact resulting from information systems vulnerability. This means risk is seen as a function of *threat-sources* which adversely affect target organizations (NIST SP 800-30). The NIST (SP 800-30) classifies system vulnerabilities as logical (**IT related**), physical (**non-IT-related**) or in combinations of both. Negative association with risk was seen in a study by Peltier (2001) who recognized threats against information systems as 'intents' to act in a

negative way against these systems. Browne et al (2000) equally established this negative association and, in an attempt to measure risk, created a framework that drew a correlation between system vulnerabilities and human activities (such as poor system administration, including failure to apply patches regularly). From the above illustration of negative risk, it is easily recognised that the whole process of managing risks by information security risk practitioners is considered difficult and daunting. Some of the ISRM activities carried out by information security practitioners require comprehensive strategies for achieving acceptable information security postures. The view that risk can be managed requires the acceptance of formalised procedures that determine the proper way to respond to risk while determining the number of controls to put in place to either eliminate risks or mitigate impacts.

Table 1. suggests a formalised but structured (functionalist) way of determining the appropriate response against threats and vulnerabilities when placing sound controls. **Table 1** illustrates three broad categories in responding to threats. It should be noted that information systems are affected by risk and vulnerabilities in three major ways; *severe* risk, *significant* risk and *minor* risk. It should be noted that **severe** risk to information systems has the potential to cripple business operations; **significant** risk can cause serious damage to business processes, while **minor** risk can cause breakdowns that typically affect day-to-day operations. A systematic and structured approach to determining risk levels and how to respond appropriately to risk is illustrated by **Table 1** below;

Table 1. Degree of Impact and Vulnerability Determine Controls. Source: Smith et al (2003).

Degree of Impact and Vulnerability Determine Controls			
	Severe Impact to information system	**Significant** Impact to information system	**Minor** Impact to information system
High Vulnerability	**Conduct** Vulnerability Analysis **Must improve controls**	**improve controls**	**Vulnerability analysis necessary**
Medium Vulnerability	**improve controls**	**Minimal** Vulnerability Analysis **improve controls**	**improve controls**
Low Vulnerability	**controls necessary**	**improve controls**	**Little-no** Vulnerability Analysis **controls**

Degree of Impact and Vulnerability Determine Controls			
	Severe Impact to information system	**Significant** Impact to information system	**Minor** Impact to information system
			unnecessary

When there is severe impact to information systems and the systems have high vulnerability, it is **mandatory to improve controls** (Smith et al 2003). When there is significant impact to information systems and the systems have medium vulnerability, information security practitioners address these threats by **improving controls**. It should be noted that with scenarios of medium vulnerabilities, it is still essential for information security practitioners to improve controls (Smith et al 2003). When there is minor impact to information systems and the information systems have low vulnerability, the resources available to information security practitioners will make it feasible to ignore security threats and hence make **controls unnecessary. Table 1** therefore shows the essential need to conduct vulnerability analysis for both severe and significant risks, particularly where controls are weak for more vulnerable systems.

This research explores activities related to the information security practitioner's cognitive understanding and responses to both the likelihood component (vulnerability) and the probability component (controls) that establish the existence of negative risk in information security risk management. These attributes are designated for conceptualization. **Figure 2** (below) provides a graphical representation of the likelihood and probability component relationships. Parkinson and Baker's (2005) perception of managerial activities considers the risk management process as that of assessing risk. They note that this process requires internalised practitioner skills and knowledge of vulnerabilities in information systems that may lead to potential system failure. They depict three types of risks: Inherent Risk (**IR**) or risk that presents itself in the normal course of doing business; Control Risk or risk that the controls set by an organisation will not detect adverse events; Residual Risk (**RR**) or the risk after controls have been taken into account.

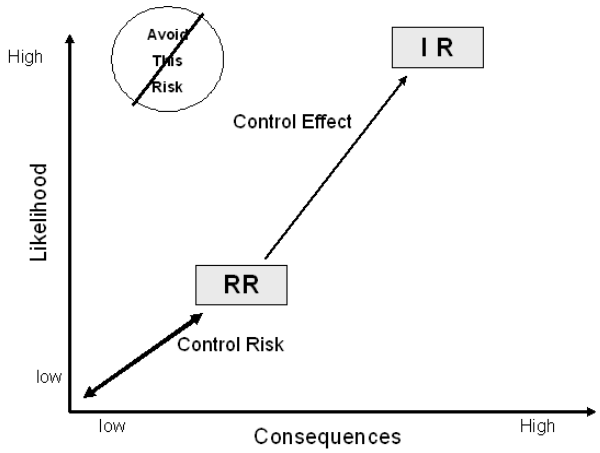


Figure 2. Managing Risk at Various Levels. Source: Parkinson M.J.A. and Baker N. J. (2005)

As pointed out in **Figure 2** above, threat is assessed upwards. By associating risk in the negative, it is established that if the likelihood of threat is low, but consequences are high, it is still very necessary for the managerial processes to initiate and pursue effective control risk policies. **Figure 2** also indicates that the threat and vulnerability components should be applicable to each of the groupings of both the tangible and intangible information assets.

2.2.2 Managing the Negative Risk; Threats and Vulnerabilities

The NIST SP (800-30) defines Risk Management as "the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level" (Burton Group 2005). Risk Management (in information systems) is a threefold process that includes *identifying* risk, *assessing* risk, and *taking steps (managing)* to reduce risk to an acceptable level. This NIST perception suggests two components of risk, i.e. likelihood and probability. To understand this definition it is important to understand the nature of information systems threats like hackers who exploit information systems vulnerabilities. This means the management process looks at the likelihood component of risk from, for example, a hacker's perspective while seeking to reduce the vulnerability of the information systems e.g. from lack of proper patching, weak passwords etc which could be exploited. The risk management process seeks also to understand the probability component, i.e. the probability that a hacker could exploit vulnerabilities. According to the NIST (2003), vulnerabilities have been associated with system weakness, in cases where there were omissions of control mechanisms for the systems or in cases where the controls were not sufficiently robust. Essentially, risk management allows organizations to approach information security in a more structured manner. This is seen as a functionalist approach to ISRM.

As early as the 1990's, threats and the negative aspects of risk were being reported in information systems; this lent to the formal recognition of ISRM. Studies by Neuman (1995) highlighted the importance of recognizing threats to information systems as potential dangers since vulnerabilities could lead to undesirable consequences. The common view of associating threats in negative terms is still maintained as evidenced by more recent studies. Siponen (2000) gives recognition to scientific studies on information security in computer science. Some of the studies, for example, show that organisations engage actively in dealing with information security but respond differently to security threats. Studies by Stoneburger *et al.* (2001) illustrate the way intentional or accidental triggers could exploit systems (or assets) rendering them vulnerable. There are four generic steps that Stoneburger *et al.* (2001) defined for risk management: *identification, measurement, monitoring* and *control*. These generic steps are explained as follows:

a) Identification

Part of the risk identification process suggested by Stoneburger *et al.* (2001) included listing and characterizing individual elements of risk and breaking these down into basic components in order to achieve an effective risk assessment. This process is seen as a useful way of identifying the assets, threats and vulnerability components.

b) Measurement

The measurement process considers consequences and likelihood of risk. Researchers have come up with numerous and varying approaches to risk measurement. Peltier (2001) identified a Risk Value formula as follows;

$$Rv = P \times I$$

Where **Rv** = Risk

P = Probability (Qualitative or Quantitative probability)

I = Impact (Qualitative or Quantitative impact) (Peltier 2001).

The above functionalist formula by Peltier (2001) can be contrasted with Browne *et al.*'s (2000) mathematical framework that associates exploits with system vulnerabilities and of the reporting of such exploits. This formula is shown below as follows:

$$C = I + S \times \sqrt{M}$$

Where **C** = cumulative count of reported risk incidents;

M = time since the first exploit cycle;

I and **S** are regression coefficients determined by analysis of the incidence report (Browne et al 2000).

c) Monitoring

In this process, managers and security risk practitioners are mandated to periodically review and evaluate risk to determine the need for additional risk management.

d) Control

Risk management control activities are designed in ways meant to avoid or mitigate adverse events on the organization. Once risks have been identified and measurement components assigned, controls are then put in place. The controls are essential for planning and understanding the *likelihood* of *threat-sources* ***exercising*** potential *vulnerabilities.* Actions taken depend on the organization's risk appetite (tolerance for risk).

2.2.3 Framework for Risk Identification, Analysis and Control

In general, Information Security Risk Management (ISRM) has two important goals; i) to assess security risks and ii) to select protection measures to reduce security risks (Yue *et al.* 2007). The main activities identified by Stoneburger *et al.* (2001) earlier include risk *identification*, measurement and monitoring (*analysis*) and risk *control*. It has been found that typically when information security practitioners do not have a complete view of the information security remedies, they follow a structured (functionalist) security planning framework to reduce system risks (Yue *et al.* 2007). The first step, *risk identification*, involves finding out information systems asset values, potential threats and potential countermeasures. The second step deals with *analysing* (measuring and monitoring) potential security risks for individual systems. Risk *analysis*, requires the identification and documentation of critical organizational resources (e.g. information, people, processes, and technologies) among a huge number of total information resources that are used to support the organizational mission (Finne 2000). Risk *analysis* includes the consideration of potential financial impacts when information systems are compromised; sometimes referred to as impact analysis (Yue *et al.* 2007). The third step, deals

with controlling risk by considering the cost and benefit relationship between risks and determining acceptable risk. This is illustrated in **Figure 3** below.

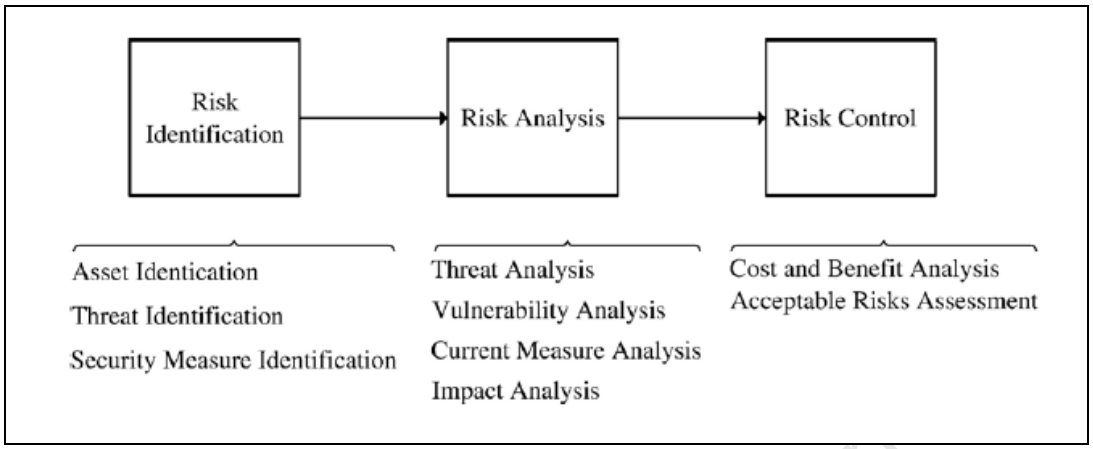


Figure 3: Framework for Risk Identification: (Yue et al.(2007)

2.2.4 Emergent Nature of Threats and Vulnerabilities

Threats and vulnerabilities that give rise to information security risk are highly emergent, highly continuous, filled with surprises, difficult to control, highly tied to circumstances and more affected by what people pay attention to than by formal plans and methodologies (Weick 1993b). It is in regard to the emergent nature of threats and vulnerabilities that information security practitioners show commitment and discipline towards putting optimal security postures in organisations. Ambivalence and recklessness on the part of information security practitioners to following sound security practises are some qualities that exacerbate risk (Forno and Baklarz 1999). Recklessness with technology has been identified by Forno and Baklarz (1999) as a quality of information security risk. They advise caution with the use of technology and stress the importance of continuous training for information security practitioners to be effective. They recognise training as '*the jewel of knowledge and power'.*

2.3 INFORMATION SECURITY RISK MANAGEMENT TERMINOLOGY

This section discusses the associated terminology that is used interchangeably within the information security and risk management field. When terminology such as Information Systems Risk Management, Information Technology Risk Management is used, sometimes these terms refer to ISRM. **Figure 4** below brings conceptual clarification to this ambiguity by classifying the following groupings; Information Security Risk Management (ISRM), Information

Technology Risk Management (ITRM), Risk Assessment, Risk Analysis and Mitigation Planning.

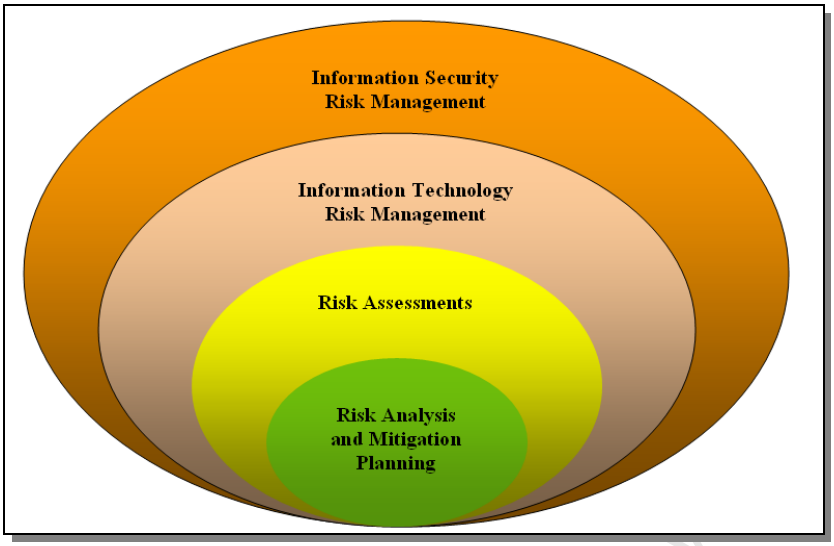


Figure 4. Information Security Risk Management: Sub-set relationships (Blakley *et al.*2001; Njenga and Brown 2008)

2.3.1 Information Security Risk Management (ISRM)

Information security risk management (ISRM) is much broader than and encapsulates these other terminologies. ISRM is the process of administering people, policies, and programs with the objective of assuring continuity of operations while maintaining strategic alignment with the organizational mission (Choobineh *et al.* 2007). ISRM activities are driven by organizational objectives so that no resources are expended on information security without an understanding of how they support the organizational mission. ISRM is therefore much broader than and encapsulates both information systems and the underlying technologies and platforms that support these systems.

ISRM often deals with activities that are associated with the assessment and mitigation planning for risk and identifies the optimal protection strategy when constrained by limited information security resources. ISRM has evolved as a required function within organizations which are concerned with their ability to mitigate the effects of a breach of information security (Finne 2000). These breaches are sometimes referred to as "*incidents*." ISRM requires an estimation of the value the resource provides to the organization based upon how it supports the organization's strategic objectives mission (Choobineh *et al.* 2007).

2.3.2 Information Technology Risk Management (ITRM)

Information Technology Risk Management (ITRM) is a sub-component of ISRM and looks at Risk in Information Technologies and how these are managed. The Burton Group (2005) defines the Risk Management Planning Methodology as a framework for dealing with the risk assessment and mitigation planning efforts and usually considers the possibilities of threats that exploit vulnerabilities in information technologies to induce sometimes fatal consequences (Burton Group 2005).

2.3.3 Risk Assessments

Parker (2001) talks of risk assessments pertaining to information security as being a means whereby information security practitioners are provided with information needed to understand factors that can negatively influence operations. Risk assessment takes the form of making informed judgments concerning the extent of actions needed to reduce risk (Parker 2001). According to Choobineh *et al.* (2007), informed judgments about risk assessments takes cognisance of the attitudes, technologies, behaviours and other phenomena that are incorporated into the risks and activities under consideration.

Assessing risk is seen as ***one element of a broader set of risk management activities***. Other elements include establishing a central management focal point, implementing appropriate policies and related controls, promoting awareness, and monitoring and evaluating policy and control effectiveness (Parker 2001). Several researchers have tried to examine the risk assessment process itself, particularly in terms of the common challenges faced by managers in approaching and executing the process (Baskerville and Portougal 2003).

2.3.4 Risk Analysis and Mitigation Planning

Information security **risk analysis** is used to identify events/incidents that can adversely affect an organisation's operations (Baskerville and Stage 1996). There are many ways in which a risk analysis can be performed. Some of the more sound risk analysis methods are based on an international best practice. One suggested international best practice includes the use of CobiT (Von Solms 2006). Risk analysis can use both quantitative and qualitative methods of analysis.

Quantitative methods take the form of formal specialised ways of determining the probability of an event/incident occurring and the likely loss should it occur (Von Solms 2006).

Quantitative risk analysis makes use of statistical data to produce a numeric probability called the 'Annual Loss Expectancy (ALE)' or the 'Estimated Annual Cost (EAC)' (Yue *et al.* 2007). This is calculated for an event by simply multiplying the potential loss by the probability. **Qualitative risk analysis** is by far the most widely used approach to risk analysis. Probability data is not required and only estimated potential loss is used. This approach makes use of estimating threats and vulnerabilities. When the information security risks have been analysed, an action plan is established (Finne 2000). This plan is called the **risk mitigation plan.** The risk mitigation plan aims to minimise the ALE or the EAC. The risk mitigation plan contains information security objectives, principles and implementation practices approved by an organisation (Finne 2000).

2.4 UNDERSTANDING INFORMATION SECURITY RISK MANAGEMENT

Historically, ISRM activities have been conducted in order to establish controls and security over information systems (Choobineh, *et al.* 2007). ISRM has therefore been a consistent way of strengthening security controls and practices at the organization level through risk analysis and continual improvement. ISRM activities such as risk analysis are usually structured in ways that assist in the management of information system threats being exploited by information system vulnerabilities (Burton Group 2005). The ISRM process has mechanisms in place designed to facilitate information security risk mitigation (Holappa and Wiander 2006) and is driven by organizational objectives. The approach to risk analysis and risk mitigation in information security provides for the characterization of the rewards or benefits of using sensitive data and information for decision making that is free of any associated risk (Choobineh, *et al.* 2007). Baskerville (2005) has described two problems faced by information security practitioners which limit the effectiveness of risk analysis practices. These include the lack of reliable empirical data concerning the frequency and amount of losses attributable to information security compromises, and the relative rarity of many kinds of information security compromises. Risk analysis and risk mitigation techniques are seen to vary in detail according to the information security risk, the purpose of the analysis and/or mitigation, and the required protection level of the relevant information.

Traditional risk analysis processes are designed to identify and evaluate threats and vulnerabilities in order to decide on the appropriate measures and controls to manage them (ENISA, 2006). Risk analysis as conducted by informational security professionals involves establishing the feasibility of information systems controls (Baskerville 1991).

In order to better understand how information security practitioners balance the risk-reward equation, this research conceptualises the nature and responses of the risks involved in securing information systems and the activities undertaken by information security practitioners to manage those risks. The research draws from studies done by several researchers in ISRM. To begin with, several researchers have tried to examine the information security risk in terms of the common challenges faced by information security practitioners in approaching and executing the ISRM process (Baskerville and Portougal 2003).

Conventional methods of examining information security risk proposed by these studies include checklists, risk analysis and evaluation (Baskerville 1993; Birch and McEvoy 1992; Dhillon and Backhouse, 2001). Miller and Engemann (1996) have argued that these techniques are deficient because they encourage perpetrators to learn the system and then circumnavigate the system. Some of these techniques have also been faulted particularly when technology changes and the checklists used do not contain all potential information security risks. The limitations of these techniques have been exacerbated by not including the socio-organisational aspects of information security, which researchers have found to be an important element in the development of an information security strategy (Backhouse and Dhillon 1996; Dhillon and Backhouse 2001).

In recent times also, the formulation of information security policies has tended to ignore issues such as the strategic information systems plan (SISP) which has minimised their effectiveness and made the process of information security deficient (Doherty 2006). Doherty (2006) has proposed the alignment of formulation of information security policies and SISP to make the process of information security risk management rich.

In order to better understand ISRM, it is important to introduce some of the concepts used by standards and best practices. (Standards, guidelines, methodologies and frameworks used in ISRM are discussed in detail in **Section 3.1.1**). The standards and frameworks used in ISRM describe the stages for managing the security of information systems.

The PDCA (plan, do, check and act) framework, introduced by Deming (1986), is an example of an ISRM standard proposed in ISO27001 (ISO/IEC 2005) which describes the process for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organisation's Information Security Management System (ISMS). Apart from this framework, there are other structured (functionalist) models based on sequence of stages of ISRM activities, such as the CobiT framework (discussed in detail in **Section 3.1.1**). The PDCA model reflects the principles set out in the OECD Guidelines (2006) governing the security of information systems and networks. By having a general understanding of some of the frameworks mentioned above, what comes across is that that many of these frameworks are guided by two main types of ISRM activities: **evaluation activities** and **implementation activities** (Deming (1986). These ISRM activities are illustrated in **Figure 5**.

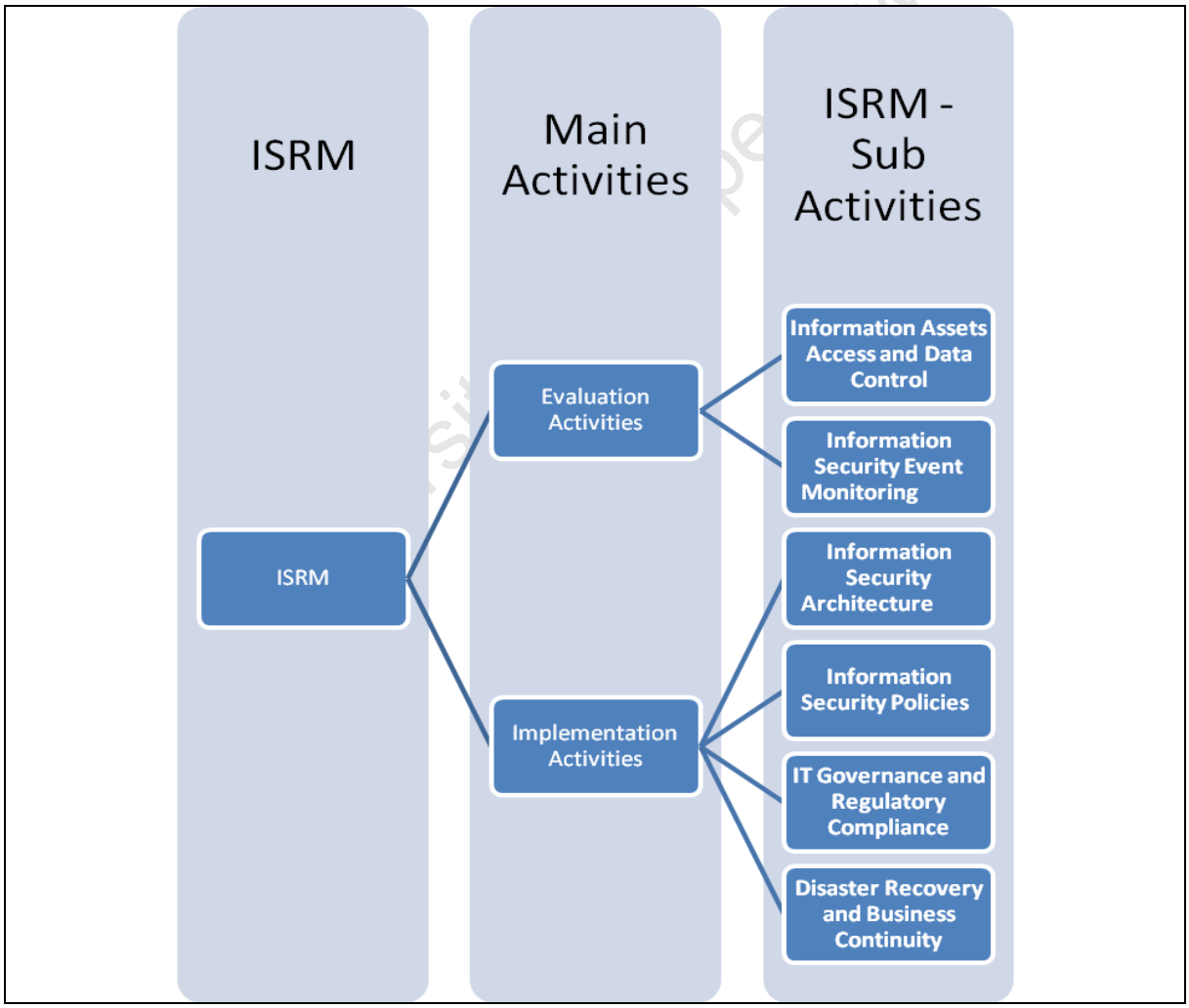


Figure 5. Suggested Structured Functionalist Information Security Risk Management Activities (Adopted from Deming 1986)

2.4.1 Evaluation Activities in ISRM

The evaluation activities in ISRM are performed by the ISRM practitioners and consist of the elements of assessment of the current information security situation ("**plan**"). These sorts of ISRM activities take into account factors such as the effectiveness of the implemented information security controls, and external events. To perform evaluations (i.e. planning and checking) on information assets within an organisation, the effectiveness of ISRM activities is typically assessed by asking questions. For instance, questions could be raised about activities related to data protection and controls as well as the security of the operating system, platform, and networks (Deming 1986).

ISRM evaluation activities are done at both physical and logical levels (Deming 1986). In the case of logical security, checks are, for instance, done on the strength of passwords. There is a higher level of information security risk if passwords are weak or have not been changed for a long time and if there are weak controls in the information systems to check this. **Checks** are also done on vulnerable information systems with the intention of obtaining knowledge of the tools intruders or hackers could use against information systems. ISRM evaluation procedures many be qualitative, semi- quantitative or quantitative or a combination of these. During ISRM evaluation, decisions have to be made concerning which risks need treatment and which do not, as well as focusing on the treatment priorities.

1. Information Assets Access and Data Control

The ISRM activity related to evaluating controls focuses on access control of information assets. According to ICASA (2008), top managers' major concern was with compliance of financial reporting. The key area that top managers felt was most important was that of using evaluating tools for managing access and changes to data (ISACA 2008). Farahmand *et al.* (2003) have argued that the lack of an access-control mechanism is a vulnerability that could allow an intrusion to occur and information assets to be compromised. They have proposed the need for organisations to conduct vulnerability assessments which involve the examination of weaknesses that could be exploited by identified threats. The need for organisations to conduct vulnerability assessment should take cognisance of the environment and existing safeguards. Farahmand *et al.* (2003) have proposed a model and framework on how this can be done. Within specific aspects of ISRM, there are many other information access control models and frameworks that have

been suggested by Castano *et al.* (1995). There have also been other methods that have incorporated information access control by considering design and security specification for information systems (Baskerville 1998; Dhillon and Backhouse 2001; Dhillon 1997). The research considers ISRM activities that relate to information assets access and data control as flagged activities for conceptualisation (see **Section 4.5.1**).

2. Information Security Event Monitoring

Another activity that is prominent in ISRM is that of events monitoring. It has been reported (Chickowski 2007) that when information security practitioners get on stage at conferences, one of their favourite analogies is that of sports car brakes. The question they often pose is, "What is the purpose of brakes on a sports car?" The obvious answer would be, "To stop the car." However, the real answer the information security practitioners are looking for is, "To enable the car to safely go faster" (Chickowski 2007).

It may be explained that similar to the brakes on a sports car, information security and security monitoring allows the IT departments to employ cutting-edge technologies to make organisations more successful, in other words, "to go faster", while at the same time mitigating the risks ("brakes") of doing so (Chickowski 2007). This becomes possible with the help of emergent technologies. Technologies such as the SIM or SIEM (security incident management or security incident and event management) systems that use applications such as *netForensics* (nFX) and *TriGeo* Security Information Manager help automate the information security event monitoring process (Chickowski 2007).

Technologies that enable information security event monitoring can contribute towards a streamlined event-analysis that provides localized real-time protection of the more widely used network services on the Internet. This means that information security practitioners can track trends and gain visibility into network behaviour which may or may not always be classified as incidents or events (Chickowski 2007). Event monitoring activities as part of the general ISRM activities have also been flagged for conceptualisation (see **Section 4.5.1**).

2.4.2 Implementation Activities in ISRM

The "**check"** ISRM activities focus on the understanding of information security controls in the implementation process performed in the organisation. Implementation represents a critical part of the ISRM activities as contained in the widely accepted standard based approaches. The "check" part of the ISRM activities ensures that information systems are properly configured, coded, and the processes are working harmoniously. Information security testing ensures that any changes to the systems do not degrade organisations' security objectives (Burton Group 2005). When information security practitioners detect anomalies and vulnerabilities through systems testing, these findings should feed into policy decision and information security risk management services that determine responses to situations (Burton Group 2005).

In the description of the "**act**" stage of the ISRM activity, the ISO27001 standard considers the need for any organisation to first understand its risk assessment approach. As defined by ISO27001, the organisation should identify a risk assessment methodology that is suited to its self and to identify its business information security, legal and regulatory requirements (ISO/IEC 2005). The organisation should develop criteria for accepting information security risks, and should identify acceptable levels of information security risks. The ISO27001 standard also suggests that the risk assessment methodology to be implemented should ensure that information security risk assessment procedures produce "comparable and reproducible results" (ISO/IEC 2005).

Information security practitioners develop policies that determine the roles for specific ISRM implementation (Burton Group 2005). Often, information security practitioners derive policies from feedback in the form of information security analysis, information security risk measurement, and other forms of monitoring. For organisations concerned, the policies address behavioural and business contexts as well as the lifecycle of people, information systems, data, and the business itself (Burton Group 2005).

There are a number of important facets that contribute to the success of implementing ISRM activities. Baskerville and Siponen (2002) make mention of information security policies as one of those facets that reflect on business objectives. They note that a successful ISRM implementation approach guided by information security policies is one that is compatible with an organisation's culture and also one that has support and commitment from management.

3. Information Security Architecture

An Information Security Architecture (ISA) is a layered architecture that is necessary for securing an environment; crucial to this are the kinds and types of controls layered into such an environment (Cavusoglu 2004). Questions have been asked about how the security controls within the organisation's architecture interact with each other and how they are implemented together within the same ISA (Cavusoglu 2004).

It has been cited that, often times, organisations need assistance in developing and implementing comprehensive and flexible enterprise Information Security Architecture (ISA) to protect the confidentiality, integrity and availability of information and the information system resources (Killmeyer and Tudor 2006). Killmeyer and Tudor (2006) suggest eight components essential to effective information security architecture. These components are listed as follows:

1. Security organisation/infrastructure
2. Security policies, standards and procedures
3. Security baselines/risk assessments
4. Awareness and training programs
5. Compliance
6. Monitoring and detection
7. Computer incident/emergency response

It has been realised that organizations are organic, dynamic entities that change over time (Choobineh *et al.* 2007). It is this fact that is often seen to undermine or invalidate sound Information Security Architecture (ISA) if an organisation is not adaptive (Choobineh *et al.* 2007). Given that ISA may be invalidated by the dynamic nature of the environment, which in turn affects the nature of the layering of security components (the architecture), questions have been asked about the value of having an ISA that is layered with multiple controls and then re-arranging these when organisations change, rather than having independent controls applied individually to each application (Cavusoglu 2004). It is questions like this that make the process of understanding ISRM and the ISA component interesting for conceptualisation. This activity has also been flagged for consideration in this research (see **Section 4.5.1**).

4. Information Security Policies

Implementing information security and assurance policies (as part of the ISRM activities) are the vehicle for managing the identified risks to the organization (Doherty and Fulford 2005). A great deal is unknown regarding the proper management and use of information security policies. Doherty and Fulford (2005) have raised a concern that the guidelines for developing and implementing security policies in organizations might not have been "tested" and are more "tied to theory". Another concern raised has been the time after which the information security policies should be retired. A few researchers have been looking into this issue (Doherty and Fulford 2005). This researcher will conceptualise ISRM activities that centre on the implementation of information security policy. This is discussed in a later section of this research paper (see **Section 4.5.1**).

5. IT Governance and Regulatory Compliance

IT governance is defined as "*specifying the decision rights and accountability framework to encourage desirable behaviour in the use of IT* "(Weill and Ross 2004). As part of the ISRM implementation procedure, Information Technology Governance (ITG) activities are an integral part of enterprise governance and consist of the leadership and information technology structure and processes which ensure the organisation sustains and extends its strategy (ITGI 2003). IT governance is the responsibility of executives and the board of directors, and consists of the leadership, organisational structures and processes that ensure that the enterprise's IT sustains and extends the organisation's strategies and objectives (ITGI 2003).

Implementing ITG requires the location of decision rights and accountabilities (Weill and Woodham 2002; ITIG 2003). It can be noted that ITG is a part of a strategic ISRM activity that aligns Information Technology (IT), IT Risk and businesses to achieve business value for the enterprise (Webb *et al.* 2006). In order to achieve organisational goals, Webb *et al.* (2006) emphasise effective information security controls, performance management and risk management in order to maximise the business value through strategic alignment of IT and businesses. The research also considers IT governance and compliance as part of conceptualising ISRM activities (see **Section 4.5.1**).

6. Disaster Recovery and Business Continuity

Business activity is subject to disruptions, such as technology failure, flooding, utility disruption and terrorism (ISACA 2008). Disaster recovery/business continuity management, which was ranked as the second most important issue for IT management professionals, has been a traditional area of focus for IT professionals (ISACA 2008). In response, some enterprises implement business continuity management (BCM) programs to improve their resilience in the event of disaster. For implementing **Section 11** of the **ISO IEC 17799**, Eloff and Eloff (2003) have designed a framework whereby organisations can determine the weak areas that need improvement in business continuity planning and compliance. In this framework, the strengthening of an information security control area (e.g. business continuity) and the implementing and managing of the processes for that specific control area is achieved through understanding the different protection classes (inadequate minimal, reasonable and adequate controls). In case of business continuity, they have highlighted the need for adequate controls.

Choobineh *et al.* (2007) identified business continuity planning and disaster recovery planning as salient issues in ISRM that are concerned with the implementation and maintenance of an organisation's information security program. They have proposed a need for further research to understand why certain firms are able to effectively implement and execute business continuity plans (which encompass various aspects of information security), whereas other firms have been struggling to do so in the face of various incidents affecting information assets (Choobineh *et al.* 2007). The research considers part of the research needs raised by Choobineh *et al.* (2007) and conceptualises business continuity (see **Section 4.5.1**).

2.5 CHAPTER SUMMARY AND CONCLUSION

As was stressed earlier, the purpose of this chapter was to examine concepts associated with information security risk management (ISRM) and to increase the understanding of ISRM thereof. This chapter examined various concepts and terminologies associated with information security risk management and gave clarity to the use of these terminologies. The chapter contributes to the overall research in two ways. First, by building on existing work on information security risk management, this chapter adds to the building of a cumulative tradition in ISRM, particularly on development research. Second, this chapter contributes to understanding (explanatory) knowledge on information security risk management.

CHAPTER THREE

This chapter presents the idea that unpredictability of the business environment drives Information Security Risk Management (ISRM) activities. The chapter challenges functionalism and structure, and presents the need to factor aspects such as unpredictability and uncertainty when assessing ISRM activities. The idea of contrasting the functionalist and incremental approaches to ISRM is also introduced. The chapter infers a gap in the literature on both the functionalist approach and the incremental approach to ISRM. The chapter concludes by suggesting that the two approaches to ISRM are inherently deficient.

Table of Content
Chapter Three

CHAPTER THREE: STRUCTURED FUNCTIONALIST vs. INCREMENTAL APPROACH TO ISRM

3.0 INTRODUCTION

Information security risk practitioners at managerial levels have on a number of occasions been faced with different approaches to conducting information security activities. Smith *et al.* (2003) consider any approach to information security as deficient if the awareness of information security issues is not prioritised. According to Burton Group (2005) approaches that are meant to serve particular risk objectives are defined for the overall architecture of the organization. These approaches are oriented towards stable security frameworks that fall broadly within the following categories: integrity, availability, confidentiality, use, control and accountability. There have been several organisational studies conducted on information security that address issues including planning, managing risk and assessing risk. The approaches to these issues have followed many sociological paradigms. The sociological paradigm or approach, i.e. the functionalist paradigm, has been predominant (Dhillon 1997; Dhillon and Backhouse 2001; Hirschheim *et al.*1996). The functionalist paradigm places emphasis on formalized rule structures in designing and managing security (Dhillon and Backhouse 2001). The functionalist structured approach is also evident in the information security planning methodologies suggested by Straub and Welke (1998) and more recently McFadzean *et al.* (2007).

The purpose of this chapter is to increase our understanding of an alternative approach to functionalism and structured approach to ISRM. The chapter reviews literature on the nature of functionalism in organizational management. The chapter also introduces the alternative approach i.e. the incremental approach.

This chapter is divided into six sections. The first section starts by providing an overview of existing structured and functionalist ISRM approaches characterized by guidelines, frameworks and standards. The second section challenges functionalism and structure. The third section introduces the concepts of organizational complexity and uncertainty that give rise to challenges faced by structure. The fourth section proposes an alternative view point that challenges structure and exemplifies the incremental approach. The fifth section examines the functionalist approach and the incremental approach and suggests that these two approaches are insufficient

when looked at in isolation. The sixth and final section summarizes the discussions in the chapter and concludes the sections.

3.1 FUNCTIONALIST APPROACHES TO MANAGEMENT

The general definition of ***functionalism*** is borrowed from sociological theory and looks at how functionalism "*involves designing a society as a functional body made up of institutions and social structures acting as organs of this body*" Parsons (1949). The leading thinker of functionalism in America was Parsons (1949) who believed that behaviour was driven by individual effort to conform to the moral code of society.

At the core of the **operational, tactical** and **strategic** levels of ISRM lie several functionalist structured methodologies, standards and frameworks that organisations deem suitable to meet the unique diverse and high technology risks associated with running computerised systems.

Hu *et al*. (2007) have catalogued studies that offer prescriptive and normative guidelines for managing secure information systems based on studies by Baskerville (1998); Staub and Welke (1998) and others.

3.1.1 Discipline Specific Guidelines, Frameworks and Standards: Predictive Knowledge

The functionalist paradigm emphasizes formalized rule structures in designing and managing security (Hu *et al.* 2007). The school of thought assumes that society and by extension organisations have a concrete existence and follow a certain order. The thinking concerns itself with providing explanations of the status quo, social order, social integration, consensus, need satisfaction, and rational choice (Hirschheim and Klein 1989).

It is the notion of predictive knowledge that has influenced the functionalist approach to formulating policies for monitoring and control. Predictive knowledge reinforces the functionalist paradigm by viewing designers and practitioners as solely technical experts (Wheeler and Venter 2006). Predictive knowledge assumes the intent by users to follow order, maintain status quo and reinforce rational choice (Wheeler and Venter 2006). It should be noted

that the question of the management of predictable and unpredictable knowledge of threats has also been investigated by Baskerville (2005) in his work "Information Warfare". It is therefore by a closer examination of the ISRM process and specifically the policy adoption process that it is realised that information security activities are guided by an approach that is multi-faceted and not restricted to only following standards and frameworks in a purely functionalist manner.

In terms of this research, it should be explained that functionalist assumptions suggest the existence of an objective and value-free world that can produce true explanatory and predictive knowledge of the reality "out there". Indeed this predictive knowledge has influenced approaches to systems design and reinforces the functionalist paradigm when viewing designers as solely technical experts (Wheeler and Venter 2006).

Creators and designers of organisational and discipline specific standards, frameworks and methodologies that guide the proper running of organizations assume the intent by users/agents to follow order, maintain status quo and reinforce rational choice. Closer examination of the ISRM process shows that ISRM activities are guided by standards and frameworks that place an emphasis on formalized rule structures, thus reinforcing the functionalist notion (Wheeler and Venter 2006).

Within information security, the functionalist processes that are defined by social order include identifying, measuring, controlling and monitoring information security risk. These activities are typically run in a top down hierarchical approach that leaves little room for reflexivity. Based on these steps, senior management evaluate business tradeoffs and manage risks accordingly.

The functionalist classical top-down approach in management has been well documented by researchers. Researchers such as Cunha (2004) have described the classical mechanistic approach whereby activities were viewed as objects of structured planning and stable design and where organizations worked in a systematic and predictable manner (Browne *et al.* 2000; Office 1996; Howard 1997). Dhillon and Backhouse (2001) note that information security research emphasises formalized rule structures in designing and managing information security. Information security researchers have recognized the significance of well planned, sound risk management policies that focus on clear methodologies and programmes (Von Solms and Von Solms 2005; Schultz 2005). **Figure 6** (below) points to one of the many structured functionalist approaches to ISRM, which employ guidelines, various methodologies and standards.

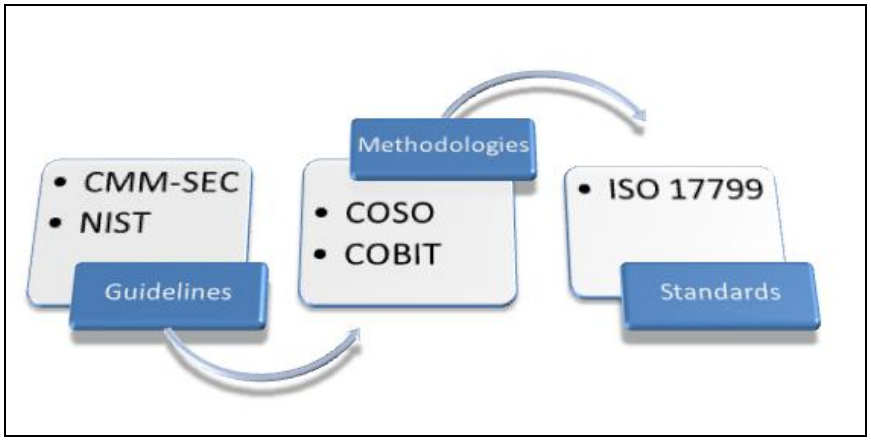


Figure 6. Structured Functionalist Information Security Risk Management Approach (Njenga and Brown 2008)

3.1.2 Guidelines

According to Burton Group (2005) a **guideline** is "*any document that aims to streamline particular processes according to a set routine*". By definition, following a guideline is never mandatory although these should be seen as essential to the process of governance. Following guidelines is never mandatory. ISRM is endowed with rich functionalist guidelines, which provide direction activities or processes to achieve set goals. The guidelines are defined for the complete risk management process. The Capability Maturity Model for Security (CMM-SEC) is an example of a guideline that defines the process an enterprise must go through to move from limited security capabilities to increasingly optimizing protection postures (Burton Group 2005). The NIST has issued guidelines under the banner of the *Risk Management Guide for Information Technology Systems* in its Special Publication 800-30 (NIST SP 800-30). The guide consists of various sections that address risk mitigation, including mitigation options available, mitigation strategies, an approach for control implementation, control categories, control cost-benefit analysis and residual risk.

The **ISO/IEC Guide 73** released jointly by the International Organization of Standards (ISO) and the International Electro-technical Commission (IEC) provides specific guidance on terms and definitions of concepts related to risk management. By design, the sections of the guide address risk from both the negative and positive impact it can have on an organization. Within the context of this research, the research considers only the negative aspects. The **ISO/IEC Guide 73** operates on the assumption that a proper communication channel exists within

organizations with the general aim of highlighting risk. The guide places great weight on the communication process.

3.1.3 Methodologies and Frameworks

Methodology refers to "*the rationale and assumptions that underlie a particular study*" (Creswell 2003). According to the *Merriam-Webster Online Dictionary (2009),* Methodology is defined as*;*

1. "*the analysis of the principles of methods, rules, and postulates employed by a discipline*".
2. "*the systematic study of methods that are, can be, or have been applied within a discipline*".
3. "*a particular procedure or set of procedures*."

Frameworks on the other hand refer to a "*structure supporting or containing something*" *(Merriam-Webster Online Dictionary 2009).* ISRM frameworks that define the methods, rationale and core sets of assumptions for the general ISRM methodology incorporate activities that *identify*, *measure*, *control* and *monitor* information security risks. Frameworks that guide these sets of activities are gathered from some of the following sources:

- CobiT™
- Turnbull Framework
- KING II Report
- IT Infrastructure Library (ITIL) for IT service management
- Sarbanes-Oxley (SOX) Act

Each of these functionalist methodologies is discussed briefly as follows:

CobiT™

CobiT (Control Objectives for Information Technology) was considered in depth in this research and comprises inputs to the development of a *Sensitsing Device* (in ***Section 4.5***) released by the Information Systems Audit and Control Association. The framework explains 34 major components of the IT processes termed domains (grouped in 4 high level domains) and how these can be used to deliver information to the business process in order to assist organizations meet defined objectives. The 4 high level domains are **planning and organization (PO),**

acquisition and implementation (AI), delivery and support (DS), and monitoring (MO). The framework looks at the business requirements and evaluates controls in terms of how the IT resources are to be used, affected or targeted. This framework then aligns these requirements to IT processes. Within the framework was an additional release termed the *Management Guidelines.* The additions introduced the following perspectives: Key Goal Indicators (KGIs), Key Performance Indicators (KPIs), Maturity Models (MMs) and Critical Success Factors (CSFs). These assist management in better assessing risk and success at the higher managerial levels. These are definition and measurement tools that explain the 'how' part of the processes (KPIs), scoring and grading tools to outline strategic thinking (MMs) and tools that outline important issues or actions for management to achieve control over their IT processes.

Turnbull Framework

In 1999, the Turnbull Framework was developed by the Institute of Chartered Accountants in England and Wales (ICAEW) and provides management with clarity on maintenance of sound internal controls, how to review these controls, and the overall effectiveness of these controls (Rushton 2005). The ICAEW committee was chaired by Nigel Turnbull, a Finance Director, to prepare guidance for boards on internal control. This committee clarified the purpose of internal control as being "*to help manage and control risk rather than to eliminate it*". The objectives of the Turnbull framework are (Rushton 2005)

a) to reflect sound business practice whereby internal control is embedded in the business processes by which a company pursues its objectives; internal control should be embedded in business processes and should not be a separate compliance exercise; internal control is seen as integral to achievement of business objectives
b) to remain relevant over time in a continually evolving business environment;
c) to enable companies to apply the guidance in a manner which takes account of their particular circumstances (Rushton 2005).

Sections of the report that provide an adequate framework for senior management in organizations to play key roles in the development of risk management programmes are relevant to this research.

KING II Report

In 1993, a committee chaired by former judge Mervyn E. King was established to investigate the role of boards of directors in South African firms. This committee released two reports: a) the King Report on Corporate Governance, 1994 - to be subsequently known as King I and b) the King Report on Corporate Governance in South Africa, 2002 - to be subsequently known as King II (Von Solms 2006).

King I includes a Code of Corporate Practices and Conduct, and was the first of its kind in South Africa. Companies listed on South Africa's JSE Securities Exchange are mandated to comply with King II which itself requires compliance with Global Reporting Initiative guidelines (Von Solms 2006). In South Africa, the King II Report is a framework designed for corporate governance and addresses the power checks in management in terms of accountability and responsibilities (Von Solms 2006). Of relevance to this research is a section of King II that deals with Risk Management (section 2) which places emphasis on risks associated with the use of information technology and considers risk management and record retention.

IT Infrastructure Library (ITIL)

The ITIL (Information Technology Infrastructure Library) Framework is an IT service related set of sub-frameworks that focus on aligning the IT infrastructure with the service delivery needs of the organization (ISACA 2006). The main ITIL framework consists of several sub-frameworks that address specific functions within IT service delivery, the key elements being Service Support and Service Delivery. Within ITIL is the inherent security focus on security tenets/components of information *availability*, *confidentiality* and *integrity* (See Section 2.1; Tudor 2001). There are aspects within each sub-framework that address information security and ISRM. The more useful tenets are **Availability Management** that addresses availability management tools, cost of availability and managing availability. The **IT Service Continuity Management** tenet focuses on recovering facilities, and considers the recovery efforts to physical infrastructure, data and processes within a specified time frame. In this research **Business Continuity Management** is considered part of ISRM and looks at elements that can impact on continuity and recovery of operations in case of adverse events.

Sarbanes-Oxley (SOX) Act

Of relevance to this research on information security risk and control in the SOX Act of 2002 is section 404. Section 404 has in mind the technology components of control and requires that in an annual report rules be prescribed (often by a commission) that will state the responsibility of management for establishing an adequate internal control structure. Though SOX was by design meant to be followed by Public Accountants in organizations, the process of financial reporting is now heavily dependent on advanced applications and information technology and systems. The reporting should therefore be seen as a means of ensuring an assessment of the effectiveness of the internal controls and processes of these IT systems.

3.1.4 Standards

The term "standard" is sometimes used within the context of information security policies to distinguish between written policies, standards and procedures (Dhillon 2007). According to Dhillon (2007), a technical standard is "*an established norm or requirement*" and is "*a formal document that establishes uniform engineering or technical criteria, methods, processes and practices*". Technical Standard can be "*controlled artifacts*" and Reference Standards "*certified reference materials have an assigned value by direct comparison with a reference base*".

A "standard" is a low-level prescription for the various ways the company will enforce the given policy (Dhillon 2007). Information security policies are high-level statements or rules about protecting people or systems. Standards are functionalist in nature and are continually developed for the purpose of serving as measures for organizations to achieve desirable ends, though they fall short of the main purpose of guidelines and frameworks. The tenets of security standards are designed to work well for the more stable technologies. However, with emergent technological changes, the rules keep changing.

ISO/IEC 17799 and ISO 27005

A prominent standard approved by the South African National Standards is the **ISO/IEC 17799** standard adopted from the British Standard BS 17799 (SABS 2000). Another prominent standard is the Australia Standard/ New Zealand Standard, AS/NZS 4360, which is a risk management standard whose objective is to provide a generic framework for establishing the context, identification, analysis, evaluation, treatment, monitoring and communication of risk. A body mandated to develop standards and best practices is the Information Security Forum (ISF)

which consists of representatives from over 200 organizations worldwide. The ISF has developed a risk management methodology known as the *Fundamental Information Risk Management* (FIRM) methodology available to member organizations.

The most recent standard, the **ISO 27005** is an example of a series of standards covering ISRM. **ISO 27005** is the name given to the prime ***27000 series*** standard covering ***information security risk management.*** The standard provides guidelines for information security risk management (ISRM) in an organization, specifically supporting the requirements of an information security management system defined by **ISO 27001**. These series of standards are designed to assist the satisfactory implementation of information security based on a risk management approach.

These standards are applicable to all types of organisations although they do not recommend any specific methodologies. Some of the contents of these standards relate to;

- Information Security Risk Assessment (ISRA)
- Information Security Risk Treatment (as explicated by **ISO 27005** this occurs through the use of prevention and detection controls, avoidance of risk, acceptance of risk, transfer of risk to another entity and some combination of these).
- Information Security Risk Acceptance
- Information Security Risk Communication
- Information Security Risk Monitoring and Review

Researchers have argued that this functionalist approach, exemplified by the above discussions on guidelines, frameworks and standards is based on formal and comprehensive planning. This functionalist approach is seen as the key to a successful ISRM posture. There is an alternative view point to this as explained in the next section.

3.2 CHALLENGING FUNCTIONALISM AND STRUCTURE

Fundamental research in ISRM assumes that composition or planning (functionalism) for information security risk usually occurs first and is followed at a later time by implementation or execution of risk mitigation strategies (Straub and Welke 1998; McFadzean *et al.* (2007). It has been argued that planning based on the functionalist approach has its limitations due to complexity and the emergent change in the business environment.

Present day business environments are seen as hyper-competitive, high speed and fast changing (Cunha 2004). Activities and behavior in hyper-competitive, high speed and emergent technology is seen as transcending mechanical routines and functionalism (Cunha 2004). Ciborra (1996) underscored the importance of action and behaviour that was influenced by environment uncertainties and unpredictability resulting from emergent technologies and the rapid change of technologies. The argument was that dynamism dismantles existing structures (frameworks) and functionalism, and gives rise to transformation of new cognitive frames, cultural views and new structural arrangements. Ciborra (1996) showed that emergent technologies created technology paradigm shifts which required an exit from functionalism.

3.2.1 Transformation: Breaking the Barrier of Functionalism

Key to breaking the barrier of functionalism is the realisation that functionalist approach means that organisations are more focused on paying disproportionate attention to beginnings and endings but not much attention to ***ongoing temporal coordinated activities*** (Barrett 1998). According to Barrett (1998) this limits innovation since organisations are too segmented, with members not sharing mutual orientations.

In the early 1970's, Kegan (1971) did a study on ways in which organisations provided employees with a supportive environment that enabled employees to generate new ways of behaving. The supportive environment was unrestricted and was effective in providing ways in which employees would perceive their own reality. Behaviours were based on open norms, with a spirit of enquiry, expanded consciousness and the recognition of choice. A fundamental theory developed then was that there would be times when constant contextual awareness was appropriate. The learning process involved employees being aware of additional options and hence being better able to choose when these options would be appropriate for a specific situation (Kegan 1971).

The early 1970's also saw scholars and researchers of systems thinking (Cleveland 1973) generate ideas concerning the need for a holistic systems approach. Cleveland (1973) argued for the need to match 'unsystematic reality' with constructive ambiguity. The argument was based on the premise that the management systems then were too exact, too clear and therefore too rigid, i.e. too functionalist. It is not surprising to find that the same attributes are still present to date in many organisations. Cleveland (1973) argued that the main problem with systems

thinking then, was that in an effort to build efficient systems, scholars were attempting to analyse everything systematically (Cleveland 1973). The shortcomings of these systematic analyses were that these early attempts did not see organisations as essentially having elements of spontaneity, but as structured and planned (Kegan 1971). Kegan (1971) saw spontaneity as permitting maximum utilisation of resources available at the moment to reach goals appropriate to the situation at hand. Structure and planning on the other hand were seen as permitting the accumulation of resources (cognitive skills, knowledge etc.) as defence against the future. At this stage it was understood that even with structure and planned processes in place, organisations still encountered resistance and unanticipated dysfunctions (Kegan 1971). The solutions proposed then were to have a blend between structure and spontaneity that would be contextual to the clients, the organisation, and the environmental conditions.

The increased competitive pressures in organisations forced transformation along the dimensions of spontaneity, reflexivity and efficiency. Adler *et al.* (1999) pointed to ways in which managers began oscillating between functionalism suited to routine tasks, (e.g. to minimise risks), and those suited to non-routine innovative tasks. They suggested four kinds of mechanisms which would influence transformation. These included:

(i) ***Metaroutines:*** these were functionalist and systematised the creative process;

(ii) ***Job enrichment:*** enables workers to be more innovative and reflexive in the course of their routine tasks

(iii) ***Switching****:* functionalist and at the same time reflexive with differentiated roles for dealing with the two kinds of task thus allowing workers time to focus on each;

(iv) ***Partitioning****:* both functionalist and at the same time reflexive. This was achieved by the differentiated structures for dealing with each kind of role and the resulting specialisation but also permitting routine and non-routine activities to be carried out simultaneously in parallel.

In arguing for efficiency, Adler *et al.* (1999) pointed out that these oscillating strategies relied on *metaroutinisation.* They illustrated for instance that in a Total Quality Management (TQM) environment, production workers doing their activities could be attentive simultaneously to the efficient implementation of routine production procedures (functionalism) and at the same time to the non-routine tasks (reflexivity) when identifying improvement opportunities. These workers might not have sat down to document suggestions or an act out of procedure, but they were still successful in their endeavours.

It was this gradual transformation caused by organizational complexities and uncertainties that forced the re-thinking of functionalism and made theorists and scholars argue for a better framework for understanding behavior and activities. The concerns of the gradual re-thinking and transformation was not on being prescriptive to any particular style of behaviour but to help in the understanding of the diverse options that feed on actions and behaviours. Reflexivity and exercising choice through increased knowledge of probable consequences of these activities or options was seen to play a key role (Kegan 1971).

3.2.2 Breaking Functionalism in ISRM

Scholars such as Ciborra (1996) began to understand and give useful insights as to how high-tech organisations were gradually undergoing transformation and encountering a blend between functionalism and reflexivity. A key characteristic of these organisations was that when task uncertainty was pronounced, the consequence was to amend or blend the organisational structures in favour of dynamic perspectives (Ciborra 1996).

Currently many authors agree that information security risk management is not only a matter of technical controls or measures (Power 2000; Dhillon 2001; Dhillon and Moores 2001; Gonzalez and Sawicka 2002; Schneier 2000). Information Security systems also involve people, organizational factors, technology, tasks people and the working environment (Carayon and Kraemer 2002; Carayon and Smith 2000). The ill-structured approach in ISRM brought about by dynamism and uncertainty has created ISRM actions ***that narrow the time gap between planning for risk and acting*** (Dhillon and Moores 2001).

Forno and Baklarz (1999) considered information security risk management as a 'soft' management issue primarily because "the information security program is dependent upon those who manage", namely people. Forno and Baklarz (1999) proposed that management be supportive of the information security risk programs that were reflexive, with the people administering these information security risk programs being knowledgeable. They acknowledged and emphasised the skilled worker first, before technology. A more coherent socio-organizational framework that explains a deviation from functionalism to a socio-cognitive has been proposed by Hu *et al*. (2007). They propose a framework that explains why managers and users behave in certain ways. The next section explores the rise of organizational complexities and the apparent need for transformation in much more detail.

3.3 ORGANISATIONAL COMPLEXITIES, UNCERTAINTIES AND UNPREDICTABILITY

With emergent, complex and uncertain technologies being used, organisations began increasingly finding themselves faced with situations of limited resources and unpredictability. Scholars began noticing the manner in which these organisations dealt with these uncertainties, challenging the functionalist approach. Organisations found themselves faced with the need to act flexibly, to subdue and be adaptive to change. This called for being dynamic. In this regard, theories of dynamism began to emerge, such as the theory of dynamic perspective (Ciborra 1996). The next section introduces dynamism with regard to functionalism and explains dynamism as leading to an alternative view to functionalism.

3.4 INCREMENTAL APPROACH TO MANAGEMENT: ALTERNATIVE VIEW TO FUNCTIONALISM

Incrementalism is defined as "*a method of working by adding to a project using many small (often unplanned) changes instead of a few (extensively planned) large jumps*" (Quinn 1978). The incremental approach to management has been popular in understanding situations of dynamism, turbulence and chaos (Minzberg 1994; Minzberg and Quinn 1996). It should be understood that the theory that deals with dynamism is the ill-structured or **incremental approach**. Dynamism has led to the incremental approach which is posited as the *oppositus* of the functionalism approach. The section describes the increasing popularity of this approach and why some scholars predicted this to be of higher value and yield to organisational success than the functionalist approach.

3.4.1 The Dynamic Perspective: An Alternative to Functionalism

The dynamic perspective viewed organisations as contexts out of which specific structures are extracted, tried out and discarded in a pragmatic manner. According to Ciborra (1996), dynamism was expressed within a meta-organisation, where formative contexts occurred and these contexts would mould structures and routines, shaping them into well-known forms such as hierarchy, the matrix and networks, but on a highly volatile basis. The incremental approach to management posits that emergent changes and uncertainties overarched by an informal conscious socio-centric approach is contrasted with functionalism (guidelines, frameworks and standards) and is characterised by unique methodical behaviour. Often the behaviour is seen to

position itself outside of centralised command and control and takes the form of internalised intuitive appeal. The incremental approach, it is argued, often leads to success as compared to the functionalist approach particularly in situations of uncertainty, complexity and unpredictability.

It should be noted that in contrast to comprehensive planning and functionalism, organizations are increasingly practicing an incremental approach (Salmela *et al*. 2000). For them, planning focuses on a few or perhaps just one theme and policies and decisions are made on a one-by-one basis (Salmela *et al*. 2000).

3.4.2 The incremental Approach and Organisational Practises

Salmela *et al*. (2000) highlighted principles of the incremental approach, when observing a particular organization's activities. They described the incremental approach as **highly reflexive**, with decisions being made at any time. The way in which the incremental approach in organizations was observed can also be compared with theories related to reflexivity such as **contingency theory**. Adler *et al.* (1999) exemplified contingency theory when making reference to efficient organisations which were designed to fit the nature of their primary tasks. This thinking entertains the adoption of mechanistic forms for simple stable systems, with efficiency being the primary goal and the adoption of organic forms for complex systems with the primary goal being reflexivity.

It should be noted that some organisations practise the incremental approach whereby functionalism takes a small part while activities and decision making are made on a one-by-one basis. The activities are informally conducted in small team units that enable actions to be independently derived. There is no specific model for these actions. Employees at operational levels are allowed and even encouraged to tinker using local cues and heuristics and to construct whatever tools and routines are at hand (**bricolage**) in order to make ad hoc decisions (Ciborra 1994).

3.4.3 The Incremental Approach in ISRM

In the minds of many information security risk practitioners/planners, planning for risk is firmly associated with the structured and rational *ipso facto* approaches (Salmela *et al.* 2000). As opposed to these *ipso facto* approaches, the incremental approach calls for the mutual sharing of ideas by small (information security risk) teams to develop a common understanding (Sambamurthy *et al*. 1994). This is achieved by informal contacts amongst (information security risk) practitioners and this facilitates interpretation and sense making behaviour required to understand risk (Sambamurthy *et al*. 1994).

The incremental approach helps in the searching for **satisfactory solutions** that deal with threats and opportunities yet remain within the current organisation's resources (Salmela *et al.* 2000). This means decisions rely on personal experience and judgment. According to Pyburn (1983), incrementalism allows decision-makers to choose a time horizon appropriate to current circumstances. It is these informal contacts and experiences that help practitioners remain continually appraised of ongoing threats and opportunities. Decisions can be made at anytime and through such practices that incremental practitioners believe they are likely to succeed in turbulent environments (Salmela *et al.* 2000).

Table 2 below summarized these two main contrasting approaches discussed above as they relate to ISRM.

Table 2. Summary of Functionalism and Incremental approaches to ISRM

Functionalist Approaches in ISRM	**Incrementalist Approaches in ISRM**
Rich in composition for planning for information security risk management.	Rich in ill-structure and non-planning characterised by unique methodical behaviour for information security risk management.
This approach in ISRM suggests the existence of an objective and value-free world that can produce true explanatory and predictive knowledge of the reality "out there".	This approach in ISRM suggests formative and subjective contexts occurring and moulding structures and routines, shaping them into well-known forms such as hierarchy, the matrix and networks, but on a highly volatile basis.
Relies on predictive knowledge and involves firstly planning then later on followed by	Does not rely only on predictive knowledge but subjective contexts for implementation

implementation or execution of risk mitigation strategies	and execution of risk mitigation strategies.
In ISRM assume the intent by users/agents to follow order(centralized command), maintain status quo and reinforce rational choice.	In ISRM assume the behaviour as positioning itself outside of centralised command and control and takes the form of internalised intuitive appeal.
The approaches are typically run in a top down hierarchical approach that leaves little room for reflexivity.	The approaches are typically run in a bottom up hierarchical approach with reflexivity evident at the bottom and at times driving agendas.

3.5 STRUCTURED FUNCTIONALISM AND INCREMENTAL APPROACHES: TWO EXTREMES THAT ARE NOT INDEPENDENTLY SUFFICIENT

The previous sections introduced two approaches; functionalism and incrementalism into ISRM. This research posits that looking at these two approaches independently will not yield sufficient insight and knowledge to understanding ISRM. What is proposed and is examined in this discourse is that both have an inherent limitation when looked at independently and in isolation. The next sections discuss the predominant and common inherent flaws and limitations.

3.5.1 The Functionalist Approach: Limitation

The ISRM process entails planning and managing for risk and has its own formal methodologies and frameworks with predefined criteria for mitigating information security risk. In the ISRM functionalist approach, there are inherent structures of control and command processes by which practitioners act and make decisions based on formally established criteria and methods (frameworks, guidelines, standards). Strategic information systems planners view these methods as guaranteeing that environmental trends including risk are considered (Salmela *et al.* 2000). The shortcoming of this viewpoint, however, is that environmental trends are unpredictable and full of unexpected events, uncertainty and contingencies. What follows is that functionalism falls short of incorporating unpredictability. In the face of these uncertainties, some scholars have advocated for organizations to choose a methodology which emphasizes external analysis (Bergeron *et al*. 1991).

From a strategic information systems planning point, there are advocates of functionalism who argue that when following structure and methods, there is a likelihood of a high chance of

success particularly in a turbulent environment (Salmela *et al.* 2000). Critics would defer and argue that in fact this would increase the chances of failure. These critics have suggested that the need to rely on formal methodologies, frameworks and predefined criteria can trivialise decision making activities so much that it becomes merely a simple top-down exercise (Vitale *et al*. 1986; Sambamurthy *et al*. 1994). ISRM activities are likely to follow the kind of activities suggested by Sambamurthy *et al*. (1994) particularly when information security practitioners perform information security activities/decisions under uncertainty and turbulence with little time to follow structure. Earl (1993) also points out that general practitioners in organizations consider comprehensive and formal methods costly and remote. Critics of functionalism and structure warn that change in a turbulent environment may be so rapid that plans become obsolete before they can be implemented (Lederer and Mendelow 1990; Salmela *et al.* 2000).

According to Salmela *et al.* (2000), arguments such as these make methodologies and frameworks susceptible to wasted efforts, misdirected investments and low morale (Vitale *et al*. 1986) When there is volatility and unpredictability in the business environment, plans, frameworks and methodology simply may not provide the necessary reflexivity to be effective (Pyburn 1983; Ciborra 1994).

3.5.2 The Incremental Approach: Limitation

The risk to the incremental approach is that this approach has not been widely examined (Earl 1993). There have been reports on why the incremental approach might not be feasible at all times. Some practitioners have expressed concern that incremental planning fails to address critical needs (Earl 1993).

Some scholars such Ciborra (1994) have suggested that small scale solutions from team efforts resulting from the incremental approach may not be fully recognized and appreciated by organizations. Ciborra (1994) gives an illustration of an instance whereby when certain team members developed new systems locally, the potentially strategic applications of these systems were dismissed as 'just end-user hacking' and never got sufficient resources to become organization-wide innovations (Ciborra 1994).

There have been some concerns raised by scholars about how the incremental approach would affect and generate future structure, methodologies and planning themes. New employees into an organization would not fully appreciate these efforts. New leadership from say, a chief executive officer (CEO), management team, or management style could erode the incremental planning process (Earl 1993). According to Raster (1994) the incremental approach has its limitations in that it creates little transparency and covers limited re-organization and re-structuring potential thus only leading to small local improvements.

3.5.3 A Proposed Holistic Approach between Functionalism and Incrementalism

Given the shortcomings of these two approaches, scholars suggest that a multi-faceted approach may prove more useful. Formulation of information security policies that take cognisance of both functionalism and incrementalism i.e. information security risk management, and strategic information systems plan (SISP) has been proposed by Doherty (2006) as a way to reducing the shortcomings of incrementalism in both disciplines. This way these two important organisational disciplines would benefit from an explicit and careful alignment which ensures outcomes of strategic importance to information system initiatives that are not compromised by security related problems.

The attributes of an approach that takes cognizance of functionalism and incremantalism has been called the **rational adaptive** approach. It has been confirmed in several studies that the rational-adaptive approach is the most successful approach (Doherty *et al.* 1999). In this approach, **rationality** is reflected as follows:

a) It is highly formalised
b) It is a top-down approach that is comprehensive in the making of decisions; and
c) It is focused on control (Doherty *et al.* 1999; Segars and Grover 1999).

Adaptation is reflected as follows:

a) Frequent informal planning cycles
b) Broad informal participation (participative)

c) Flexible and loose integration with organisation strategy (Segars et al. 1998; Doherty et al. 1999).

According to Grover and Segars (2005), this balanced **rational–adaptive** approach is shown to be more effective and provides strong implications for both research and practice. This research extends the above discussed views and proposes that a multi-faceted approach incorporating functionalism and incremental approaches be used. In this research, this **rational–adaptive** approach would be viewed as ***being among other expressions of the multi-faceted improvisation.*** In general *improvisation* is to be taken as the key central fusion of these two approaches. This is discussed in detail in **Chapter 4.**

3.6 CHAPTER SUMMARY AND CONCLUSION

The chapter called for a paradigm shift to facilitate the understanding of functionalism and its influence on approach towards ISRM activities. The chapter also explained an alternative approach, namely; the incremental approach. This was not, however, suggested as a replacement of functionalism. The chapter showed that both approaches when adopted in isolation are incomplete, reactive and do not address or include all the variables and disciplines related to the ISRM processes. The chapter ends with a caution that any new approach must be built on the strengths of both approaches while being comprehensive and holistic. The chapter has built a foundation for examining a more holistic guide to ISRM.

CHAPTER FOUR

The previous chapter called for a paradigm shift to facilitate the understanding of functionalism and the incremental approaches to ISRM activities based on identified shortcomings. This chapter grounds this understanding and attempts to close the gaps by building on the strengths of both the incremental and the structured functionalist approaches. The chapter argues for a comprehensive and holistic approach known as *improvisation*.

Table of Content

Chapter Four

CHAPTER FOUR: SYNTHESIS OF APPROACHES TO ISRM

4.0 INTRODUCTION

While the previous two chapters discussed and distinguished between functionalism and incrementalism as two contrasting approaches to ISRM, this chapter seeks to propose an alternative approach. The chapter argues that the proposed approach should combine these two approaches to describe the holistic approach. This view should be held with the understanding that the reality of ISRM underlies the importance of having holistic information security practises by information security professionals.

Understanding ISRM from a holistic view entails viewing the entire spectrum of an organization's ISRM activities and procedures, and the approach to these ISRM activities and procedures by skilled information security practitioners. A holistic understanding of how human expertise effectively handles uncertainty in ISRM is appreciated by looking at human expertise in other disciplines and how such skilled expertise handles creativity, innovation in situations of uncertainty and ill-structure. In the case of this research, the best example has been drawn from Jazz.

The purpose of this chapter is to explain the constraints to the functionalism and incrementalism approaches to ISRM discussed in the previous chapter and to propose viewing the duality of these two approaches in a holistic manner. This chapter grounds our understanding of the theories of social and cognitive sciences in the management disciplines. The Jazz metaphor and analogy adopted from the social sciences will henceforth become a useful lens in understanding ill-structure in ISRM activities. The jazz metaphor therefore helps explain the holistic approach. Creativity and *improvisation* in Jazz will become a useful way of bringing understanding into creativity and *improvisation* in ISRM.

The chapter is divided into six sections. The first section establishes the context for a holistic approach by suggesting that the approaches be seen as a combination and not as isolated choices of approach to ISRM. The second section argues for holistic examination and suggests *improvisation* as essentially comprising these dual elements of structure and instrumentalism.

The third section provides a lens of understanding *improvisation* from a jazz metaphor context while the fourth section contextualises *improvisation* in ISRM. The reasoning in all these sections filters into the fifth section which provides solid ground for researching *improvisation* in ISRM. The sixth section concludes by proposing the creating of a sensitizing device that incorporates a fusion of the two approaches. The sensitizing device is deemed a useful tool in framing the research.

4.1 NOT A MATTER OF EITHER STRUCTURE OR INCREMENTAL BUT BOTH: A SYNTHESISED APPROACH

The researcher posits that the holistic synthesised approach sees information security risk practitioners as being faced with a two way synergy between the incremental approach and that of functionalism i.e. as *improvisation* (Njenga and Brown 2006b; Njenga and Brown 2008). It is proposed that this two way synergy eventually creates a holistic approach to ISRM. Galbraith (1977) established a concern about orthodoxy and bureaucratically designed structures and system use and offered an alternative perspective particularly by introducing *improvisation* as a phenomenon of interest. He notes that the "picture of organisational human action which seems to rule out *improvisation* [is] derived from a particular approach to the analysis and design of organisations, *the information-processing perspective*". The research adopts Galbraith's (1977) perspective in evaluating ISRM by observing extemporaneous and spur-of-the-moment action like *improvisational* action outside of ordinary hierarchies of planning (Galbraith 1977). The complexity of human sense-making as the situation emerges will be a critical area of focus (using recognised qualitative methods of evaluating information systems) as demonstrated by the works of Kaplan and Maxwell (1994).

It becomes important to understand reflexivity and extemporaneous actions outside of ordinary hierarchies of planning and to use the understanding as lenses for creating explanatory frameworks. The fundamental emphasis of reflexivity and extemporaneous actions are based on the idea that there will be times when constant contextual awareness is appropriate, that behaviour and actions would be based on open norms, with a spirit of enquiry, expanded consciousness and the recognition of choice (Kegan 1971). The research proposes to give perspective to a new way of evaluating ISRM through viewing the expert/skilled human mind as an *open system* subject to external influences that results in extemporaneous actions derived from tacit knowledge (Polanyi 1966; Baumard 1999; Njenga and Brown 2006a). Tacit

knowledge can be "tweaked" by system inputs/influences such as system exploits, security awareness, and security experience (Baumard 1999; Njenga and Brown 2006a). There has also been growing realisation that ISRM is no longer a "computer security matter" but an "information assurance issue" (Parker 2001). Indeed Parker (2001) acknowledges a wider window of perspective of risk management by suggesting that "auditors must realize that any proposed solution to an information security problem should not fixate solely on technology". Parker (2001) also acknowledges that the security process must be continuous and that each part of the solution to the problem has about an 18-month half-life (doing it over and over and over again).

4.1.1 Introducing a New Alternative and Synthesised Approach

Researchers such as Bjo¨rck (2004) have realized the need to look at organizations afresh by postulating a neo-institutional theory in studying IT security issues in organizations. Bjo¨rck (2004) argues that the revolutionized modern organization requires new ways of explaining why formal security structures and actual security behavior differ and why organizations often create formal security structures without implementing them fully. Furthermore, the increasing emphasis on techno-based compliance issues derived from explicit methodologies as awareness tools, has helped draw attention away from actual security activities (Jackson 2006). The danger here is that getting too involved with compliance issues may not necessarily translate to improved security (Jackson 2006).

Cleveland (1973) realised that future managers would be living in environments where nobody would effectively be in charge, hence the exponential multiplications of decision-making activities, and the enormous personal responsibility of hundreds of decision-makers for the organisation's sense of direction and "*playing it by ear*". The managers would then have no higher priority task than keeping his/her eyes and ears on the purpose. Organisations have tended to forget how much *improvisation* and bricolage are required to complete daily tasks. According to Cunha (2004), bricolage is facilitated 'by the ingenious use of intimately known materials'. Barrett (1998) contends that organisations tend to de-skill tasks by breaking them into formal descriptions of work procedures to be followed automatically. The outcome therefore becomes controlled and stifles creativity.

4.1.2 Responding to Contingencies and Emergencies

Some authors see '*playing it by ear*' or '*taking things as they come'* as acceptable ways of responding to unforeseen contingencies (Ciborra 1999). Contrary to much held conventional wisdom, "*people continually learn and improvise while working*" (Brown and Duguid 1991). A lot has been written concerning *improvisation*, strategy formulation and implementation (Perry 1991). Much of Perry's (1991) work on strategy formulation particularly in emergency situations can be contextualised as inferences for *improvisational* roles for strategic choices and problem solving in ISRM.

Many of the actions taken to respond to contingencies and uncertainty bear empirical characteristics influenced by the emergent nature of technology and knowledge (as examined earlier). These actions provide for reflexivity in the sense that they could be done '*now one way, now another and each way may perfectly or finely fit the situation'* (Scribner 1984). This reflexivity is a reactionary outcome in emergencies and would normally be considered useful, since *improvisation* can be deployed to **fill the unavoidable gaps between** formal procedures/standards and emergent events. The researcher posits that understanding *improvisation* as a problem solving technique in management in general and ISRM in particular can be useful in helping align everyday activities of (information security) practitioners with organisational value (Scribner 1984; Njenga and Brown 2008). Information security practitioners may not have time to analyse a problem, though they may come up with a plan and develop responses by acting on the problem as the situation occurs (Njenga and Brown 2008).

4.2 IMPROVISATION AS AN EXAMPLE OF SYNTHESISED FUNCTIONALIST AND INCREMENTAL APPROACH

Information security research is often premised on standards, planning, analysis and structuring risk (functionalism). Functionalist studies have made a contribution to ISRM by highlighting risk in computer usage and have suggested formal ways (standards, methodologies and tools) to address vulnerabilities and mitigate risk (Browne et al 2000; Office 1996; Howard 1997). These studies are useful and form a foundation for a synthesis with the incremental approach. From an incremental approach, researchers investigating creativity have noted that practitioners sometimes use resources that are material and cognitive (characterised by acquired skills, knowledge and memory) in their day-to-day managerial activities (Cunha 2004).

Cunha (2004) posited the most efficient way of using cognitive resources is when practitioners become familiar with their every day routines, which create patterns of insights capable of behavioural novelty (improvisation). From this view, it is noted that the practitioners do not abandon functionalism (which is embedded cognitively) but creatively draw from functionalism in an incremental way (ill-structured way) to generate new ways of achieving an intended outcome, namely *improvisation* (Njenga and Brown 2008). The foundation for this view point was developed by Ciborra *et al.* (2000) who considered improvised activities as **simultaneously structured** (functionalist) and **unpredictable**; planned but emergent; purposeful but opaque; effective but irreflexive; discernible after the fact but spontaneous (incrementalism) in its manifestation. The holistic approach therefore sees *improvisation* **as a fusion** between these two extreme approaches, namely the functionalist approach and the incremental approach to ISRM (Njenga 2007). The approach is illustrated below in **Figure 7**:

Figure 7. The holistic view of ISRM (Njenga 2007)

Many studies in information security do not account for positive extemporaneous actions sometimes evident in ISRM. Anecdotes and literature about ISRM suggest that information security practitioners follow a functionalist approach that include the comprehensive review of risks, threats, vulnerabilities, technical controls, governance, and a host of closely related issues (Browne *et al.* 2000; Peltier 2001; Von Solms and Von Solms 2005;Yue *et al.* 2007).

Despite the wide acceptance of the view that ISRM constitutes structured functionalist techniques and methodological frameworks, this process should increasingly be seen as an art rather than a science (Winkler 2007; Njenga and Brown 2008). It is possible to see inherent shortcomings of functionalism in ISRM using solely standards and frameworks (Chebrolu et al 2005). In order therefore to obtain a richer picture of how information security practitioners' handle both structured by ill-structure activities, it is essential to have a different (qualitative-interpretivist) assessment (Chebrolu *et al.* 2005), an assessment which considers *improvisation* as drawing from functionalism.

The value of *improvisation* can be exemplified in the following example. When an information security practitioner detects inherent vulnerabilities and exploits by a hacker, the functionalist approaches suggests information security risk planning (Winkler 2007). The danger is that the practitioner will plan for exploits and vulnerabilities he/she is trained to detect. It requires a creative skilled information security practitioner to plan, detect and act on novel attacks, unknown attacks or even variants of common attacks (Chebrolu et al 2005). This therefore requires a mix of skills and resources, cognitive or otherwise (e.g. *improvisation*), since the reactive approaches embodied by functionalist methods are not feasible for detecting malicious attacks (Chebrolu et al 2005). What may be postulated is that a more descriptive and holistic understanding of how information security practitioners go about addressing threats by employing extemporaneous, cognitive and innovative abilities to counter these threats becomes necessary. The next sections describe this holistic understanding by introducing *improvisation*, its nature and typology.

4.2.1 Improvisation

Improvisation, derived from the Latin word "*improvisus*" is defined as "situated performance where thinking and action occur simultaneously and on the spur-of-the-moment" (Ciborra 1999). Improvised activities are deemed purposeful and "***simultaneously rational (functionalism) and unpredictable***", meaning these activities are discernible only after the fact. Barrett (1998) uses the Latin term of "*improvisus"* meaning "not seen ahead of time". It is the highly exploratory and tentative nature of this action that creates worries for potential failure and incoherency. Weick (1993b) sees improvised action as "***deliberate and extemporaneous***". *Improvisational* performance may only be *relatively* novel, meaning that it had been done before but that it was never (1) used by those undertaking the *improvisation* and / or (2) in the situation that triggered

the *improvisation* (Moorman and Miner 1998). *Improvisation* is also considered from the context of social negotiations as a "coherent sequence of relational, informational, and procedural actions and responses created, chosen and carried out by the parties during the process of social interaction" McGinn and Keros (2002).

Cunha et al (1999), also suggest that improvised activities "***occur during action***". Ciborra (1999) perceives such activities as "falling outside the glance of rational, awake attention during the action" and reckons "*they could be inferred by an outsider, or made explicit by the actor, but as a result of a reflection after the fact*". There is consensus with both Weick (1993b) and Ciborra (1999) that *improvisation* is a human practice from which there is purposeful action; as such, the actions or activities represent a tool for communication and interaction that seems crucial in the context in which they occur. McGinn and Keros (2002) viewed improvised acts as inherently both active and interactive and contained both familiar moves and unique approaches. They noted that interaction between parties reflected the social contexts within which the interactions took place.

4.2.2 Dimensions of Improvisation

The major dimensions of *improvisation* have to do with: (1) *impromptu* action in an organizational context, and (2) bricolage, or the ability to draw on the available material, cognitive, affective and social resources, in order to solve the problem at hand (Cunha 2004). *Impromptu* action is seen as improvised since such action did not have previous routine to tackle issues and the action is required, not optional (Cunha 2004). The qualities of *improvisation* are summarized in **Table 3.**

Table 3. Qualities of Improvisation (Cunha 2004)

Qualities	Description
Deliberate	Intentional efforts on behalf of the organization and/or any of its members
Extemporaneous	An attempt to enhance the deliberateness of the emergent part of organizational strategy and action
Occurs during action	Organizational members do not stop to think of what would be the best response to a problem or the best way to take advantage of an opportunity. Instead they develop their response by acting on the problem or opportunity

Qualities	Description
Uses resources	The resources used are: *(i)* **Material***:* encompasses all those resources that lay 'outside' the individual and the organizational social system. *(ii)* **Cognitive:** comprising the set of mental models held by the individual members of the organization. *(iii)* **Social:** the social structures present among members performing *improvisation*. These structures include not only formal relationships, but also explicit and tacit rules and informal patterns of interaction.

4.3 ANALOGY: UNDERSTANDING IMPROVISATION IN ORGANISATIONS - USING THE JAZZ METAPHOR

Organisational structures are much more reflexive and more often improvised than usually recognised (Barrett and Peplowski 1998). By using anecdotal and empirical evidence (Crossan and Sorrenti 1997; Moorman and Miner1998), formal definitions of organizational *improvisation* were developed. By means of grounded theory, propositions that aimed at explaining organisational *improvisation* in organizational settings were developed and tested by Moorman and Miner (1998). They defined **organisational** activity as **'***actions taken by one or more individuals on behalf of a team, an organization and / or a project' while looking at* **improvisation** as **'***the conception of action as it unfolds, drawing on available material, cognitive, affective and social resources'.* Organisational *improvisation* is seen as transposing within the organizational context the characteristics of both *improvisation* and bricolage (Crossan and Sorrenti 1997).

4.3.1 Organisational Improvisation and the Jazz Metaphor

The idea whereby organisations could be designed for maximising learning and innovation was noted by Barrett (1998). In organisations, some employees have a passion for learning and innovation; similarly, jazz musicians have a passion for creating new musical material, surprising themselves and others with spontaneous, unrehearsed ideas (Barrett 1998). With jazz music, *improvisation* is possible since what the jazz musician does with the notes is what actually counts. This reflexivity makes it possible for the jazz musician to turn a bad situation into a good one. Barrett and Peplowski (1998) point out that in jazz "*there is no such thing as a bad note*". The transformation of the jazz musician is actualised when the musician is able to

export material from different contexts and vantage points and by combining, extending, and varying the materials adding and changing notes, varying accents, to produce something new (Barrett 1998). They are able to "*breathe life into these forms*" (Barrett 1998).

The linking of organisational *improvisation* by applying the jazz metaphor has been considered in great depth by several scholars (Barrett 1998; Ciborra 1999; Weick 1993b). These scholars note that the main difference between jazz music and the various kinds of organisational activity is that, in jazz, there is no clear prescription of what is to be played. Barrett and Peplowski (1998) pointed out that the secret to the success of jazz musicians was in *improvisation* and in the way they 'learn how to listen'. This is important because, without it, jazz musicians would be going off in all directions creating a sort of musical anarchy. *Improvisation* in jazz therefore took the form of "*reworking pre-composed designs in relation to unanticipated ideas conceived, shaped and transformed under the special conditions of performance*" (Barrett and Peplowski 1998).

While understanding both the way jazz musicians think while they are playing and their ability to master the structured rules that govern musical progression, Barrett (1998) suggested ways in which organisational *improvisation* could be understood. He further outlined that after many years of practicing and absorbing music, jazz musicians train their ears to recognise what phrases fit between different forms, the various options available, within the constraints of various chords and songs. Once the music was integrated into their mental frames, the jazz musicians' rules for chords and songs become tacit and amenable to complex variation and transformation (Barrett 1998). Barrett (1998) draws a parallel between what jazz players do and what managers in organisations would be doing to fabricate and invent novel responses without a pre-scripted plan and without certainty of outcomes, discovering the future of their actions as it unfolds.

Barrett (1998) was able to translate jazz *improvisation* into the organisational setting by examining a model of diverse specialists living in a chaotic turbulent environment, making fast and irreversible decisions, highly interdependent on one another to interpret equivocal information. The interdependence and working together was also noted by Mcginn and Keros (2002). They saw *improvisation* in organisations taking the form of opening up, working together or haggling (Mcginn and Keros 2002).

4.3.2 Analogy of Jazz Musicians and Information Security Practitioners

Many authors are in agreement that organisational *improvisation* aims to solve particular problems or to manage events. This form of organisation *improvisation* happens in varying degrees and occurs along a continuum ranging from the spur-of-the-moment action to entirely structured planning (Cunha *et al.* 1999; Moorman and Miner 1998). Barrett (1998) suggested that any improviser employs automatic thinking to execute patterns and that the improviser is free to plan strategy while, in a sense, being aware of sub-routine details at peripheral levels and reserving the central conscious control for strategic planning.

Drawing the analogy into ISRM, in conditions of complexity and uncertainty, where ISRM and planning have little effect, ISRM practitioners can learn from jazz musicians when looking at the jazz band as a sort of corporation engaging in an activity. Though not much has been written on ISRM and jazz, Barrett (1998) makes a point that managers in general (including information security practitioners) often find themselves doing what jazz players would be doing, e.g. inventing novel contextual responses without certainty of outcomes.

Within ISRM activities the need to solve problems, such as securing systems, designing and re-designing systems, all have to take place in conditions of unprecedented complexity and uncertainty (Rosenhead and Mingers 2001a). *Unprecedented complexities and uncertainty are situations that would allow ISRM practitioners to improvise.*

Barrett (1998) outlines seven characteristics that allow specialists (including information security practitioners) to improvise coherently in conditions of complexity. The outcomes while being purposeful, serve to maximise social innovation in a co-ordinated manner. These include:

(i) ***Provocative competences***, or deliberate effort to interrupt habit patterns;
(ii) ***Embracing errors*** as a source of learning***;***
(iii) ***Shared orientation*** towards structures that allow maximum reflexivity;
(iv) ***Distributed task***- continued negotiation and dialogue towards dynamic synchronisation;
(v) Reliance on ***retrospective sense making***; "Hanging out"- ***membership in a community of practise***; and
(vi) Taking turns soloing ***and supporting***.

4.3.3 Improvisation in Managerial Disciplines: Relevance to Information Security Risk Management

The foundation for improvised activities in management discipline in general and specifically ISRM lies on the premise that information systems are no longer stable, discrete entities, but part of elaborate networks and information infrastructures that are subject to constant adjustments and adaptation (Ciborra *et al.* 2000). This understanding suggests a calling for a unique way of managing information system security as an art form (Winkler 2007).

When trying to understand how information systems developers deal with unstable, discrete systems, Ciborra *et al.* (2000) considered how these practitioners improvised and noted that their activities contained elements of purposeful planning and opaqueness. Although Ciborra *et al.* (2000) were not referring to ISRM *per se*, but rather the management and planning aspects of information systems, it is important to realise that the *improvisation* phenomenon would not be ruled out of other managerial disciplines including ISRM. It can, for instance, be noted that some ISRM activities are seen as effective but "irreflexive", (Forno and Baklarz 1999) a key attribute of *improvisation*. Though Forno and Baklarz (1999) did not necessarily mention *improvisation*, they highlighted the spontaneity and irreflexiveness of ISRM activities. They demonstrated various ways information security practitioners would draw upon the action space (improvisational) to counter emergent unprecedented threats from hackers who used social engineering. Social engineering as used by hackers and the artistic countermeasures by information security practitioners for such activities has been documented by scholars who were once hackers themselves (Mitnick 2005; Mitnick *at. al.* 2002).

Cunha (2004) acknowledged this although he was not expressly talking about ISRM. The argument extended was that a practitioner's cognisance of external representations creates patterns of insights inside the practitioner. This cognitive space is capable of behavioural novelty which can guide information security risk management and information security risk mitigation processes.

Though there is less explication about *improvisation* in ISRM, (Njenga and Brown 2008), extending this interdisciplinary research into the contemporary ISRM workplace would be an

interesting way of understanding its meaning and its contextual relevance. This interdisciplinary approach to ISRM activities may give deeper insights about the goals and intentions of information security practitioners who carry out these activities.

4.4 TYPOLOGY OF IMPROVISATION: COGNISANCE OF A WIDER MEANING

According to Cunha and Cunha (2001), the approach to *improvisation* in organisations is primarily based on three principles. However, they observe that these principles are more likely to change than to be followed rigidly. They include:

a) **Principle 1**: Plan to remain flexible (incrementalism)
b) **Principle 2**: Rely on structure to promote initiative (functionalism)
c) **Principle 3**: Use pressure to boost creativity. (Note: Pressure links functionalism and incrementalism)

It should be noted that these three principles have broader implications for organisations as they embark on formulating ISRM policies/ structure. Ideal causal conditions for improvisation would be:

a) Lack of organisational discipline. New plans are made as people go along and this stems from lack of existing plans and lack of rigour to follow plans (Kamonche *et al.* 2002).
b) Deliberately encouraging spontaneous activities that are inconsistent with prior plans (Kamonche *et al.* 2002).
c) Logic of responsiveness; in the face of uncertainty and unpredictability that make prior plans irrelevant or incomplete and faced with a context in which it is difficult to refrain from taking action (Kamonche *et al.* 2002).
d) Turbulence; lots of change in the current environment (Kamonche *et al.* 2002).

4.4.1 Various forms

Improvisation in its various forms is summarised as follows:

(a) ***Individual Improvisation*:** this is where planned or deliberate individual behaviour creates *improvisation* (Moorman and Miner 1998). As an illustration, an individual's deliberate

behaviour may play an important role in speeding the development of highly iterative and experiential new products (Moorman and Miner 1998; Eisenhardt and Tabrizi 1995).

(b) ***Collective Improvisation*:** this is the combined effort of several individuals/organizations (Cunha 2004); Research suggests that interactions among people who are improvising frequently produces collective *improvisation* (Cunha 2004; Crossan and Sorrenti 1997). There are suggestions that collective *improvisation* often builds on and incorporates individual *improvisation* (Moorman and Miner 1998). In an *improvisational* group, for example, one member might make a comment, to which a second will respond with an association between the comment and another topic, and then a third member might link these issues to a third, inclusive topic (Mangham 1986). The group might not have planned what to say in advance, and the pattern that arises is not a simple sum of independent *improvisational* actions but a collective system of interaction that creates and enacts the scene simultaneously (Moorman and Miner 1998). The idea that a system of interaction can produce collective *improvisation* was first suggested by Moorman and Miner (1998). It can also be noted that the behaviour of teams sharing a collective mind (Leede *et al.* 1999) fosters long and strong collective experiences in co-operation, both in training situations and in practice. Leede *et al.* (1999) contends that, to a large extent, behaviour in a collective mind is standardised and therefore predictable and that this standardisation creates the necessary sound base for collective *improvisation*, for creative and intelligent collective action (Leede *et al.* 1999).

(c) ***Process Improvisation*:** this relates to the "content, character and sequence of previous routines"; process *improvisations* affected the manner in which these products were developed Miner *et al.* (2001). Vera and Crossan (2004) have used the jazz metaphor to emphasizes that good *improvisation* (in theatre) arises because its main focus, in contrast to the focus of organisations, is more on the process of improvising and less on the outcomes of *improvisation*.

(d) ***Product Improvisation*:** this affects the substantive nature of products and outcomes of the organization (Cunha 2004; Miner *et al.* (2001). Another way of viewing product *improvisation* is through composition (music composition, or any sort of a recreation of a process) which is a way to turn process *improvisation* into product *improvisation* (Belgrad 1998).

4.4.2 Improvisation as a Fusion of Functionalism and Incrementalism

Hu *et al.* (2007) has argued for a more coherent socio-organizational framework that explains a deviation from a functionalist centralized structure to a socio-cognitive one that explains why managers and practitioners behave in certain ways. By extending on Hu's *et al.* (2007) socio-cognitive approach, it would be interesting to consider the "reality" of ISRM activities.

It has been discussed at length how functionalist notions of order-seeking, near-to-equilibrium social arrangements are inappropriate because these do not take into account notions of complexity (Hu *et al.* 2007). Reed and Harvey (1992) have pointed out that complexity and unpredictability in systems defy standard positivist and functionalist canons of description, prediction and explanation. On the other hand, incrementalism accounts for complexity and takes into cognizance issues such as adaptation, deliberative behavior, intelligent behavior, reproduction and evolution (Marion 1999).

A holistic fusion approach would incorporate the functionalist and incremental approaches which argues for the principles of 'dissipative systems' which are open and capable of assimilated change from environments and are increasingly structurally complex (Reed and Harvey 1992). The neo-institutional theory stresses organizations as rational entities with structures, rules, and procedures designed to perform certain tasks efficiently. The institutional theory argues that organizations are socially constructed, in the sense that organizational structures are adaptive vehicles ''shaped in reaction to the characteristics and commitments of participants as well as to the influences and constraints from the external environment'' (Scott 1987)

4.5 DEVELOPING A SENSITISING DEVICE TO UNDERSTAND IMPROVISATION IN ISRM

Improvisation (as a fusion approach) helps reconcile tension between structure (functionalism) and reflexivity (incrementalism) since it comprises a rich mixture of centralised structure and novel spontaneity (Cunha 2004; Ciborra *et al.* 2000; Segars and Grover 1999).

4.5.1 Device Development

The objective of this research is to explore and conceptualise this fusion of innovation with centralised structure, as a vehicle of understanding these contrasting and often opposite perspectives and dichotomies. It is believed that with this understanding, there will be important implications for management practice. **Table 4** introduces structured functionalist ISRM activities as stipulated by ISO IEC 17799. This initial framework (**Table 4**) will acts as inputs for developing a *Sensitising Device* to be used in the research. ISO IEC 17799 acts as a functionalist representation of the ISRM activities stipulated in ISRM frameworks, methodologies and standards discussed earlier. The reason ISO IEC 17799 has been singled out as functionalist input for the *Sensitising Device* is that ISO IEC 17799 is deemed to apply, both in relevance and practicality, to a large number of organisations (Von Solms and Von Solms 2005; IT Gov 2000; ISO / IEC 2002). The other reason is that ISO IEC 17799 has been suggested as a framework that identifies information security requirements in organisations (Furnell *et al*. 2006). ISO / IEC 17799 (ISO / IEC 2002) lists some of the following activities conducted by information security practitioners. (***ISO 27005 has not been used as an input for the sensitising device since this research predates the publication of the standard).*** The names of some of the activities (**Table 4**) have been changed in this research to reflect the generic nature of the activities. **Six** of these activities are singled out for conceptualisation in the research as follows:

1. Information Security Policy- ***See section 2.4.2 of this research*** (Section 3 of ISO 17799)
2. Information Security Architecture- ***See section 2.4.1 of this research*** (Section 4 of ISO 17799)
3. Information Assets Control Section- ***See section 2.4.1 of this research*** (5 of ISO 17799)
4. Information Security Event Monitoring - ***See section 2.4.1 of this research*** (Section 9 of ISO 17799)
5. Regulatory Compliance - ***See section 2.4.2 of this research*** (Section 12 of ISO 17799)
6. Disaster Recovery and Business Continuity Management - ***See section 2.4.2 of this research*** (Section 12 of ISO 17799)

These **6 ISRM** activities identified in **Section 2.4**, have been selected since they are deemed easy to trace and observe, and hence for purposes of practicality and feasibility the research

focuses only on these. The **Table 4** shows a mapping of the ISRM activities selected with ISO IEC 17799.

Table 4. Mapping ISO 17799 Domains to ISRM Activities (Njenga and Brown 2008)

CORE ISRM Activities ISO/ IEC 17799 Sections				**Covered in Research**	**ISRM Activities** ***(listed in order of research analysis)***
	ISO/IEC 17799 Section	**Type of Activity (Domain)**			
	1	*Introduction Reference text n/a*		n/a	n/a
IDENTIFY	**2**	*Introduction Reference text n/a*		n/a	n/a
	3	Information Security Policy		Yes	**3 Information Security Policies**
	4	Security Organisation		Yes	**2 Information Security Architecture**
	5	Information Asset Classification and Control		Yes	**1 Information Assets Access and Data control**
ANALYSE	**6**	Personnel Security		***No**	
	7	Physical and Environmental Security		***No**	
	8	Communications and Operations Management		***No**	
RESPOND	**9**	Access Control (section 9.7)		Yes	**4 Information Security Event Monitoring**
	10	System Development and Maintenance		***No**	
	11	Business Continuity and Management		Yes	**6 Business Continuity and Disaster recovery**
	12	Compliance with Legal Requirements		Yes	**5 IT Governance and Regulatory Compliance**

**No – technical areas were not considered feasible hence not researched*

The purpose of the *Sensitising Device* incorporating ISO IEC 17799 is to help the researcher empirically understand and describe ISRM activities within the contexts of functionalism, incrementalism and the fusion of both of these. Functionalism as described in the *Sensitising Device* is drawn from ISRM literature focusing on ISO IEC 17799. Functionalist approaches described in the *Sensitising Device* are frameworks that focus on planning and implementing procedures and guidelines as contained in standard codes of practice such as ISO IEC 17799 (Eloff and Eloff 2003; ISO 17799). **Table 4** maps ISRM functionalist approaches in literature (ISO 17799) to be conceptualised against incrementalism. The detail to which functionalism and incrementalism is translated as improvised action in the **6 ISRM** activities will be the research's concern.

4.5.2 The Device

To contribute to the development and empirical validation of a comprehensive framework for *improvisation* in ISRM, a conceptual model know as a *Sensitising Device*, that fuses the functionalism and the incrementalism approach towards ISRM was developed. This model

explains the fusion derived from variations between functionalism and incremetalism in ISRM. The variations are derived and contrasted through the specification and examination of *organisational frameworks, standards and policies which are* determinants of ISRM activities and also incrementalism where socio-contextual and emergent activities that fall outside of these frameworks are examined. The fusion framework confirms the contextual determinants of *ISRM success* by exploring *improvisation* and is illustrated in **Figure 8** below.

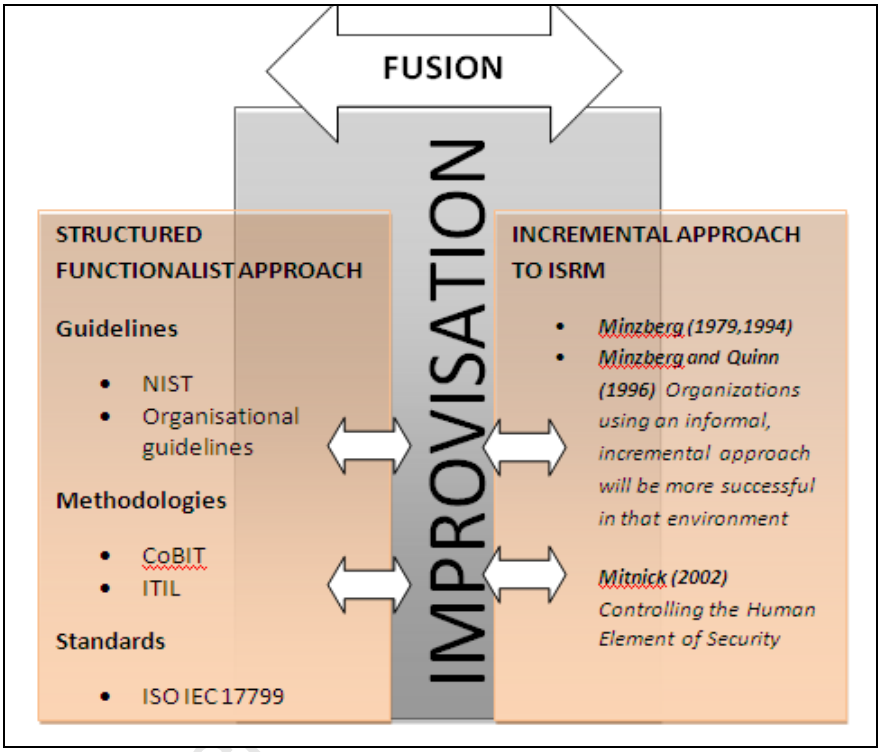


Figure 8. Fusion between Functionalism and Incrementalism in ISRM

Figure 8. summarises what has been discussed and is a fusion of the functionalist and incremental approaches. Both of these approaches are summarised as follows:

Structured Functionalist Approaches

The functionalist approach takes the view that organizations will be successful in coping with a turbulent environment only when they incorporate **formal planning** (Salmela *et al.* 2000). The formal planning could be based on **Guidelines** (NIST, organisational guidelines), **Methodologies** (CobiT, ITIL) and **Standards** (ISO IEC 17799). As depicted in **Figure 8** functionalist ISRM activities conducted within an organisation, would be seen to characterise the following;

1. Activities (e.g. ISRM) are complicated and highly integrated with overall strategy (Premkumar & King 1994).
2. Activities (e.g. ISRM) are formal and comprise multiple analyses which are used to derive order and control (Raghunathan & Raghunathan 1991; Bergeron *et al.* 1991).
3. Activities (e.g. ISRM) are based on formal representations from many different organisational groups (Earl 1988).
4. The formal methods and criteria are the basis for (e.g. ISRM) decisions (Ein-Dor and Segev 1978).
5. Activities (e.g. ISRM) are periodically reviewed to adapt to changing circumstances (Galliers 1987).

Incremental Approaches

The incremental approaches sees change in a turbulent environment as so rapid that plans are obsolete before they can be implemented therefore making the functionalist approach susceptible to wasted efforts, misdirected investments, and low morale (Vitale *et al.* 1986). As depicted in **Figure 8** incremental ISRM activities conducted within an organisation, would be seen to characterise the following;

1. Activities (e.g. ISRM) are simple, informal and loosely integrated with overall strategy (Ciborra 1994).
2. Activities (e.g. ISRM) are based on personal experiences and judgment to derive order and control (Vitale *et al.* 1986).
3. Activities (e.g. ISRM) are based on an informal network of few key individuals (Vitale *et al.* 1986).
4. Shared group (collective) understanding of a few key individuals is the basis for (e.g. ISRM) decisions (Ciborra 1994).
5. Activities (e.g. ISRM) are reflexive and are continuously reviewed to adapt to changing circumstances (Vitale *et al.* 1986).

The Fusion (Improvisation)

Figure 8 also depicts a fusion between these two approaches. This fusion is what the researcher denotes as *improvisation.* By its earlier definition, *improvisation* was seen as purposeful, and

***simultaneously* rational (functionalism) and unpredictable (incrementalism).** This means *improvisation* bears the characteristics of both approaches. When practitioners improvise, they *improvise* within the boundaries of frameworks, methodologies and standards, while at the same time, following practices specifically adapted for coping with a turbulent contextual environment (incrementalism). The researcher therefore sees i*mprovisational* activities in ISRM are those engaged when searching for satisfactory solutions that deal with threats and opportunities yet remain within the organization's current frameworks and methodologies.

It can be seen that in stable environments, ISRM is seen as unchallenging, and it is agreed that in stable environments functionalism can work (Vitale *et al.* 1986), but no research has validated either the incremental or functionalist approach in ISRM to verify this. The subsequent *Sensitising Device* is the more detailed fusion framework that helps serve as a lens into the areas to explore the general idea and meaning into *improvisation* in ISRM. This is shown as **Table 5.**

Table 5. Detailed Fusion Framework between Functionalism and Incrementalism in ISRM

STRUCTURED (FUNCTIONALIST) APPROACH				IMPROVISATION				INCREMENTAL APPROACH
ISRM Functional Approach				Collective Improvisation	Individual Improvisation	Product Improvisation	Process Improvisation	ISRM Incremental Approach
ISRM Activities	**ISO 17799 Sections**	**ITIL**	**CobiT**					
1. Information Asset Access and Data Control	5.2 Information classification	**Application Management, Control Methods and Techniques** 7.2 Understanding the applications relationship to IT services	**DS 11** Manage Data					
2. Information Security Architecture	4.1 Information security infrastructure	**ICT Infrastructure Management, Technical support** 5.4	**PO 2** Define the information architecture					
3. Information Security Policies	3.1 Information security policy	**Security Management;** *Fundamental of Information Security;* 4.1 Control	**DS 5** Ensure Systems Security					
4 Information Security Event Monitoring	9.7 Monitoring system access and use	**Service Level Management** 4.4.7 Establish monitoring capabilities	**DS 10** Manage Problems and Incidents					
5 IT Governance and Regulatory Compliance	12.1 Compliance with legal requirements 12.3 System audit considerations	**The Technical Support** 5.4 The technical support process	**PO 8** Ensure compliance with external requirements					
6. Disaster Recovery and Business Continuity	11.1 Aspects of business continuity management	**Availability Management** 8.3 The availability management process	**DS 4** Ensure Continuous Service **DS 10** Manage Problems and Incidents					

Unknown ISRM Data:

Improvisation in ISRM to be conceptualised

(Chapter 6 and Chapter 7)

- ***Minzberg (1979,1994)***
- ***Minzberg and Quinn (1996)*** *Organizations using an informal, incremental approach will be more successful in that environment*
- ***Mitnick (2002)*** *Controlling the Human Element of Security*

4.5.3 Synthesis of Approaches and Apparent Contradictions

From the synthesis of the apparently contradictory approaches of functionalism (standards/frameworks like CobiT, ITIL, ISO IEC 17799) and incremental approaches, the argument posited in this research is that *improvisation* has become a way of considering these as fused elements. Indeed researchers have noted that there is a limitation of scope and understanding for people who view ISRM from one of either perspective or approaches. Yates and Orlikowski (1992) have successfully pointed out the dichotomies and contradictions in perspective in organisational studies. Weick (1998) argues that organizational analysts are limited in perspective and often end up tempted to choose between either of the opposing or contradicting conceptual dichotomies, "the issue in most organizations is one of proportion and simultaneity rather than choice". The fusion framework or the '*Sensitising Device'* offers a lens to which the opposing and contradicting dichotomies are seen as fusing into one whole with *improvisation* being the core of this whole.

4.6 CHAPTER SUMMARY AND CONCLUSION

The earlier sections of this chapter demonstrated *improvisation* as holistic, incorporating elements of functionalism and incrementalism. The knowledge obtained in the chapter has contributed to the theoretical understanding of *improvisation*'s role in ISRM. A common thought is that both functionalism and structure are indispensable enablers of ISRM order and control. Although the potential of structure and functionalism in organizations is acknowledged, evidence increasingly points to the importance of human agency expressing improvised acts. The chapter has demonstrated an alternative approach that shows the resourcefulness of human agency in terms of inventiveness. The chapter has also given us useful insights that reveal that practitioner activities go beyond rules, structure and formalization.

CHAPTER FIVE

The previous chapters have secured our theoretical understanding and have helped us conceive information security risk management and the activities therein. What remains is the generation of data and the conceptualization of the phenomenon of *improvisation* in these activities. This chapter introduces the methods and the methodology by which data was drawn. The chapter explains the data collection methods that were used. The chapter concludes by justifying the case for using grounded theory techniques to analyze this data. The philosophy of the research makes the case for the research.

Table of Content

Chapter Five

CHAPTER FIVE: RESEARCH METHODOLOGY

5.0 INTRODUCTION

This chapter discusses the philosophical assumptions underpinning the research problem presented in the first chapter of this thesis. In the introduction, it was mentioned that little research had been undertaken on *improvisation* in ISRM. The purpose of this chapter is to discuss a formal scientific way of dealing with the gaps identified in literature by introducing a sound research methodology. This chapter discusses the research methodology underpinning the research and the manner in which the gaps in ISRM identified in the first chapter are explored.

This chapter is concerned with the methodological approach to the problem posed in **Chapter 1**. The chapter details the research strategy, approach to theory and the challenges experienced. The qualitative approach to research is introduced as a means of providing richer meaning and insight to the research.

Section 5.1 revisits the research questions. This section exemplifies the meaning of *improvisation* by re-visiting the research questions identified in **Chapter 1.** These questions make the qualitative approach to research amenable to finding meaning of *improvisation* in ISRM. Section 5.2 outlines some principles of research and the competing dichotomies identified in literature that guide researchers' approaches towards research. This section explains the need to account for these dichotomies and why some of the approaches were singled out for this research. Section 5.3 and 5.4 describe both the ontology and epistemology of the research. Section 5.5 describes the approach to theory and to research. Section 5.7 discusses the research strategy. The single case study research strategy is presented, the data collection methods outlined, and the various research themes/topics for interviews discussed. This section explains how the research questions established earlier are met in collaboration with the organisational participants. Section 5.7 introduces the single case and explains why this case was selected. This section shows how this single case study is well integrated with the wider objectives of this research. Section 5.8 explains the data collection techniques used in the single case while section 5.9 justifies the reason for using grounded theory techniques to analyse the data collected. The last section gives a summary of the chapter.

5.1 RESEARCH QUESTIONS

This section deals with the research question that laid a foundation for the research. Finding the meaning of *improvisation* with the aim of improving ISRM activities was seen as the main objective. The research considered the deeper meaning underpinning *improvisation* in ISRM. The research question formulated earlier on in **Chapter 1** was aimed at directing attention away from the functionalist ISRM approach present in larger more complex organisations which have comprehensive information security policies in place to focusing on *improvisation*.

5.1.1 Objectives and Questions - Revisited

Research Question

> ***How is improvisation manifested in Information Security Risk Management (ISRM) activities and how can improvisation in ISRM be conceptualised?***

While considering the above question, the following sub-set questions amplify this question and deal with understanding ISRM activities outside of functionalism as follows:

- *What ISRM activities are in an organisation and how are they carried out?*
- *How is improvisation manifested in these ISRM activities in the organisation?*
- *How can improvisation in ISRM be conceptualised**?***
- *How is improvisation used as a foundation for Positive ISRM?*

Understanding the above questions meant employing research methods that would be deemed appropriate. The methods used (described in detail in the sections that follow) were seen by the researcher as compatible with the wider objectives of this research. The methods aimed at giving the researcher the optimal data required to comprehensively investigate the research questions posed. Care was taken by the researcher to select methods that could complement each other and methods that were feasible given the constraints of resources. The methods selected aimed at capturing *lived experiences*, deeply held beliefs, opinions and feelings, and world views as understood by information security risk practitioners. The researcher was the main meaning

maker of inquiry. There was balance between what was explained as having happened out there and the practitioner's interpretation and "reality".

5.2 DICHOTOMIES OF RESEARCH

This section introduces the various research dichotomies (Lee 1989) and explains why certain approaches were singled out and adhered to in this research. The section explains the approaches used while assessing these approaches in terms of feasibility to meet research objectives. When looking at the research approaches, the researcher realised that there are a number of competing dichotomies identified in the literature that guide researchers' approaches towards research. Some of these are seen as dichotomous to each other (Guba and Lincoln 1994; Lee 1989). Fitzgerald and Howcroft (1998) have listed these to include:

1) Realist v. Relativist
2) Interpretivist v. Positivist (V. Critical Realism: Orlikowski and Baroudi 1991)
3) Subjectivist v. Objectivist
4) Qualitative v. Quantitative
5) Exploratory v. Confirmatory
6) Induction v. Deduction
7) Relevance v. Rigour

5.2.1 Not Dichotomous After All

In the recent past researchers have recognised that Information Systems research is **multimethod.** This means it is not one paradigm **verses** the other, one **or** the other, but a multimethod approach may be used (Mingers 2001). The explanation for this is because Information Systems "*draws on and provides a nexus for many diverse research fields and disciplines*" (Mingers 2001). Information Systems also encompasses very different research traditions. Mingers (2001) agrees that research needs to be done on the cognitive and cultural obstacles that stand in the way of multimethod. According to Mingers (2001), the real world is ontologically stratified and differentiated, consisting of a plurality of structures that generate the events that occur. Different paradigms each focus attention on different aspects of the situation, and *so* multimethod research is necessary to deal effectively with the full richness of the real

world. Each of the competing views (paradigm) is defined and the researcher's stance explained in the following sections.

5.3 ONTOLOGY

> *"The question about ontology refers to whether an object of cognition exists beyond subjective imagination and perception"* (Bunge 1977).

Table 6 outlines two competing views: the relativist view and the realist view.

Table 6. Ontological Research Approach

SOFT APPROACH	**HARD APPROACH**
ONTOLOGICAL LEVEL	
Relativist Belief that multiple realities exist as subjective constructions of the mind. Socially-transmitted terms direct how reality is perceived and this will vary across different languages and cultures. Fitzgerald and Howcroft (1998)	**Realist** Belief that external world consists of pre-existing hard, tangible structures which exist independently of an individual's cognition. Fitzgerald and Howcroft (1998)

From **Table 6** above it can be shown that ontology seeks to explain whether the perception of social and physical reality exists subjectively as a construction of the mind or whether the reality is objective and exists independently of an individual's cognition. It should be noted that research in cognitive science shows that universal immediate knowledge of reality is impossible in principle (Maturana and Varela 1980).

Stance

This research is **relativist** and fits into a view point that holds onto a subjective reality which is perceived as only existing as an aggregate of socially constructed multiple realities. This ontological understanding fits with the researcher's overall aim which is to understand the phenomenon of *improvisation* in ISRM activities through the relative socio-construction of meaning that information security practitioners assigned to these activities i.e. the **relative** meaning of *improvisation* in ISRM in its context.

In this research it can only be said that the "truth" about the reality of *improvisation* in ISRM is **relative** and waiting to be discovered (Crotty 1998). Truth as conceived by the researcher exists

only through understanding the interaction with the realities of the world. This view assumes ***meaning is constructed rather than discovered*** (Crotty 1998).

The researcher's soft approach and ontological stance (**relativist**) was justified by the fact that there has been a noticeable shift in IS research from technological to managerial and soft organisational issues. This growth of a softer stance to research was evidenced, for example, by an increase in the number of IS journals publishing interpretive studies (Walsham 2006). There is also evidence of a shift in editorial policy of some main IS journals, notably *MISQ*, that found acceptance of interpretive studies (Mingers 2001).

5.4 EPISTEMOLOGY

> *"Epistemology is concerned with providing a philosophical grounding for deciding what kinds of knowledge are possible and how we can ensure that they are both adequate and legitimate"* (Crotty 1998).

Table 7. outlines competing views, namely the interpretivist, the positivist, the subjectivist and the objectivist views which provide various knowledge types.

Table 7. Epistemological Research Approach

SOFT APPROACH	**HARD APPROACH**
EPISTEMOLOGICAL LEVEL	
Interpretivist No universal truth. Understand and interpret from researcher's own frame of reference. Uncommitted neutrality impossible. Realism of context important. Fitzgerald and Howcroft (1998)	**Positivist** Belief that world conforms to fixed laws of causation. Complexity can be tackled by reductionism. Emphasis on objectivity, measurement and repeatability. Fitzgerald and Howcroft (1998)
Subjectivist Distinction between the researcher and research situation is collapsed. Research findings emerge from the interaction between researcher and research situation, and the values and beliefs of the researcher are central mediators. Fitzgerald and Howcroft (1998)	**Objectivist** Both possible and essential that the researcher remain detached from the research situation. Neutral observation of reality must take place in the absence of any contaminating values or biases on the part of the researcher. Fitzgerald and Howcroft (1998)

The core of epistemology deals with the relationship of cognition acquired by the subject to the object of cognition (Becker and Niehaves 2007). From **Table 7.** above, it can be explained that the interpretivist researcher focuses more on the subjective propositions that are regarded as relevant when striving for knowledge, while the positivist researcher theoretically claim an

intersubjective validity for their research results (Becker and Niehaves 2007). According to Pozzebon (2003), the terrain in which the interpretive research takes place is continually shifting and is characterised by openness rather than stability and closure.

It should be noted that the main area of contention between a positivist and an interpretivist perspective lies in the understanding of 'reality' (Burrell and Morgan, 1979; Walsham, 1993). Interpretive research attempts to understand phenomena by exploring the meaning people assign to them and the context in which that person acts. An interpretive approach is based on the assumption that data is socially constructed and value laden (Byrne and Sahay 2007). Byrne and Sahay (2007) consider data collected in interpretive research as being transformed into information and then knowledge through the interpretation and meaning people assign to it, which influences knowledge and actions.

Stance

The epistemological viewpoint held in this research is that of *interpretivism*. It is thus seen as a researcher's own interpretation of the ISRM practitioners' interpretation of the reality of information security risk. It was acknowledged from the onset that an **interpretivist** stance (Klein and Meyers 1999) would help establish successful collection of data and interpretation through in-depth interviewing. What led to this research generally being taken and classified as interpretive was a primary assumption that the researcher's knowledge of reality was to be gained through social construction such as language, consciousness, shared meanings documents, tools and other artifacts (Klein and Meyers 1999).

The construction of knowledge about *improvisation* was also gained iteratively through the researcher's own interpretations. This meant that this knowledge was to grow incrementally, with meaning of language, consciousness, and shared meaning of ISRM activities growing successively at each iterative step, allowing the researcher to take advantage of what was being learned, and then to proceed to the next higher level (Miyake 1997).

The researcher rejects objective reality, and much of the research work could be taken as **subjective** and tending to construct meaning. The research was inclined towards the *meaning-oriented methods* as opposed to those methods that were positivist measurement-*oriented methods* (Myers 1997b). Thus this is where the researcher became the meaning maker of this reality of *improvisation* in ISRM. This inherent subjectivity lies at the core of richness of this

research. It should be noted that Rubin and Rubin (2005), have viewed the iterative process as being **very subjective** and varying from one researcher to another. Rubin and Rubin (2005) postulated that, "*Though the analysis is based on the descriptions presented by the interviewees, the interpretations in the final reports are those of the researcher*". While the positivist holds that reality is "out there", waiting to be discovered and that this reality is reflected in universal laws that may be discovered by the application of objective, replicable and "scientific" research methods, the interpretive position argues that the world is subjective and reality is socially-constructed and hence relative (Lincoln and Guba, 2000).

5.4.1 Qualitative and Quantitative Research (Data Types)

> *"Qualitative Research is any type of research that produces findings not arrived at by statistical procedures or other means of quantification. It can refer to research about persons' lives, lived experiences, behaviours, emotions, and feelings as well as about organizational functioning, social movements, cultural phenomena, and interactions between nations"* (Strauss and Corbin 1998).

> *"Quantitative approach to research is any type of research that involves quantification and measurements (statistical procedures) applied to populations, since the populations' data exists independently from the researcher's opinions and feelings. Being objective implies that other individuals should agree with the researcher's observations and measurements applied to populations" (Welman, et al. 2007).*

Table 8 outlines two competing methodological approaches namely the qualitative and the quantitative.

Table 8. Methodological Research Approach

Qualitative	**Quantitative**
Determining what things exist rather than how many there are. Thick description. Less structured and more responsive to needs and nature of research situation Fitzgerald and Howcroft (1998)	Use of mathematical and statistical techniques to identify facts and causal relationships. Samples can be larger and more representative. Results can be generalised to larger populations within known limits of error Fitzgerald and Howcroft (1998)

From the descriptions on **Table 8** above, it can be determined that both positivistic and interpretive research can apply qualitative and quantitative methods (Creswell 2003). Qualitative research can also either be positivist, be interpretive or use the critical research perspective (Mingers 2001). **Qualitative** approaches emphasize meaning-oriented methods while quantitative approaches look at results and outcomes as stemming from causal relationships. The **quantitative** methods use mathematical and statistical data to show these relationships.

Stance

In this research, qualitative research methods were used to examine the socio-technical phenomenon of *improvisation* in ISRM. **Thick descriptive** data were used. The qualitative approach was used to help the researcher understand *improvisation* in ISRM as seen from the information security practitioners' perspective. The information security practitioners would yield qualitative data about "*lived experiences, behaviours, emotions, and feelings as well as about organizational functioning".*

In general terms, not all qualitative research is interpretive (Klein and Meyers 1999). Within qualitative research methods, the employment of the *hermeneutic method* is what distinguished this qualitative research to one that would be recognized as being interpretive (Klein and Meyers 1999). The hermeneutical method was considered to fit well with the concerns of *attempting to achieve coherence over the whole process and finding overall meaning (of improvisation in ISRM)* (Schultze 2000).

The Hermeneutical Circle: this is the view that '*understanding the meaning of the whole, is done by understanding the meaning of its constituent parts and, also by understand the meaning of the verbal parts of a linguistic whole, there must be some prior sense of the meaning of the whole'* (Klein and Meyers 1999). The hermeneutical circle is the foundation of all interpretive work. How the hermeneutical circle was applied in this case was in the understanding of a complex whole of ISRM (functionalism and incrementalism), the preconceptions about meaning attributed to of its parts (functionalism and incrementalism) and their interrelationships. The process of interpretation in this research moved from a precursor of understanding the parts (texts and meaning) to understanding the whole and from a global understanding of the whole context back to an improved understanding of each part (Klein and Meyers 1999).

Thus the whole process was circular in approach. This circular accumulation of understanding is exemplified in **Chapter 6 and 7**. The interpretation in **Chapter 7** was based on both the researcher's and the information security practitioners' preliminary understanding (and interpretation) of the research question/gaps. Interpretation would be concluded by understanding the whole which would consist of the shared meaning that emerged based on these interactions (Klein and Meyers 1999).

5.5 APPROACH TO RESEARCH

> *"The exploratory approach to research is concerned with discovering patterns of data "*(Fitzgerald and Howcroft 1998).
>
> *"Confirmatory research is concerned with theory testing and verification"* (Fitzgerald and Howcroft 1998).

It should be noted that the approach to research can be either exploratory, explanatory or a combination of both.

Table 9 outlines the two approaches to research namely the exploratory approach and the confirmatory approach.

Table 9. Approach to Research

SOFT APPROACH	HARD APPROACH
APPROACH TO RESEARCH	
Exploratory Concerned with discovering patterns in research data, and to explain/understand them. Lays basic descriptive foundation. May lead to *generation* of hypotheses Fitzgerald and Howcroft (1998) **Confirmatory** Concerned with hypothesis testing and theory verification. Tends to follow positivist, quantitative modes of research Fitzgerald and Howcroft (1998)	

Table 9 above should be viewed as suggesting that exploratory research may incorporate either soft, hard or both approaches. The same may be said on confirmatory research.

Stance

No Previous research studies have been done of *improvisation* in ISRM; therefore this research was **exploratory** and was concerned with **discovering new patterns of data** (*improvisation* in ISRM). A lot of ideas incorporated in the research were exploratory and were drawn from the domains that incorporated cognitive philosophy and thinking dominant with social scientists well as industry managers. Exploring new ideas meant that the researcher would explain the phenomenon under study well and also would a lay a foundation of descriptive ideas for understanding *improvisation* in ISRM activities. Exploration was possible in the research since at the heart of qualitative and interpretive research lays the premise of *openness*.

5.6 APPROACH TO THEORY

> *"The inductive researcher derives understanding based on the discussion"* Krueger (1989).

> *"The deductive researcher derives understanding based on testing or confirming a preconceived hypothesis or theory"* Krueger (1989).

Table 10 outlines the two approaches to theory: the inductive approach and the deductive approach.

Table 10. Research Approach to Theory Development

SOFT APPROACH	HARD APPROACH
APPROACH TO THEORY	
Induction Begins with specific instances which are used to arrive at overall generalisations which can be expected on the balance of probability. New evidence may cause conclusions to be revised. Criticised by many philosophers of science, but plays an important role in theory/hypothesis conception. Fitzgerald and Howcroft (1998)	**Deduction** Uses general results to ascribe properties to specific instances. An argument is valid if it is impossible for the conclusions to be false if the premises are true. Associated with theory verification/falsification and hypothesis testing Fitzgerald and Howcroft (1998)

As **Table 10**. suggests, the research approach to theory can be either inductive, deductive or both. The inductive research approach usually forms the basis for most qualitative research methods and may at times be treated as 'suspicious' because subjectivity introduced into research makes the findings 'challenged' or 'not measurable'. However, it is this inherent

subjectivity that makes an inductive research approach rich and descriptive (Rubin and Rubin 2005).

Stance

Because of the existence of a prior theoretical framework and *Sensitising Device,* whereby discussions about the nature of ISRM as incorporating both functionalism and incrementalism apply to this research, it was safe to acknowledge that the research was not **purely inductive**, but consisted of **both deductive** and **inductive** elements. The derivation of a *Sensitising Device* aimed at a preliminary "testing" of the fundamentals of ISRM in the organisation was determined by existing frameworks; thus the research was **deductive.** The data analysis (open coding) part of this research was seen as independent and not influenced by pre-existing data sets, making it **inductive.** It was possible to identify some deductive element expressed in the form of the *Sensitising Device* and consequently in the arguments that stemmed from its use in the latter stages of the research. Inductive reasoning was not suppressed by the researcher.

5.6.1 Approach to Research at Axiological Level

> *"Rigour refers to hypothetical-deductive testing with emphasis on internal validity"* (Fitzgerald and Howcroft 1998).

> *"Relevance refers to applying research questions to practice with emphasis on external validity"* (Fitzgerald and Howcroft 1998).

Table 11. outlines the two approaches at the axiological level namely rigour and relevance.

Table 11. Axiological Research Approach

SOFT APPROACH	HARD APPROACH
AXIOLOGICAL LEVEL	
Relevance External validity of actual research question and its relevance to practice is emphasised, rather than constraining the focus to that researchable by 'rigorous' methods Fitzgerald and Howcroft (1998)	**Rigour** Research characterised by hypothetico-deductive testing according to the positivist paradigm, with emphasis on internal validity through tight experimental control and quantitative techniques Fitzgerald and Howcroft (1998)

Rigour has sometimes been mistakenly confused with positivist, quantitative research. It is for this reason that much attention has been devoted to rigorous hypothetico-deductive testing according to the positivist paradigm; this has been at the expense of relevance. The price that has been paid is that the hypotheses being tested have often been trivial, resulting in sterile research (Fitzgerald and Howcroft 1998).

Fitzgerald and Howcroft (1998) contend that researchers need to establish relevance and that research may be greatly constrained if there is too much emphasis on rigour only. They see a focus on rigorous approaches only as one way of failing to ensure the validity of the actual question being researched. They propose a need to lay down a critical foundation of meaningful and relevant constructs, in other words, "*relevance should come first and drive rigour*". However, "*relevance does not excuse inattention to rigour*" (Fitzgerald and Howcroft 1998).

Stance

This research needed to be **rigorous** and **relevant**, particularly in using the methods employed in data analysis. Relevance in this research was achieved by asking the following questions when examining data: "*what is this data saying from the through processes of the information security practitioner and the researcher"*? "*What was the ultimate relevance of the data"*? Rigour from an interpretive, qualitative perspective was achieved by following the principles and guidelines for conducting interpretive qualitative case study research (Darke *et al.* 1998). **Rigour** was also achieved in the way data was analysed.

It was accepted that conceptualisation and analysis process was greatly dependent on rigour and relevance, i.e. the researcher's "*rigour, clarity and creativity of his or her conceptual thinking*" (Lewis and Ritchie 2003). This means that the researcher made every attempt to make this research both rigorous and relevant, since making sense of the data was the ultimate goal of this research.

The next sections look at the research strategy and propose the single case study as the most appropriate strategy to achieve the research's ontological epistemological, methodological and axiological objectives.

5.7 RESEARCH STRATEGY: CASE STUDY

Yin (1994) defines a case study as an "*empirical inquiry that investigates a contemporary phenomenon within its real-life context, especially when the boundaries between phenomenon and context are not clearly evident*". "*Case study research involves in-depth study of a few people, an organization or an event"*. This definition directed the researcher's understanding of the need to use case studies when the intention was to cover contextual conditions (Yin 1994). Yin (1994) identified five components of research strategy that are important for the single case study considered in this research. They are listed as follows:

1) Research questions (***See Section 1.2)***
2) Propositions, if any (Not applicable for this single case)
3) Unit(s) of analysis (***See Section 1.2)***
4) The logic linking the data to the research question (***Section 5.1.1 and Section 6***)
5) The criteria for interpreting the findings (***See Chapter 7***) (Yin 1994).

A fundamental difference between case studies and any other alternative method is that the case study researcher may have less *a priori* knowledge of what the variables of interest will be and how they will be measured (Benbasat *et al.* 1987). In this particular instance, the researcher developed a *Sensitising Device* to act as a reference point into understanding *improvisation* in ISRM since knowledge about *improvisation* in ISRM was still insufficient at this stage. That is why this research should not be construed to imply that it is a purely **inductive** research **(**as discussed previously, **Section 5.5**).

5.7.1 General Myths: Debunking and Justifying Case Study Research

Some arguments suggest that case studies are subjective and this makes them only suitable for pilot studies. Some have also suggested that one cannot generalise from case study research. In other words, they would not be considered fully fledged research schemes. The conventional wisdom has been that case study research cannot be of value in and of themselves; they "need to be linked to hypotheses following a known hypothetical deductive model" (Flyvbjerg 2006). When such criticism is repeated often enough it may be taken as truth - *argumentum ad infinitum* (Flyvbjerg 2006).

This researcher agrees with Flyvbjerg's (2006) notion that this conventional wisdom about case study research is not valid since there are reasons why case study research should merit full fledged research recognition. Case studies are multi-perspective (Feagin *et al.* 1991), meaning that any research that adopts case study strategy considers not just the voice and perspective of the actors, but also of the relevant groups of actors and the interaction between them. The following are some of the myths discussed by Flyvbjerg (2006) and how these have been debunked. **Table 12** below explains these myths. What follows is a brief justification for the use of case studies for each myth.

Table 12. Case Study Research

Myths	Nature	Description
1	Knowledge comparison	General theoretical (context-independent) is more valuable than concrete practical (context-dependent) knowledge. **Flyvbjerg (2006)**
2	Generalisation	One cannot generalise on the basis of an individual case; The case study cannot contribute to scientific development. **Flyvbjerg (2006)**
3	Research Completeness	The case study is useful only in generating hypothesis (first stage of process) while other methods are more suitable for hypothesis testing and theory building. **Flyvbjerg (2006)**
4	Bias	The case study contains bias towards verification; tendency to confirm the researcher's preconceived notions. **Flyvbjerg (2006)**
5	Summarisation	It is difficult to summarise and develop a general proposition and theories on the basis of specific cases **Flyvbjerg (2006)**

Each of these issues above will be discussed in turn.

1. Knowledge Comparison

Myth: ***General theoretical (context-independent) is more valuable than concrete practical (context-dependent) knowledge.***

Stance

This research produced context-dependent knowledge about the phenomenon of *improvisation* in information security and risk management in one organisation. It is believed that this knowledge is of value to both industry and practice **(Flyvbjerg 206)**. Information security risk practitioners should be seen by all as experts in their everyday social, technical and intellectual skills while operating on the basis of intimated knowledge of numerous concrete cases in information security risk. It is such context-dependent knowledge that the researcher acknowledged as the method of understanding ISRM activities. It was the closeness of the case study to the real-life situation and its wealth of details that was important and added to these rich insights in two respects: the development of a nuanced view of reality and that this case was important in the researcher's own learning processes.

2. Generalisation

Myth: ***One cannot generalise on the basis of an individual case; the case study cannot contribute to scientific development.***

Stance

The researcher agrees with other researchers who have identified generalisations of case study research as being a challenge (Lee and Baskerville (2003). The challenge applies to whether the results from this research can be abstracted and applied to other settings. However, the researcher also agrees with Walsham (1995) who extended the notion of generalisations from interpretive case studies by arguing that generalisations can be viewed as "*tendencies*" and are best "*seen as explanations of a particular phenomena derived from empirical interpretive research in specific IS settings which may be valuable in the future in other organisations and contexts*". Walsham (1995) also outlines four types of generalisation from interpretive case studies that this researcher considered significant. The researcher saw this work as generalisable in the following manner:

a) **Development of concepts** (Walsham 1995; Lee and Baskerville (2003). (concepts generated in this research to theory can be generalised **Chapter 6**).
b) **Drawing specific implications** (Walsham 1995) (specific implications in this research can be generalised **Chapter 8**).
c) **Developing rich insights (**Walsham 1995) (insights produced by this research can be generalised **Chapter 6,7, and 8**).

d) **Generating theory** (Walsham 1995) (the framework in use in this research can be generalised **Chapter 7 and 8**).

It should also be observed that Lee and Baskerville (2003) have provided a framework for classifying the concept of generalisability particularly for research that falls outside of the bounds of sampling-based (statistical) research. According to Lee and Baskerville (2003), generalisation in qualitative research should not be "*proven statements*" but rather to be taken as "*untested yet well-founded statements*". Yin's (1994) view on generalisability is that statistical generalisability is an inappropriate measure of quality of case studies because case studies involve a different form of inference. This researcher concurs and adapts the above listed points in terms of generalising this work.

3. Research Completeness

Myth: ***The case study is useful only in generating hypothesis, (first stage of process) while other methods are more suitable for hypothesis testing and theory building.***

Stance

According to Lee and Baskerville (2003), this myth is invalidated by the fact that many researchers have built theories from case study research. Lee and Baskerville (2003) make mention of Eisenhardt's (1989) work which describes how to build theories in case study research. This is demonstrated when Eisenhardt (1989) explicitly subscribes to Yin's case study method and to Glaser and Strauss' (1967) grounded theory in providing ground for theory building in case studies and warranting full recognition. This researcher concurs with these arguments.

4. Bias

Myth: ***The case study contains bias towards verification; tendency to confirm the researcher's preconceived notions***.

Stance

Although it can be stated that case studies contain a bias towards verification and is understood as a tendency to confirm the researcher's preconceived notions, this researcher explains bias as follows: bias was not to be seen as an inherent characteristic of case study research but as a fundamental human characteristic. This is a problem all researchers including this one have had

to deal with. Although the allegation would be that this research allowed more room to be subjective and arbitrary, this research presented its own rigour particularly in data analysis which minimised bias and subjectivity. The strength of this research was that the researcher focused on real-life situations of ISRM practises and tested against these views directly to *improvisational* theory as these activities unfolded in practise.

5. Summarisation

Myth: ***It is difficult to summarise and develop general propositions and theories on the basis of specific cases***

Stance

Though this research yielded thick descriptive data, it was not the intension of the researcher to summarise greatly, nor was this desirable. This was because "it is simply that the very value of the case study, the contextual and interpenetrating nature of forces, is lost when one tries to sum up in large and mutually exclusive concepts". (Peattie 2001). The dense case study is, according to Peattie (2001), more useful for the practitioner and more interesting for the social theory than either factual "findings" or the high level generalisations of theory.

5.7.2 Single and Multiple Case Study Research

Case study research can be a **single case** or a **multiple case study** (Eisenhardt 1989; Yin 2003). An organization can provide a single or a multiple case study appropriate for building an understanding of how practitioners undertake tasks for theorizing based on this understanding (Eisenhardt 1989; Yin 2003). There can also be more than one organization that will provide for multiple cases (Yin 2003).

Stance

The research **adopted a single case** with multiple embedded units of analysis to investigate the phenomenon of *improvisation* in ISRM. The use of embedded or multiple **units of analysis (6),** was necessary for cross comparison and analysis (Eisenhardt 1989; Yin 2003) (See **Chapter 6 and 7**). The single case study research is accepted as a valid research strategy within the IS research community (Klein and Meyers 1999).

5.8 THE SELECTION OF A SINGLE CASE STUDY IN CONTEXT

The researcher identified and selected a single case on the assertion that this case was ***uniquely positioned*** to generate a full variety of evidence including documents, artefacts, interviews and observations. In general, the single case was considered suitable due to a series of key characteristics identified for this particular research. These key characteristics have been summarized and shown in **Table 13** below.

Table 13. Reasons for Selecting the Single Case (Adopted from Benbasat *et al.* 1987)

Key Reason	Covered in this research
*Phenomenon (of improvisation) could be examined in its natural setting in this case (***Benbasat *et al.* 1987)**	Improvisation and ISRM: Chapter 4
*It was possible to collect data by multiple means in this case setting (***Benbasat *et al.* 1987)**	Data Collection: Chapter 5
It was possible to examine one or few entities (person or group) in this case (**Benbasat *et al.* 1987)**	Single Case Study: Chapter 5
*It was possible to study intensively the complexity of the units of analysis singled out in this case (***Benbasat *et al.* 1987)**	Units of Analysis: Chapter 1,5,6
This case study was suitable for the exploration and classification **(Benbasat *et al.* 1987)**	Approach to Research: Chapter 5
No experimental controls or manipulation would be involved in this case (**Benbasat *et al.* 1987)**	Approach to Theory: Chapter 5
The results derived in this case would depend heavily on the integrative powers of the researcher(**Benbasat *et al.* 1987)**	Data Analysis and Interpretation : Chapter 6 and 7
It remained possible to change site selection and data collection methods if the researcher developed new insights about the case (**Benbasat *et al.* 1987)**	Methodology : Chapter 5
It was possible to study the "why" and "how" questions in the case because these deal with operational links to be traced over time **(Benbasat *et al.* 1987)**	Questions: Chapter 1,5
The focus is the case was of a contemporary event. **Benbasat *et al.* (1987)**	Objective: Chapter 1,2,5

5.8.1 Reason for Selecting the Single Case

Site Selection

The researcher began the site selection process by considering the nature of *improvisation* and ISRM. There was an initial recognition that both ISRM and *improvisation* were organization-level phenomena, hence the need to select a suitable organisation that would richly express such phenomena. The characteristics of large multinationals were then examined to determine best fit and most likely case. The factors used (Benbasat *et al.* 1987) to determine these included:

a) Organisational size
b) Organisational structure
c) Public or private ownership (due to accessibility)
d) Geographical proximity (due to resource limitation)

In identifying a suitable single case, the researcher located a "***most likely***" case that could be large enough to confirm the phenomenon of *improvisation* in ISRM and would fit the above listed criteria. The researcher focused on local multinationals and singled out 5 large multinational companies. Also included in this list was a large government organization. The researcher finally settled down on one organisation which has the following characteristics.

Organisational size

The organisation is a large retailer which sells a selected range of food products, clothing and house wares in 230 stores in South Africa. The organisation also has franchised outlets throughout Africa as well as the Middle East. The organization has demonstrated high levels of business performance as shown by a preliminary review of its key performance indicators (KPIs). The organisation employs approximately 14,000 employees and has an annual revenue of approximately $2.1 billion. In terms of its IT infrastructure, the organisation has in the immediate past rolled out a modern stock replenishment information system that manages approximately 1,100 styles of information. Recently this stock replenishment information system could no longer support the organisation's growth.

Organisational structure

The organization did not want this data (information) to be disclosed in any format, generic or otherwise. The Business Continuity manager suggested that the interviews and document analysis should suffice. Due to confidentiality, the researcher opted not to try and obtain more information about the structure of this organization than was necessary. The structure of this organization is not in the public domain. The upside of this was that the organization had put structures (units) in place that were identifiable ***making this case ideal and suitable.*** That was why the researcher was easily able to select the units of analysis in this organization. (For the structure of the units of analysis for this organization see **Section 5.9.2 –** structuring interviews.)

Public or Private ownership (due to accessibility)

The organization remains a holding limited company with local (South African) franchise stores and international franchise stores throughout Africa and Middle East.

Geographical proximity (due to resource limitation)

The host organization was selecting due to its size, structure, profit base and, most importantly, ***accessibility.*** The headquarters of this organization was close to where the researcher lived and studied.

5.8.2 ISRM in the Selected Single Case

It was established that the organization frequently conducts information security assessments and uses established frameworks for carrying out information security audits. The organization has a sound information security architecture, with its network systems, virtual private networks (VPN) and firewalls equipped with cutting edge technology. The organization pioneered a web based approach to internal and external transactions in its operations with real-time connection and integration to customers, manufactures, distributors and point of sale representatives.

The organization's Information Security department is responsible for co-coordinating secure distribution channels for its retail and financial services in real-time for its critical applications. Since the organization was and has been offering financial services, it placed importance in working within a strict regulatory environment. Customers using its systems are found to be extremely strict about and sensitive to the security of their personal information. The concerns

were particularly sound given the publicity of information security incidents present in the public domain.

The organization has been conducting ISRM activities such as business continuity assessments, disaster recovery exercises, information security policy and procedures review, and information security audits. The purpose of these exercises as explained to the researcher was to guarantee information security to all its partners, customers and stakeholders, while ensuring the highest degree of protection from hostile attacks.

The Information Security and Business Continuity Department was mandated to ensure that there was minimal interruption of critical production networks, applications and especially data. The primary objective of this department was to ensure applications were run in a secure and protected way from attack (external or internal). It was explained that this was to be accomplished through comprehensive information security auditing and assessments. Fundamental to these assessments was an ISRM approach contextual to the organisation which was designed to:

- probe and validate the organisation's information security state of applications through penetration testing and vulnerability assessments;
- review the on-going information security practices, policies, and processes.
- manage information security posture in the context of the information security industry best practices, baselined against industry standards. It was during the research that the organisation had just rolled out CobiT as an acceptable best practice approach to ISRM.

In terms of benchmarking itself with the industry best practices, the organization used CobiT (as previously mentioned), ISO IEC 17799, Open source security testing methodologies and the National Institute of Standards and Technology (NIST) Network Security Testing Guidelines. The benchmarking and comparative scoring for its applications was found to be on level-2 security, meaning consensus best practice was at a high level of due care where most of its critical applications connected to the internet..

From this preliminary background of the organization, the researcher was able to maximize the utility of information derived from this single case organization to successfully achieve the initial aims and objectives stipulated for this research. The next section explains how the units of analysis in the single case were examined and reviewed.

5.8.3 Defining Units of Analysis in the Single Case

The organisation followed set procedures as directed by the CobiT, ITIL, ISO IEC 17799 frameworks and methodologies. It was therefore easy to map out the units of analysis as activities defined by these frameworks, since these activities ***were already implemented*** in the organisation. There was also a clear structure of how these activities were to be implemented and performed (based on CobiT, ITIL, ISO IEC 17799). Each of these activities also ***had a leadership that was contactable.*** The research then simply defined the units of analysis as the ISRM activities defined earlier in literature. **See Section 2.4.**

The units of analysis identified in this organisation were those that would yield distinct themes as well as rich and context specific activities that characterised ISRM activities. It was feasible to compartmentalise these ISRM activities into themes guided by functionalist frameworks such as CobiT, ISO IEC 17799, and ITIL. The researcher identified the core sets of activities, rich in distinct themes from an initial framework, the *Sensitising Device* (***See Section 4.5.2)*** developed earlier on. These distinct ISRM activities (themes) were notably evident, based on preliminary interviews held with a senior practitioner from the organisation.

The units of analysis (previously ISRM activities) as deductively understood from the *Sensitising Device* contained a summary of ISRM techniques used by information security risk practitioners in those specific themes. The units when viewed and considered in aggregate constituted the holistic corporate information security risk management practises of the single case study. The ISRM activities and hence the units of analysis are summarised in **Table 14** below.

Table 14. Units of Analysis

No.	Units of Analysis	ISO IEC 17799	ITIL	CobiT
1	Information Assets Access and Data Control *(Section 2.4 of this thesis)*	***Section 3 of ISO 17799***	**Application Management, Control Methods and Techniques** 7.2 Understanding the applications relationship to IT services	**DS 11** Manage Data
2	Information Security Architecture *(Section 2.4 of this thesis)*	***Section 4 of ISO 17799***	**ICT Infrastructure Management, Technical support** 5.4	**PO 2** Define the Information Architecture

3	Information Security Policies *(Section 2.4 of this thesis)*	***Section 5 of ISO 17799***	**Security Management;** *Fundamental of Information Security;* 4.1 Control	**DS 5** Ensure Systems Security
4	Information Security Event Monitoring *(Section 2.4 of this thesis)*	***Section 9 of ISO 17799***	**Service Level Management***;* 4.4.7 Establish monitoring capabilities	**DS 10** Manage Problems and Incidents
5	IT Governance and Regulatory Compliance *(Section 2.4 of this thesis)*	***Section 12 of ISO 17799***	**The Technical Support** 5.4 The technical support process	**PO 8** Ensure Compliance with External Requirements
6	Disaster Recovery and Business Continuity *(Section 2.4 of this thesis)*	***Section 12 of ISO 17799***	**Availability Management** 8.3 The availability management process	**DS 4** Ensure Continuous Service **DS 10** Manage Problems and Incidents

The units of analysis (functionalist ISRM activities) were seen as appropriate for generating the required information. The *Sensitizing Device* discussed in ***Section 4.5.2*** therefore served as a lens for initially deductively understanding which areas the researcher would investigate and which information security risk practitioners the researcher would interview.

5.9 DATA COLLECTION IN THE SINGLE CASE STUDY

Initiating rapport, engaging with the selected organization and finally gathering primary data on information security proved challenging. This was not considered a unique experience nor did this experience discourage the researcher. Kotulic and Clark (2004) conducted a study and found a number of reasons for this. An important reason that stands out is that ***in matters of information security, organizations are reluctant to share information about information security policies with individuals from outside the company***. In fact, according to Kotulic and Clark (2004), "***Information security research is one of the most intrusive types of organization research"*** …and "***there is undoubtedly a general mistrust of any 'outsider' attempting to gain data about the actions of the information security practitioner community***." The next section describes how the researcher overcame some of these challenges.

5.9.1 Data Collection Procedures

Negotiating Entry

Before data collection could begin, the senior information security officer (Information Security and Business Continuity Department) was contacted for a meeting. This was done via a series of telephone calls and email. The preliminary purpose was to set an appointment and discuss the research. The researcher began by spelling out clearly in a letter sent via email what the intentions and objectives of the researcher were. The researcher was not explicit on the topic concerning *improvisation*, though. This was important so as not to arouse mistrust or misgivings about whether the researcher was in fact in the right place. Once a meeting was scheduled, the researcher then proceeded to have a direct face-to-face conversation with the information security practitioner. The information security practitioner's seniority and tenure made it possible to easily arrange meetings with other section heads. This would benefit the theoretical sampling approach used later on when conducting and obtaining primary data from other practitioners (see ***Appendix 10***).

For purposes of structuring the interview processes, it was important that units of analysis be identified from the onset. Once this was done, it would be easy to explain the purposes and objectives within each distinct unit being researched and the source of primary data (see ***Appendix 1***). It would also enable the appropriate sets of questions to be placed for each unit so as to yield rich distinct themes for each unit. It was important to establish the units and themes early on since this approach would help establish a balance of structure that would enable the selected organisation to make certain distinct resources available as early as possible. There was a situation where representatives represented more than one unit of analysis as their duties tended to overlap. This however was noted early on and interviews were structured to accommodate more than one unit of analysis.

At times planning, arranging and finally obtaining the required level of participation proved very difficult as most of the information security practitioners were very busy people who were generally committed to their work and had very little time. This did not discourage the researcher although it was evident that this would affect the research outcome in general. The units of analysis as identified from the onset (see ***section 4.5.2***) formed the deductive focus areas of information security risk concerns particularly with regard to the use of technology and, more

specifically, to the knowledge hot spots for information security and controls. Anecdotal evidence suggested that these units of analysis (themes) had been the focus areas by management on ISRM to meet baseline standards required by the board.

Data Collection in the Units

The primary data collection methods used included in-depth interviews, review of documentation (and artefacts) and observation. The richness of the choice of this methodology was vindicated by the richness of data obtained. The following techniques are explained in detail:

1) In-depth interviews
    a. High level questionnaire (sent first to determine interview questions ***Appendix 8***)
2) Review of artefacts and documentation
3) Observation

5.9.2 In-depth Interviews

Before the interview process could begin, the researcher designed and sent a high level questionnaire (***Appendix 8***) to only one person. The purpose was to elicit information that would enable the structuring of the interview schedule in ***Appendix 1.***

The interview guide as reflected in ***Appendix 1***. was developed as follows;

1. The researcher divided the main ISRM activities suggested by literature review into units. The researcher indentified 6 units in all.
2. The researcher then looked at the open questionnaire sent to one information security practitioner for the host organization and looked at how some of the questioners were answered. This gave an over view of how the guide was to be developed.
3. The researcher then looked at **ISO/IEC 17799** which is explicitly about control issues with respect to the above units.
4. Control issues from **ISO/IEC 17799** were re-worded to serves as impetus for the interview guide.

The primary data was gathered in two phases. The first phase consisted of a series of 11 in-depth interviews. The in-depth interviews were open-ended and discovery oriented. The interviewees

were senior information security practitioners including one who sat on the board. The list was drawn up from contacts provided by the senior information security practitioner (Information Security and Business Continuity Department) earlier on. The researcher constantly liaised with the senior practitioner in order to plan subsequent meetings with other heads. The sampling strategy used was theoretical sampling where participants were selected to maximize the opportunities for augmenting the pool of relevant data. During the actual interviews, a tape recorder was used to collect primary data. Permission to use the recorder was sought before any interview commenced.

The interviewees were encouraged to talk in an atmosphere of mutual trust and confidence and were encouraged to reflect on any aspect of *improvisation* they had themselves encountered or initiated as potential contribution to change in risk mitigation or enhancing information security posture of the host organisation. **The interviewees were requested to focus on the strong potential for *improvisation*, originality, creativity** and of fostering new ways of doing things outside of their normal structures. The whole process was easygoing since the researcher expressed himself in such a manner as to show interest in what was being talked about. However, there were times that the whole discussion had to be re-directed back to the main topic if the interviewee turned to "other interesting topics". The researcher realised that the best way to re-direct the discussion was to ask a direct question which would "scaffold" the thinking and discussion process, and that the researcher still maintained control of the process. The objective of the interview process was to understand the different sets of practitioner activities and relationships that create a different form of risk management process.

All interviews were tape recorded. After each interview, the information was transcribed verbatim in writing. In addition, notes were taken as the interviews progressed. It is from the transcribed responses from the interviewees that the research formed the contextual case for the phenomenon of *improvisation* being investigated. The interviews were conducted for 60 to 90 minutes per session. This generated close to 700 transcript minutes for data analysis. Phase two consisted of 3 additional interviews that enabled the researcher to explore some of the mentioned issues in phase one in more detail. These interviews also lasted up to 60 minutes. The interviews were based on open-*ended questions* and the researcher gave the respondents room for open answers. The interviewees were, as a matter of encouragement, given room for reflexivity in answering questions. The discourse of the interview was perceived by the researcher to be "an act of knowledge making its own rules"; the researcher saw the interviewees as "social actors"

who were interacting with the interviewer while at the same time being involved in discursive practise. The profile of respondents interviewed and the positions they occupy are given in **Table 15** below.

Table 15. Profile of Respondents within the Units of Analysis

CORE ISRM ACTIVITIES ISO 17799 Sections/ CobiT/ ITIL			Covered in Research	Activities analysed and labelled as units in this research	Interviewee and Position
	Section	**Type of Activity**			
IDENTIFY					
	3	Security policy	Yes	**Information Security Policy**	**Group Information Security Officer**
	4	Security organisation	Yes	**IT Governance and Regulatory Compliance**	**IT Executive** **IT Security team**
	5	Information Asset Classification and Control	Yes	**Information Assets and Control**	**IT Executive** **IT Security team**
ANALYSE					
	6	Personnel Security	*No research on this section*		
	7	Physical and Environmental Security	Yes	**Security of Information Architecture**	**Head of Architecture Forum** **Enterprise Middle ware Team** **IT Executive** **Business Continuity Manager**
	8	Communications and Operations Management	*No research on this section*		
RESPOND/CONTROL	**9**	Access Control	Yes	**Event Monitoring**	**Manager of Microsoft Platform, Operations** **Group Enterprise Architect**
	10	System Development and Maintenance	*No research on this section*		
	11	Business Continuity and Management	Yes	**Disaster Recovery/ Continuity**	**Business Continuity Manager**

Initiating Rapport during the Interview

Rapport was a necessary part of the in-depth interview process since, by initiating this strategy, it was easy to notice a shift into informal discussions and social communication and back again into more formal aspects. Rapport enabled the researcher to get acquainted with the information security practitioners early on and "break-the-ice". Although they maintained their distance (which was picked up easily by the researcher--they seem to hold and hoard critical information they valued), the researcher developed an understanding about each of the interviewees.

Meaning Co-construction during the In-depth Interview

The researcher perceived the interviewees as co-constructors of meaning even though at times the interviewees did not necessarily indicate their knowledge of this. The researcher would often interject with words like '*hmmm*" or expressions indicating that the interviewee continue the narration after a pause. Sometimes subtle encouragement was necessary especially when the interviewee was not sure if what they were saying was relevant.

Managing Interview Relationships

The researcher conscientiously wanted an environment which would encourage free and natural conversation. The researcher had the privilege of controlling the direction and flow of discussion. The good thing about this was that at an earlier stage through emails and various correspondences, the researcher alerted the interviewee of the interview process. This sort of introduction gave impetus for such control especially when seen in the light of what took place in the actual discussions.

5.9.3 Review of Artefacts and Documentation

In order for the researcher to have a preliminary understanding of the selected case for study, a reasonable time was spent reviewing documents that gave information about the host organisation. The key approach to document analysis was **content analysis.** In this approach, the researcher looked at what was being done in the organisation and what was emerging in these documents. In using **content analysis,** the researcher focused on the actual content of the documents so as to determine the presence of certain words, concepts and phrases. This was done in order to quantify these concepts or phrases in an objective manner.

The researcher was not analysing whole documents but looking at chunks of data in these documents, i.e. looking at lines and phrases at a time. Only those phrases that were relevant to

the units being analysed were coded. A detailed discussion of the document review and the analysis process is listed in **Chapter 7** STEP 3.

5.9.4 Observation

Observation of ISRM activities was very limited. The researcher ensured observations were conducted in the context of the experiences of the information security risk practitioners. Observations were intended to capture the world of the information security practitioners without prescribing a structure in which the information security practitioners must reflect in this world in her data-yielding actions; thus they were free and open. The organisation organised disaster recovery exercises in two locations. The researcher was invited to participate in the one that was 18 km from the organisation's headquarters. The researcher observed the activities that were carried out in the disaster recovery exercise. In the disaster recovery exercise, the researcher did not become part of "the furniture" but went to the scene to explore issues that would reveal more about the phenomenon of *improvisation*. The researcher had in mind a way that he would collect data; an observation protocol/ schedule was designed prior to going to the site and the researcher filled in the schedule what was observed. **Table 16** below is a template for the on site observation. The full recording of the observation is detailed in ***Section 7.7 Table 39 and Appendix 3.***

Table 16. Template for Observation: Disaster Management Exercise

<table>
<tr><td></td><td colspan="2">Location : Name and Description of Location</td></tr>
<tr><td></td><td colspan="2">Access to this site is restricted and everyone is issued a temporary access ID.</td></tr>
<tr><td rowspan="2">Start Time:
9: 00 am</td><td>Description of Activity</td><td rowspan="2">Observation Notes</td></tr>
<tr><td>Description of Activity</td></tr>
<tr><td rowspan="3">End Time:

9:30 am</td><td>Description of Activity</td><td rowspan="3">Observation Notes</td></tr>
<tr><td>Description of Activity</td></tr>
<tr><td>Description of Activity</td></tr>
<tr><td colspan="3">CONCLUSION
Key notes</td></tr>
<tr><td colspan="3">DISCUSSION</td></tr>
</table>

The researcher also developed some field notes which complemented observation with data that shed light of the various parts of the inquiry. The advantage of this process was that the whole exercise was able to assist the researcher mentally organise and fit in specific pieces of information that would not have been obvious through interview only.

5.10 USING SELECTED GROUNDED THEORY TECHNIQUES AS A METHOD OF DATA ANALYSIS

5.10.1 The Grounded Theory Method

Grounded Theory Method (GTM) is a "*systematic qualitative research methodology in the social sciences emphasizing generation of theory from data in the process of conducting research*". (Allan 2003). GTM works in a reverse approach from traditional research and at first may appear to be in contradiction of the scientific method (Allan 2003).

GTM works by firstly collecting data through a variety of methods then marking the data with a series of codes which are extracted from text. The codes are grouped into similar concepts in order to make them more workable. From these concepts, categories are formed, which are the basis for the creation of a theory. This contradicts the traditional model of research, where the researcher chooses a theoretical framework, and only then applies this model to the studied phenomenon (Allan 2003).

In this research, the Grounded Theory Method (GTM), (Glaser and Strauss 1967; Glaser 1978; Strauss 1987; Strauss and Corbin 1990; Glaser 1992) has been used as a form of **content analysis** to find and conceptualise underlying issues amongst a myriad of confusing data. Glaser (1992) established this technique as a qualitative way of inductively deriving theory. This technique was proved attractive due to its systematic procedures for inductive reasoning and conceptualisation particularly at case study level. As established earlier, many cases are contextual and therefore would need a deeper understanding (Orlikowski 1993).

Grounded Theory Method has been noted as a useful interpretive method for theory generation (Bryant 2002; Strauss and Corbin 1998). The researcher's choice of this method was to generate a descriptive and exploratory theory of *improvisation* in information security risk management, rooted in the experiences of specific information security practitioners. Grounded theory has

been used successfully in both organizational and information systems research in the past (Orlikowski 1993; Trauth and Jessup 2000; Urquhart 1997).

The basic elements of Grounded Theory Method include generating concepts and categories, the concepts being the most basic units of analysis. Since the whole purpose of the research was inherently conceptualisation, it was important for the researcher to derive concepts from primary data. The development of concepts stemming from the inductive nature of grounded theory techniques encourages researchers to steer thinking *out* of the confines of literature (deductions) and avoid standard ways of thinking about the data (Strauss and Corbin 1990).

"All is Data" ***Glaser (2001)***

One essential dictum raised by Glaser (2001) which is a pillar on which the units of analysis in ***section 5.7.2*** stand is the idea that '*all is data'*. The researcher noted that the collection of data was primarily for conceptualisation of what was meant to be in the researcher's eyes, that is, theory. The theory emerging from the data would then be compared with the *Sensitising Device* formulated earlier (***Section 4.5.2)***.

Glaser (1992) proposes a way in which concepts and categories should be seen to emerge naturally. While it may seem that Glaser (1992) has validity in this proposition, the history of how this data has been treated by researchers; Strauss (1987), Strauss and Corbin (1990), does point out that many have used this method as a 'rule of the thumb' rather than static rules. As a note to this work, the researcher has been flexible in modifying the approach in a way that lets the data 'speak for itself', and in a sense establish the concepts as actual derivatives of the qualitative data being analyzed. *This method was suitable for the inductive element of research.*

5.10.2 Using Open Coding as a Grounded Theory Technique

A number of ways were considered in analysing primary data. The researcher finally settled on the use of open coding, grounded theory techniques. The choice of the technique gave the researcher comfort in the possible richness and insights the data streams would yield. The value of these techniques was considered for two primary reasons: (i) The approach would draw on deeper features of case study research which would be undiluted from preconceived ideas of other researchers, through searching for new concepts and ideas (Glaser and Strauss 1967); (ii) New concepts would emerge that would aggregate into categories that would be used to establish

theory. Strauss (1987) talked of open coding forcing the researcher to break apart and fracture the data analytically.

5.10.3 Applying Open Coding

This was what was done initially and is explained in detail in **Chapter 6.** This process is described in **Table 17** below. **Table 17** shows the structured way followed by the researcher in the data analysis phase.

Table 17. Process of Data Analysis using Grounded Theory, Open Coding

RESEARCH PROCESS			
Process 1	Analyse data relating to **unit s of analysis and to conceptualise improvisation**	Use open coding	Develop concepts and categories relating to improvisation in ISRM activities
Process 2	Theoretical Sampling	Literal and theoretical replication across cases (select interviewees for data until saturation)	Confirms, extends and sharpens theoretical framework by analysing the rest of the units of analysis
Process 3	Analyse data relating to **the subsequent other units of analysis to conceptualise improvisation**	Use open coding	Develop concepts and categories relating to improvisation in ISRM activities
Process 4	Reaching closure	Theoretical saturation when possible	Ends process when marginal improvement becomes small

Table 17 shows that the first process was to determine codes using open coding as grounded theory technique of analyzing data. The coding was done until theoretical saturation. In a sense the whole process was to start inductively. Sense making became integral to the coding process, in such a way that the sense making process (contextualising data) blended inductive and deductive thinking in ways that produced meaning and relevance. The researcher spent less time worrying about the 'correctness' of data Glaser (2001) and more on the relevance of what was being coded. This meant placing greater emphasis on concept generation that would be more fitting to the phenomenon of *improvisation* in ISRM activities. This whole process was iterative and is depicted in the **Figure 9.**

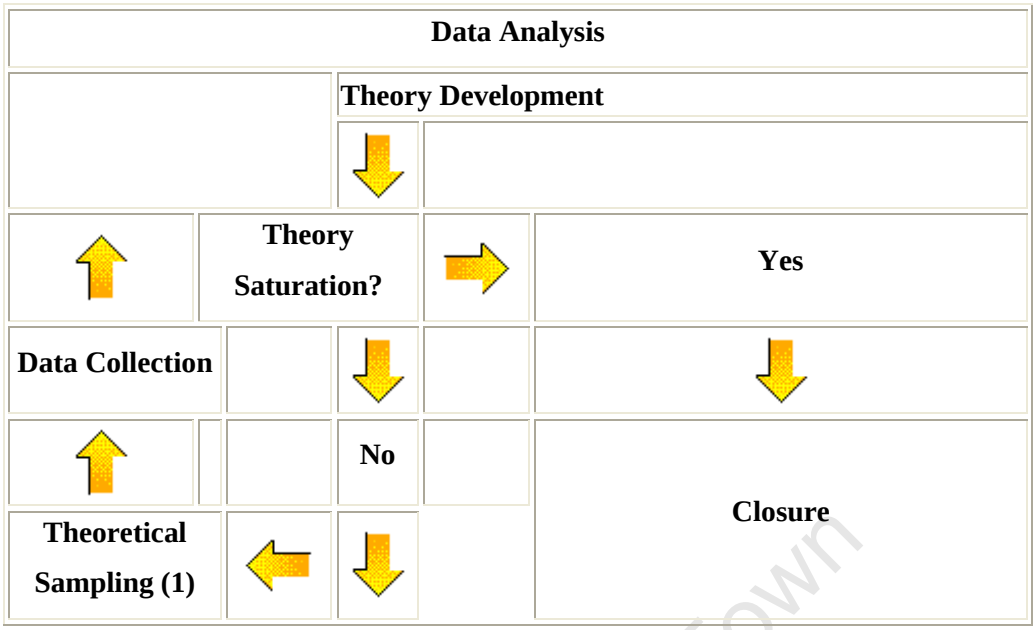


Figure 9. The Interrelated Processes of Data Analysis, to Building Theory (Pandit 1996)

This coding process went on until the researcher was sure about the categories emerging i.e. saturation. This approach is not without criticism as was acknowledged in earlier studies. Glaser (1992) has been critical of this method. He notes his concern with the approach which leads to '**forced conceptualisation'** of qualitative data (exemplified in Strauss 1987; Strauss and Corbin 1990). The framework in **Figure 9** guided data analysis for each unit of analysis and involved generating concepts through the process of *open coding* and breaking down data, conceptualising this data and putting it back into new ways.

5.10.4 Iterative Theorising and Constant Comparison

Data should be analyzed and inferences drawn from the empirical data itself and not inferences, prejudices or association of ideas directly from the researcher (Glaser 1992; Strauss and Corbin 1998). Though this proved difficult, the researcher was guided by the constant comparison between emergent theory (codes and categories derived) and the new data. The constant comparison helped the researcher confirm the data and hence theoretical constructs up to a level of theoretical saturation, which would mean that new data would add significantly to what was already known. Through constant comparative analysis, the researcher took time searching for relationships between the concepts derived, and the phenomenon of *improvisation* in ISRM. The researcher adopted a middle order approach (Dey 1993) where some broad distinctions were

initially drawn based on common sense categories. Analysis proceeded towards sub-categorization and the comparison between the middle order categories. In order not to lose focus and also to maintain relevance, constant comparative analysis was applied not only from a code-to-code, theme-to-theme and concept-to-concept but also by looking holistically at what the literature said. So, in a way, the comparison was done holistically and iteratively. This approach is critical to any interpretive research applying grounded theory techniques to analyze and interpret data (Schön 1983). This means the whole process reflected an inductive-deductive research cycle that is required in the learning process. The iteratively theorized approach used to conceptualize *improvisation* through constant comparison not just for sections but for chapters is shown in **Figure 10** next page.

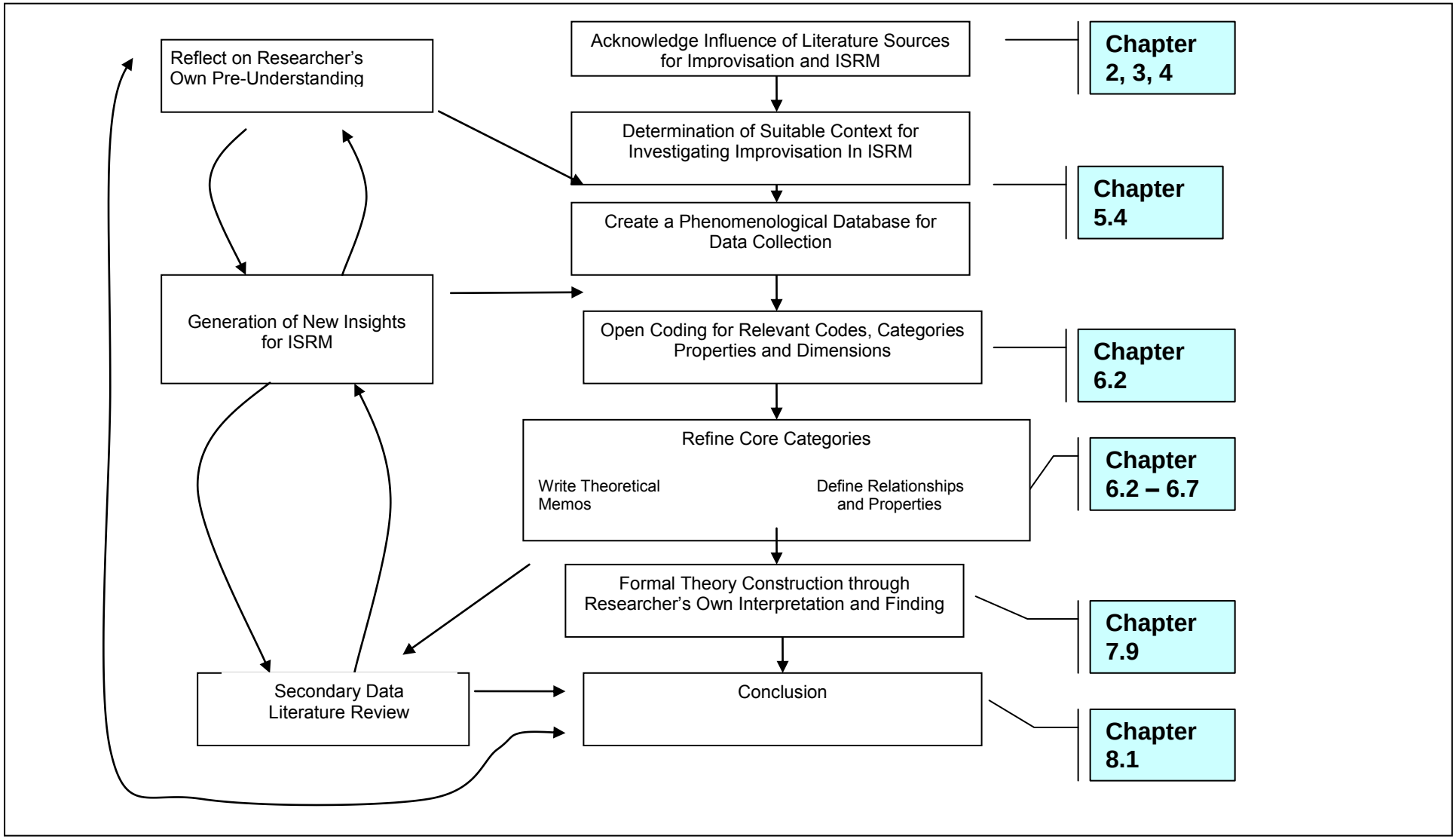


Figure 10. Iterative Theorising and Constant Comparison.

5.10.5 Researcher's Role and Ethical Consideration

The research for all purposes abided by and followed on the proposals from the ethics committee which has developed quality control criteria and procedures based on traditional forms of qualitative research. Based on these procedures, this research emphasises **consent** and **confidentiality**. It is for this reason that the researcher made explicit to the selected host organisation that there would be a mutual understanding that the research contents would be confidential while safeguarding the interests of the participants of research. The other ethical consideration for this research was the intended value to the research participants.

With the aim of providing value, the researcher strove to find meaning in the phenomenon of *improvisation* in ISRM by attempting to see the bigger picture. "Raw" empirical information was turned into qualitative descriptions in order to give a meaningful description of *improvisation* as it was contextually applied. The researcher made attempts to present "**thick descriptions**" by providing ample empirical evidence from various data sources and by using a systematised approach.

From an ethical perspective, the researcher was the main instrument of the research and made meaning of data from the engagement with the information security risk practitioners. Meaning was also derived from what was consequently interpreted of the data. This approach was consistent with other studies (Henning 2002; Henning 2004). Every attempt was made to ensure that the meaning assigned to data and the interpretations thereof were linked and drawn from the data collected and from the theory that explicated the phenomenon of *improvisation* in ISRM (*Sensitising Device*). The understanding that the knowledge and skills base of participants would grow in line with the stated objectives provided the ethical value of this research to the selected host organisation.

5.11 CHAPTER SUMMARY AND CONCLUSION

The methodology chapter adds value to this research by explaining the research philosophy and approach to research. This chapter revisits the research problem and focuses on shaping the problem into questions for which appropriate methods of inquiry were used. Insight is also added in this chapter regarding the methods, and nature of data collection, and finally how the data are analyzed. By introducing the use of grounded theory techniques to analyze

data, this chapter has demonstrated in detail how this is achieved in as far as helping to meet the underlying research objectives stipulated in the first chapter of this thesis. The chapter deliberates the research strategy, debates and justifies the use of grounded theory techniques applied in the data analysis section. The research methodology and research methods of inquiry introduced in this chapter exemplify:

1) better understanding of raw data,
2) rich data that provides for reflexivity in interpretation.

The next chapter is a detailed discussion of the procedure of data analysis as applied using grounded theory techniques. This chapter analyses data from distinct units and themes.

CHAPTER SIX

This chapter attempts to increase the natural knowledge of what is already know in ISRM and *improvisation* by grounding this understanding with contemporary present day data, specifically focusing on primary data analysis. The chapter takes us through the steps of analyzing and interpreting this contemporary data. This permits an interpretation of the practitioner's own understanding of *improvisation* in ISRM into new ways that largely harmonizes with what is already known. The chapter sectionalizes the analysis into units of various themes and draws out new knowledge.

Table of Content
Chapter Six

CHAPTER SIX: DATA ANALYSIS – OPEN CODING

6.0 INTRODUCTION

Formal data analysis as explained in this chapter started as soon as data was collected. What followed was the coding of data. The coding happened iteratively with analysis. This chapter gives a detailed discussion of how the collected data was coded and analyzed and is a step closer towards a full conceptualization of *improvisation* in ISRM activities. The purpose of this chapter is to make it possible to develop a deeper understanding and meaning of *improvisation* as analyzed from the various units of analysis. The data analysis chapter demonstrates scientific rigor as shown by the approach and techniques used in data analysis. This chapter helps establish understanding of raw data using tested and sound data analysis techniques.

The chapter is divided into four sections. The first section explains how open coding as a grounded theory technique was used to analyse data. This section explains the steps that were carried out in open coding. The second section describes how open coding was applied to all ISRM units of analysis. The third section is a collective summary of findings while the fourth section concludes the chapter.

6.1 EXAMINATION OF UNITS OF ANALYSIS BY APPLYING OPEN CODING TECHNIQUES

While adhering to the grounded theory techniques for analysing the data, (Strauss and Corbin 1998), the essential guide posts for the **data-sets** examined in this chapter are illustrated by the steps listed in **Table 18.** What follows is a detailed explanation for each step.

Table 18. Open Coding of Improvisational Date Incidents

STEP 1 **Data Incidents (Transcribed Interviews)**	**STEP 2** **Context of Data Incident**	**STEP 3** **Researcher's memos** Determine Codes in vivo and other generated as underlined)	**STEP 4** **Level**	**STEP 5** **Concepts generated**	**STEP 6** **Categories** (See Section 4.4.1)
Step 1 Data	***Step 2 Data***	***Step 3 Data***	***Step 4 Data***	***Step 5 Data***	***Step 6 Data***
(For a full list of steps and work done, see Appendix 2 – 7).					

6.1.1 STEP 1: Extracting Data Incident

As soon as the researcher had finished the interview process and transcribed the recordings, the researcher started "engaging the data". The researcher started by looking for elements of *improvisation.* Data was fractured or "compartmentalised" into cells (to be referred to as **data-sets**) for analysis and traces of *improvisation*. The compartmentalisation process involved breaking down data. The process of breaking down and analysing the data and assigning labels is described as **content analysis** by researchers (Glaser and Strauss 1967). These **data-sets** are listed in ***Appendix 10***. A documented shortcoming to this approach was that major themes would be "lost" in contextual detail or lead to "**over-conceptualisation'** (Glaser 1992). In order to overcome this suggested shortcoming, the researcher tried as much as possible to retain the original meaning inherent in the **data-sets. Data-sets** were compared with other **data-sets** (constant comparative analysis) so that the meaning of what was said would not be lost. The other reason for the compartmentalisation was to enable triangulation of data and finally classification of data into distinct themes relating to the identified ISRM units of analysis. That was the reason for ***Appendix 10.***

Traces of *improvisation* (elements of fusion between incrementalism and functionalism) were noted in researcher's memos. The units as defined by literature review (See **Section 5.8.3**, **Table 12**) were (6) six in total, meaning these **data-sets** would in the end be categorised into 6 parts with each part representing a distinct unit of analysis. This was not difficult since the persons being interviewed represented distinct units of analysis and so what was said would generally fit into the **data-set** for that particular unit. However there were times when a practitioner would mention activities relating to other units and this data was moved to its respective **data-set.** The final result of the 6 part categorisation was the generation of ***Appendix 2*** to ***Appendix 7.*** Data incidents that pertained to *improvisation* were then extracted from these high level **data-sets.**

6.1.2 STEP 2: Determining Context of Data Incident

It was easy to see that the compartmentalised data in the **data- sets** (***Appendix 10***) would not make sense by simply glancing at the data. Through **conversation analysis** (Denzin *et al.* 2003) the researcher provided the context for selected data in the **data-sets** for incidents that reasonably suggested *improvisational* elements. In order to give relevance and context for

data incidents, the researcher followed procedures suggested by Glaser (1978), when examining data and providing contexts. These procedures involve asking a series of questions relating to the data incidents in the **data-sets**. The following questions as suggested by Glaser (1978), were re-written to suit the research purpose and are listed as follows;

- What aspect of both incrementalism and functionalism does this data imply?
- What *improvisation*al concept does this explanation suggest/indicate?
- What is actually happening in the data incident?

Once these questions were addressed the researcher wrote memos relating to the context the data incidents happened. These memos are also shown in ***Appendix 2 to* Appendix 7**, STEP 2.

6.1.3 STEP 3: Deriving Open Codes from Researcher's Memos

The process of writing memos that would guide open coding (grounded theory technique) in STEP 3 involved several sub-steps. The first step was to examine *in-vivo* codes. Note: *In-vivo codes* are derived from the language and terminology used by participants (interviewees) in the study (Rodon and Pastor 2007). It is from this direct language that scientific constructs are derived. Strauss (1987) refers to *in-vivo* codes as being taken from or derived directly from the language used by the actors (participants or interviewees) themselves. *In-vivo* codes have 'analytic usefulness' as they are often used precisely by the participants, and they often have very vivid imagery (Strauss 1987). Once this preliminary examination concluded, the researcher then wrote additional memos. These memos proceeded from **data-sets** (STEP 2) that were searched for *improvisation* elements and can be illustrated as follows:

[Data set]

The data-set containing the data incident "*...so we quickly had to make [create] a few more categories...so"* had the following memo "attached" to the incident;

[Memo]

"Implies quick reaction in terms of profiling users and determining data security and classification levels based on information requirements" (See **Table 14).**

The researcher then underlined words from these memos that related to specific activities. These underlined words are the initial codes. The researcher also wrote memos about the nature of that activity by coding deductively from literature the nature of activity. For instance, the classification for the above data incident was given *"**Control and Classification of Information Assets".*** These classifications were useful in structuring the narratives that describe *improvisation* in **Section 6.2** onwards.

The researcher treated these memos as heuristic tools rather than as objective representations of facts. The researcher used these memos as flags/signposts to point to the phenomenon of *improvisation* in the data. Memos helped the researcher gain insights into the kind of data that was needed for further analysis, and the data that was required to be viewed from multiple angles. This facilitated useful discoveries.

6.1.4 STEP 4: Determining Level

The inductive aspect of analysing data was made possible by extracting and understanding data that reflected aptitude for a fusion of structure and creative thinking simultaneously at three organisational levels. Deductively, the ISRM activities from the **data-sets** were to be considered from three levels: **Strategic**, **Tactical** and **Operational**. **Data-sets** that seem to suggest that an *improvised* activity was carried out at operational level were coded as "operational". Three level codes i.e. *strategic*, *tactical* and *operational* were defined for each selected **data-set** identified and coded as an *improvisational* activity.

6.1.5 STEP 5: Creation of Codes and High Level Concepts Deductively and Inductively

Deriving codes (using both deductive and inductive approaches) was a lengthy and time consuming process. Although there were many codes that could have been derived and could have been relevant, for purposes of meeting the objectives of this research, the researcher restricted open coding to only those instances where there were answers to questions asked in STEP 2. Through a combination of deductive and inductive reasoning coding for *improvisation* was possible. STEP 5 was conducted as follows;

1) **Data-sets** were coded and examined in-depth. **Data-sets** found to fit the phenomenon of *improvisation* in ISRM were carefully selected and filtered out for in-depth

examination i.e. moved from ***Appendix 10*** and to the generation of ***Appendix 2*** (memo writing). Deductively identifying the codes was assisted by the use of the *Sensitising Device*. The researcher first developed lower level practitioner language codes or '*in-vivo coding'* iteratively from STEP 2 (mentioned previously).

2) Careful analysis was done and *in-vivo* codes from **data-sets** generated. These codes provided reasonable first level understanding as to how information security risk practitioners engaged in their daily activities. Finally the researcher developed finer and more detailed higher level (specific) codes of the **data-sets** that were derived from multiple readings iteratively.

3) To illustrate how **data-sets** were examined and coded for *improvisation*, the data-set containing the data incident "*…so we quickly had to make [create] a few more categories…so"* was coded for **Quick–reaction**. (Codes identified in this research are distinguished as being both **bold** and underlined.

   Note: ***The above open code demonstrates one (1) conceptual instance of improvisation within this data-set. Conceptual Density was determined to represent the total number of conceptual instances in a data-set relating to a distinct unit of analysis and is represented as a numeric figure at the end of Chapter 6 and 7.This is not to be confused with quantitative research methods.***

4) The comprehensiveness of the **data-sets** provided reasonable generality of *improvisation* in ISRM. (The generality was later to be used for theory development in **Chapter 7**).

Once the coding process was done, certain theoretical ideas began to emerge which appeared central to the study of *improvisation* in ISRM. The purpose of coding was to help the researcher conceptualise and make sense of each coded data element. The researcher also embarked on looking for patterns and relationships between the collected codes and also across other collections and **data-sets.** This would help in making insightful discoveries about *improvisation* in ISRM.

6.1.6 STEP 6: Generating Types of Improvisation

Section 4.4.1 identified the typology of *improvisation* as being either *Collective, Individual, Product* or *Process.* **Data-sets** were examined holistically to determine the type of *improvisation* occurring. This was coded as being one of the above.

It should be noted that the *improvisational* codes generated were neither inherently objectivist nor heuristic, meaning the terms coined only related to how the researcher chose to describe the conceptualisation and the use of the codes being generated. The researcher understood that the codes were representations of the phenomenon of *improvisation*, though there was no assurance that this kind of *improvisation* as conceptualised was the type mentioned in other instances.

The following sections are a unit by unit analysis of data and the generation of *in-vivo* codes, and categories. ***Although the following sections list the STEPS described above, these sections take the form of narratives for easy readability.***

6.2 UNIT BY UNITS DATA ANALYSIS

The following sections describe a unit by unit analysis following all the above steps.

6.2.1 Analysis - Information Assets Access and Data Control

Section 2.4.1 of this research dealt with issues regarding this unit of analysis. The following section conceptualizes *improvisation* within activities relating to information assets access and data control. Conceptualizing *improvisation* in this unit followed the 6 steps listed in the previous section. This is demonstrated by **Table 19** as follows;

Table 19 Open Coding for Information Assets and Data Control (***Extract of Appendix 2***)

STEP 1 **Data Incidents** **(Transcribed Interviews)**	**STEP 2** **Context of Data Incident** (Researcher's Memo)	**STEP 3** **Researcher's memos** Determine Codes in vivo and other generated as underlined)	**STEP 4** **Level**	**STEP 5** **Concepts generated (inductively)**	**STEP 6** **Types of Improvisation** (See Section 4.4.1)
"…so we quickly had to make [create] a few more categories…so it doesn't just get as simple as you just having internet access ..and you don't get this.. [but rather] you having internet access and you belong to marketing…and you belong to IT…" [1]	Profiling users based on user activities was found to be critical. However, it was the nature of the profiling as observed that was to be found interesting. Multiple users had multiple requirements. The creation of extra categories outside of the normal categories was improvised as it had never been done before. i.e. new ways of defining categories that allowed for innovative information access.	***Control and Classification of Information Assets*** 1. Implies quick reaction in terms of profiling users and determining data security and classification levels based on information requirements	**Operational** Activity	**Quick reaction** to data access security levels	(Process) Improvisation
"*…and we did and worked on exactly what they said.. and of course within the first few days.. of putting access controls in [the system]…we got hundreds and hundreds of calls…saying they couldn't get through.. they said that they wanted to go to selling sites.. whatever…and they couldn't go to see what was on hundreds of other sites…"* [2]	The IT team improvised (employed automatic thinking towards) new control frameworks that guided the abuse of internet by users and helped place appropriate security controls to users.	***Accountability of information assets through access control*** 1. Implies being resourceful and providing reflexivity by placing data security controls	**Operational** Activity	**Being resourceful** in placing data access security controls	(Process) Improvisation

[1] C120-Appendix 10
[2] C119-Appendix 10

The following were the data classification as described in STEP 3 (2nd paragraph) and are derivatives of interview transcripts for this unit of analysis (***see Appendix 2).*** These classifications are listed as follows:

1. Control and Classification of Information Assets
2. Accountability of Information Assets through Access Control
3. Authorization Process of Information Facilities
4. Data Warehouse Management and Information
5. Authorization Process for Program Source Library

Each of the above classification is explained in turn.

1. Control and Classification of Information Assets

The **ISO IEC 17799 Section 5** prescribes how information security practitioners should treat information assets. **Section 5.2** prescribes acceptable ways for information control and classification while **Section 5.1.1** identifies how practitioners should compile an inventory of all information assets depending on their value to the organisation. The **CobiT** objectives **Section DS5.9** gives a mechanism for centralised control and identification with proper procedures for access rights management. **ITIL Section 4.2** (*Security Management*) describes the best way to implement information security management measures. Asked how the organisation carried out activities relating to the control and classification of information assets, one information security practitioner responded this way:

> *"All requests for access are done via control application which is authorised by the relevant executive, with final authorization given by the IT Risk and Continuity manager."*[3]

It was during the interview process that the information security practitioners revealed that they actually followed procedures set by **ITIL**, **CobiT** and **ISO IEC 17799.** Some of these procedures determined control levels for sensitive information. In terms of controlling access to sensitive information, when questioned about whether there was

[3] Q25-Appendix 8

delegation of security responsibilities between asset owners, the same practitioner noted that this was indeed the case:

> *"Delegation, yes in terms of recommendation levels of access."*[4]

What this practitioner was saying was that they delegated responsibilities to designated persons to determine various access levels to sensitive information. There was no form of *improvisation* noted in terms of the delegation process.

Data incident

There were times when the practitioners would be forced to address information security control and access issues. In fact for one particular instance, it was noted that access to sensitive information was granted spontaneously:

> *"…so we quickly had to make [create] a few more categories…so it doesn't just get as simple as you just having internet access and you didn't get this..."* [5]

This act of spontaneity in determining access levels was a demonstration of the need to quickly address information access needs and called for **quick reaction**[IMPROV-1]. This was coded as such. It should be noted that at the heart of this *improvisation* was the ability for the practitioner to react quickly and ingeniously to overcome emergent constraints. The creation of these new categories to the end-users was interpreted as the constraint that was addressed by this quick thinking i.e. improvised. The nature of this reaction was collective since this involved more than one person. This act was interpreted to suit the occurrence of *collective improvisation*[IMPROV-1] and was seen to occur more at tactical level since these were tactical decisions that would affect access levels in the short to medium term.

2. Accountability of Information Assets and Access Control

Another ISRM activity examined was that of accounting for access control. The need to account for control meant the need to not only control the granting of access to

[4] Q 27- Appendix 8
[5] C120-Appendix 10

employees but to also account for whom and why certain persons were or were not being given access. The information security practitioners appreciated that there were different approaches to providing accountability and access to information assets as prescribed by **ISO IEC 17799 Section 5.2.1.** **Section 5.2.1** prescribes the manner in which the information assets classification system restricts access to information when deemed necessary. The **CobiT** objectives **Section DS5** provides a mechanism for data classification, with the key areas being data sensitivity and the disposition and sharing of data. **CobiT** objectives **Section DS5.3** suggests procedures for security of online access to data by providing measures for access security control. **ITIL Section 4.2.2** (*Security Management*) also gives guidelines on the implementation of security management measures, while **ITIL Section 4.2.4** suggests requirements for access control**.**

It was understood that the organisation was following the above recommendations (frameworks and standards) as explained by one respondent. When asked about how the organisation ensured accountability and confidentiality of information so that the information would not accidentally be passed on to any unauthorised person in or out of the organisation, it was explained that there were certain procedures in place:

> *"We do this by developing access hierarchies and permissions."*[6]

No form of *improvisation* was coded for the development of access hierarchies and permissions since the development ***was structured*** and determined by set procedures.

Data incident

An example of a data incident where practitioners acted on the spur-of-the-moment could be illustrated when practitioners skilfully remedied situations. They achieved this by providing pragmatic solution when faced with challenges. This is illustrated by the following data incident:

> *"…and we did and worked on exactly what they [Management] said, and of course within the first few days of putting access controls in [the system], we*

[6] Q38-Appendix 8

> *got hundreds and hundreds of calls saying they [end-users] couldn't get through…*[7]
>
> *"Roles [end users roles] were then specifically split into two areas, technical response and the process, procedures and people element"*[8]

The context for this data incident as explained by the respondent was that the practitioners were faced with a situation where they had granted end users incorrect profiles and access permission to systems. The granting of access was based on what the frameworks had made provisions for. What was not anticipated was that the end user profiles had changed, forcing the review of end user access rights. This turned out to be a wrong decision and many end users had difficulty accessing certain files in the systems leading to frantic calls. The frameworks used to assign profiles were generic, making it difficult for practitioners to anticipate these emergent problems. To facilitate continuity of work, the practitioners contextually determined those people requiring technical access (system administrators) and those requiring process/procedural based access (end users). They then determined procedural based access by assigning new group profiles.

This data incident suggests that the information security practitioners exhibited a degree of resourcefulness (**being resourceful**[IMPROV-2]) and this act was coded as such. The practitioner responsible for splitting access roles into technical and process understood the contextual needs at the time and also addressed emergent needs that the functionalist frameworks had no provision for at the time. These were process based operational activities, and were therefore interpreted to mean an occurrence of *process improvisation*[IMPROV-2].

3. Authorization Process of Information Facilities

Another ISRM activity identified from the interview discussions was that of the need for information security practitioners to conduct the authorisation processes for use of facilities carrying sensitive information. **ISO IEC 17799 Section 4.1.4** takes cognisance of the authorisation process for information processing facilities. **CobiT** objectives **Section DS5.6** suggests ways of determining user control, by creating designated user

[7] C119-Appendix 10
[8] Q26-Appendix 8

accounts (or group accounts) through a structures mechanism to oversee these accounts. The **CobiT** objectives **Section DS11.16** also gives a controlled way of issuing security provisions for output reports while **ITIL Section 4.1** (*Security Management*) explains information security management measures for information control.

Data Incident

An interesting way in which the information security practitioners adopted these provisions (frameworks) was that they knew they had the freedom to interpret what control mechanisms to put in place. At times their interpretations were consultative as explained by the following data incident:

> *"…we have established that we don't have to give them that [administration group] kind of access, but then we [deliberated] about restricting internet…*[9]

This sort of incident demonstrated that the consultations and deliberations constituted some level of deliberation (**being deliberative**[IMPROV-3)] from the consultative group. The context of the deliberation was to ensure that "determining user control" was appropriate to the situation/need. Determining this need was achieved at group level and entailed imaginative thinking in order to comply with information security provisions. As a process based activity (operational level), this ISRM activity also demonstrated *collective improvisation*[IMPROV-3] that was strengthened through practitioners' skills and experience.

4. Data Warehouse Management and Information

ISO IEC 17799 Section 5.1.1 suggests the need for management to compile an inventory of assets as an important aspect of risk management. The **ISO IEC 17799 Section 5.2.2** guides the management in setting procedures for labelling these assets, after the compilation process. The **CobiT** objectives **Section DS5.8** suggests a manner for information assets classification, and suggests mechanisms that provide for data sensitivity and the sharing of data. **ITIL Section 4.2** (*Security Management*) gives direction on how to implement these measures. The importance of the above identified

[9] C117-Appendix 10

ISRM activity ensures that sensitive information (assets) was appropriately labelled and handled as such.

Data incident

From the interview it was revealed that the information security practitioners were carrying out this activity as the procedures stipulated. One practitioner highlighted how this was carried out:

> *"… [This is carried out] in terms of safety of information, manipulating information, metadata around information and stuff like that…"* [10]

It was indeed interesting that the information security practitioner mentioned the word "*manipulating*". The context of why the word manipulation was mentioned was the idea that when looking at safety of information (data), if data is threatened in any way, it is not that its integrity is threatened or the information is invalid in anyway. It is just that whoever has access to this information (data) may use it in an illegal/illegitimate way. What can be shown is that practitioners had devised and manipulated the system (and information) holding the data in creative ways to protect the information and hinder/minimise illegal access. This data incident revealed that the skilled information security practitioners considered the safety of information to the level they through to **manipulate**[IMPROV-4] the data base was an ideal way of risk minimization. This act suited the contextual need at the time and was coded. Since this act was at a higher level (strategic activity), and the manipulation involved more than one information security practitioner at the time, it was interpreted to demonstrate *collective improvisation*[IMPROV-4].

5. Authorization Process for Program Source Library

The **ISO IEC 17799 Section 10.4.3** issues strict guidelines on access control to program source libraries. This reduces the risk of potential corruption to associated and main source programs that control data in the databases. The **CobiT** objectives Section **DS8.4** suggest a way of monitoring clearance of source information in a timely manner and of

[10] C59-Appendix 10

investigating outstanding incidents that affect source information/libraries. Similarly **CobiT** objectives **SectionDS5.4** gives procedures for user account management, and shows access privileges and the necessary security procedures to be followed when third parties access source information/libraries. **ITIL Section5.4.3** (*Service Support*) gives direction on general incident management and a structure for investigation and diagnosis of general incidents which includes source library incidents. By interpreting the above frameworks, it seems that these frameworks give little room for flexibility in terms of access and authorisation towards source programs, source codes, and source libraries.

Data incident

In the interview, it was established that the information security practitioners understood the procedures relating to accessing source programs well. However, in their capacity to understand what was contextually happening, they set procedures that would override underlying restrictions. This was done provided that the overriding actions would not jeopardize system security. This was explained by one interviewee as follows:

> *"…Because, we had to do it…in those groups… what happens in the access aspect is that they actually modified the database…and [name withheld] actually approved this…"* [11]

The context of the data incident was that, in this organisation, user access management transcended departmental boundaries, meaning the Human Resource Department was involved (in assigning job descriptions), the IT Department (in assigning group profiles) and the Information Security Officer (in assigning policy). What happened was that certain employees' job designations from Human Resource were inappropriate for the assigned group profiles given by IT and hence could not access certain information. It was at the moment of this realisation, that the practitioner on the spur-of-the-moment ("*we had to do it*") modified the database to accommodate this need. This data incident allowed the practitioners to be quick in thinking and was coded as **quick-wittedness**[IMPROV-5]. The database modification was authorized at operational level and *process improvisation*[IMPROV-5] was coded in this instance.

[11] C123-Appendix 10

Summary of the First Unit of Analysis

Table 20 summaries the total number of **conceptual instance** in the previous narrative for this unit as follows:

Table 20. Conceptual density of Improvisation when examining Information Assets and Data Control

Units of Analysis Activities related to;	**Core Categories**	**Concepts generated within the types of improvisation**				**Conceptual Density**
		Collective Improvisation	**Individual Improvisation**	**Process Improvisation**	**Product Improvisation**	
Assets control	**Strategic**	*Manipulating*[IMPROV-4]				1
	Tactical	*Quick reaction*[IMPROV-1]				1
	Operational	*Being deliberative*[IMPROV-3],		*Being resourceful*[IMPROV-2], *Being Quick-witted*[IMPROV-5]		3

As shown in the previous section, the analysis of the first unit of analysis has been illustrated by a descriptive narrative that explicates *improvisation* in the way information security practitioners control the access to information as value assets. The next section examines how the researcher expounded on this narrative for the five (5) remaining units analysis using this preliminary knowledge and understanding and a similar approach. This narrative approach was useful in helping this researcher think critically and systematically about coding data and deriving *improvisation* concepts. This knowledge was then appropriated to the rest of the units of analysis in complex ways and through constant comparative analysis and the validation and re-questioning of data.

6.2.2 Analysis – Information Security Architecture

Information Architecture (IA) refers to the organisation labelling and structuring information and systems that hold the information, the design of these and their navigation in order to allow users to realise their information needs. **Section 2.4.2** of this research dealt with issues regarding this unit of analysis. The following section conceptualizes *improvisation* within activities that relate to information security architecture. Conceptualizing *improvisation* in this unit followed the 6 steps listed in **Section 6.1.** This is demonstrated by **Table 21** as follows:

Table 21 Open Coding for Information Security Architecture ***(Extract of Appendix 3)***

STEP 1 **Data Incidents** **(Transcribed Interviews)**	**STEP 2** **Context of Data Incident** (Researcher's Memo)	**STEP 3** **Researcher's memos** Determine Codes in vivo and other generated as underlined)	**STEP 4** **Level**	**STEP 5** **Concepts generated (inductively)**	**STEP 6** **Types of Improvisation** (See Section 4.4.1)
and whether there is compliance, you know considering security you know whether there are best solutions to match the technology platform… stuff like that [12]	The current architecture and technology platform (a fusion of many platforms) could not be matched with proposed policy compliance models so the nature of compliance had to be innovative based on the technology architecture, resulting in the process of compliance being improvised	***Compliance Efforts and Information Architecture Specification*** 1. Implies being rational adaptive in ensuring compliant information architecture.	**Tactical** Activities	Being **rational adaptive** in determining compliant architecture	(Process) Improvisation
[The] middleware team...gives a human aspect to the way we design things...such that the whole way we design things is very middleware driven.. we've got a rich...middleware architecture [13]	The middleware team was socially driven with the social conditions permitting the middleware team to explore and discover new technical designs that interfaced between people, business processes and technology. Their discoveries were shaped by time and resources.	***Security Design requirements and Specifications*** 1. Implies lateral thinking by the middleware team charged with designing the security requirements of middleware architecture	**Tactical** Activities	**Lateral thinking** in designing middleware architecture	(Process) Improvisation

[12] C62-Appendix 10
[13] C66-Appendix 10

The following are the data classifications as described in STEP 3 (2nd paragraph) and are derivatives of interviews transcripts for this unit of analysis (***see Appendix 3).*** These classifications are listed as follows:

1. Compliance Efforts and Information Architecture Specification
2. Information Security Design requirements and Specifications
3. Information Architecture Requirements on Risk
4. Information Architecture Forum for Information Security
5. Information Architecture Design and Acceptance
6. Operational Procedures and Responsibilities

Each of the above classification is explained in turn.

1. Compliance Efforts and Information Architecture Specification

Procedures that stipulate the way this ISRM activity is to be carried out are explained as follows. In terms of compliance requirements for information architecture specifications, the **ISO IEC 17799 Section 12.1.1** explains the management obligation to design, operate and use information systems in ways that meet and address requirements stipulated by statutes, regulatory and contractual frameworks. The **CobiT** objectives **Section AI5.13** suggests a manner for evaluation and meeting user requirements through post-implementation review to assess whether user needs are being met. **ITIL Section3.5.4** (*ICT Infrastructure Management*) gives direction on system deployment and acceptance testing. Most of these procedures are incorporated in the overall information architecture specifications.

Data incident

The information security practitioners carried out this particular ISRM activity through a series of co-ordinated efforts based on their inherent skills and experience. Experience was a necessary aspect of managing ISRM activities as shown by the following data incident.

> *"We use our own experiences and [sometimes] solicit the expertise of outside agencies such as Gartner, etc."*[14]

[14] Q28-Appendix 8

The interview revealed that a great deal of emphasis was placed in the information security practitioners experience towards understanding how to design an information architecture that met compliance requirements. The following is a data incident recorded that illustrates the contextual need:

> *"…there has been a lot of good stuff that these guys for instances like [name withheld], in Enterprise Risk [Architecture] have done…they have complied with every possible standard/ framework…"* [15]

The context of this data incident is that the organisation's Enterprise Risk Architecture Program (ERAP) as designed by [name withheld] provided a critical component of the information security program. To this end, the ERAP's objective was to identify and evaluate threats to the organisation's risks and mitigation controls. At lot of good work was done but it was how this was done that proved exceptional. The good work mentioned here was a demonstrated ability to comply with frameworks and other requirements and to meet ERAP's objectives at the background of emergent contextual factors. The practitioners designed the ERAP to determine critical systems. Not all systems were to be protected equally due to limited resources. Under ERAP, systems classified as critical would be assigned significant protection. The skills and experience to determine critical systems under ERAP epitomised **exceptionality**[IMPROV-1] and was coded as such. The experience and exceptionality demonstrated *process improvisation*[IMPROV-1] in the way compliance requirements for ERAP at strategic level were met by the practitioners.

Data incident

Another data incident relating to enterprise architecture compliance noted by the researcher involved situations where compliance requirements were "silent", i.e. did not fully address the contextual organisational requirements of the organisation at the time. These situations forced solutions. The following data incident illustrates this:

> *"…and without preparation, [we needed] getting to know whether there is compliance, considering, information security you know whether there are best solutions to match the technology platform… stuff like that…"* [16]

[15] C9-Appendix 10

The context of this incident was that the organisation was in possession of a new technology platform with features not addressed by frameworks, making compliance requirements contextual to the new technology and the risk involved. When faced with the challenge of identifying best solutions at the time, the information security practitioners demonstrated an ability to match compliance needs for this new platform while piecing together an elaborate secure information architecture. An important part about this data incident was that the practitioners acknowledged that compliance considerations were done without *preparation* and therefore on the spur-of the-moment. This on the spur-of-the-moment extemporaneous act was made possible when practitioners drew on past experience. This was interpreted to be **rational adaptive**[IMPROV-2]. This rational adaptive mode exemplified *process improvisation* [IMPROV-2] at strategic level.

2. Information Security Design Requirements and Specifications

The **ISO IEC 17799 Section 10.1.1** explains the need for organisations to issue statements of requirements specifications for new systems, or on the enhancements of existing systems which specify the architecture requirements for controls. **Section 10.1.1** further notes that such architecture specifications should consider automated controls to be incorporated in the system, and the need for supporting manual controls. Part of the design requirements and specifications revealed in the research were the set password requirements for users and system accounts.

Data incident

When asked what the security design requirements for system passwords were, it was explained that the:

> *"User sign-ones' are unique to each user and passwords are required to alpha/special character/numeric format and a 30 day expiry lifespan."*[17]

The context of this data incident was that the organisation had put in place user sign-ons and authentication or the verifying of identity of the users (employees) through the use of

[16] C62-Appendix 10
[17] Q62-Appendix 8

passwords. The policy was instituted to create a system that would give passwords a 30 day expiry lifespan. This meant employees had to change passwords after a 30 day period. The information security practitioners explained that the password design requirements and specification for passwords was to be designed in context with the enterprise architecture. The design was therefore to be considered primarily from two perspectives: an enterprise wide perspective and a technical perspective. These two issues influenced how password design specifications would be met. This simply meant the designs would accommodate complex passwords for technical users while maintaining simplicity for ordinary users yet rejecting simple, easy to crack passwords. The information security practitioners developed a **lateral thinking**[IMPROV-3] approach in the way a system for passwords within the enterprise architecture was to be designed. One interviewee puts it this:

> *"… [The] middleware team gives a human aspect to the way we design things...such that the whole way we design things is very middleware driven… we've got a rich...middleware architecture…"* [18]

The lateral thinking at operational level that enabled the generation of secure designs (including passwords) was interpreted to be *process improvisation*[IMPROV-3].

3. Information Architecture Requirements on Risk

In terms of information architecture requirements on risk, **ISO IEC 17799 Section10.1.1** explains that the information security requirements and controls should reflect the corporate value of the information assets involved, and the potential business damage which might result from a failure or absence of information security. The **CobiT** objectives **SectionAI5.10 determines** through information security testing and accreditation, the need to understand the information security levels and the residual risk in the system. **ITIL Section3.5.2** (*Service Support*) shows the proper way to install systems in a working environment.

Data Incident

From one specific data incident, when asked if the organisation's network and computer systems were risk monitored for network intrusions as a risk element the response was:

[18] C66-Appendix 10

"Yes…"[19]

Asked what the organisation considered as confidential information and how was protected from information security risk, the respondent recalled that the risk would be realised when information deemed confidential was accessible to the wrong persons and impacted wrongly on the brand:

> *"Any information that would, if made accessible to the wrongs persons, and negatively impact the brand, is regarded as confidential."*[20]

ISO IEC 17799 Section 10.1.1 points out that while the framework for analysing information security risk requirements and identifying controls to fulfil them is through risk assessment, the controls implemented at the design stages are significantly cheaper to implement and maintain than those included during or after implementation. This ISRM activity was explained by one information security practitioner when asked about the security of computers with regard to internet connections:

> *"We ensure at the beginning, that the level of security on these computers/servers would offer the company the necessary protection."*[21]

The context of this data incident was that the organisation's mission critical applications required certain measures for security and access controls. Users and processes were to be allowed access based on the principle of least privileges (need to know basis). What was important was that the information security practitioners extemporaneously implemented controls over configurations of systems to disallow potential malicious use. By analysing the above data incidents, the researcher established that the information security practitioners identified system requirements for risk while at the same time contextualizing ways to address information protection. This illustrated that the information security practitioners were **rational adaptive**[IMPROV-4] at tactical level. The information security practitioners jointly acted within a range of options for information architecture requirements that determined best fit and was seen as *collective improvisation* [IMPROV-4].

4. Information Architecture Forum for Information Security

[19] Q64-Appendix 8
[20] Q58-Appendix 8
[21] Q59-Appendix 8

The **ISO IEC 17799 Section 10.1.1** explains that while information security should be a responsibility shared by all, it proposes the formation of a management forum. Part of the proposition advanced by **Section 10.1.1** helps ensure that within the organisation; there is clear direction and visible management support for information security initiatives. The **CobiT** objectives **Section AI5.14** suggests that responsibility for ensuring security through the roll out of any new system rests on the management and stipulates benefits realisation through a post-implementation review. **ITIL Section4.2** (*Service Support*), Release Management, gives direction on how to implement a new system in a working environment. Ideally, the forum should promote information security within the organization through appropriate commitment and adequate resourcing, while undertaking the following:

- Reviewing and approving information security policy and overall responsibilities;
- Monitoring significant changes in the exposure of information assets to major threats;
- Reviewing and monitoring information security incidents;
- Approving major initiatives to enhance information security.

When one particular information security practitioner was asked who co-ordinated the implementation of security controls, the response suggested that the organisation was following procedures stipulated by the mentioned frameworks:

> *"The technical component resides within the technology enablement group / forum as they respond to the policies and procedures provided by the IT Risk and Continuity management."*[22]

No *improvisation* was coded for this data incident.

Data incident

In one other data incident, one interviewee identified the importance of forums. These forums were to give a clear direction to management on best ways to review and monitor information security incidents and any other information security initiative:

[22] Q16-Appendix 8

"…We have got the Architecture forum, which sits under [name withheld]… and uum, we also have [another forum], which I'm more involved in, in making sure that there is compliance architecture…[23]

The context of the data incident was that these forums allowed for unplanned outcomes and were seen as contextually relevant. The outcomes of the forums and workshops ultimately shaped risk perceptions and compliance requirements. The forums and workshops at tactical level were interpreted by the researcher to influence the processes for information security architecture and design. These were coded as *collective improvisation*[IMPROV-5] since the outcomes of the perceptions within the forums occurring overtime were meant to be **deliberative**[IMPROV-5] and to eventually fit within the corporate risk profile.

5. Information Architecture Design and Acceptance

The **ISO IEC 17799 Section 8.2.2** advances the idea that the acceptance criteria for new information systems with upgrades and new versions being established and suitable tests of the system carried out prior to acceptance. The **CobiT** objectives **Section AI 5.13** also suggests the need for an evaluation of systems to test acceptance of user requirements. **ITIL Section 9.6.3** (*Service Support*), Release Management, gives direction on release acceptance procedure and working environment. The criteria for accepting new systems was established by a management framework which controlled the organisation's systems acceptance and implementation criteria. The management review of the criteria was explained to have been done in the year preceding the research:

"This was undertaken last year with the inclusion of Information Security into Business Intelligence competency." [24]

Data incident

Data incidents for this ISRM activity revealed that the way the information architecture was designed and tested for acceptance was both innovative and novel. While there was a general acknowledgement by information security practitioners that part of their organisational systems were not designed with security in mind, nevertheless, the practitioners designed

[23] C60-Appendix 10
[24] Q19-Appendix 8

suitable novel acceptance criteria which was supported by innovative procedures as fusion of the technical and the socio-cognitive. Indeed the acceptance criteria for the security and use of systems seemed to be "made up as they went along" or "*as were being defined*":

> *"…to ensure that they comply with whatever policy and standards that they have devised or as was being defined by the board…"* [25]

The context of this data incident was that the organisation had identified board members who were experienced and understood not only the business goals of the organisation but also had a measure of technical knowledge to understand information security issues. It is this proficiency by representatives of the board that enabled compliance in novel ways. The *improvisational* aspect of this **novel**[IMPROV-6] approach was that the board recognised this specialised knowledge area and included provision for delegation to skilled information security practitioners who would design the compliance criteria and report this to the board only when a need arose. There had not yet been provision for this in the organisation's policy. This was interpreted as *collective improvisation* [IMPROV-6].

6. Operational Procedures and Responsibilities

The **ISO IEC 17799 Section 8.1.2** requires the need to control changes to information processing facilities and systems through the provision of technical specifications. It follows that inadequate control of changes is a common cause of system or information security failures. **Section 8.1.2** advances the need for formal management responsibilities and procedures to be put in place to ensure satisfactory control of all operational procedures. The **CobiT** objective **Section DS51.3** suggests procedures for checking performance through governing relationships and communication. **ITIL Section 4.7** (*Service Delivery*) Service Level Management gives direction on Key Performance Indicators (KPI's) and metrics for SLM efficiency and effectiveness.

Within the context of above frameworks, the researcher raised the question of how often the organisation monitored (a) dormant accounts; (b) antivirus updates; (c) shared files; (d) account lock out; (e) the use of regular passwords. The response was that this was done regularly:

[25] C7-Appendix 10

"This monitoring is done on a regular basis by our Active Directory administrators."[26]

The importance of the regular monitoring of operational procedures and having someone responsible was an important ISRM activity, and the organisation seemed to place great importance on this. The **ISO IEC 17799 Section 8.1.2** stresses the need to be constantly vigilant of changes and incidents and that wherever practicable, operational and application change control procedures should be integrated. These procedures and specifications include:

- Specifications for the identification and recording of significant changes;
- Specifications for the assessment of the potential impact of such changes;

Data incident

The review of data incidents highlighted that there was vigilance in monitoring changes to applications and that there were adequate procedures and specifications that covered these ISRM activities. The following data incident illustrates this:

"…we developed requirements specifications for reviewing the [operational] process. We had systems requirement specifications, integration specifications in terms of how the system sends information to another system…or the middleware stuff…"[27]

The context of this data incident was that the organisation had created access rules and specification, by virtue of the estimated magnitude of risk that could potentially arise within each of the organisation's critical processes. The challenge here was for practitioners to determine at operational level who was to enforce the requirement specifications, while at the same time not burdening other practitioners who ultimately had no liability at stake for some of the processes. This was not easy and there were signs and elements of **resourcefulness**[IMPROV-7] on the part of those deciding who among the practitioners would be responsible for determining the requirement specifications. Determining this was interpreted as *process improvisation*.[IMRPOV-7].

[26] Q60-Appendix 8
[27] C69-Appendix 10

Summary of the Second Unit of Analysis

A key differential with this unit of analysis is that there is a reasonable level of *collective improvisation* at strategic level and tactical levels. It is evident that *process* improvisation is conceptually dense at the operational end, the reason being the key role that information security practitioners play between balancing short term to immediate solutions. **Table 22** summarises the total number of **conceptual instances** in the previous narrative for this unit as follows:

Table 22. Conceptual density of Improvisation when examining Control over Information Architecture Security

Units of Analysis Activities related to;	**Core Categories**	**Concepts generated within the types of improvisation**				**Conceptual Density**
		Collective Improvisation	**Individual Improvisation**	**Process Improvisation**	**Product Improvisation**	
Information Security Architecture	**Strategic**	*Novel*[IMPROV-6],		*Exceptionality*[IMPROV-1],		2
	Tactical	*Rational adaptive*[IMPROV-4] *Deliberative*[IMPROV-5]				2
	Operational			*Rational adaptive*[IMPROV-2], *Lateral thinking*[IMPROV-3], *Being resourceful*[IMPROV-7]		3

6.2.3 Analysis - Information Security Policies

Section 2.4.2 of this research dealt with issues regarding this unit of analysis. The following section conceptualizes *improvisation* within activities that relate to implementing information security policies. Conceptualizing *improvisation* in this unit followed the 6 steps listed in **Section 6.1.** This is demonstrated by **Table 23** as follows;

Table 23 Open Coding for Information Security Policies **(*Extract of Appendix 4)***

STEP 1 **Data Incidents** **(Transcribed Interviews)**	**STEP 2** **Context of Data Incident** (Researcher's Memo)	**STEP 3** **Researcher's memos** Determine Codes in vivo and other generated as underlined)	**STEP 4** **Level**	**STEP 5** **Concepts generated (inductively)**	**STEP 6** **Types of Improvisation** (See Section 4.4.1)
what they did was… they took the notebooks…they gave those new notebooks to people…and they gave the old notebooks that people had that were still on working conditions to other people [28]	Policy dictated that the old laptops be replaced by new ones. The old could not be used as their warranty had lapsed and it could be expensive to maintain. A way was devised and the practitioners improvised by rotating the old with new to control costs. This had never been done before.	***Information Security Policy Co-ordination*** 1. Implies being ingenious in situations resulting from limited resources	**Tactical** Activity	**Being ingenious** on Information Security Policy	(Collective) improvisation
and most of them.. they can't even document all that stuff [29]	The lack of documentation for some of the critical activities done, provided clear motivation for some activities to be improvised as there were no explicit guidelines to follow upon.	***Accountability and Reporting of Information incidents*** 1. Implies unexpected incidents where practitioners lack of documentation have to be imaginative in their contextual activities providing grounds for improvisation.	**Tactical** Activity	**Being imaginative** with policies when none	(Process) improvisation

[28] C99-Appendix 10
[29] C79-Appendix 10

The following were the data classification as described in STEP 3 (2nd paragraph) and are derived from interview transcripts for this unit of analysis (***see Appendix 4).*** These classifications are listed as follows:

1. Information Security Policy Co-ordination
2. Accountability and Reporting of Information Incidents
3. Co-operation and Training on Information Security Policy
4. Policy on Access and Control of Information Users
5. Control of internal Processes and Change Management

Each of the above classification is explained in turn.

1. Information Security Policy Co-ordination

In light of the requirements that companies should implement appropriate controls and co-ordinate implementation across critical business processes, the **ISO IEC 17799 Section 4.1.2** requires that a cross-functional forum of management representatives from relevant parts of the organization co-ordinate the implementation of information security controls. The **CobiT** objectives **Section AI6.1** stipulates the policies and procedures guide management in terms of changes in control of information with regard to system and control changes, categories, responsibilities, priorities status and urgencies. **ITIL Section 4.2** (*Service Support*) suggests policies for change management by highlighting the basic concepts of change management.

Data Incident

Analysis of the data incident revealed that the ISRM activity regarding information policy co-ordination was also present in the organisation. One information security practitioner was asked about how the organisation ensures that the co-ordination of security controls are representative of the organisation's needs as well as the needs of the employees. It follows that holistic needs were considered:

> *"The intent of our policies is to offer our organisation the necessary protection, but also to provide the assurance of the protection of the integrity of the individuals who use the system."*[30]

[30] Q18-Appendix 8

"Our organisations security roles and responsibilities are documented in the [name withheld] Corporate Information Security Policy."[31]

In terms of co-ordinating these efforts, **ISO IEC 17799 Section 4.1.2** proposes that a forum be constituted to:

- agree on specific roles and responsibilities for information security across the organization;
- agree on specific methodologies and processes for information security, e.g. risk assessment, information security classification system.

Data incident

Analysing a section of a data incident revealed that the organisation's board had made recommendations for sweeping changes regarding co-ordination of Information Security policies. While previously this responsibility was left to one practitioner with a familiarity on procedures stipulated by CobiT control methodology, the Board's new strategy was to incorporate an efficient team that would include participation by users. This was to be achieved through a change in the existing mind-set of all users. There was initial resistance as expressed by one interviewee:

"...so that was the real challenge in terms of getting...their minds [my mind] to change…nobody wants to be [held responsible]…"[32]

The resistance and the changing of mind-set regarding the functionalist policies were not isolated. Indeed one information security practitioner expressed the concern as stipulated by **ISO IEC 17799 Section 4.1.2** in a subtle way but understood by the researcher, regarding agreeing on specific methodologies. When asked if the practitioner felt liberated or constrained by security policy and methodologies, the response was:

"I feel that the policy provides both a liberating and constraining feeling insofar as you are aware of the parameters within which you have to work."[33]

This sort of both liberating and constraining feeling seemed to have influenced that approach and attitude towards Information Security policy. The feeling also influenced how the outside opinion including benchmarks and best practice was to be perceived, appreciated and rolled out

[31] Q2-Appendix 8
[32] C37-Appendix 10
[33] Q5-Appendix 8

internally to the organisation. When one information security practitioner was asked whether there were times when there was conflict of opinion between the organisations' internal experts and external experts in relation to information security policy, it was revealed that:

> *"I would not regard it as conflict, rather a variance of views in terms of company needs and external stringent adherence to best practices."*[34]

It was interpreted that this sort of "*variance of views*" was fertile grounds for *improvisation* to occur particularly in information security policy formulation and roll-out. One data incident which demonstrated "variance of views" between information security policy and its co-ordination, showed this to be true. One particular information security practitioner narrated how it was policy for old laptops (notebooks) to be discarded, once the warranty had expired, since it would be expensive to maintain these. But because of limited resources, the board recommended the continued use of old laptops. The continued use of old laptops meant increased costs and risk to the company because of warranty issues (expired warranties). Policy was tactically and creatively overridden collectively to ensure that work continued and at the same times risks were kept in check. This is illustrated by one interviewee as follows:

> *"…what [the practitioners] did was… they took the notebooks…they gave those new notebooks to people…and they again gave back the old notebooks that people previously had that were still on working conditions to other people…"* [35]

The above data incident illustrates *product improvisation*[IMPROV-1]. This can be explained as follows. The context of the data incident was that the policy in place meant that out-of-warranty notebooks should not be used. This meant the available notebook "products" were insufficient to meet the work objectives of the organisation at the time. At operational level, an innovative way was found whereby old out-of-warranty notebooks that were partially damaged but were still functioning were revived and given to those people without notebooks (circumventing policy). The manner in which these notebooks were revived was coded as **being ingenious** [IMPROV-1]. This data incident was interpreted by the researcher to be an extemporaneous way of coping with an unplanned for situation as it was arising.

2. Accountability and Reporting of Information Incidents

[34] Q23-Appendix 8
[35] C99-Appendix 10

The **ISO IEC 17799 Section 6.3.1** proposes the need to establish formal processes to document information security incidents procedures and of the reporting of these through appropriate management channels as quickly as possible. This section proposes the establishment of a formal incident response procedure, together with an incident response which sets out action to be taken on receipt of an incident report. The **CobiT** objectives **Section DS3.3** suggests the ideal ways for monitoring and for the reporting of information security incidents, while **ITIL Section 8.5.1** (*Service Delivery*) states that, in terms of information systems availability management, there should be structured ways of determining availability requirements.

The need for continuous reporting of information security incidents was consider critical since it was good practise to report information security incidents by following procedures of reporting of these incidents through appropriate management channels. It was revealed that the organisation had put in place measures to educate and make users aware of the documenting and reporting requirements of information security issues in general and of information security incidents in particular.

Data incident

When asked what sorts of measures were taken by the organisation to encourage a multi-disciplinary approach to information security reporting of incidents, it was revealed that:

> *"By regular communications with the broader [name withheld] community we have heightened the need for corporate response to security."*[36]

However, analysis of data incidents suggested that this was not always the case. For instance, it was common for some users to encounter information security incidents while failing to report/document these. The lack of documenting incidents or even the manner of resolving these incidents was highlighted in the interview as follows:

> *"…and most of them… they can't even document all that stuff …"* [37]

[36] Q24-Appendix 8
[37] C79-Appendix 10

In light of the fact that some employees were not aware of these documentation procedures, it became challenging for information security practitioners to monitor incidents. The following data incidents reveal the challenge faced:

> *"There were certain inconsistencies highlighted from the last [audit] review and these were addressed and remedied."*[38]

The context of the above data incident was that the organisation did not put in place proper procedure to monitor and report system activity. That was why the audit revealed "*inconsistencies*". However, it was the addressing and remedying of these inconsistencies at tactical level that was coded as *process improvisation*[IMPROV-2]. This is explained as follows. In the light of the inconsistencies brought to light by third party audits, the practitioners had to **be imaginative**[IMPROV-2] to remedy the situation. What was done was that they used a combination of automated and manual tools to monitor system activity. They automated the process of determining systems logs (running continually in the background) while spontaneously manually auditing specific user activity when a contextual need arose. As suggested by the information security practitioners, they had a way of "*remedying*' the situation.

3. Co-operation and Training on Information Security Policy

The **ISO IEC 17799 Section 6.2.1** proposes that all employees of the organization should receive appropriate training and regular updates in organizational policies and procedures. The **CobiT** objectives **Section DS7.1** proposes a mechanism for identification of training needs, through a training curriculum for each group of employees. **ITIL Section 6.8** (*Service Support*) establishes procedures for dealing with problems through proactive problem management. This includes information security requirements, legal responsibilities and business controls as well as training in the correct use of information processing facilities.

Data incident

One information security practitioner was asked who (between employees and third parties), played a greater role in helping define the organisation's information security needs and policy? It was revealed that the role was spilt:

[38] Q40-Appendix 8

"There is an equal level of contribution in balancing the needs of the company and those advised by third parties."[39]

Part of **ISO IEC 17799 Section 6.2.1** aims at ensuring users are aware of information security threats and concerns, and are equipped to support organizational information security policy in the course of their normal work. From parts of the interview with one information security practitioner, it was established that information security training and education on policies, tools, methodologies and control frameworks was initially the sole prerogative of the IT Risk and Continuity Manager.

At strategic level, the IT Risk and Continuity Manager expressed a level of challenge in getting users to a level where they could understand information security guidelines as stipulated by CobiT. The organization had already implemented CobiT but its reception was poor. That is why the IT Risk and Continuity Manager had to be creative and employ **lateral thinking**[IMPROV-3] to get the users accustomed to and familiar with CobiT requirements. This *improvisational* element was coded as such. The researcher interpreted the lateral thinking of the IT Risk and Continuity Manager as *individual improvisation*[IMPROV-3]. Once the users began to understand the intrinsic befits of CobiT, then they began to appreciate his efforts. The whole mindset and attitude towards these frameworks changed because of this individual. This is revealed by what this practitioner said in the interview:

"…it was perfect…when they actually saw the CobiT…exception results…they actually came to like it… because we are here to [show them]…"[40]

Making CobiT clear to users and explaining its importance with regard to the organization's information security posture seemed to be borne by the IT Risk and Continuity Manager, though it seems this role was handled well.

4. Policy on Access and Control of Information Users

The **ISO IEC 17799 Section 9.6.1** gives guidelines to users of applications who should be provided access to information and application systems in accordance with defined access control policies. The **CobiT** objectives **Section DS5.2** suggests a manner for identification,

[39] Q 3 -Appendix 8
[40] C38-Appendix 10

authentication and access requirements for users by establishing procedures for logical access to and use of resources, and restriction to authorised personnel. **ITIL Section 4.2.4** (*Security Management*) gives direction to the information security management measures to be taken on access controls.

Data incident

The researcher asked one information security practitioner the criteria the organisation used to assign the responsibilities for implementing information security policy. It was established that experience and extensive knowledge played a big role.

> *"Relevant experience in an IT environment. Clear understanding of Information Security Extensive knowledge of IT strategies, best practise processes and standards. Thorough working knowledge of analysis and design methodology and modelling techniques."*[41]

When also asked what the organisation's security roles and responsibilities were based on, the information security practitioner responded by stating that:

> *"Our roles and responsibilities are based on providing the preservation of confidentiality, integrity and availability.* ***Confidentiality*** *– ensuring that accessibility is only for those authorised.* ***Integrity*** *– safeguarding of accuracy and completeness of information.* ***Availability*** *– ensuring authorized users have access to information."*[42]

The above data incidents corroborate the literature review finding that describes the tenets of information security (explained in **Section 2.1,** literature review). These were the same tenets that guided this organisation. The tenets as analysed from the data incidents seemed to guide the organisation towards putting controls in place that supported access restriction requirements such as:

- users being providing with menus to control access to application system functions;
- restricting users' knowledge of information or application system functions which they are not authorized to access; and
- controlling the access rights of users, e.g. read, write, delete and execute;

[41] Q43-Appendix 8
[42] Q1-Appendix 8

How this was done and communicated to the users was through the organisation's intranet as explained by one information security practitioner.

> *"We use our Intranet,[name withheld]. Information days, regular e-mails are posted as reminders of the policy".*[43]

In the interview process it was revealed that sometimes policies and guidelines on control of users were indeed accommodated and innovatively crafted and *process improvised* IMPROV-4 to reflect user requirements. This sometimes called for practitioners to **being quick-witted**IMPROV-4 in terms of making provisions for policy amendments. One practitioner states as follows:

> *"…Well most of the times we try and keep us much access control as we can but most of the times that we do, people don't want to follow the right procedures… I mean they are willing to [jump levels] and would do whatever they need to do to get their stuff across…"* [44]

The context of *process improvisation* for the above data incident was that the employees seemed to disregard set policies and procedures.

> *"Adherence to the e-mail usage policy seems to be disregarded by many users."*[45]

The information security practitioners had challenges enforcing policy and would often be faced with the softer "people" issues. The need to be quick witted in dealing and interacting with users was interpreted by this researcher as comprising elements of *improvisation* that were used to re-create new patterns of approach and this was only possible because the information security practitioners displayed skills and experience when dealing with the users:

> *"We ensure that our knowledge is kept current by the subscription to the relevant professional bodies and the attendance of conferences and seminars."*[46]

When asked what assurances the organisation had with regard to ensuring users were capable of applying information security policy and procedures and thus minimising security risks, the information security practitioner suggested the need to keep security awareness an on-going practice.

[43] Q6-Appendix 8
[44] C126-Appendix 10
[45] Q4-Appendix 8
[46] Q45-Appendix 8

"Whilst there are no absolute assurances, we believe that adherence to the Security policies would lend itself to that assurance."[47]

5. Control of Internal Processes and Change Management

In terms of areas of risk to data and information, particularly when accessed by users and support staff, the **ISO IEC 17799 Section 10.2.2** identifies **risk** by highlighting ways that data and information that have been correctly entered can be corrupted by processing errors or through deliberate acts by users/support staff. The section proposes validation checks which should be incorporated into systems to detect such corruption. The section suggests looking at the design of applications and ensuring that restrictions are implemented to minimize these processing risks and failures that lead to a loss of integrity. The **CobiT** objectives **Section AI6.3** stipulates the need to control changes in the information systems environment while considering proper change management procedures that guide software control and distribution, integrated configuration management, changes recorded and tracked. **ITIL Section 7.9** (*Service Support*) guides the proper procedure for configuration management particularly with regards to relationships of information systems to other processes.

Data incident

When analyzing a specific data incident, it was revealed that in matters of prioritizing for information security, this often called for adjustments in the way the applications and controls were used. One practitioner had this to say:

"…and obviously now when we reflect on it…[policy] it has not been too bad on business, but now when we hit certain areas, is that we have to make some kind of adjustments… because there are so many applications out there…and the thing is that, to be working…these needs to run on the administration rights of the machine…" [48]

The data incident suggested the need to intertwine information security policies with contextual and pragmatic requirements. The information security practitioners made attempts to draw upon their past experiences and practices in understanding policy requirements and making

[47] Q46-Appendix 8
[48] C137-Appendix 10

necessary changes to accommodate business process changes. Through this incident, the researcher was able to interpret a degree of thorough intuitive and technical understanding on the part of the information security practitioners in making improvised adjustments. This collective understanding was interpreted to mean a form of *collective improvisation* that called for **rational adaptive**[IMPROV-5] thinking.

Creativity and intuitiveness was also coded in the following data incident:

> *"……so we actually made provisions, that we could do it..[amend policy] when we looked at the group policy…on administration rights issues…"* [49]

The context of this data incident was that, although the intent of policies for administrative rights issues was to give administrators of systems full access rights to systems, the practitioners' spur-of-the-moment actions were **inventive**[IMPROV-6] and made provision for system access by certain users based on unique user identification. The users used this unique identification to gain full access to systems. At tactical level, the need for this was justified. The above data incident was interpreted to reflect *process improvisation*[IMPROV-6].

Yet, another data incident that seemed to corroborate this incident and which suggested that the information security practitioners were pragmatic when it came to dealing with policies was when information security methods, policies and procedures were seen as not being practical. When one security practitioner was asked to recollect on those incidents, it is by hindsight that the following revelation was brought to bear:

> *"Due to certain design of our systems it becomes impractical to fully apply all our security [guidelines] particularly with regard to access to data. As a result hereof full application of the policies are not always fully supported."* [50]

The researcher interpreted the above incident to mean that there were elements of *process improvisation*[IMPROV-7]. This means that at operational level, while the practitioners' respected frameworks/guidelines, between themselves they left provisions where they could act freely outside of these guidelines and frameworks. This was coded as being **creative**[IMPROV-7] and was seen as a pragmatic way of "dealing with the issues as they arose". This creativity is also exemplified in the following data incident.

[49] C138-Appendix 10
[50] Q13-Appendix 8

"…we could give those users…whatever…administration rights on the machine centrally… but [only] if we could manage those users who got admin rights on the machine …" [51]

Summary the Third Unit of Analysis

Table 24 summaries the total number of **conceptual instance** in the previous narrative for this unit as follows:

Table 24. Conceptual density of Improvisation when examining Control over Information Security Policy

Units of Analysis Activities related to;	**Core Categories**	**Concepts generated within the types of improvisation**				**Conceptual Density**
		Collective Improvisation	**Individual Improvisation**	**Process Improvisation**	**Product Improvisation**	
Information Security Policy	**Strategic**	*Rational adaptive*[IMPROV-5]	*Lateral thinking*[IMPROV-3]			2
	Tactical			*Being* imaginative[IMPROV-2] *Being inventive* [IMPROV-6]	*Being ingenious*[IMPROV-1]	3
	Operational			*Being quick-witted*[IMPROV-4] *Being Creative*[IMPROV-7]		2

6.2.4 Analysis – Information Security Event Monitoring

Section 2.4.1 of this research dealt with issues regarding this unit of analysis. The following section conceptualizes *improvisation* within activities that relate to Information Security Event Monitoring. Conceptualizing *improvisation* in this unit followed the 6 steps listed in **Section 6.1.** This is demonstrated by **Table 25** as follows;

[51] C139-Appendix 10

Table 25 Open Coding for Information Security Event Monitoring ***(Extract of Appendix 5)***

STEP 1 **Data Incidents** **(Transcribed Interviews)**	**STEP 2** **Context of Data Incident** (Researcher's Memo)	**STEP 3** **Researcher's memos** Determine Codes in vivo and other generated as underlined)	**STEP 4** **Level**	**STEP 5** **Concepts generated (inductively)**	**STEP 6** **Types of Improvisation** (See Section 4.4.1)
Which increases the admin side which increases everything else, but in the long run it is probably [felt] it is the right thing to do [52] *well… what you see… well what happens is that it is all about saving money* [53]	The downside of implementing innovative measures and controls for information security was the increased costs which the practitioners were not comfortable with, though deemed necessary.	**Monitoring Equipment Placement and Protection** 1. Implies even though there are security control implementation challenges for ensuring robust security posture, the practitioners have to be practical about it	**Operational** Activity	**Being practical** on Security controls Implementation	(Process) improvisation
so there are those little things…that we do just to help us and to help the business.. coz it's those quick little things that…we need to do better [54]	Through continuous internal control assessments, the practitioners appreciated that they were not operating optimally and would continually open up to new ways of improving controls, discovering novel purpose and accomplishing desired objectives.	**Monitoring Security incidents and requirements** 1. Implies being reflexive and quick-witted in dealing with internal controls	**Operational** Activity	**Being quick-witted** in Internal control	(Process) improvisation

[52] C122-Appendix 10
[53] C104-Appendix 10
[54] C96-Appendix 10

The following were the data classifications as described in STEP 3 (2nd paragraph) and are derived from interview transcripts for this unit of analysis (***see Appendix 5).*** These classifications are listed as follows:

1. Monitoring Information Security Incidents and Requirements
2. Monitoring Application Usage
3. Monitoring Processes and Application Integration
4. Monitoring Application Classification Guidelines
5. Monitoring and Assessing Application Risk
6. Exceptional Reporting
7. Monitoring Operational Procedures and Responsibilities
8. Monitoring Equipment Placement and Protection

Each of the above classification is explained in turn.

1. Monitoring Information Security Incidents and Requirements

The **ISO IEC 17799 Section 9.7** specifically issues guidelines for monitoring systems in order to detect deviation from access control policy and also to record events that provide evidence of information security incidents/breaches and/or abuse. The **CobiT** objectives **Section M1.1** suggests a mechanism for collecting monitoring data benchmarks, proprietary nature and integrity of data by looking at relevant performance indicators. **ITIL Section 6.2** (*Service Delivery*) gives direction on the proper way of handling capacity, through capacity management and demand management while **Section 6.8** suggests ways of proactive problem solving and notes the importance of system monitoring in order to allow the effectiveness of controls adopted to be checked.

Data Incident

In order to understand how incident reporting took place, the researcher asked one practitioner the procedures involved in ensuring users reported observed information security weaknesses. It was mentioned that:

> *"Whilst no formal [procedure] is in place we depend on the various competencies within the organisation report potential breaches."*[55]

The above data incident demonstrated a degree of flexibility and informality in carrying out reporting activities. Data analysis however revealed that the organisation had at least a working mechanism (competencies) for the capturing and reporting of security incidents. When one practitioner was asked whether there were policies for reporting incidents, and whether there were procedures to follow as laid down by the organisation when reporting incidents, it was reported that:

> *"Yes, incidents are generally reported to IT Risk management or via our External Service Provider through their network monitoring mechanism."*[56]

It was also reported that there were mechanisms in place to ensure that most of the critical information security incidents were captured and reported. This was explained by one information security practitioner as follows:

> *"There is a formal meeting held monthly, however if serious breaches are detected emergency meetings are convened. There are also automated alerts prompting us of potential threats, specifically external threats."*[57]

The information security practitioner also mentioned that the reporting of the incidents was happening as it occurred:

> *"[incidents] are reported as they occur or detected by our external service providers who monitor our network activity. We have a monthly meeting to analyse incidents received."*[58]

What was interesting to the researcher was the way the information security practitioners carried out checks to confirm incidents. From the interviews held, it was also mentioned by one interviewee that the monitoring process was carried out based on set standards and if there were deviations, then these would be reported.

[55] Q53-Appendix 8
[56] Q49-Appendix 8
[57] Q50-Appendix 8
[58] Q15-Appendix 8

"…[We carried out] particular checks around [form] abuse…which forms part of our information security requirements to ensure confidentiality and integrity basically at more or less operational level…" [59]

The way this monitoring process was done at operational level revealed that the practitioners were **practical**[IMPROV-1] in the approach. This was coded as such. The context of this can be explained as follows: in order to be responsive to monitoring system access and use, and at the same time being efficient with the use of resources, the organization carried out periodic and at times spontaneous log files reviews in a practical manner. The log review exemplified the information security tenets of confidentiality, integrity and availability. It was established that the practitioners did not have any specific rigid method for following the tenets yet they were practical and managed successfully to monitor reports and comply with information security policies. The researcher interpreted this to mean that *collective improvisation*[IMPROV-1] was manifest. The reason for the success was because the information security practitioners and their peers were able to collectively extemporize the requirements (without prior preparation) while considering the tenets of information security. This data instance was coded as such. Extemporization and contriving the information security requirements as they were arising was established to be necessary.

Data Incident

In another data incident, it was noted that at times users did not follow procedures, as demonstrated by the following data incident:

"…everyday, I mean, it would actually be too easy if [users] followed procedure…" [60]

The context of this data incident was that the organisation had informally established four areas for monitoring: monitoring authorisation access, monitoring privileged operations, monitoring unauthorised attempts and monitoring system alerts. In this context, users were not following procedure when it came to accessing systems. They would log into systems using other users' passwords, or having concurrent log-ins and therefore invalidating the monitoring process. This made monitoring authorisation access difficult on the part of the practitioners. It was as a

[59] C5-Appendix 10
[60] C97-Appendix 10

result of this that at tactical level the practitioners had to **be inventive**[IMPROV-2] in formulating procedures and methods for checking and monitoring the users and the systems. The practitioners were faced with security alternatives/options which would be devised to ensure they kept tabs on who was doing what. It was how the practitioners managed those users that the researcher coded as *process improvisation*.[IMPROV-2.] The *improvisation* occurred when the practitioners minimised the incidents caused by users who were not following procedure.

Data incident

It terms of monitoring the other areas, namely monitoring privileged operations, monitoring unauthorised attempts and monitoring system alerts, that the practitioners were asked how they managed to do this. One practitioner responded as follows:

> *"By the application of pragmatic access policies, use of firewalls, message filtering, etc."*[61]

There was a general feeling that the monitoring process was not optimally conducted. This was exemplified by the following statement:

> *"…so there are those little things…that we do just to help us and to help the business…because it is those little things that…we need to do better…"* [62]

The context of this data incident was that reviewing logs required a considerable amount of time and resources. As explained earlier, the monitoring process was semi-automated and spontaneous. This meant that it was not optimal and the practitioners felt they needed to do things (monitoring) slightly better than they had been doing previously.

The researcher interpreted the words "*those little things*" as those makeshift activities that were contrived to make it possible for the monitoring process to function well. At operational level, those informal makeshift activities that were outside the radar of formality were conveniently done to improve on processes. Those kinds of activities were necessary to achieve their intended objectives, and were coded as **being novel**[IMPROV-3] in approach. Those "*little things*"

[61] Q48-Appendix 8
[62] C96-Appendix 10

exemplified thinking outside the box. This is what the researcher interpreted to constitute *process improvisation*[IMPROV-3].

2. Monitoring Application Usage

The **ISO IEC 17799 Section 9.7.2** defines the proper procedures and areas of risk when monitoring system/application use. The section calls for establishing procedures for monitoring use of information processing facilities. Such procedures, the section states are necessary to ensure that users are only performing activities that have been explicitly authorized. The **CobiT** objectives **Section DS3.8** talks of resource availability, and talks of procedures for monitoring application use through looking at availability requirements, fault tolerance, prioritisation and resource allocation, while **CobiT Section M 1.2** considers the assessing performance targets on a continuing basis. **ITIL Section 8.3** (*Service Delivery*), points to the proper manner of monitoring application use by considering the availability management process. The level of monitoring required for individual facilities should be determined by a risk assessment. Areas that are considered by this section include:

- authorized access
- all privileged operations, e.g. use of supervisor account;

Data incident

When interviewed, one of the information security practitioners suggested that they were flexible in the manner in which they used monitoring tools to monitor user activity particularly when monitoring different user profiles. Within the organisational setting, it was noted that users had different application needs. The difference in user needs required that users be granted different log-in profiles and privileges. This is exemplified by the following comment:

> *"…[In this organisation]… it's the way…the [monitoring] applications…and the people that use them [that] are a bit…different… so…[our] users are quite different from [say other's] users…because they've got different applications running on the servers…and they've got probably different ways of logging in…"* [63]

[63] C84-Appendix 10

It can be inferred from the above data incident that the organization required many different tools and techniques to monitor profiles and different applications. The context was that the practitioners at tactical level were using several packages (tools) that brought these disparate applications and types of information into one convergence. How they did this was very contextual to the applications in use, the profiles of the users, and the monitoring tools, such that the approach would have not been replicated elsewhere. It was this approach that the researcher coded as **being original**[IMPROV-4]. The context of using different monitoring applications provided for *process improvisation* [IMPROV-4].

3. Monitoring Processes and Application Integration

ISO IEC 17799 Section 9.7.2.2 is more specific on the monitoring process particularly when looking at application integration and the exposure to risk. It states that when considering risk, the results of the monitoring process need to be reviewed regularly. The **CobiT** objectives **Section M1.1** stipulates procedures for monitoring data benchmarks and the proprietary nature and integrity of data. **CobiT Section DS5.2** also suggests a manner for forecasting the workload of applications through capacity planning and trend analysis. **ITIL Section 4.2** (*Service Delivery*) has established mechanisms for capacity management, analysis, and the production of the capacity plan. The organisation was following **ISO IEC 17799 Section 9.7.2.2** recommendations and monitoring applications exposure to risk incidents as shown:

> *"Incidents are prioritised and "red flagged". The "red flag" incidents become part of the audit report with the required management response."*[64]

It should be noted that the frequency of the review depended on the risks involved. The following are some of the risk factors that the section proposes to be considered:

- the criticality of the application and integration processes;
- the extent of system interconnection and integration (particularly public networks).
- the value, sensitivity or criticality of the information involved;
- the past experience of system infiltration and misuse;

Data incident

[64] Q56-Appendix 8

The practitioners acknowledged that the difference and uniqueness between theirs and any other organization's monitoring process and how the monitoring was integrated or 'put together'. The following data incident shows this pragmatic consideration:

> *"…what they are trying to do, holistically in the [monitoring] process …it is all based on the criticality of the business processes, what's important and what's not…"* [65]

The context of the above data incident was that the practitioners had their own pragmatic and unique ways of creating monitoring solutions. Why this was necessary, as explained, was that previously the organization had deployed monitoring systems but then there was no one to look at the data logs. At strategic level, the organization realized that they were wasting a lot of money. To address this issue they designed a "*holistic monitoring process*" that would allow for regular or periodic review based on mission critical systems. The organization also assigned designated people to various monitoring processes, and determined how often this was to be done. This holistic solution was coded as **being <u>resourceful</u>**[IMPROV-5] and was seen as a form of *process improvisation*[IMPROV-5] that addressed what was important and what was not.

Data incident

One other data incident that seemed to corroborate the need for a *holistic monitoring solution* was exemplified by the following statement from one practitioner:

> *"…and we configured those [monitoring] things together and we come up with 'IBAS' which stands for integrated business architecture solutions…"* [66]

The context of this data incident is that the practitioners realized they needed to deploy an elaborate system that would gather data from various sources within departments and user profiles into convergence. From this converged silo, the monitoring system would generate reports to make the data useable and understandable. At strategic level, the result of this was (a product) they called the "*integrated business architecture solutions".* The researcher coded this way of using technology as **<u>being ingenious</u>**[IMPROV-6] as demonstrated by the manner in which the practitioners handled the monitoring process holistically. The novel action and thought

[65] C149-Appendix 10
[66] C75-Appendix 10

together, combined with the element of deciding what was and was not important enabled the creation of a product "*integrated business architecture solutions"* and was a form of *product improvisation*[IMPROV-6].

4. Monitoring Application Classification Guidelines

The **ISO IEC 17799 Section 9.7.2.2** points to the need for a comprehensive way of monitoring application classification. Applications are classified to indicate the need, priorities and degree of protection. The information held in these applications has varying degrees of sensitivity and criticality. The **CobiT** objectives **Section DS9.7** equally has established procedures for configuration management, critical components identified, classified and managed, while **CobiT Section M1.3** assesses the need to monitor satisfaction levels of customers while highlighting the shortfalls. **ITIL Section 7.11.1** (*Service Support*) gives procedures for the level of control while **Section 4.4.8** considers monitoring the applications for the purpose of understanding customer satisfaction and base classification guidelines for items that may require an additional level of protection or special handling.

Data incident

An information classification system should be used to define an appropriate set of protection levels and communicate the need for special handling measures. From the review of one data incident, it was confirmed that one practitioner was mandated to create an information classification system that would highlight the mission critical, tier 1 systems. This is evidenced by the following data incident:

> *"…I put a huge enterprise around that…I picked all the main applications and [classified] them on a spreadsheet…"* [67]

The context of this data incident was that this particular individual creatively designed a classification system that was colour coded to highlight the main applications (mission critical, tier 1 systems) that would be singled out for intense monitoring. The reason given for the need for this classification was that should the main tier 1 systems be exposed to incidents, then these had the potential to cause serious disruptions that would have a long term effect on

[67] C51-Appendix 10

operations. There was therefore a need to classify these systems. By analysing one specific data incident, it was discovered that the practitioners had their own **creative**[IMPROV-7] way of designing a classification system. By using colour codes for each system, with the stronger **red colour** for mission critical, tier 1 systems and the less important systems with **blue colour,** the individual improvised ways to determine appropriate levels for monitoring the organisation's applications at tactical level. The researcher interpreted this to imply *individual improvisation*[IMPROV-7].

5. Monitoring and Assessing Application Risk

The **ISO IEC 17799 Section 10.5.2** proposes the continuous reviewing and monitoring of applications in terms of any changes to these applications. The **CobiT** objectives **Section M1.4** suggests proper ways of management reporting for risk mitigation. **ITIL Section 4.5.1** (*Service Delivery*) highlights the need to define service level management which incorporates monitoring and reporting. **Section 4.4.9 of ITIL** recommends the need to define reporting and review procedures. **ISO IEC 17799 Section 10.5.2** provides guidelines for detailed technical reviews for periodic assessments to check on changes to applications and operating systems and covers some of the following:

- review of application control and integrity procedures to ensure that they have not been compromised by the operating system changes
- ensuring that notification of operating system changes is provided in time to allow appropriate reviews to take place before implementation;
- ensuring that appropriate changes are made to the business continuity plans

In order to understand how this ISRM activity was taking place, the researcher asked how the organisation determined and quantified information security risk relative to use and how risk was monitored. The information security practitioner to whom the question was directed stated that some of these efforts were rather technical and complex. The need to quantify information security was done procedurally by determining mission critical systems:

> *"Risk quantification is determined by the criticality of data on specific servers."*[68]

Data Incident

[68] Q57-Appendix 8

During the interview it was noticed that the risk assessment activity followed suggested guidelines that gave opportunity for those assessments to be contextualized. One security practitioner noted how they were assessing risk in out of warranty machines:

> *"…and also they must, like as you say, assess the risk. If the machine is out of warranty and it is a tier one application (critical application), and it is going to be down for some time…"* [69]

The context of this data incident was that the organisation had determined a criticality rating for the systems and application (machines) held. The criticality rating, i.e. determining tier 1 mission critical systems, was a useful metric since the organisation did not want to dedicate all its resources to just monitoring. An innovative and thoughtful way whereby the organisation made decisions on how to allocate time and money for monitoring and assessing risk was to balance controls with practitioner productivity. While ensuring they remained compliant with regulations, they designed at operational level, a spontaneous approach that could prioritise and allocate monitoring resources to critical applications when and where necessary. This approach was coded by the researcher to imply **lateral thinking**[IMPROV-8] and was interpreted as *process improvisation*[IMPROV-8] since the need to assess risk against a critical tier one application was extemporaneous and would occur on a more improvised fashion than controlled fashion.

Data Incident

This capability of understanding criticality of application was also demonstrated by analysing another data incident. The researcher asked one information security practitioner how they ensured they continued to learn and gain the necessary skills and capabilities in order to continue addressing information security risks adequately. It was explained that this was an operational activity that called for prioritising incidents, and of the reporting of these. The reports would then be studied in order to obtain a deeper understanding. The confidence placed by the information security practitioners in the assessment process was strengthened by the fact that the practitioners were equipped with sufficient knowledge, experience and right attitude towards the risk assessment processes.

> *"…I mean, our actions [are] based on the criticality of the application…obviously… experience plays a lot, if the heat comes from the*

[69] C115-Appendix 10

executives and that kind of thing ... we know which applications are critical and which [ones] are not…" [70]

The context of this data incident was that the information security practitioners were tasked to develop defensive (and at times offensive) strategies to protect and defend the organisation's information and information systems asset/applications. In order to do, this they had to demonstrate at strategic level that they had sufficient experience and understanding of the systems/applications, the risks, the criticality of applications and how these systems are sensitive to compromise. That is why one practitioners stated, "*our actions [are] based on the criticality of the application".* The researcher coded this incident as an expression of **being practical**[IMPROV-9] based on experience and understanding. The researcher interpreted the contextual determination of the 'right risk' appetite based on understanding and experience as reflecting some degree of *process improvisation*[IMPROV-9].

6. Exceptional Reporting

The **ISO IEC 17799 Section 12.2.2** proposes a guideline for technical compliance checking and for the generation of reports for interpretation by specialists. The need for regular checking and reporting of information systems is of importance particularly in ensuring compliance with information security standards. The **CobiT** objectives **Section M2.4** suggests a manner for internal control level reporting where exception reporting and guidelines for reporting needs analysis is given. **ITIL Section 4.4.5** (*ICT Infrastructure Management*) suggests proper ways of managing and controlling all aspects of ICT operational security.

The researcher needed to know how the exceptional reports were being generated. One information security practitioner was asked how the organisation assured itself that the reporting procedures for security incidents were correctly followed and the exceptional reports correctly captured. The practitioner explained to the researcher the procedure for reporting as follows:

"Formal reports have to be forwarded to the IT leadership team and a Risk Matrix is maintained and included in the Monthly Board report."[71]

[70] C144-Appendix 10
[71] Q51-Appendix 8

When the same practitioner was asked how the organisation ensured that it had studied and learnt from the exceptional reports, it was noted that the organisation regularly studied the reports:

> *"By regular security review [of report]…"*[72]

Data Incident

The analysis of the data incidents revealed that the process of exceptional reporting was manually performed at operational level, and that the reports highlighted instances when hardware and software controls were not correctly been implemented. Exceptional reporting was shown to be taking place as suggested by the following data incident:

> *"…so [name withheld] run certain exception reports and actually reported the behavior…"* [73]

The context of this exceptional reporting within the organization was that the organisation had set up a mechanism for all users to be responsible for recognizing unusual or suspicious activity in systems, e.g. reporting on slow networks, bouncing e-mails with error messages etc. From the data incident above, it shows that one practitioner was dedicated to responding to incidents. At tactical level, this was the practitioner who was notified of any incidents that occurred (by reviewing reports) and who fostered pragmatic, creative solutions. It was this pragmatic, creative way of handling the responses that was most interesting to the researcher. The solutions provided from the interpretation of these reports by the information security practitioners often involved the need to be **rational adaptive**[IMPROV-10]. Using skills and experience of understanding the risks involved, the interpretations and the solutions thereof would be interpreted by the researcher to constitute grounds for *individual improvisation*[IMPROV-10] to occur.

7. Monitoring Operational Procedures and Responsibilities

[72] Q52-Appendix 8
[73] C6-Appendix 10

The **ISO IEC 17799 Section 8.1** highlights the need for responsibilities and procedures concerning the management and operation of all information processing facilities. The **CobiT** objectives **Section M 2.4** suggests the need for monitoring operational information security and internal control assurance through self assessments, independent audits, and identifying vulnerabilities and information security problems. **ITIL Section 4.2** (*Security Management*) gives direction on how to implement these measures. Development of appropriate operating instructions and incident response procedures are needed to monitor operations and check for incidents. **ISO IEC 17799 Section 8.1.3** pays specific attention to incident management responsibilities and procedures. It emphasises the need for procedures to be established to ensure quick, effective and orderly response to information security incidents. **ISO IEC 17799 Section 8.1.3** places emphasis on the following controls over information security incidents:

- information system failures and loss of service;
- errors resulting from incomplete or inaccurate business data;

In order to obtain a deeper conceptualisation of how monitoring operational procedures were carried out, it was necessary for the researcher to ask how the organisation monitored its security incidents. It was explained by one information security practitioner as follows:

> *"This is done by means of both internal and external monitoring of both data access and network activity. Internet usage is also very closely monitored and measured."*[74]

Data incident

Data analysis revealed that the monitoring activities were operational level activities that were meant to safeguard the loss of service deemed critical to the organization. All necessary measures were taken to ensure that there were minimal disruptions. This was particularly true in the 'mobile environment' where users and practitioners used mobile enhanced technologies like laptops (notebooks) to help the function. This is exemplified by statements from the following interviewee:

> *"…I mean, if a person has got a broken notebook, then they can't work…you see? So I mean they had to do something, and we've been trying to give them little injections with these notebooks to keep them going…"* [75]

[74] Q47-Appendix 8

The context of this data incident was that the practitioners were battling with continuity of work and processes while being faced with limited resources. At operational level, the aspect of "*doing something*" constituted a reflexive manner of handling contingencies as they arose and acting on the spur-of–the-moment. The "*little injections*" was an expression coded as **being ingenuous**[IMPROV-11], and was seen as an important trait that assisted the practitioner to contextualize contingencies as they arose. The way "*they had to do something*" was coded as an example of *collective improvisation*[IMPROV-11] to ensure continuity of services.

8. Monitoring Equipment Placement and Protection

The **ISO IEC 17799 Section 7.2.1** highlights the need to monitor and protect equipment from risks and environmental threats and also from the risk of opportunities for unauthorized access. The **CobiT** objectives **Section M2.1** gives provision for the monitoring of internal controls, and suggests procedures for comparisons, reconciliations, deviation analysis, corrective action reporting and communication. **ITIL Section 4.6.2** (*ICT Infrastructure Management*), suggest the tools to be used i.e. scheduling tools for workload and resilience testing. **ISO IEC 17799 Section 7.2.1** suggests some of the following controls measures:

- Equipment should be sited to minimize unnecessary access into work areas.
- Information processing and storage facilities handling sensitive data should be positioned to reduce the risk of overlooking during their use.
- Items requiring special protection should be isolated to reduce the general level of protection required.
- Controls should be adopted to minimize the risk of potential threats including theft, fire, etc.

The **ISO IEC 17799 Section 7.2.1** as implemented by the organization under study seems to have been constrained by resource limitations.

Data incident

[75] C106-Appendix 10

The problem expressed by one interviewee about security and equipment protections was the costs involved vis-à-vis the inherent risk to the equipment. No solution was previously found which enabled the quantification of the risk against the value and cost of its protection. This was done in an ad hoc fashion as the equipment kept coming. Evident from the interview was the apprehension about costs and budgets for this. This is demonstrated as follows:

> *"…Which increases the admin side which increases everything else, but in the long run it is probably [felt] it is the right thing to do…"* [76]

The context of this data incident was that practitioners were conscious of the cost element vis-à-vis information risk and productivity. At tactical level, it was the balancing of these needs at operational level that the information security practitioners were interpreted to have been **rational adaptive**[IMPROV-12] about equipment protection. Equipment protection was pragmatic and based on costs, productivity, risk and criticality of operations. The approach towards equipment protection as analyzed from the data incidents was interpreted as a form of *process improvisation*[IMPROV-12]. This interpretation was based on the understanding that equipment protection was based on budget constraints. The fact that financial resources were a consideration to this pragmatism was expressed as follows:

> *"…well… what you see…what happens is that it is all about saving money…"* [77]

Data incident

Financial constraints were singled out as significantly influencing the approach towards compliance efforts. At tactical level, the practitioners adopted informal ways to comply with the frameworks as revealed by the following statement from one interview:

> *"… I mean some of them…these people have got…notebooks that have got a mouse [attached to] it and they've got a keyboard [attached to] it…and they've got this [whole thing] attached to a monitor…because they don't have a PC…"* [78]

An interesting insight revealed by the above data incident signifies the unique way the practitioners and users dealt with the challenging circumstances. The practitioners found use for discarded notebooks even though these were not working because of missing components.

[76] C122-Appendix 10
[77] C104-Appendix 10
[78] C107-Appendix 10

"…because the monitor (computer screen) is not working…the mouse isn't working...and the keyboard isn't working…" [79]

The information security practitioners **became creative**[IMPROV-13] by suggesting extemporaneously that the laptops and PCs be modified in new ways i.e. using working parts of each (integrating the two products). The researcher interpreted this data incident to be an expression of *product improvisation*[IMPROV-13.]

Summary of the Fourth Unit of Analysis

Table 26 summaries the total number of **conceptual instance** in the previous narrative for this unit as follows:

Table 26. Conceptual density of Improvisation when examining Event Monitoring

Units of Analysis Activities related to;	Core Categories	Concepts generated within the types of improvisation				Conceptual Density
		Collective Improvisation	Individual Improvisation	Process Improvisation	Product Improvisation	
Event Monitoring	**Strategic**			*Being resourceful*[IMPROV-5] *Being practical*[IMPROV-9]	*Being ingenious* [IMPROV-6]	3
	Tactical		*Being creative*[IMPROV-7] *Rational adaptive*[IMPROV-10]	*Being inventive*[IMPROV-2] *Being original*[IMPROV-4] *Rational adaptive*[IMPROV-12] *Being creative*[IMPROV-13]		6
	Operational	*Being practical*[IMPROV-1] *Being ingenuous*[IMPROV-11]		*Being novel*[IMPROV-3] *Lateral thinking*[IMPROV-8]		4

6.2.5 Analysis – IT Governance and Regulatory Compliance

Section 2.4.2 of this research dealt with issues regarding this unit of analysis. The following section conceptualizes *improvisation* within activities that relate to IT Governance and Regulatory Compliance. Conceptualizing *improvisation* in this unit followed the 6 steps listed in **Section 6.1.** This is demonstrated by **Table 27** as follows:

[79] C108-Appendix 10

Table 27. Open Coding for IT Governance and Regulatory Compliance **(*Extract of Appendix 6)***

STEP 1 **Data Incidents** **(Transcribed Interviews)**	**STEP 2** **Context of Data Incident** (Researcher's Memo)	**STEP 3** **Researcher's memos** Determine Codes in vivo and other generated as underlined)	**STEP 4** **Level**	**STEP 5** **Concepts generated (inductively)**	**STEP 6** **Types of Improvisation** (See Section 4.4.1)
yes and when I developed that spreadsheet and showed it to the management…it was [an eye opener]…I was like jeez… I mean it was like we were focusing on applications [that were not critical] [80] *so they actually have to adjust…I mean the big guys.. the executives… committee,…whatever…so we gave them all the facts and figures…all the notebook stuff* [81]	This was an instance when planning and action was occurring together in a synthesized 'real-time' strategy. The management liked the innovative ideas of the practitioner planner	***Technical Compliance Checking*** 1. Implies <u>inventiveness in planning and checking</u> measurement tools to achieve <u>compliant technology</u>	**Tactical** Activity	**<u>Being inventive</u>** in developing measurement tools	(Individual) improvisation
yes but …like I said…had we not adopted CobiT at the board level, we would have made it far more difficult [to implement], but … and the challenge being the audit report [82]	Prior to this, CobiT was the accepted and understood framework at board level, so an innovative way was proposed to use the same tool in IT security governance, which was done with minimal implementation challenges	***Compliance and System Audit Control*** 1. Implies <u>being inspired</u> to adopt CobiT tool and fit this with processes that ensures information compliance and <u>monitoring international standards</u>	**Strategic** Activity	**<u>Being inspired</u>** to ensure best compliance methods	(Product) improvisation

[80] C53-Appendix 10
[81] C109-Appendix 10
[82] C45-Appendix 10

The following were the data classifications as described in STEP 3 (2nd paragraph) and are derived from interview transcripts for this unit of analysis (***see Appendix 6).*** These classifications are listed as follows:

1. Technical Compliance Checking
2. Compliance and System Audit Control
3. Information Security Reviews
4. Compliance with Information Protection Legislation and IT Governance
5. Information Security Reviews of IT Application Systems
6. Review of Risk

Each of the above classification is explained in turn.

1. Technical Compliance Checking

The **ISO IEC 17799 Section 12.2.2** proposes a guideline for technical compliance checking to be carried out by specialists and authorised persons. The guidelines emphasises that technical compliance checks should only be carried out by, or under the supervision of, competent, authorized persons. The **CobiT** objectives **Section M.2** suggests procedures for technical compliance to take into account operational security and internal control assurance. **ITIL Section 4.2** (*ICT Infrastructure Management*) has provision for technical compliance which procedures for technical support and the processes that require technical support. The risk involved here is that non-specialists would either perform incorrect checks/procedures or focus the checks in the wrong areas.

Data incident

The interview revealed that at times at tactical level, the compliance checks were performed on non-critical applications as explained by one practitioner:

> *"…yes and when I developed that spreadsheet and showed it to the management, it was [an eye opener], I mean it was like we were focusing on applications [that were not critical]…"* [83]

[83] C53-Appendix 10

The context of this data incident was that practitioners were not balancing productivity with risk and were focusing resources on non-tier 1 mission critical systems. What seemed to have happened was that, by focusing on non critical applications, the practitioners were affording themselves little time to focus on the more critical items. One practitioner realized this and took it upon himself to devise a procedure that would remedy this. This practitioner designed a procedure whereby practitioners would now dedicate resources to critical applications. This act was coded as **being novel**[IMPROV-1.] It was the individual intervention and reasoning that enabled compliance. This was coded as *individual improvisation*[IMPROV-1] and is corroborated by the following data incident.

> *"…so they actually had to adjust. I mean, the executive committee, we gave them all the facts and figures…"*[84]

2. Compliance and System Audit Control

The **ISO IEC 17799 Section 12.2** points out the need for having appropriate audit tools to review information security policy and technical compliance. This section proposes that audits be performed against the appropriate information security policies and the technical platforms and information systems. The **CobiT** objectives **Section M3.2** suggests having compliance requirements and systems audits done by an independent party. **Section M3.1** gives guidelines for independent information security and internal control review by an accredited party. **ISO IEC 17799 Section 12.3.1** points to the audit requirements and activities involving checks on operational systems. It suggests that these activities be carefully planned and agreed upon to minimize the risk of disruptions to business processes. It proposes the following to be observed in the audits:

- Audit requirements should be agreed upon with appropriate management.
- The scope of the checks should be agreed upon and controlled.
- The checks should be limited to read-only access to software and data

Data incident

[84] C109-Appendix 10

In the interview, it was established that the information security practitioners had established a vision for adopting CobiT as a guiding control framework to assist in checking compliance requirements. At strategic level, the framework was familiar to the board and therefore rolling it down to operational level proved a small challenge and this helped avoid implementation problems. The idea of using CobiT was earlier **inspired**[IMPROV-2] by one practitioner and the decision to use this particular framework extensively across other operations was taken positively. As a strategic activity, CobiT would be implemented on a module by module basis where relevant. This was a form of *product improvisation* [IMPROV-2] and is illustrated by the comments of one practitioner:

> *"...yes but ...like I said...had we not adopted CobiT at the board level, we would have made it far more difficult [to implement], but ... and the challenge being the audit report..."* [85]

The implementation of CobiT was also revealed to have been an individual initiative by one particular practitioner. This particular practitioner was already aware of the strengths of this framework and wanted it rolled out extensively. The practitioner strategically devised a way of doing this without encountering great opposition. The way this was carried out demonstrated some level of **rational adaptation**[IMPROV-3] expressed as *individual improvisation*.[IMPROV-3]. Rational adaptation was interpreted to have been achieved from the onset, when the board adopted CobiT, and the practitioners were left to find relevant explanations for the rest of the user community for the reason CobiT was suitable, how it would be used and its effects. This argument is collaborated by the following data incident:

> *"...so in line with that approach, it was a good idea that the strategy that I was formulating made it so much easier to adopt [CobiT]..."* [86]

3. Information Security Reviews/Forums

The **CobiT** objectives **Section M3.3** suggests a manner for independent reviews and assurance of effectiveness of IT services through conducting routine independent checks of effectiveness. **ISO IEC 17799 Section 12.2.1** points to the need for having regular reviews which ensures the

[85] C45-Appendix 10
[86] C20-Appendix 10

organisation's compliance with information security policies and standards. The section proposes that the reviews should include:

- information systems;
- systems providers;
- owners of information and information assets;
- users of information systems; and
- management

ISO IEC Section 12.2.1 places the owners of information systems as carrying the responsibility for supporting regular reviews of the compliance of their systems with the appropriate information security policies, standards and any other information security requirements. In the interview process, it was established that there were forums mandated by management to ensure and review systems, users and even the methodologies being used. One such forum was the architecture forum (mentioned earlier) mandated to do such task as explained as follows:

> *"…so you've got a methodology, so basically all of the things that come out go through the architectural forum for scrutiny…"* [87]

Data incident

In order to obtain a deeper understanding of how the forums were operating, the researcher asked one practitioner how these forums assisted in promoting information security. It was explained that the forums would be used to set information security awareness through the use of "*balanced scorecards*".

> *"We ensure that we place security awareness on our balanced scorecard."*[88]

The researcher interpreted the above data incident to imply that the design and construction of balanced scorecards would involve some degree of contextual creativeness. At strategic level, the forum would engage **creatively** IMPROV-4 in the way it designed the scorecards to meet the set information security requirements which required understanding the security posture of the integrated performance measures (scorecards) and describing the performance measures

[87] C70-Appendix 10
[88] Q14-Appendix 8

currently in use (contextually). The sitting together and deliberating on these measures was constituted to also imply a degree of *collective improvisation* .[IMPROV-4]

4. Compliance with Information Protection Legislation and IT Governance

ISO IEC 17799 Section 12.1.1 suggests that the way an organisation should carry out compliance requirements with regard to information security policies and standards. It mentions this important need in order to help organisations avoid breaches of any criminal or civil law, statutory, regulatory or contractual obligations and of any information security requirements. The **CobiT** objectives **Section M 3.5** suggests an independent assurance of compliance with laws and regulatory requirements and contractual commitments through routine independent compliance checks. **ITIL Section 4.2** (*Security Management*) gives procedures for the need to have audits and evaluate information security reviews of IT systems. It should be noted that the design, operation, use and management of information systems may be subject to statutory, regulatory and contractual information security requirements. **ISO IEC Section 12.1.1** informs on specific controls and individual responsibilities to meet these requirements and mentions the need for organisations to document all relevant statutory, regulatory and contractual requirements for each information system.

Data incident

During the interview, it was noted that practitioners considered themselves to be well above average in terms of meeting compliance requirements. One practitioner stated:

> *"…in terms of how we…have been meeting certain compliance requirements in terms of ECT Act…"* [89]

The general feeling was that the practitioners were conscious of the need to comply with other relevant statutory ACTs as explained by one practitioner:

> *"…or any other critical ACT in line with all the information reporting and all this … do we all play…"* [90]

[89] C29-Appendix 10
[90] C30-Appendix 10

What was interesting was that although at strategic level the practitioners were aware of the compliance needs and requirements, they were not sure how these would apply in their contextual circumstances. So far, no situation had arisen yet to warrant the need to "test the Act" i.e. no one had as yet been prosecuted in order to test and see how the Act was understood and interpreted. Indeed this issue was highlighted by one practitioner as follows:

> *"…Yes, a lot of Acts have been…introduced… but…I don't think they have been tested yet….so we want to comply to the bare minimum…"* [91]

This was interpreted by the researcher to mean that the practitioners were **resourceful** IMPROV-5 in meeting regulatory requirements at the time. It was also interpreted that the decision to "*comply to the bare minimum*" was not arrived at single-handedly but was a collective effort of establishing a mechanism to comply to the bare minimum. As a form of strategic activity, the researcher interpreted the data incident to imply that the practitioners exhibited *collective improvisation*IMPROV-5.

Data incident

In a similar data incident, the practitioners knew of their responsibilities towards meeting compliance requirements:

> *"…but I still have a role to play in terms of compliance…"* [92]

The context of this data incident was that the practitioner was aware of the need for the organisation to remain in compliance with regulatory, statutory and contractual security requirements. It was, however, the mechanism to verify such compliance (at tactical level) that was interesting to the researcher. The practitioners had stated that they "*wanted to comply to the bare minimum".* In a sense they seemed to be **getting by**IMPROV-6 so long as no major non-compliance incidents were being highlighted in audits. This was coded as so.

One way of getting by was to look at some of the suggestions in the frameworks, methodologies and ACTs and to see how these would fit into the current organisational practices and activities. The manner in which this was done by practitioners required a deep

[91] C31-Appendix 10
[92] C35-Appendix 10

understanding of these requirements and contextually fitting these requirements into the organisation. This was coded as *collective improvisation* IMPROV-6

Data incident

In yet another data incident, the practitioner's impression of the CobiT framework and his interpretation thereof was as follows:

> *"…if you look at the CobiT core systems there are certain modules that relate to core requirements…"* [93]

> *"…Do you know CobiT processes? the 34 processes [in CobiT]? Once you adopt CobiT, there are certain levels of every process that you have to accept. There is high, low and medium…"* [94]

The context of this data incident was that the organisation had implemented CobiT at operational level. CobiT framework made provisions and guidelines that the organisation would follow to meet compliance requirements of its operations. At operational level, the practitioners had suggested that they were looking at and interpreting these requirements in CobiT selectively, although as it is suggest in the data incident, they were well aware of what CobiT stipulated. This was coded as **managing**IMPROV-7 compliance requirements. The practitioners had a creative way of managing their understanding of the business process security risks, the criticality of these processes, and the need to use specific guidelines to meet compliance requirements. It was the contextualisation of the risk based on the provisions of CobiT that the researcher interpreted to imply that the practitioners were *process improvising*IMPROV-7.

Data incident

In another data incident, one practitioner explained the implementation of the CobiT framework was a process that involved the understanding of contexts of the critically of the processes. At strategic level, the processes would be rated high, medium, or low depending on the contextual level of risk. This understanding was coded as **lateral thinking**IMPROV-8 and was interpreted to have occurred when the practitioners viewed the CobiT and other compliance frameworks as tools not to be applied rigidly but to apply flexibility to the changing of these

[93] C16-Appendix 10
[94] C40-Appendix 10

tools to fit contextual needs. This form of *product improvisation*[IMPROV-8] was explained as follows:

> *"…I think frameworks can be deceiving… we actually incorporate 3 frameworks…we incorporate the overall framework, to govern the enterprise architecture solution distribution which is basically the Zachman Framework…"* [95]

> *"…but if you look in the Zachman's framework and you go right down to….the system's design.. basically those three of the Zachman's Framework.. then there is the CobiT and ITIL… are the ones that come into play in governing mostly the IT… processes…uum.. so we have an over-encapsulating…methodology…which is the Zachman's Framework …"*[96]

The "*Zachman's framework"* (product) was the new tool to be used as an element of *tinkering* with CobiT. In this regard, CobiT was modified to reflect a new compliance/governance framework. This new product established a new way of compliance approach and was therefore coded as an *improvisation*.

Data incident

From the discussions held, what would not be overlooked was the important role that planning, implementation and compliance of CobiT played. The planning, implementation and compliance efforts manifested as practitioners' actions. The fused framework (*Zachman Framework*) made the process of managing framework implementation easier because of this contextualization and understanding. At operational level, it was important to understand that the positive appeal of the implementation process, where actions were conceived as events unfolded, served as impetus for future planning. The knowledge achieved was seen as an **ingenuous**[IMPROV-9] way of implementing the framework creatively; similarly, the fused framework that was contextually applied was interpreted as an expression of *product improvisation.*[IMPROV-9.]

> *"…In the Zachman framework, a fusion of ITIL, CobiT, the same principles are applied because there has to be an understanding of the business process for all the different areas…"* [97]

[95] C73-Appendix 10
[96] C74-Appendix 10
[97] C76-Appendix 10

5. Information Security Reviews of IT Application Systems

In terms of actual reviews of IT applications, **ISO IEC 17799 Section 3.1.2** points to the need for maintaining a review policy document that ensures reviews are carried out in accordance with defined processes. The **CobiT** objectives **Section DS5.5** suggests procedures for information security surveillance and the need for IT security administration and information security violation reports. **ITIL Section 4.2** (*Security Management*) gives procedures on the information security management measures to be implemented.

ISO IEC Section 3.1.2 proposes that the review process takes place in response to any changes affecting the basis of the original risk assessment, e.g. significant information security incidents, new vulnerabilities or changes to the organizational or technical infrastructure. The section proposes a schedule of review which considers:

- the policy's effectiveness, demonstrated by the nature, number and impact of recorded information security incidents;
- impact of controls on business efficiency;

During the interview process, it was revealed that by using frameworks for security controls, review not only made work easier for the practitioners but also motivated them and helped them improve in certain operational areas. The following data incident highlights this;

> *"…so it sort of made my job so much more easier, but now when I talk to them around these security components, you know immediately the guys want to go for higher…targets, higher maturity levels of (say 4)…"* [98]

The researcher interpreted the above data incident to imply that a degree of **creativity**[IMPROV-10] and extemporisation occurred when the practitioners' used the framework to simplify work load and also motivate fellow colleagues about the benefits vis-à-vis immediate job demands. This was achieved through the processes of dialogue and communication and was coded as *process improvisation* [IMPROV-10].

[98] C43-Appendix 10

Data incident

It was also noted in the interview that at tactical level, when the practitioners had properly **managed**[IMPROV-11] the implementation of CobiT maturity requirements, then the review process that followed provided a high degree of motivation. The researcher interpreted this to mean that the practitioners had realised set goals. This was possible since CobiT had been rolled out jointly with the help of users and practitioners. At tactical level, it was how the practitioner dealt with the users during the rolling out process that was seen and coded as c*ollective improvisation*[IMPROV-11] and this *improvisational* approach gave impetus to users to achieve even higher levels of optimal information security requirements. This was demonstrated by the following data incident:

> *"…yes it was a dream come true, the information security [maturity] levels of CobiT are brilliant. When you give a presentation and you say look here, if you have managed 3/4 of the requirements, maturity level number 4's [you are fine] …*[99]

Collective improvisation was demonstrated by how the implementation of the CobiT maturity requirements was redesigned to suit a particular approach which contextually fitted practitioners and users, one which was "*manageable and practicable"*[100]. This approach simultaneously helped realise set goals ("*dream come true*").

> *"…you certainly felt that you would attempt higher say 3 or 4… So it is manageable and practicable…"* [101]

6. Review of Information Security Risk

ISO IEC Section 7.1 proposes that the review process for risk by establishing secure areas of operations. The **CobiT** objectives **Section DS4.6** suggests a manner for testing the IT continuity plan through regular testing of risk and implementing an action plan. **ITIL Section 7.3**.4 (*Service Delivery*), IT Service Continuity Management, proposes an approach to minimise risk by operational management.

[99] C47-Appendix 10
[100] C48-Appendix 10
[101] C48-Appendix 10

It was established that the organisation had its own concerns about information security risk that stemmed from external threats. One practitioner noted:

> *"Most organisations are faced with constant hacking and intrusion attempts."*[102]

When one practitioner was questioned on how this particular organisation went about creating awareness of information security risk, the practitioner noted that there were formal procedures in place:

> *"A formal notification was done a year ago, "Security Awareness Week". This was done in the form of an internal competition with staff having to answer certain aspects of the policy."*[103]

From further analysis of other data incidents, the researcher realized that there were established beliefs that the frameworks being used needed to be contextualized to this organization and not any other. Meaning that even though there were similarities in the risk exposure, how risk was handled and reinterpreted would be different and contextual as shown by the following data incident:

> *"…Maybe our risk profile has got to be entirely different…from the CobiT one…maybe we have to re-look our risk profile too…right? maybe that area that CobiT say's is high…maybe low*[104]

The researcher interpreted this to mean that it was inevitable that there should have been a contextualisation of the CobiT implementation process. This re-thinking was coded as **rational adaptive**[IMPROV-12]. Contextualisation was seen as a response to the changing organisational requirements and called for the re-thinking of CobiT. This rethinking of CobiT differently to suit the immediate needs was what was seen as *product improvisation*[IMPROV-12]

> *"…and the irony is, and I've got to give them credit for it…they've (IT users) been doing a lot of work, but they've probably been focusing on the wrong way…"* [105]

[102] Q55-Appendix 8
[103] Q10-Appendix 8
[104] C55-Appendix 10
[105] C54-Appendix 10

This meant that there was a difference between what this practitioner was interpreting certain CobiT procedures to mean and what the other IT users interpreted the same CobiT procedures to mean. In this case it was felt that the users were interpreting CobiT wrongly and were focusing on the wrong aspects.

Summary of the Fifth Unit of Analysis

Table 28 summaries the total number of **conceptual instance** in the previous narrative for this unit as follows;

Table 28. Conceptual density of Improvisation when examining IT Governance and Regulatory Compliance

Units of Analysis Activities related to;	**Core Categories**	**Concepts generated within the types of improvisation**				**Conceptual Density**
		Collective Improvisation	**Individual Improvisation**	**Process Improvisation**	**Product Improvisation**	
Governance and Regulatory Compliance	**Strategic**	*Being inspired*[IMPROV-2] *Rational adaptive*[IMPROV-3] *Creative-ness*[IMPROV-4] *Resourceful*[IMPROV-5]			*Lateral thinking*[IMPROV-8] *Rational adaptive*[IMPROV-12]	6
	Tactical	*Getting by*[IMPROV-6] *Managing*[IMPROV-11]	*Being novel*[IMPROV-1.]			3
	Operational			*Managing*[IMPROV-7]	*Creativeness*[IMPROV-10] *Being ingenuous*[IMPROV-9]	3

6.2.6 Analysis – Disaster Recovery and Business Continuity

Section 2.4.2 of this research dealt with issues regarding this unit of analysis. The following section conceptualizes *improvisation* within activities that relate to Disaster Recovery and Business Continuity. Conceptualizing *improvisation* in this unit followed the 6 steps listed in **Section 6.1.** This is demonstrated by **Table 29** as follows;

Table 29. Disaster Recovery and Business Continuity ***(Extract of Appendix 7)***

STEP 1 **Data Incidents** **(Transcribed Interviews)**	**STEP 2** **Context of Data Incident** (Researcher's Memo)	**STEP 3** **Researcher's memos** Determine Codes in vivo and other generated as underlined)	**STEP 4** **Level**	**STEP 5** **Concepts generated (inductively)**	**STEP 6** **Types of Improvisation** (See Section 4.4.1)
to give to the people …that they gave…and got the ones that [were] broken…they had to think quick...and make that kind of a judgment… [106]	Practitioners were initially not thought of as being rational when they re-issued old laptops to ensure processes continued to run; no one could predict that their quick judgment would later prove useful	***Business Continuity management Process*** 1. Implies being quick-witted in unpredictable, unexpected circumstances in information decision making	**Strategic** Activity	**Being quick-witted** in decision making	(Collective) improvisation
and it all boils down to budgeting.... now they didn't budgets for it … so they had to justify why…they had to do it… so that was the main kind of thing [107]	The efficient operation of Processes were hampered when laptops broke, creating need for extra resources. With limited resources, an innovative budget (justification) was generated	***Business Continuity Planning Framework*** 1. Implies being resourceful in ensuring business continuity and limited budgets over runs	**Operational** Activity	**Being resourceful** and ensuring business continuity	(Process) improvisation

[106] C103-Appendix 10
[107] C105-Appendix 10

The following were the data classifications as described in STEP 3 (2nd paragraph) and are derivatives of interview transcripts for this unit of analysis (***see Appendix 7)***. These classifications are listed as follows:

1. Business Continuity Planning Framework
2. Continuity on Critical Operations
3. Decision Making Procedures and Communication Arrangements
4. Disaster Scenarios and Critical Operations
5. Recovery Time Monitoring and Objectives

Each of the above classification is explained in turn.

1. Business Continuity Planning Framework

ISO IEC 17799 Section 11.1.1 considers the need for putting in place a managed process for developing and maintaining business continuity throughout the organization. The **CobiT** objectives **Section DS4.2** proposes the need to establish an IT continuity plan, a strategy and philosophy which aligns with the overall business continuity plan. **ITIL Section 7.3** (*Service Delivery*), the IT Service Continuity Management, postulates the need for a risk-based approach in the continuity of IT processes and services. **ISO IEC 17799 Section 11.1.1** proposes the following key elements of business continuity management:

Data incident

Data analysis revealed that the organisation had put in place a process for maintaining business continuity. The challenge to the process was that there was always an unanticipated event that resulted to making practitioners think extemporaneously and quickly. This thinking is illustrated in the following incident where for the sake of continuity the practitioners made collective judgment and was forced to issue old out of warranty lap-tops:

> *"…they had to think quick...and make that kind of a judgment…"* [108]

[108] C103-Appendix 10

The context of this data incident was that information security practitioners are constantly faced with emergent situations (fluctuations between normal and abnormal operating business conditions) that require judgement. It is from experience and skill that the types of judgement expressed by these practitioners display distinct emergent properties such as being quick-witted. This sort of data incident demonstrated **quick-wittedness**[IMPROV-1] and was interpreted by the researcher to imply *collective improvisation*.[IMPROV-1].

Data incident

During the interview it was realised that at operational level, a model suitable for **managing**[IMPROV-2] contingencies was created. This model (scenario planning model) categorised data, listed items of criticality and mapped these items to potential events that would cause interruptions. This was achieved by use of creative scenario analysis. The flexibility of scenario analysis created cognitive knowledge that would potentially be ideal for feedback, leaving practitioners open to determine innovative solutions. It was observed that one particular practitioner (in consultation with other practitioners) used the classification/categorisation model that focused on processes from a business recovery point of view innovatively. This is evidenced by the following data incident:

> *"…yes and [we] categorised those items… we specifically focused on [those items], particularly from a disaster recovery and also business continuity…"* [109]

The context of this data incident was that scenario planning was essential to determining business continuity and business recovery measures. The scenario plans however did not restrict the approach to creative solutions, and the practitioners were free to consciously expand their thinking to manage these activities. That was why the researcher coded managing as *collective improvisation*[IMPROV-2], collective because scenario planning and solutions were jointly determined.

Data incident

Devising plans and making decisions/judgments as situations arise (on the spur-of-the-moment) was exemplified at operational level, when activities required that new budgets be

[109] C52-Appendix 10

formulated. On the part of the practitioners, they had to be **resourceful**[IMPROV-3] in finding new ways of ensuring continuity.

> *"…now they didn't budget for it, so they had to justify why, they had to do it so that was the main kind of thing* [110]

The data incident notes that it was in hindsight that they were asked what they did and why they did so. *"…they had to justify why they had to do it".* This was interpreted by the researcher to be a situation whereby the practitioners had to justify an act of rapid inference to a situation that was affecting business processes forcing them to *process improvise.*[IMPROV-3] and become resourceful. It was coded as such.

2. Continuity on Critical Operations

ISO IEC 17799 Section 7.2 talks of the general information security of equipment/systems and the risks associated with these that impact on business continuity. The **CobiT** objectives **Section DS4.10** suggests the need for a framework that establishes critical IT resources which should be identified. Once identified, there should be a framework for user departmental alternative processing backup procedure in case of failure of these critical systems, through a continuity methodology. This is postulated in **CobiT Section DS4. ITIL Section 7.3** (*Service Delivery*), the IT Service Continuity Management, postulates the need for a risk-based approach in the continuity of IT processes and services. **ISO IEC 17799 Section 7.2.1** examines equipment security and proposes guidelines that mitigate or prevent loss, damage or compromise of assets and interruption to business activities. This section proposes the need for equipment to be physically protected from information security threats and environmental hazards. The need for protection of equipment (including that used off-site) is necessary to reduce the risk of unauthorized access to data and to protect against loss or damage.

Data incident

Discussions were made with practitioners to understand the business continuity measure taken by the organisation. One practitioner was of the opinion that the suggestions given by guidelines were important, but when there were gaps in these guidelines, they were left with

[110] C105-Appendix 10

little option but to draw on their experience and any other cognitive or physical resource available. In their words, "*they did what they had to do*" This was explained by one practitioner as follows:

> *"…I think our main thing here is to keep [going]… I mean we have a lot of good uses in policies when it comes to keeping the system going, certain time we do what we have to do to keep the [systems] going…and sometimes we don't…know if it is the right thing to do…"* [111]

The context of the data incident was that during emergencies, there were no clear guidelines to follow hence "*sometimes we don't…know if it is the right thing to do".* While following procedure would mean following what was set, *improvisation* would mean looking at procedure but re-creating new routines. In this case the practitioner showed that they acted outside of formal procedures. This was coded as being **rational adaptive**[IMPROV-4]. At tactical level, this sort of "doing whatever it takes" at the time constitutes *process improvisation*[IMPROV-4]. Earlier discussions of *improvisation* in **Chapter 2** revealed the salient differences between *improvisation* and following structure and procedure.

3. Decision Making Procedures and Communication Arrangements

The **ISO IEC 17799 Section 11.1.1**, part b) requires making on-the-spot decisions and understanding the impact interruptions to business processes are likely to have on the business including making quick decisions that provide solutions to handle smaller incidents, as well as serious incidents that could threaten the viability of the organization. The **CobiT** objectives **Section DS4.13** suggests the need to have "wrap-up" procedures which entail assessing adequacy of plans and planning updates. **CobiT Section DS4.11** takes cognisance of the need for decision making on back-up site and hardware, while identifying contracts for service provision. **ITIL Section 7.3.4** (*Service Delivery*), IT Service Continuity Management, stipulates procedures for operational management in continuity of operations.

Data incident

There was an instance where the speed of a system was noted as an issue.

[111] C124-Appendix 10

"…Well… it is kind of working at the moment, it is just that it is a bit slow, at the moment… [we shouldn't do anything]…" [112]

The context of this data incident was that slow systems were affecting output and productivity. This means at operational level, on-the-spot decisions were to be made about systems and productivity. The researcher was more interested in the intervention mechanism (on-the-spot decision) that illustrated how the slow systems were addressed. It was observed that the practitioners were less concerned since "*it is kind of working at the moment* ". This data incident was coded as **getting by**[IMPROV-5]. It should be noted that at the heart of *improvisation* is expressive individuality. This knowledge grows through interaction with systems. The functioning of the systems provokes responses. The responses could be active or passive but they remain responses. It was interpreted that the practitioners responded to the slow systems (passively but) in a way that balanced productivity with resource issues and risk. At expressive individual level this balancing was coded as *individual improvisation*[IMPROV-5].

Data incident

One data incident revealed how information security practitioners were open about certain decisions they had made. At tactical level, they were open to the idea that judgments/decisions made at the time could be wrong. This is evidenced as follows:

"…maybe we should actually do this in a different way… [113]

The context of this data incident was that the practitioners were contextually aware of the ripple effect of their decisions. It is this awareness and re-thinking that was coded as **rational adaptive**[IMPROV-6]. Being rational adaptive was influenced by the practitioners' internalised unconscious understanding of the processes around them. "*We*" being the most critical component of the aspect. This incident was coded as *collective improvisation*[IMPROV-6].

Data incident

[112] C129-Appendix 10
[113] C131-Appendix 10

It was revealed that during crisis events, the practitioners' ability to react correctly was influenced by time and resource pressures. This is evidenced as follows:

> *"…so those kinds of things are hard to [do], because…they are under a lot of pressure at the time…"* [114]

The context of this data incident is that practitioners must be responsive to emergent situations irrespective of any internal or external pressures faced at the time. It should be noted that at operational level, the decisions being made under pressures like these are recognised as highly cognitive and reflexive, often drawing on past experiences in order to do certain "*things that are hard*". The act of doing these under pressure was coded as **exceptionality**[IMPROV-7]. This exceptionality would affect business processes and would be based on contextual understanding of contingencies. This was coded as *process improvisation*[IMPROV-7.]

Data incident

ISO IEC 17799 Section 11.1.1, part (a) proposes the understanding of risks the organization is facing in terms of their likelihood and impact, including an identification and prioritization mechanism on which future plans are based. This understanding to which planning is based is draws heavily on past experience, as explained in the following comment:

> *"…I mean…a lot of it is in based on experience, and just knowing what is important and what's not, we sit…and we put together our plan…for next year …"* [115]

This understanding and planning process at strategic level was interpreted as **lateral thinking**[IMPROV-8] in risk management and planning for continuity. The data incident was coded for *collective improvisation*[*IMPROV-8*] since the practitioners were seen as jointly/collectively "*putting together plans*".

4. Disaster Scenarios and Critical Operations

[114] C132-Appendix 10
[115] C145-Appendix 10

ISO IEC 17799 Section 11.1.4 provides guidelines for a clear framework to deal with emergencies and to develop emergency procedures, manual fallback plans and resumption plans which should be within the responsibility of the owners of the appropriate business resources or processes involved. The section calls for fallback arrangements for alternative technical services, such as information processing and communications facilities.

Data incident

The interviews revealed that sometimes without fallback plans, decisions were arrived at on an *ad hoc* basis. During discussions, it was mentioned that the process of supporting continuity was subject to making quick decisions based on the event and criticality of operation. If critical systems went down on a weekend, remediation would be of utmost importance. Conversely if these were non-critical, this would justify delay till the next working week. This scenario was exemplified and explained by one practitioner as follows:

> *"…if we get a call on a Saturday…for something that is down, [we] don't worry, we will look at it on a Monday...since it is not a high level one...but if you get a call for something that you know is high level you will come in…"* [116]

In reality systems do go down from unanticipated causes and it is the decisions that follow that would normally be of interest. At operational level, decisions made quickly to discern if systems require immediate attention or not are necessary. In this instance, the practitioners demonstrated quick judgement and this was coded as **being quick witted**[IMPROV-9] and was seen as a form of *individual improvisation*[IMPROV-9]. The need for quick thinking is justified with emergent systems, crisis situation and contingencies which force systems to go down. The idea that systems do go down is a reality well understood by practitioners:

> *"…correct…something will always happen…"* [117]

5. Recovery Time Monitoring and Objectives

It should be noted that the **ISO IEC 17799 Section 11.1** considers aspects of business continuity management by proposing monitoring and planning for recovery time. The

[116] C147-Appendix 10
[117] C133-Appendix 10

section recommends the use of tools for monitoring business continuity and business recovery (recovery time) creating options and opportunities. The **CobiT** objectives **Section DS4.5** suggests a manner for monitoring and testing the IT and maintaining the IT continuity plan through change control to reflect changes in business requirements. **ITIL Section 5.7** (*The Business Perspective*) proposes understanding the business viewpoint and making business recovery efforts and business continuity based on the business viewpoint. **ISO IEC 17799 Section 11.1.5** proposes guidelines for creating business continuity plans and for the provision of a variety of techniques that are aimed at providing assurance that the plan(s) will operate in real life. These plans are continuously tested and monitored.

Data incident

During the interview, it was revealed that continuous monitoring for usage and also for business continuity was routinely done. One practitioner mentioned the following with regards to the use of monitoring tools:

> *"…they have monitoring tools monitoring the network, we have the monitoring tools monitoring Microsoft users, so we actually have two…we have the small…one and then we have the big one, called the Microsoft operations Manager (MsOM)…"* [118]

It should be noted that at operational level, using two (2) software technologies and applications for purposes of monitoring provided opportunities for spontaneity and flexibility. This sort of understanding is stated by the following comment:

> *"…The small one, we find is quite nice, and flexible, because it is quick and easy and it can monitor. Say you need something immediately, it can do it for you immediately, and then we can move it on to the other one, as an additional kind of monitoring, .in a different kind of way…"* [119]

In this instance, and at operational level, the data incident was coded as **being innovative**[-10.] This can be explained as follows. The organizational capacity to procure the two (2) tools/technologies and the individual practitioner's capacity to understand and utilise these tools was seen as innovative. This argument can be justified by the following comment by one practitioner:

[118] C91-Appendix 10
[119] C92-Appendix 10

"…well, we've always had both, it has always been the kind of thing that it's just easier, we actually use one to monitor, [and the other to] seek and give us a better clearer indication of the things that are up or down …"[120]

The statement needs to be understood in the context of *process improvisation*[IMPROV-10] whereby these practitioners applied two (2) tools and demonstrated the ability to be reflexive and innovative.

Summary of the Sixth Unit of Analysis

Table 30 summarises the total number of **conceptual instance** in the previous narrative for this unit as follows:

Table 30. Conceptual density of Improvisation when examining Disaster Recovery and Business Continuity

Units of Analysis Activities related to;	**Core Categories**	**Concepts generated within the types of improvisation**				**Conceptual Density**
		Collective Improvisation	**Individual Improvisation**	**Process Improvisation**	**Product Improvisation**	
Business Recovery and Business Continuity	**Strategic**	*Being quick-witted*[IMPROV-1] *Lateral thinking*[IMPROV-8],				2
	Tactical	*Rational adaptive*[IMPROV-6]		*Rational adaptive*[IMPROV-4]		2
	Operational	*Managing*[IMPROV-2]	*Being quick-witted*[IMPROV-9] *Getting by*[IMPROV-5]	*Being resourceful*[IMPROV-3] *Exceptionality*[IMPROV-7] *Being innovative*[IMPROV-10]		6

[120] C93-Appendix 10

6.3 COLLECTIVE SUMMARY OF ALL UNITS OF ANALYSIS

This section provides a summary of units of analysis and the data-sets examined in each unit. In total, a series of **54 concepts** (high level concepts) were generated that were interpreted to be *improvisational* (**See Table 31**) actions in ISRM. These concepts have been illustrated in narrative form in the previous sections of this chapter. Although some of these concepts look similar (share the same name attribute), these concepts were to be taken as being distinct and contextually different. This for instance means that a concept such as **rational adaption** appeared twice within the same unit of analysis. This was taken to mean that rational adaption could have occurred at, for example, an individual level (*individual improvisation*) or at collective level (process *improvisation*). An important point about *improvisation* here is that it is engaged by both individuals and collective groups. If the *improvisation* was coded as being at the individual level, this simply meant that key information security practitioners were at an individual level altering their roles to meet the heightened demands of the emergency. The converse would apply to *collective improvisation* although both were coded as **rational adaption.** **Table 31.** (next page) provides a summary of the conceptual instances (concepts) of improvisation. **Table 31.** shows, for instance, that there were more conceptual instances of concepts relating to *process improvisation* at Event Monitoring activities. Also *process improvisation* in general had the greatest number of conceptual instances (**23 in total**). This simply meant that **conceptual density** (number of conceptual instances) of *process improvisation* as opposed to any other type of *improvisation* was the greatest in the Event Monitoring activity. The researcher interpreted this kind of finding to mean that information security practitioners were short-circuiting or bypassing established procedures, frameworks and standards by *process improvising* Event Monitoring techniques as opposed to any other activity. **Table 31.** also shows that *collective improvisation* had the second highest number of conceptual instances (**19 in total**), thus interpreted to have had a lower conceptual density as opposed to *process improvisation. The researcher interpreted these findings to mean that* information security practitioners were collectively taking responsibility as teams for tasks over which they ordinarily had no immediate authority to perform and were bypassing broader norms, using makeshift tools or technology to flexibly perform their roles. The researcher wanted to confirm these by findings by also conducting an internal document analysis to find out why they were doing what they were doing. Discussion and interpretation of **Table 31** was done once document analysis was also finalised. These discussions are in **Section 7.8** (using **Table 45** *which is the same table in a different format*).

Table 31. Summary of Conceptual density of Improvisation

Units of Analysis Activities related to:	Level	Sub Categories				Conceptual Density
		Collective Improvisation	Individual Improvisation	Process Improvisation	Product Improvisation	
1 Information Assets Access and Data Control	**Strategic**	*Manipulating*[IMPROV-4]				1
	Tactical	*Quick reaction*[IMPROV-1]				1
	Operational	*Being deliberative*[IMPROV-3],		*Being resourceful*[IMPROV-2], *Being quick-witted*[IMPROV-5]		3
2 Information Security Architecture	**Strategic**	*Novel*[IMPROV-6],		*Exceptionality*[IMPROV-1],		2
	Tactical	*Rational adaptive*[IMPROV-4] *Deliberative*[IMPROV-5]				2
	Operational			*Rational adaptive*[IMPROV-2], *Lateral thinking*[IMPROV-3], *Being resourceful*[IMPROV-7]		3
3 Information Security Policies	**Strategic**	*Rational adaptive*[IMPROV-5]	*Lateral thinking*[IMPROV-3]			2
	Tactical			*Being* imaginative[IMPROV-2] *Being inventive* [IMPROV-6]	*Being ingenious*[IMPROV-1]	3
	Operational			*Being quick-witted*[IMPROV-4] *Being creative*[IMPROV-7]		2
4 Information Security Event Monitoring	**Strategic**			*Being resourceful*[IMPROV-5] *Being practical*[IMPROV-9]	*Being ingenious* [IMPROV-6]	3
	Tactical		*Being creative*[IMPROV-7] *Rational adaptive*[IMPROV-10]	*Being inventive*[IMPROV-2] *Being original*[IMPROV-4] *Rational adaptive*[IMPROV-12] *Being creative*[IMPROV-13]		6
	Operational	*Being practical*[IMPROV-1] *Being ingenuous*[IMPROV-11]		*Being novel*[IMPROV-3] *Lateral thinking*[IMPROV-8]		4
5 IT Governance and Regulatory Compliance	**Strategic**	*Being inspired*[IMPROV-2] *Rational adaptive*[IMPROV-3] *Creativeness*[IMPROV-4] *Resourceful*[IMPROV-5]			*Lateral thinking*[IMPROV-8] *Rational adaptive*[IMPROV-12]	6
	Tactical	*Getting by*[IMPROV-6] *Managing* [IMPROV-11]	*Being novel*[IMPROV-1.]			3
	Operational			*Managing*[IMPROV-7]	*Creativeness*[IMPROV-10] *Being ingenuous*[IMPROV-9]	3
6 Disaster Recovery and Business Continuity	**Strategic**	*Being quick-witted*[IMPROV-1] *Lateral thinking*[IMPROV-5]				2
	Tactical	*Rational adaptive*[IMPROV-6]		*Rational adaptive*[IMPROV-4]		2
	Operational	*Managing*[IMPROV-2]	*Being quick-witted*[IMPROV-9] *Getting by*[IMPROV-5]	*Being resourceful*[IMPROV-3] *Exceptionality*[IMPROV-7] *Being innovative*[IMPROV-10]		6
		19	*6*	*23*	*6*	***54***

6.4 CHAPTER SUMMARY AND CONCLUSION

Based on the selected case, this chapter has offered solid, internally valid evidence of *improvisation* in ISRM activities as demonstrated by *in-vivo* codes. This has been demonstrated in each of the units of analysis. *Improvisation* has been demonstrated to occur, i.e. to be more conceptually dense, in some units of analysis as opposed to others. Based on clearly defined parameters of analysis, this chapter has offered reliable ways of identifying *improvisation* concepts. The chapter has relied heavily on grounded theory techniques (open coding) as a preliminary basis for theory development. The data dictum that "all is data" guided the researcher in this chapter. This chapter shows that practitioners' engagement with information security was dependent on their perception of and attitude towards risk i.e. the risk appetite which was contextualized and at times improvised to suit circumstances. Additionally, this chapter used the data gathered from the interviews to develop a conceptual summary model as a basis for a preliminary theory of *improvisation* in ISRM. The data analysis chapter offers useful insights that have practical implications for helping to understand and develop future ISRM issues and agenda.

CHAPTER SEVEN

This analysis chapter is a development from **Chapter 6** and refines our knowledge of ISRM and the phenomenon of *improvisation* in relation to managerial issues. This chapter extends data analysis conducted in the previous chapter and introduces in-depth document analysis. Observation has also been documented in this chapter. As this chapter explains, documents were seen as being part and parcel of the research and are examined in detail. Finally, the chapter interprets and conceptualizes the summary of findings (**Chapter 6** and **7**) from all the units of analysis and presents a theoretical framework.

Table of Content
Chapter Seven

CHAPTER SEVEN: DOCUMENT ANALYSIS AND CONCEPTUALISATION OF IMPROVISATION IN ISRM

7.0 INTRODUCTION

It has been demonstrated in the previous chapter that as a *de facto* measure, frameworks are used only as guides and in fact ***improvisation does take place in ISRM***. This research accessed this "*reality*" through socially constructed means (information security practitioner's language, consciousness and shared meaning). The social construction of *improvisation* in its variety of forms/types was ***demonstrated on all the units of analysis*** conceptualised. This chapter grounds the researcher's interpretation of this *reality* by reviewing the organisation's internal documents (organisation policy) and interpreting why practitioners acted the way they did.

The chapter seeks to give a detailed interpretation of *improvisation* within the context of each unit of analysis and within the context of the organisation's **Corporate Information Security Policy (2007).** This chapter also documents observations from ISRM activities relating to Business Continuity and Recovery. The chapter begins by defining a series of steps that were followed in document analysis. What follows is a detailed examination of each unit of analysis using the *Sensitizing Device* developed in **Chapter 4.** This device was found to be useful in constant comparative analysis of functionalist and incremental approaches towards ISRM. The *Sensitizing Device* is contextualized for each unit of analysis. Finally from a summary of all the units of analysis, the chapter interprets and conceptualizes *improvisation* in ISRM. This interpretation is based on data analysis from **Chapter 6** and **Chapter 7** and a theoretical framework about *improvisation in ISRM* is drawn.

7.1 DOCUMENT ANALYSIS

Document analysis was a means by which this researcher elicited rich information that would determine the context for ISRM activities (and *improvisation*) identified by detailed data analysis. This was made possible courtesy of the organisation which made primary data available for the researcher in the form of documents. The primary data sources that were considered relevant to meet the objectives of this research were the **[name withheld]**

Corporate Information Security Policy (2007) (made available by the organization's Business Continuity Manager) CobiT, ITIL and ISO IEC 17799 frameworks.

The purpose of the document analysis was to compare interview data with stated policies and to find meaning for *improvisation* by understanding practitioner's own interpretations of their actions. The chapter analysis **Chapter 6** findings about *improvisation* in ISRM. This chapter is the researcher's own explanation and interpretation of what was done.

The following steps were followed in analysing the documents. It should be noted that for documentation purposes these steps have been listed in sequence. However, in the real sense these steps were iterative and went hand-in-hand with the **Data Analysis** (defined in **Chapter 6**).

7.1.1 STEP 1: Defining Relevant Documents in Use

The first step was to peruse the documents available on the organisation's intranet. The researcher wanted to stay within the scope of the research and so only picked out documents that would assist in the research. There were four documents that were found to be useful:

a) **[name withheld]** Corporate Information Security Policy (2007)
b) **[name withheld]** User Password and Confidentiality Policy (2007)
c) **[name withheld]** Policy on Disaster Recovery and Business Continuity (2007)
d) **[name withheld]** Policy on Protection and the Proper use of Information Assets (2007)

Out of these four documents, the researcher selected the first document for review since it was much broader and, moreover, incorporated aspects that related to the other policies. The researcher analysed the **Corporate Information Policy (2007)** document held in the intranet. The intranet also held other useful policies and guidelines for users in the IT department. Frameworks and standards including **CobiT**, **ITIL** and **ISO IEC 17799** were analysed and compared with **[name withheld]** Corporate Information Security Policy (2007). The only secondary source of documents comprised the researchers own memo's.

7.1.2 STEP 2: Ensuring Confidentiality by Documenting only Generic Aspects of Policy

The researcher had agreed to be confidential towards disclosing any material that would easily have been traced back to the organisation. Since the research was conducted with the promise of confidentiality, the researcher only extracted generic policy statements from the **[name withheld]** Corporate Information Security Policy (2007) that were also freely available in the public domain. These generic policy statements are also available on **CobiT, ITIL** and **ISO IEC 17799** frameworks and were selected since these could apply to any organisation that had a medium to large IT department.

7.1.3 STEP 3: Extracting Appropriate Data from the Documents

The researcher reviewed the **[name withheld]** Corporate Information Security Policy (2007) in cognisance with agreed confidentiality and extracted relevant but generic policy statement. The extraction took the form of **content analysis.** Using this approach entailed focusing on actual content of the **[name withheld]** Corporate Information Security Policy (2007). The researcher used **content analysis** to determine the presence of certain words and themes within this document. The researcher coded these selected words, phrases and themes into manageable categories as inputs to the *Sensitising Device.* The researcher then extracted selected classified words and put them in the *Sensitising Device* in an objective manner. This was done for each unit of analysis. Words, phrases and themes that did not serve any purpose to the *Sensitising Device* for each unit of analysis were omitted. This approach of categorising words or phrases into specific categories is known as **relational analysis.** The results are displayed in the *Sensitising Device* and these results were then used to make inferences about the messages inherent in the **[name withheld]** Corporate Information Security Policy (2007). These inferences have been incorporated in the subsequent statements and serve as foundations for understanding ISRM activities.

7.1.4 STEP 4: Constant Comparison, Interpretation and Conceptualisation of Improvisation in ISRM activities

In this step the researcher re-visited *improvisation* concepts derived from **Chapter 6** and ,made a list. These conceptual instances were then illustrated diagrammatically using graphs. This step should not be construed to indicate that this research was in any way quantitative. The graphical illustration was selected as the easiest representation of conceptual density of *improvisation* for each unit of analysis by a glance. The researcher then used the *Sensitising Device* derived in **Chapter 4** for each unit of analysis. The *Sensitising Device* was contextualised for each unit of analysis.

The *Sensitising Device* was useful in helping the researcher present and document the conceptualisation process. It became easy for the researcher then to start a comparison analysis between unit and unit, between primary data and also between the organisation's documents. That is why the *Sensitising Device* contains the following representative data elements:

a) Concepts generated from **data-sets** for each unit of analysis
b) Generic extracts of the **[name withheld]** Corporate Information Security Policy (2007)
c) Combined/Mapped ISO IEC 17799, CobiT and ITIL frameworks and Standards
d) The various typologies of *improvisation* for each unit and the conceptual density of *improvisation* for each unit.

Once a complete picture of the *Sensitising Device* was created for each unit, the researcher then proceeded to conceptualise and interpret conceptual density of *improvisation* for each unit and then finally for all the units combined. This final combination and interpretation is covered in the last section of this chapter. This section conceptualises *improvisation* in ISRM and has proposed a theoretical framework that is a documentation of this understanding. The following sections are a unit by unit analysis of *improvisation.* These sections follow the above outlined steps. It should be noted these steps were iterative rather than in sequence.

7.2 INFORMATION ASSETS ACCESS AND DATA CONTROL

The organisation was seen as setting context for the control of information assets based on the following extract of its Corporate Information Security Policy (2007):

> *"Information is an asset which has value to the organization and consequently must be protected. Owners must take steps to ensure appropriate controls are utilized in storing, handling distribution, and usage of information under their control. Custodians must protect the information assets in their possession from unauthorized access, alteration, destruction by using logical access control mechanisms."*
>
> **Source: Courtesy of [Name withheld] Corporate Information Security Policy (2007)**

The researcher discerned contextualisation of ISRM activities relating to information assets control with what was being stated in the above policy statement. The researcher's interpretation of *improvisation* was based on information security practitioners' belief in their own ability to perform specific tasks related to controlling information assets. Findings reveal that there were **3** conceptual instances of *collective improvisation* and **2** conceptual instances of *process improvisation* regarding control of information assets. These are listed as follows:

Collective improvisation

- Manipulating
- Quick reaction
- Being deliberative

Process improvisation

- Being resourceful
- Being Quick-witted

There was no conceptual instance of *individual* or *product improvisation* identified for this unit of analysis. **Figure 11.** gives a graphical illustration of this.

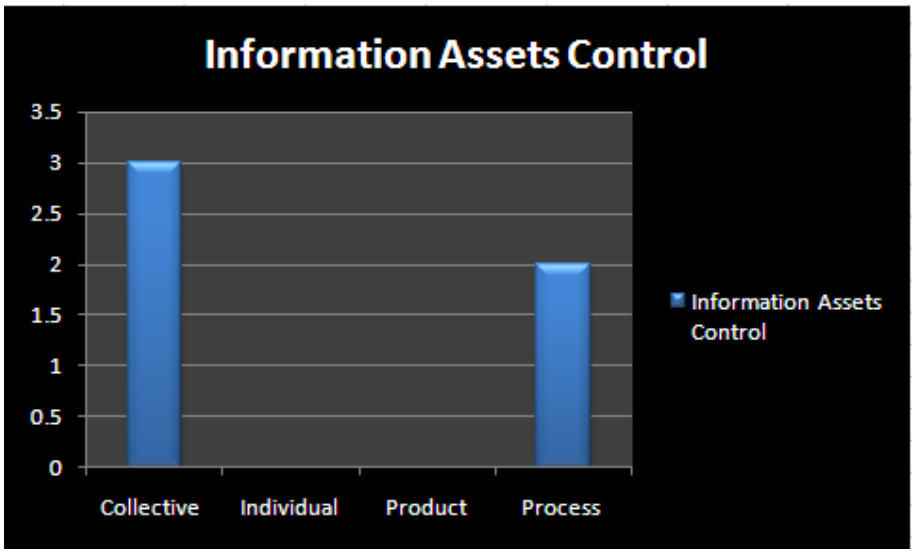


Figure 11. Conceptual Density of Improvisation in Information Assets Access and Data Control (Activities)

It can be discerned that the reason *collective improvisation* was conceptually dense for this activity was the inherent element of self-efficacy expressed and facilitated by quick reaction and being deliberative which in turn manifested as *improvisation*. Practitioners applied these attributes when engaging in ISRM activities related to information assets. These self-expressive attributes provided rich grounds for *improvisation* and were based on every practitioner's own predisposition to security around processes relating to information assets.

The manner in which information security practitioners as individuals exercised control over their thoughts and actions were *improvised* expressions of control. These expressions were noted as a progression and on-going confidence developed by practitioners as new knowledge reinforced previous knowledge about control (of information assets). **Table 32** (page 221) regarded as the *Sensitizing Device*, shows ***five (5) conceptual instances*** of *improvisation* noted by the researcher when conceptualizing this ISRM activity.

Table 32 (*Sensitizing Device*) can be interpreted as follows: the functionalist approaches to ISRM dictate formal procedures for the control of information assets as stated by **ISO IEC 17799. CobiT Section DS 5.9** suggests a mechanism for doing this. The organization's own corporate information security policy document states that "*owners must take steps to ensure appropriate controls are utilized in storing, handling distribution, and usage of information under their control*". What **Table 32** shows is that, although these mechanisms have been

suggested, there were ***5 conceptual instances*** where practitioners were using *improvisation* to by-pass these suggestions or were creative in applying these suggestions in ways that were not yet explicit. **Table 32** also qualifies these improvisational activities as having been performed within the contexts of these guidelines and frameworks. The two-direction arrows show that improvisational acts were drawn from what was already explicated in the literature and what was incremental.

7.2.6 Table 32. Sensitizing Device: Assessing Improvisation in Activities related to Information Assets Access and Data Control

STRUCTURED (FUNCTIONALIST) APPROACH					IMPROVISATION				INCREMENTAL APPROACH
UNIT OF ANALYSIS (EMBEDDED CASES)	**ISRM Functional Approach**				**Collective Improvisation**	**Individual Improvisation**	**Product Improvisation**	**Process Improvisation**	
	ISO 17799	**ITIL**	**CobiT**	**INTERNAL DOCUMENT ANALYSIS Organization's Guidelines**					
2. Information Asset Control	**5.1** Inventory of information assets **5.2** Information classification	**ITIL Section 4.2** (*Security Management*)	**Section DS5.9** gives a mechanism for centralised control of information assets	Information is an asset which has value to the organization and consequently must be protected Owners must take steps to ensure appropriate controls are utilized in storing, handling, distribution and usage of information under their control. Custodians must protect the information assets in their possession from unauthorized access, alteration and destruction by using logical access control mechanisms.	*1* ☑ *2* ☑ *3* ☑			*4* ☑ *5* ☑	

These improvisational acts were seen to be working within the boundaries of the corporate policies, CobiT, ITIL and ISO IEC 17799.

1. *Manipulating*
2. *Quick reaction*
3. *Being deliberative*
4. *Being resourceful*
5. *Being Quick-witted* ***(5 Conceptual instances See Figure 9)***

7.2.1 Understanding Information Assets Access and Data Control Using the Sensitising Device

Table 32 is best understood when considering the following statement from Cavusoglu (2004);

> "*The first rule of IT security is that [firms] should never spend more to protect something than a thing is actually worth*."

This means the responsibility of ensuring IT security by information security practitioners should be context specific. Specific descriptions of the **Table 32** frameworks (CobiT, ITIL, and ISO IEC 17799) as applied in context specific scenarios are amplified by **Table 33** below. **Table 33** prescribes specific measures as described by these frameworks when looking at the value of protection. The researcher interpreted the findings in this unit of analysis to mean that although the practitioners had the knowledge (prescriptive frameworks-**Table 33**), they nevertheless exhibited context specific *improvisation* tendencies when following these frameworks. The reason for this is understood when Cavusoglu's (2004); statement above is put into context. This it seems is what the practitioners did: they found mechanisms to contextualise and to be *resourceful*, *deliberative* and *quick-witted* for instance when finding the "*best way to implement information security management measures*" (**ITIL Section 4.2**). The understanding is also demonstrated by the findings of conceptual density of *improvisation* in information assets control shown in **Table 33** below. Information security practitioners therefore appropriately balanced information security assets control needs and the costs involved (financial or otherwise).

Table 33. Descriptive Frameworks for Information Assets Access Data Control and Improvisation

ISO IEC 17799	CobiT	ITIL	Description	Improvisation Concepts
	CobiT Section DS5.9		*The mechanism for centralised control and identification.*	
		ITIL Section 4.2 (*Security Management*)	*Best way to implement information security management measures.*	
ISO IEC 17799 Section			*Information assets classification system restricts access to*	

5.2.1			*information when deemed necessary*	
	CobiT Section DS5.3		*Procedures for security of online access to data through providing measures for access security control*	*1. Manipulating* *2. Quick reaction* *3. Being deliberative* *4. Being resourceful* *5. Being Quick-witted*
		ITIL Section 4.2.2 (*Security Management*)	*Guidelines on the implementation of security management measures*	
ISO IEC 17799 Section 4.1.4			*Authorisation process for information processing facilities*	
	CobiT Section DS5.6		*Determining user control, by creating designate user accounts (or group accounts)*	
		ITIL Section 4.1 (*Security Management*)	*Information security management measures for information control*	

Both **Table 32** and **Table 33** show that controlling information assets was a form of situated performance determined by the cognitive predisposition of what each practitioner understood in terms of the risk to the information asset and the level of confidentiality to be bestowed on this information asset. The fact that the guidelines were open to interpretation by the practitioners created an avenue whereby the practitioners were able to use their knowledge and common sense to determine classification and information control needs. The findings and interpretation of this unit used as a build-up to **Chapter 6** can be summarised as follows:

- The practitioners overcame the emergent difficulties and challenges of controlling information assets by trusting in their own ability to handle these challenges. The information security practitioners' capacity to contextually understand the immediate information assets control environment facilitated this e.g. by *improvisational* action.

7.3 INFORMATION SECURITY ARCHITECTURE

The organisation also established sound systems for designing architecture around information systems with information security in mind. The organisation's corporate information security policy (2007) statement set the context for the way the information security practitioners' reviewed information security architecture. The statement that follows describes this context:

> *"The level of protection required must be adequate and dependent on the value of information to the business and the risk of disclosure, loss or compromise. Information resources and supporting infrastructure are primarily for business purposes."*
>
> **Source: Courtesy of [Name withheld] Corporate Information Security Policy (2007)**

The researcher discerned from the interviews that time and resource constraints at operational level were one of the contextual reasons why practitioners expressed a degree of flexibility identified as *process improvisation. Collective improvisation* was also demonstrated when it came to designing optimal and secure information system architecture. The practitioners wanted to spend as little time as possible understanding each system's IT security requirements. A creative way around this was the identification and establishment of mission critical systems and the creation of a secure infrastructure around those systems. Mission critical systems were seen as those that would adversely affect business operations should anything interrupt these. The research findings show that *collective* and *process improvisation* were conceptually dense for this ISRM activity. From the discussions that took place with the information security practitioners, it was established that supporting infrastructure served specific business purposes (mission critical systems) and the architecture around these was modified, altered and re-designed.

The following concepts that were generated from discussions helped the researcher understand and interpret the conceptual density. Findings reveal that there were **3** conceptual instances of *collective improvisation* and **4** conceptual instances of *process improvisation* as follows:

Collective improvisation

- Novel
- Rational adaptive
- Deliberative

Process improvisation

- Exceptionality
- Rational adaptive
- Lateral thinking
- Being resourceful

Figure 12. gives a graphical illustration of this.

Figure 12. Conceptual Density of Improvisation in Information Security Architecture (Activities)

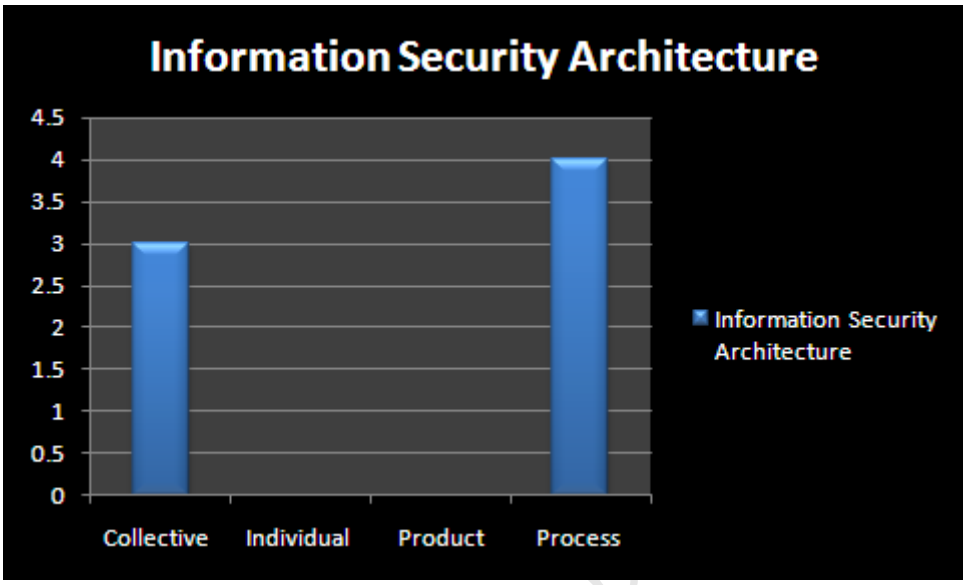


Figure 12. demonstrates that *collective* and *process improvisation* at operational level for this ISRM activity seem to have been dependent on a combination of organizational and personal factors which, when examined closely, explain the social-contextual and novel approach used (as the information system architecture and technology changed and emerged).

These *improvised* methods contextualized the organization's current and on-going architecture and supporting infrastructure for its security processes, information systems, and personnel. The need for this was the justification for aligning information security architecture with the organization's core goals and strategic direction. This ISRM activity was also interpreted to be socially constructed. As an illustration of this social construction, **CobiT Section AI 5.9** provides a **"**c*riterion that determines final acceptance of information systems"* criteria It should be noted that during the discussions held with the information security practitioners, it was established that the organisation's strategic goals were emergent, meaning the adaptation for supporting infrastructure and architecture was also flexible and contextualised. For instance, acceptance of information systems was based on predicting threats to systems analysing risks presented in the infrastructure. Practitioners' contextualised information architecture risk and the type of security threat underlying existing architecture

and re-modified this to account for appropriate countermeasures. Practitioners did not want to spend time on threats they did not understand. They contextualised risk to understand the consequences of threats and the "*final acceptance of the information system*" criteria. The proactive adaptation of these criteria was best illustrated by Table **34** (next page), the *Sensitizing Device*, which shows seven ***(7) conceptual instances*** of *improvisation* underlined in the CobiT, ITIL and ISO IEC 17799 framework.

Table 34 (*Sensitizing Device*) can be interpreted as follows: the functionalist approaches to ISRM dictate formal procedures for Activities related to Information Security Architecture as stated by **ISO IEC 17799**. **ISO IEC 17799 Section 12.1.1** suggests procedures management should follow in designing, operating and using information systems. **CobiT Section AI 5.13** suggests a mechanism for evaluation and meeting user requirements through post-implementation review. The organization's own corporate information security policy document states that "*The level of protection [of information] required must be adequate and dependent on the value of information to the business and the risk of disclosure, loss or compromise.*" What **Table 34** shows is that although these mechanisms have been suggested, there were ***7 conceptual instances*** where practitioners were using improvisation to by-pass these suggestions or were creative in applying these suggestions in ways that were not yet explicit. **Table 34** also qualifies these improvisational activities as having been performed within the contexts of these guidelines and frameworks. The two-direction arrows show that improvisational acts were drawn from what was already explicated in the literature and what was incremental.

7.3.6 Table 34. Sensitizing Device: Assessing Improvisation in Activities related to Information Security Architecture

STRUCTURED (FUNCTIONALIST) APPROACH					IMPROVISATION				INCREMENTAL APPROACH
UNIT OF ANALYSIS (EMBEDDED CASES)	**ISRM Functional Approach**				**Collective Improvisation**	**Individual Improvisation**	**Product Improvisation**	**Process Improvisation**	
	ISO 17799	**ITIL**	**CobiT**	**INTERNAL DOCUMENT ANALYSIS Organization's Guidelines**					
3. Information Architecture Security	**Section 12.1.1** management obligation to design, operate and use information systems **Section 4.1** Information security infrastructure	**ITIL Section 3.5.4** (*ICT Infrastructure Management*) gives direction on system deployment and acceptance **ICT Infrastructure Management, Design and Planning;** 2.4, 2,5 2.8, 4.3. 6.14,	**Section AI5.13** suggests a manner for evaluation and meeting user requirements through post-implementation review	The level of protection required must be adequate and dependent on the value of information to the business and on the risk of disclosure, loss or compromise. Information resources and supporting infrastructure are primarily for business purposes.	*1.* ☑ *2.* ☑ *3.* ☑			*4.* ☑ *5.* ☑ *6.* ☑ *7.* ☑	

These improvisational acts were seen to be working within the boundaries of the corporate policies, CobiT, ITIL and ISO IEC 17799.

5. *Novel*
6. *Rational adaptive*
7. *Deliberative*
8. *Exceptionality*
9. *Rational adaptive*
10. *Lateral thinking*
11. *Being resourceful* ***(7 Conceptual instances See Figure 10)***

7.3.1 Understanding Information Security Architecture Using the Sensitising Device

Table 34 (above) was the *Sensitizing device* that served as a lens to show the reason behind the contextualization of information systems configuration. The configuration, design and consequently the architecture of the information systems was based on the suggestions of the frameworks (CobiT, ITIL, ISO IEC 17799) shown on **Table 35** below. *Collective* and *process improvisation* (**Table 34**) was expressed, for instance, as *resourcefulness* and *lateral thinking* through the manner in which information security practitioners were able to meet users requirements. (**Table 35,** CobiT Section AI 5.3) in the following statement;

> *"…Maybe our risk profile has got to be entirely different…from CobiT …maybe we have to re-look our risk profile too…right? Maybe that area that CobiT says is high…maybe low* [121]

Table 35. Descriptive Frameworks for Information Security Architecture and Improvisation

ISO IEC 17799	CobiT	ITIL	Description	Improvisation Concepts
ISO IEC 17799 **Section 12.1.1**			*Management obligation to design, operate and use information systems*	*1.Novel* *2.Rational adaptive (collective)* *3.Deliberative* *4.Exceptionality* *5.Rational adaptive (process)* *6.Lateral thinking* *7.Being resourceful*
	CobiT Section AI5.13		*Manner for evaluation and meeting user requirements through post-implementation review*	
		ITIL Section 3.5.4 (*ICT Infrastructure Management*)	*Direction on system deployment and acceptance testing.*	
	CobiT Section AI5.9		*Criteria that determine final acceptance of a system through formal evaluations of system requirements and the approval of tests*	
		ITIL Section 9.6.3 (*Service Support*)	*Direction of release management procedure for system acceptance and testing*	
	CobiT Section		*Determines information security*	

[121] C55-Appendix 10

	AI5.10		*testing and accreditation, the need to understand the information security levels and the residual risk*	
ISO IEC 17799 **Section 8.2.2**			*Acceptance criteria for new information systems, upgrades and new versions should be established and suitable tests of the system carried out prior to acceptance.*	

From **Table 35** above, it can be seen that information security practitioners looked at the framework (CobiT, ITIL, ISO IEC 17799) from a pragmatic and contextual approach. This pragmatic approach helped them re-design information architecture and scrutinise designs before approval. This collective process was seen to be a popular, innovative and resourceful way of ensuring an optimal information security posture. The outcome was that the information architecture specifications developed were novel and context specific. For instance, it was mentioned in the discussion that information security practitioners would ask themselves important questions about what CobiT proposed. They also asked questions about the information security architecture around systems by considering the value of each information security control in relation to controls that already existed in place.

7.4 INFORMATION SECURITY POLICIES

One of the research activities conducted by the researcher was the review of the organisation's corporate information security policy. This was the document set the tone for establishing control and protection requirements for information assets. According to this organisation:

> *"Information security policy establishes procedures for the protection of information from a wide range of threats in order to ensure business continuity. The information security process links into and supports the business risk process and objectives."*
>
> **Source: Courtesy of [Name withheld] Corporate Information Security Policy (2007)**

The discussions revealed that at both tactical and strategic levels, it was not easy to predict or establish with certainty how the corporate policy was to be applied. This was because of the emergent environment and the changing systems requirements. The overarching guide was,

however, to do what was necessary to secure "*the protection of information from a wide range of threats*". Since it was also not possible to establish with a high degree of certainty what the threat sources/incidents would be or the kind they would manifest themselves as, a wide window of opportunity for *collective* and *process improvisation* at both tactical and operational level was opened. *Improvisation* was a necessary measure to ensure that work continued and, at the same time, risks and threats were kept in check; this meant there was co-ordination in the manner policy was followed and implemented. This sort of tactical activity was interpreted by the researcher as an expression of concepts such as being *imaginative* and being *ingenious*. Findings reveal that there was **1** conceptual instance of *collective improvisation,* **1** conceptual instance of *individual improvisation,* **1** conceptual instance of *product improvisation,* and **4** conceptual instances of *process improvisation* as follows:

Collective improvisation

- Rational adaptive

Individual improvisation

- Lateral thinking

Product improvisation

- Being ingenious

Process improvisation

- Being imaginative
- Being inventive
- Being quick-witted
- Being Creative

Figure 13. gives a graphical illustration of the above concepts.

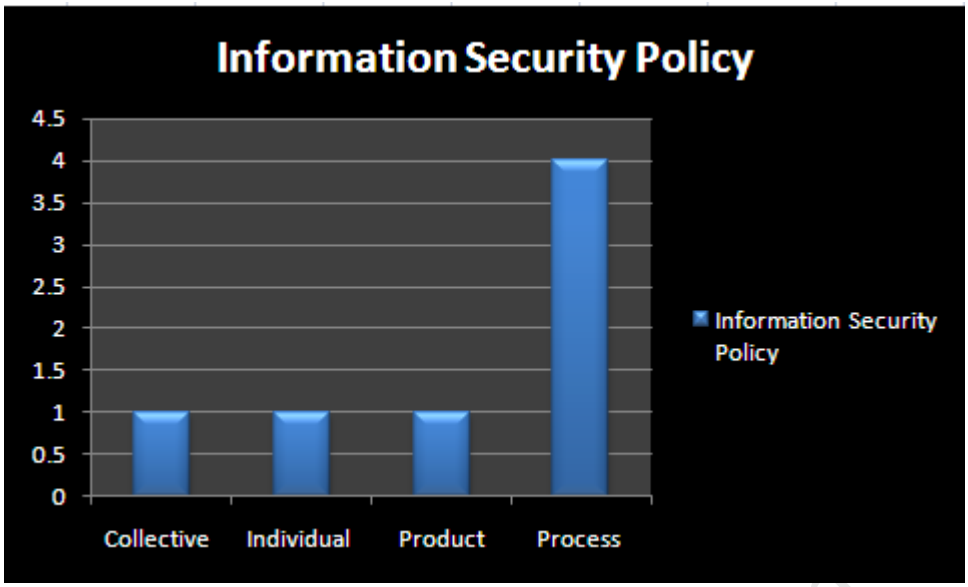


Figure 13. Improvisation in Information Security Policies (Activities)

From the discussions it was revealed that the emergent nature of computer security incidents and threats (considered undesirable phenomenon) and the way the practitioners followed policy to protect information systems against these incidents showed how policy acquired a different meaning. The way the information security practitioners applied policy was demonstrated effectively by how application of policy was occurring in the organization. This application is exemplified as follows:

> *"Due to certain design of our systems it becomes impractical to fully apply all our security policies particularly with regard to access to data. As a result hereof, full applications of the policies are not always fully supported."*[122]

The idea that resonates from this statement was interpreted by the researcher to mean that the support for policy would go as far it was contextually relevant and essential. The researcher saw this as a way in which information security practitioners subjectively understood their interaction with emergent technology, processes and new information systems. This interaction was based both within a set of formal guidelines such as the corporate information security policy, CobiT, ITIL, and ISO IEC 17799 while at the same time within the real-time composition of novel policy management and implementation processes. This was demonstrated as a form of *process improvisation*. By conceptualising the duality of how the information security practitioners functioned within a set of formal guidelines and also real-time composition (*improvisation*) for this ISRM activity, the researcher noted that it was the

[122] Q13-Appendix 8

"unknown" that provided avenues for collective acceptance of change and flexibility of information security policy thus yielding good grounds for *improvisation*.

According to this understanding, the duality of the ISRM activity can be taken into consideration as follows. On the one side, information security practitioners were faced with emergent "unknown" incidents and threat issues. These issues were produced both by internal threats (unpredictable users' behaviour) and external threats (hackers, viruses, worms) due to the nature of technology in the organisation. On the other hand, the practitioners devised mechanisms as stipulated by policy for protection against only those threats that were "predictable". Unknown threats left the information security practitioners to be *creative* and *imaginative* on how to apply policy. **Table 36** (next page), the *Sensitizing Device*, shows ***seven (7) of these conceptual instances*** of *improvisation* noted by the researcher when conceptualizing this ISRM activity.

Table 36 (*Sensitizing Device)* can be interpreted as follows: the functionalist approaches to ISRM dictate formal procedures for activities related to Information Security Policies as stated by **ISO IEC 17799. ISO IEC 17799 Section 4.1.2** suggests the need for an organization to have a cross-functional forum for the management of information security policy or its co-ordination. **CobiT Section AI 6.1** stipulates the various kinds of policies and procedures that guide management in terms of changes in control of information. The organization's own corporate information security policy document states that "*Information security should protect information from a wide range of threats in order to ensure business continuity.*" What **Table 36** shows is that, although these mechanisms have been suggested, there were ***7 conceptual instances*** where practitioners were ***using improvisation within these forums*** to collectively by-pass policies or creative avenues in which polices were contextualized. **Table 36** also qualifies these *improvisational* activities as having been performed within the contexts of these guidelines and frameworks. The two-direction arrows show that *improvisational* acts were drawn from what was already explicated in the literature and what was incremental.

7.4.6 Table 36. Sensitizing Device: Assessing Improvisation in Activities related to Information Security Policies

STRUCTURED (FUNCTIONALIST) APPROACH					IMPROVISATION				INCREMENTAL APPROACH
UNIT OF ANALYSIS (EMBEDDED CASES)	**ISRM Functional Approach**				**Collective Improvisation**	**Individual Improvisation**	**Product Improvisation**	**Process Improvisation**	
	ISO 17799 Sections	**ITIL**	**CobiT**	**INTERNAL DOCUMENT ANALYSIS Organization's Guidelines**					
1. Information Security policy	**Section 3.1** Information Security policy **Section 4.1.2** cross-functional forum of management for policy co-ordination	**Security Management;** *Fundamental of Information Security;* **Section 4.1** Control **Section4.2** (*Service Support*) change management suggests policies for change management	**DS 5** Ensure Systems Security **Section AI6.1** stipulates the policies and procedures that guide management in terms of changes in control of information	Information security protects information from a wide range of threats in order to ensure business continuity. The information security process links into and supports the business risk process and objectives.	*1* ☑	*2* ☑	*3* ☑	*4* ☑ *5* ☑ *6* ☑ *7* ☑	

These improvisational act were seen to be working within the boundaries of the corporate policies, CobiT, ITIL and ISO IEC 17799.

1. *Rational adaptive*
2. *Lateral thinking*
3. *Being ingenious*
4. *Being imaginative*
5. *Being inventive*
6. *Being quick-witted*
7. *Being Creative* ***(7 Conceptual instances See Figure 11)***

7.4.1 Understanding Information Security Policy Using the Sensitising Device

Table 36 is best understood when the subjective reasoning of the information security practitioners is put into context. It is the fusion of the dual nature of information security (following frameworks) based on predictive knowledge (**Chapter 3**, Section 3.1.1) and the emergent real-time composition of policy implementation based on the "unknown", which allowed the researcher to conceptualize and understand policy implementation. It was understood that this fusion was expressed as *collective improvisation*. It should be noted that frameworks provided a mechanism whereby practitioners would collaborate and work together; *"A cross-functional forum of management representatives"* (**Table 37**, ISO IEC 17799 **Section 4.1.2).**

This *improvisation* manifested information security practitioners' creativity and helped them to be rational adaptive to information security policy. The sense of collective responsibility helped create a synergy of contribution based on expertise and experience and, in this way, information security policy was easily disseminated to meet emergent information security requirements. **Table 37** (below) illustrates how one side of the duality (frameworks) describes what needed to be done and that other side shows how this was done (improvised concepts).

Table 37. Descriptive Frameworks for Information Security Policies and Improvisation

ISO IEC 17799	**CobiT**	**ITIL**	**Description**	**Improvisation Concepts**
ISO IEC 17799 **Section 4.1.2**			*A cross-functional forum of management representatives co-ordinate the implementation of information security controls*	*1.Rational adaptive* *2.Lateral thinking* *3.Being ingenious* *4.Being imaginative* *5.Being inventive* *6.Being quick-witted* *7.Being Creative*
	CobiT Section AI6.1		*Stipulates the policies and procedures that guide management in terms of changes in control of information with regard to system*	
		ITIL Section 4.2 (*Service Support*)	*suggests policies for change management*	
ISO IEC 17799 **Section**			*Employees of the organization should receive appropriate training*	

6.2.1			*and regular updates in organizational policies and procedures*	
	CobiT Section DS7.1		*Mechanism for identification of training needs, through a training curriculum for each group of employees*	
		ITIL Section 6.8 (*Service Support*)	*Establishes procedures for dealing with problems, through proactive problem management.*	
ISO IEC 17799 **Section 9.6.1**			*Guidelines for users of applications for information and application systems in accordance with defined access control policies*	
		ITIL Section 4.2.4(*Security Management*)	*The information security management measures to be taken on access controls.*	
		ITIL Section 7.9 (*Service Support*)	*Proper procedure for configuration management particularly with regards to relationships of information systems to other processes*	

What was observed and can be interpreted was that the information security practitioners' activities were a form of expression on the principle of continuous and reflexive transformation in the use, understanding and communicating guidelines to the users. The expressions were based on everyday meanings and common sense notions about information security requirements for specific systems in which the practitioners saw themselves as custodians. Understanding policy was more like problem-solving and at the same time *improvising.* The practitioners were seen to possess unique abilities to assess emergent changes in accordance to policy guidelines and act accordingly. This sort of unique, immediate, personal intervention was interpreted to constitute ground for *improvisation.*

7.5 INFORMATION SECURITY EVENT MONITORING

The research established that the organisation had set procedures for tracking malicious activities and threats to information systems across its organisational networks. It also established that the corporate information policy had created provisions for who were to be responsible for monitoring information systems. The corporate information security policy

therefore set the context for how information security event monitoring was to take place in the organisation:

> *"Custodians are responsible for establishing, monitoring Information systems consistent with standards issued by the information security office. Users must report all suspicious activities and security breaches to management and the Information Security Office"*
>
> **Source: Courtesy of [Name withheld] Corporate Information Security Policy (2007)**

It was noted that for this process-based ISRM activity, *process improvisation* was conceptually dense. From an information security practitioner's perspective, finding a good solution path for network monitoring was deemed a critical process activity. The research focused on how this monitoring was taking place. By revisiting **Section 6** of this thesis; it was observed that there was a higher degree of conceptual density for *process improvisation* for this ISRM activity at operational level.

The organisation had complex distributed software environments involving many processes and activities. The environments were faced with many kinds of events and information affecting these. The information security practitioner found rational adaptive ways of enabling the monitoring and quantification of the risk/threat to information systems particularly against the value and cost of protection. The practitioners were seen as resourceful and quick witted in the monitoring process.

> *"Incidents are prioritised and "red flagged". The "red flag" incidents become part of the audit report with the required management response."*[123]

> *"This is done by means of both internal and external monitoring of both data access and network activity. Internet usage is also very closely monitored and measured."*[124]

These expressions were seen as improvisation. Findings reveal that there were **2** conceptual instances of *collective improvisation*, **2** conceptual instances of *individual improvisation*, **1** conceptual instance of *product improvisation*, and **8** conceptual instances of *process improvisation* as follows:

Collective improvisation

- Being practical

[123] Q56-Appendix 8
[124] Q47-Appendix 8

- Being ingenuous

Individual improvisation

- Being creative
- Rational adaptive

Product improvisation

- Being ingenious

Process improvisation

- Being resourceful
- Being practical
- Being inventive
- Being original
- Rational adaptive
- Being creative
- Being novel
- Lateral thinking

Figure 14. gives a graphical illustration of the above concepts.

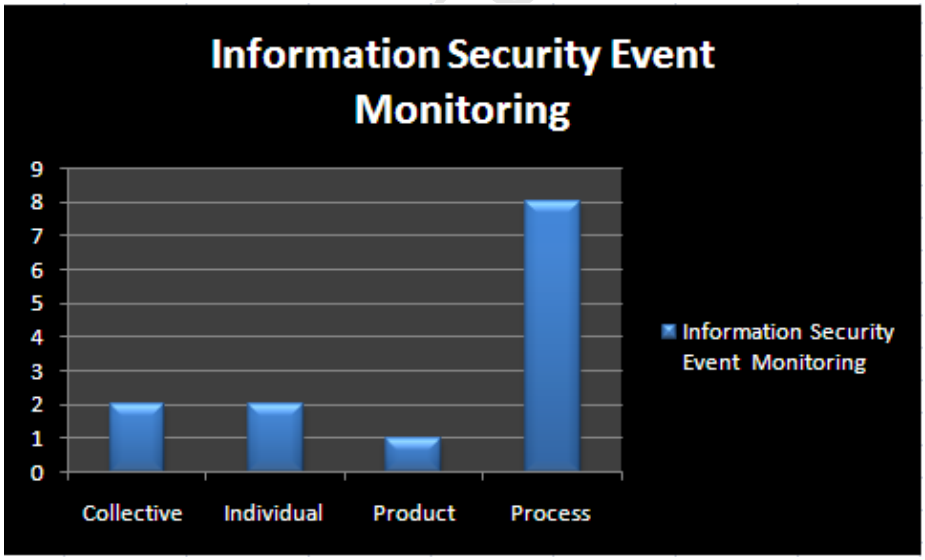


Figure 14. Improvisation in Information Security Event Monitoring (Activities)

It was observed that the best monitoring solutions were those that were context specific and driven by creativity that would mitigate risk. Since there probably was no single best solution, the number of solution paths to be taken given any monitoring process was limited, and this provided avenues for *improvisation* and hence the generation of the above concepts.

Table 38 (next page) the *Sensitizing Device*, shows ***thirteen (13) conceptual instances*** of *improvisation* noted by the researcher when conceptualizing this ISRM activity.

Table 38 *(Sensitizing Device)* can be interpreted as follows: the functionalist approaches to ISRM dictates formal procedures for activities related to Information Security Event Monitoring as stated by **ISO IEC 17799, CobiT and ITIL. ISO IEC 17799 Section 9.7** suggests the need for an organisation to put in place measures to monitor system access and use. **CobiT Section M 1.1** stipulates mechanisms an organisation may use for collecting monitoring data benchmarks, proprietary nature and integrity of data through looking at relevant performance indicators. The organization's own corporate information security policy document states that "*custodians [designated information security practitioners] are responsible for establishing, monitoring information systems consistent with standards issued by the information security office.*" What **Table 38** shows is that although these mechanisms have been suggested, there were ***13 conceptual instances*** where practitioners were using improvisation to by-pass these suggestions or were creative in applying these suggestions in ways that were not yet explicit. **Table 38** also qualifies these improvisational activities as having been performed within the contexts of these guidelines and frameworks. The two-direction arrows show that improvisational acts were drawn from what was already explicated in the literature and what was incremental.

7.5.4 Table 38. Sensitizing Device- Assessing Improvisation in Issues of Information Security Event Monitoring

STRUCTURED (FUNCTIONALIST) APPROACH					IMPROVISATION				INCREMENTAL APPROACH
UNIT OF ANALYSIS (EMBEDDED CASES)	**ISRM Functional Approach**				**Collective Improvisation**	**Individual Improvisation**	**Product Improvisation**	**Process Improvisation**	
	ISO 17799 Sections	**ITIL**	**CobiT**	**INTERNAL DOCUMENT ANALYSIS Organization's Guidelines**					
4 Security Event Monitoring	**Section 9.7** Monitoring system access and use	**Section 6.8** proactive problem solving and notes the importance of system monitoring in order to allow the effectiveness of controls adopted to be checked. **Service Level Management** *;* 4.4.8 Establish monitoring capabilities **Security Management Measures;** 6.8 Audit and Evaluate security reviews of IT systems	**Section M1.1** mechanism for collecting monitoring data benchmarks, proprietary nature and integrity of data through looking at relevant performance indicators **DS 10** Manage Problems and Incidents	Custodians are responsible for establishing, monitoring Info systems consistent with standards issued by the info security office Users must report all suspicious activities and security breaches to management and the Information Security Office.	*1* ☑ *2* ☑	*3* ☑ *4* ☑	*5* ☑	*6* ☑ *7* ☑ *8* ☑ *9* ☑ *10* ☑ *11* ☑ *12* ☑ *13* ☑	

These improvisational acts were seen to be working within the boundaries of the corporate policies, CobiT, ITIL and ISO IEC 17799.

1 Being practical *2 Being ingenuous*
3 Being creative *4 Rational adaptive*
5 Being ingenious *6 Being resourceful*
7 Being practical *8 Being inventive*
9 Being original *10 Rational adaptive*
11 Being creative *12 Being novel*
13 Lateral thinking ***(13 Conceptual instances See Figure 12)***

7.5.1 Understanding Information Security Event Monitoring Using the Sensitising Device

Table 38 can be looked at from an operational level. The information security practitioners were practical and original in the monitoring procedures. This was possible since the frameworks were open to interpretation and were left to the practitioners to come up with "*a mechanism for collecting monitoring data benchmarks"* (**Table 37**, **CobiT** Section **M1.1)**

Table 39 (below) which is an amplification of **Table 38**, shows suggested procedures for monitoring and the concepts generated from discussions that explained how the monitoring was done. This interesting insight reveals the way practitioners at process level used integrating monitoring tools creatively.

Table 39. Descriptive Frameworks for Information Security Event Monitoring and Improvisation

ISO IEC 17799	CobiT	ITIL	Description	Improvisation Concepts
ISO IEC 17799 **Section 9.7**			*issues guidelines for monitoring systems in order to detect deviation from access control policy*	*1 Being practical* *2 Being ingenuous* *3 Being creative* *4 Rational adaptive* *5 Being ingenious* *6 Being resourceful* *7 Being practical* *8 Being inventive* *9 Being original* *10 Rational adaptive* *11 Being creative* *12 Being novel* *13 Lateral thinking*
	CobiT Section M1.1		*suggests a mechanism for collecting monitoring data benchmarks, proprietary nature and integrity of data*	
		ITIL Section 6.8 (*Service Delivery*)	*proactive problem solving and the importance of system monitoring to allow the effectiveness of controls adopted to be checked*	
ISO IEC 17799 **Section 9.7.2**			*proper procedures and areas of risk when monitoring system/application use*	
	CobiT Section M1.2		*assessing performance targets on a continued basis*	
	CobiT Section DS3.8		*resources availability, and talks of procedures for monitoring application use through looking at availability requirements, fault*	

			tolerance	
		ITIL Section 8.3 (*Service Delivery*),	*proper manner of monitoring application use by considering the availability management process*	
	CobiT Section M1.3		*the need to monitor satisfaction levels of customers while highlighting on the shortfalls*	
		ITIL Section 4.4.8(*Service Support*)	*monitoring the applications for the purpose of understanding customer satisfaction*	
ISO IEC 17799 **Section 10.5.2**			*continuous reviewing and monitoring of applications in terms of any changes to these applications*	

The way the monitoring process as an operational activity was carried out revealed that the practitioners were *practical* while improvising. As part of the monitoring process, they had firmly established in their minds the information security tenets of confidentiality, integrity and availability of information as they performed the monitoring activities. There was bricolage with monitoring tools, with bricolage representing the capacity of the information security practitioners to tinker with the monitoring tools currently available within the organisation. In this manner, a group of monitoring tools were combined according to the needs of a specific context contributing to new ways of acting.

> *"…they have monitoring tools monitoring the network, we have the monitoring tools monitoring Microsoft users, so we actually have two…we have the small…one and then we have the big one, called the Microsoft operations Manager (MsOM)…"* [125]

> *"…The small one, we find is quite nice, and flexible, because it is quick and easy and it can monitor. Say you need something immediately, it can do it for you immediately, and then we can move it on to the other one, as an additional kind of monitoring, .in a different kind of way…"* [126]

The analysis of the above data by the researcher was interpreted to constitute *improvisation*. This was noted where the monitoring tools, the technology and the practices were re-interpreted by the information security practitioners.

[125] C91-Appendix 10
[126] C92-Appendix 10

7.6 IT GOVERNANCE AND REGULATORY COMPLIANCE

The research revealed that IT governance was championed by the organisation's executives and the board of directors. The executive fostered leadership and established organisational structures and processes which ensured that the organisation's IT facilitated strategies and business objectives. There were also measures taken by the organisation to ensure compliance with IT governance procedures and other external requirements as stipulated by the corporate information security policy as follows:

> *"The Internal Audit periodically performs compliance checks to make sure that information security requirements are consistently observed. Custodians are forbidden from changing the production information in their possession unless given explicit permission from the Owner or authorized User."*
>
> **Source: Courtesy of [Name withheld] Corporate Information**

The IT governance frameworks were seen to lack expressiveness and were detached from the practitioners. That was the reason the component of *improvisational* skill, inventiveness and the achievement of coherence enabled the practitioner to fix skill and experience into the IT governance mechanism i.e. to give IT governance a human feel. Findings reveal that there were **6** conceptual instances of *collective improvisation*, **1** conceptual instance of *individual improvisation*, **4** conceptual instances of *product improvisation*, and **1** conceptual instance of *process improvisation* as follows:

Collective Improvisation

- Being inspired
- Rational adaptive
- Being Creative
- Resourceful
- Getting by
- Managing

Individual Improvisation

- Being novel

Product Improvisation

- Lateral thinking

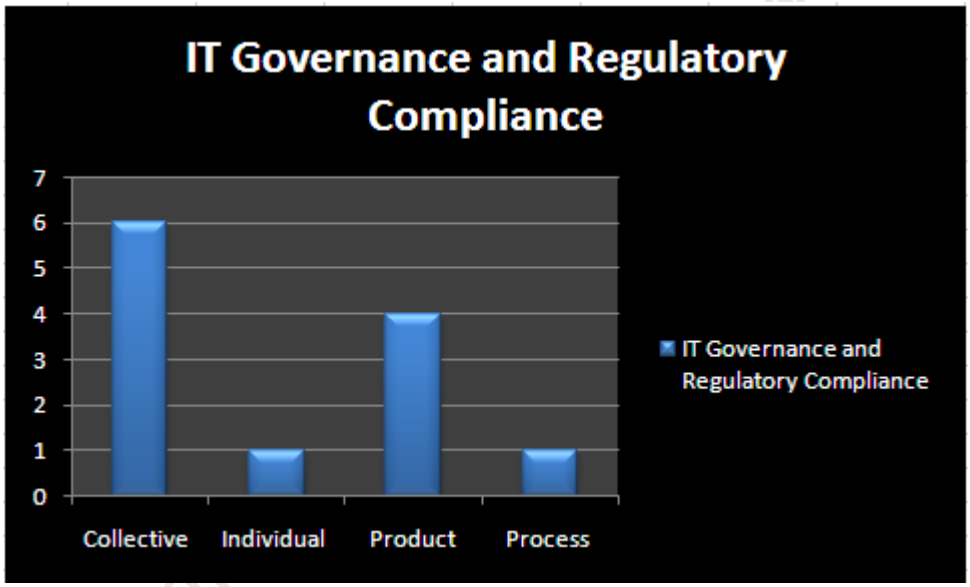
- Rational adaptive
- Creativeness
- Being ingenuous

Process Improvisation

- Managing

Figure 15. gives a graphical illustration of the above concepts. The above concepts illustrate the *improvisational* expressions by the information security practitioners who applied flexible methods.

Figure 15. Improvisation in IT Governance and Regulatory Compliance (Activities)



There was a greater conceptual density for *collective improvisation* for this IRSM activity. At strategic level, the information security practitioners were governed in the way they conducted audits. They had established a vision for adopting CobiT as a guiding control framework to assist in IT governance and compliance requirements. The research identified *improvisational* concepts that demonstrated the flexibility on the IT governance and compliance procedures implemented on the ground.

It was established that the lack of clear guidelines inspired information security practitioners to find new ways to deal with emergent situations but at the same time to ensure compliance.

"…Yes, a lot of Acts have been…introduced… but…I don't think they have been tested yet….so we want to comply to the bare minimum…" [127]

In the discussions, the practitioners also mentioned flexibility in compliance requirements and it seems likely that this sort of flexibility created room for the increasingly efficient application and implementation of compliance methods. This was achieved through the following:

1. Understanding guidelines well enough to draw up patterns of knowledge/skill sufficient to facilitate compliance.
2. Focusing attention on compliance activities and contextualisation.

Table 40 next page (*Sensitizing Device*) can be interpreted as follows: the functionalist approaches to ISRM dictates formal procedures for activities related to IT Governance and Regulatory Compliance as stated by **ISO IEC 17799, CobiT and ITIL. ISO IEC 17799 Section 12.1** suggests the way an organisation should carry out compliance requirements with regard to information security policies and standards. **CobiT Section M 3.5** gives guidance on how organisations should independently assure themselves of compliance with laws, regulatory requirements and contractual commitments through routine, independent compliance checks. The organization's own corporate information security policy document states that "*the Internal Audit [designated information security practitioners] periodically performs compliance checks to make sure that information security requirements are consistently observed.*" What **Table 40** shows is that there were ***12 conceptual instances*** where practitioners were using improvisation to by-pass these suggestions or were creative in applying these suggestions in ways that were not yet explicit. **Table 40** also qualifies these improvisational activities as having been performed within the contexts of these guidelines and frameworks. The two-direction arrows show that improvisational acts were drawn from what was already explicated in the literature and what was incremental.

[127] C31-Appendix 10

7.6.6 Table 40. Sensitizing Device: Assessing Improvisation in IT Governance and Regulatory Compliance

STRUCTURED (FUNCTIONALIST) APPROACH / UNIT OF ANALYSIS (EMBEDDED CASES)	ISRM Functional Approach: ISO 17799	ITIL	CobiT	INTERNAL DOCUMENT ANALYSIS Organization's Guidelines	IMPROVISATION: Collective Improvisation	Individual Improvisation	Product Improvisation	Process Improvisation	INCREMENTAL APPROACH
5 Governance and Regulatory Compliance	**Section 12.1.1** suggests that the way an organisation should carry out compliance requirements with regard to information security policies and standards. **Section 12.3** System audit considerations	**Section 4.2** (*Security Management*) procedures for the need to have audits and evaluate information security reviews of IT systems. **Operations** 4.4.1 Management of all ICT infrastructure events, 4.4.2 Operational control, components and their configuration	**PO 8** Ensure compliance with external requirements **M3.5** independent assurance of compliance with laws and regulatory requirements and contractual commitments, through routine independent compliance checks	The Internal Audit periodically performs compliance checks to make sure that information security requirements are consistently observed. Custodians are forbidden from changing the production information in their possession unless given explicit permission from the Owner or authorized User.	1 ☑ 2 ☑ 3 ☑ 4 ☑ 5 ☑ 6 ☑	7 ☑	8 ☑ 9 ☑ 10 ☑ 11 ☑	12 ☑	

These improvisational acts were seen to be working within the boundaries of the corporate policies, CobiT, ITIL and ISO IEC 17799.

1 Being inspired *2 Rational adaptive*
3 Being Creative *4 Resourceful*
5 Getting by *6 Managing*
7 Being novel *8 Lateral thinking*
9 Rational adaptive *10 Creativeness*
11 Being ingenuous *12 Managing*

(12 Conceptual instances See Figure 13)

7.6.1 Understanding IT Governance and Regulatory Compliance Using the Sensitising Device

Table 40 illustrates that IT governance decision-making was an issue (strategic) that was emphasised when the information security practitioners' understanding of the contextual situation affected the decisions to be made and the solving of practical solutions thereof. The information security practitioners were guided by frameworks which gave "*provision for technical compliance and technical support"* **(Table 36, CobiT** Section **M.2).** It was established that the issues regarding how each decision was carried out, such as assigning decision-making authority, coordinating resources, and aligning IT decision-making with external factors was done flexibly and contextually.

> *"in terms of how we…have been meeting certain compliance requirements in terms of ECT Act…"* [128]

> *"or any other critical ACT in line with all the information reporting …*[129]

The researcher interpreted this to mean that that the decision-making processes that facilitated compliance provided the practitioners an enriched personal perspective. This enriched perspective contextualised scenarios and guided the information security practitioner on how best to respond and undertake compliance measures. It is this enriched experience that draws from the cognitive and taps into reality that was seen to encourage *improvisation*. The improvisation concepts generated for this ISRM activity included creativity and inventiveness. Other concepts are listed on **Table 41** below.

Table 41. Descriptive Frameworks for IT Governance / Compliance and Improvisation

ISO IEC 17799	CobiT	ITIL	Description	Improvisation Concepts
ISO IEC 17799 Section 12.2.2			*Guideline for technical compliance checking to be carried out by specialists and authorised persons.*	*1 Being inspired* *2 Rational adaptive*

[128] C29-Appendix 10
[129] C30-Appendix 10

	CobiT Section M.2		*Procedures for technical compliance to take into account operational security and internal control assurance*	*3 Being Creative* *4 Resourceful* *5 Getting by* *6 Managing* *7 Being novel* *8 Lateral thinking* *9 Rational adaptive* *10 Creativeness* *11 Being ingenuous* *12 Managing*
		ITIL Section 4.2 (*ICT Infrastructure Management*)	*Provision for technical compliance which procedures for technical support and the processes that require technical support.*	
ISO IEC 17799 Section 12.2			*Having appropriate audit tools to review information, security policy and technical compliance.*	
	CobiT Section M3.3		*Manner for independent reviews and assurance of effectiveness of IT services through conducting routine independent checks of effectiveness*	
	CobiT Section M3.5		*Assurance of compliance with laws and regulatory requirements and contractual commitments, through routine independent compliance checks*	

The above concepts **(Table 41)** suggest that the aggregation of decision-making for meeting compliance requirements formed the basis of cognitive assembles (new skills and knowledge) and the practitioners would then autonomously access these new assembles as guides to creative compliance. This meant that IT governance and compliance was seen as a complicated and interconnected process of applying knowledge structures and explicated frameworks.

7.7 DISASTER RECOVERY AND BUSINESS CONTINUITY

The research established that the organisation had developed plans that enabled the organisation to deal with unanticipated contingencies. These plans were seen as proactive measures that were designed to reduce the impact of a disaster should this happen. The plans

were set up to ensure business continuity as explicated by the organisation's corporate information security policy.

> *"Business Risk Management will provide input into the information security process related to risk and continuity planning. Business Continuity Plans must be implemented and regularly tested to ensure availability of critical information*."
>
> **Source: Courtesy of [Name withheld] Corporate Information Security Policy (2007)**

At the heart of this corporate information policy was a proactive measure to ensure that creative ideas and skills would be developed by the practitioner. The practitioners would in turn have an increased knowledge about better ways of designing disaster recovery frameworks for business continuity, equipment failure, floods, fire etc. The objective would therefore be:

1) To better the management of business continuity;
2) To benchmark the actual way in which business continuity was management against emergent frameworks.

Section 6 of this thesis revealed that there was a high degree of conceptual density for *collective* and *process improvisation* for this IRSM activity specifically at operational level. It was established that the organisation prioritised these in terms of their role in reviving operations. The information security practitioners assessed the relative value of continuity of business along the dimensions of *availability.*

> *"…if we get a call on a Saturday…for something that is down, [we] don't worry, we will look at it on a Monday...since it is not a high level one...but if you get a call for something that you know is high level you will come in…"* [130]

> *"…yes and [we] categorised those items… we specifically focused on [those items], particularly from a disaster recovery and also business continuity…"* [131]

It was by understanding the meaning behind these statements that the researcher realised that it required skills and experience to be *rational adaptive* towards emergent contingencies. Concepts such as these were recorded as forms of information security practitioners' creativeness and improvisation. This was seen as the information security practitioners'

[130] C147-Appendix 10
[131] C52-Appendix 10

unique way of handling situations. Findings reveal that there were **4** conceptual instances of *collective improvisation*, **2** conceptual instances of *individual improvisation* and **4** conceptual instances of *process improvisation* as follows:

Collective improvisation

- Being quick-witted
- Lateral thinking
- Rational adaptive
- Managing

Individual improvisation

- Being quick-witted
- Getting by

Process improvisation

- Rational adaptive
- Being resourceful
- Exceptionality
- Being innovative

Figure 16. gives a graphical illustration of the above concepts.

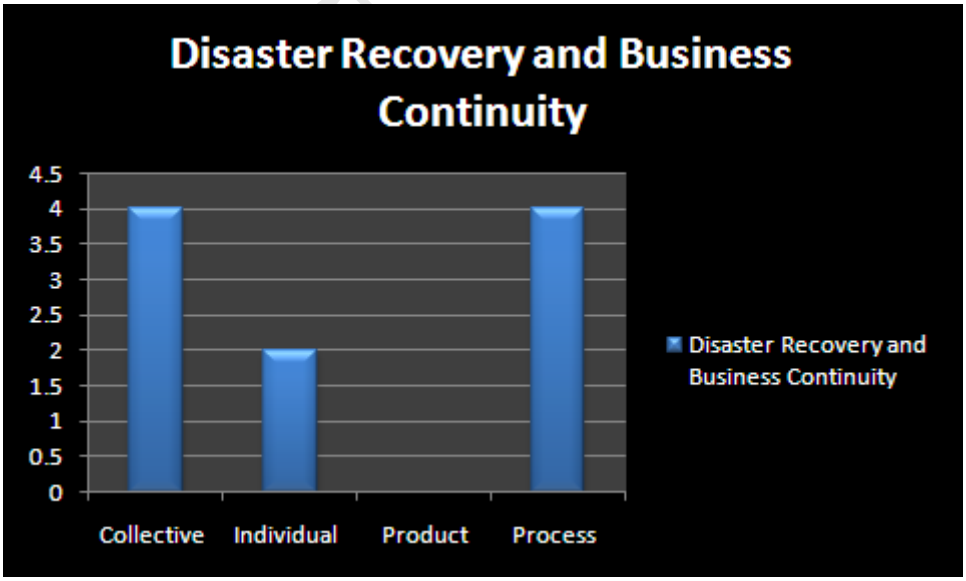


Figure 16. Improvisation in Disaster Recovery and Business Continuity (Activities)

The above concepts derived from interviews with information security practitioners and interpretation by the researcher demonstrated the way the organization's information security

practitioners handled the disaster recovery procedures. Other activities that show varied levels of *improvisation* included the way the disaster recovery tests were carried out. The researcher was able to observe the disaster recovery exercise at location and recorded this in ***Appendix 3***.

The following was observed in the following **Table 42. (*See Appendix 3 for full details*).**

Table 42. Observation: Disaster Recovery Management exercise

Start 9: 00 am	1. Equipment testing 2. Data testing	**Notes** Disaster Recovery Site has **12** PC's**.** There were also 6 personnel manning PC's each with a designated duty. At this stage the development area Switch (a virtual section in the database designated for testing data) had earlier on been switched off, meaning the activities were delayed.
9:30 am	1. Isolation of Development Area 1 Disaster recovery Manager leaves after making the call 2 The rest of the 5 people seem busy concentrating on 1 particular PC. 1 Unix systems link up to the main frame. 2 Select data date and time. Restore data based on selected data and time 3 Restore from back-ups brought using the main frame channel.	For the Disaster recovery process to continue, the Development Area Switch had to be switched on again. (This usually takes time due to formal procedures to be followed). Apparently the development team were unaware of the timing of the disaster recovery date. To address this, the Disaster Recover Manager made frantic calls back to the Office. After the call, he leaves the venue. In a matter of time the area was switched on. At this stage another person enters the secure room. Soon after, the Disaster Recover Manager comes back again. He explains that on normal occasions there are 2 tests of this nature once a year. **Manifest file** A manifest file (a check list) of the recovery procedures is produced. It documents the steps to be followed in the recovery process.
10:00am	1 Review of Manifest file 2 Unix environment goes live for recovery. 3 Back-ups selected for recovery.	There is a Data Analysts who sits and observes everything. The Analyst seems to give instruction to the *CSC personnel about the recovery process. The four essential items to be checked in the back-ups include; • The back-up date • Return Number • Seal number • Container number While one person reads the manifest file the other types the instructions

		in the UNIX environment. * *Computer Science Corporation (CSC) have been sub-contracted to handle the mainframe capability although the equipment is owned by [name withheld] .*
10:30	1 Two serves restored successfully	At this time 2 servers have been restored successfully, the time taken being 30 minutes. Information from these two contains server information about the following; Food Server P670 Textile Server P 670 RMS Server P570 FDS/TMS Server P650 ECS/APPWORX Server P650 QUEST Server P615 The reason given for the quick recovery by the teams is that they have done this more than once and have internalised the process. It was noted that no documentation is being taken.

From the observations (**Table 42**), it was noted that the exercises were very technical and comprehensive and were aimed at covering all relevant aspects (predictive knowledge) and factors that would adversely affect the running of the information systems. Also critical was the *down-time* (the duration systems were be out of operation) and how long it would take to revive these systems and data from backed-up data and standby servers.

It was observed that the framework used in the disaster recovery exercises for managing contingencies was created to categorise data and list items of criticality though this was not sufficient enough to apply to all situations. This rendered some plans unworkable, and hence required practitioners to draw cognitively from their own skills and past experiences. **Table 43** (next page) the *Sensitizing Device*, shows how this was done and the concepts that were derived by the practitioner in understanding creativity in these ISRM activities. There were ***ten (10) conceptual instances*** of *improvisation* noted by the researcher when conceptualizing this ISRM activity.

Table 43 (*Sensitizing Device*) can be interpreted as follows: the functionalist approaches to ISRM dictate formal procedures for activities related to Disaster Recovery and Business Continuity as stated by **ISO IEC 17799, CobiT and ITIL. ISO IEC 17799 Section 11.1** defines the various aspects of Business Continuity Management. **CobiT Section DS 4.2** proposes the need for an organisation to establish an IT continuity plan, a strategy and philosophy which align with the overall business continuity plan. What **Table 43** shows is

that there were ***10 conceptual instances*** where practitioners were using improvisation to by-pass these suggestions or were creative in applying these suggestions in ways that were not yet explicit. **Table 43** also qualifies these improvisational activities as having been performed within the contexts of these guidelines and frameworks. The two-direction arrows show that improvisational acts were drawn from what was already explicated in the literature and what was incremental.

7.7.4 Table 43. Sensitizing Device: Assessing Improvisation in Disaster Recovery and Business Continuity

STRUCTURED (FUNCTIONALIST) APPROACH					IMPROVISATION				INCREMENTAL APPROACH
UNIT OF ANALYSIS (EMBEDDED CASES)	**ISRM Functional Approach**				**Collective Improvisation**	**Individual Improvisation**	**Product Improvisation**	**Process Improvisation**	
	ISO 17799	**ITIL**	**CobiT**	**INTERNAL DOCUMENT ANALYSIS Organization's Guidelines**					
6. Disaster Recovery and Business Continuity	**Section 11.1** Aspects of Business continuity management	**Availability Management;** 8.3 The availability management process **Section 7.3** (*Service Delivery*), the IT Service Continuity Management, postulates the need for a risk-based approach in the continuity of IT processes and services.	**DS 4** Ensure Continuous Service **DS4.2** need to establish an IT continuity plan, a strategy and philosophy which aligns with the overall business continuity plan **DS 10** Manage Problems and Incidents	Business Risk Management will provide input into the information security process related to risk and continuity planning Business Continuity Plans must be implemented and regularly tested to ensure availability of critical information.	*1* ☑ *2* ☑ *3* ☑ *4* ☑	*5* ☑ *6* ☑		*7* ☑ *8* ☑ *9* ☑ *10* ☑	

These improvisational acts were seen to be working within the boundaries of the corporate policies, CobiT, ITIL and ISO IEC 17799.

1 Being quick-witted *2 Lateral thinking*
3 Rational adaptive *4 Managing*
5 Being quick-witted *6 Getting by*
7 Rational adaptive *8 Being resourceful*
9 Exceptionality *10 Being innovative*
(10 Conceptual instances See Figure 14)

7.7.1 Understanding Disaster Recovery and Business Continuity Using the Sensitising Device

Table 43 illustrates extemporaneous acts for continuity management catalysed by training/experience and expressed as *improvisation* practice. The context laid for the organisation's information security practitioners was set by frameworks that explicated the "*need to establish an IT continuity plan, a strategy and philosophy which aligns with the overall business continuity plan"* **(Table 44, CobiT** Section **DS 4.2).** The research established that the issues regarding how business disaster recovery and business continuity decisions were carried out, such as deciding on the data and application software that need to be recovered and restoring this for the business to resume in case of a disaster. The researcher interpreted this to mean that it was difficult to establish what would be lost (i.e. predict the future) and to estimate the recovery time for that data. One simple way was to devise mechanisms for whole data recovery rather than parts. This option, however, proved expensive for very large data sets for this specific organisation.

That is the reason why understanding these activities made it possible to find the essence of *creativity*, *flexibility* and *rational adaptation* and to see that the practitioners were trying to find the best way to establish *a risk-based approach in the continuity of IT processes and services* (**Table 44, ITIL Section 7.3** *Service Delivery*) It was thus noted that the business continuity management process was filled with creative activities spontaneously arising during normal operating conditions while at the same time following the predefined frameworks. These activities were characterised in part by the selection of appropriate procedure in the event that planned-for contingencies arose. **Table 44** (below) shows some of the guidelines proposed by the frameworks and the concepts that were derived by the researcher to establish how this was done on the ground.

Table 44. Descriptive Frameworks for Disaster Recovery and Business Continuity

ISO IEC 17799	CobiT	ITIL	Description	Improvisation Concepts
ISO IEC 17799 **Section 11.1.1**			*need for putting in place a managed process for developing and maintaining business continuity*	*1 Being quick-witted* *2 Lateral thinking* *3 Rational adaptive*

	CobiT Section DS4.2		*need to establish an IT continuity plan, a strategy and philosophy which aligns with the overall business continuity plan*	*4 Managing* *5 Being quick-witted* *6 Getting by* *7 Rational adaptive* *8 Being resourceful* *9 Exceptionality* *10 Being innovative*
		ITIL Section 7.3 (*Service Delivery*)	*postulates the need for a risk-based approach in the continuity of IT processes and services*	
ISO IEC 17799 **Section 7.2**			*general information security of equipment/systems and the risks associated with those that impact on business continuity*	
	CobiT Section DS4.10		*need for a framework that establishes critical IT resources which should be identified.*	
ISO IEC 17799 **Section 11.1.1**			*making on-the-spot decisions and understanding the impact interruptions to business processes are likely to have on the business*	
	CobiT Section DS4.13		*the need to have "wrap-up" procedures which entail assessing adequacy of plans and planning updates*	
	CobiT Section DS4.11		*cognisance of the need for decision making on back-up site and hardware, while identifying contracts for service provision*	
		ITIL Section 7.3.4 (*Service Delivery*),	*IT Service Continuity Management, stipulates procedures for operational management in continuity of operations*	
ISO IEC 17799 **Section 11.1.4**			*clear framework to deal with emergencies and provide a need for*	

			emergency response procedures, and manual fallback plans	

Table 44 above demonstrates that the process of supporting business continuity and disaster recovery management was subject to creativity and flexibility giving rise to decisions based on the contextual event and the criticality of the incident. It is this quick decision making that gave rise to *improvised* acts.

> *"…correct…something will always happen…"* [132]

> *"…I think our main thing here is to keep [going]… I mean we have a lot of good uses in policies when it comes to keeping the system going, certain time we do what we have to do to keep the [systems] going…and sometimes we don't…know if it is the right thing to do…"* [133]

The previous statements show that in reality systems at times went down due to unanticipated causes and this often called for information security practitioners to be *quick witted*. It seems that the way the specific disaster recovery activities were carried out depended on requirements as dictated by contextual business needs, costs, extent of exposure to disaster, type of disaster and the disaster recovery opportunities within the organization. The following were noticed as activities that demonstrated this contextual understanding by information security practitioners:

- Choices were "composed" (in real-time) based on the available disaster recovery exercises options present e.g. on-site mirror arrangement for backups.
- Choices to be made based on remote arrangement within organization, such as "hot", "warm" or cold sites". Where hot sites would be accessed immediately if the main applications in the organisation went down, cold sites would experience some delay ranging from hours to days, with warm sites being somewhere in the middle.

It was concluded that the individual information security practitioner's capacity to understand and utilise disaster recovery and business continuity planning tools and the holistic manner in which all these activities were performed contained elements of *improvised* acts. The researcher interpreted that a successful rational adaptive response to disaster recovery and

[132] C133-Appendix 10
[133] C124-Appendix 10

business continuity planning as expressed by the practitioner was not to be seen as a failure of pre-event/continuity or recovery time planning, but as an emergent creative act.

7.8 SUMMARY OF FINDINGS OF ALL UNITS: CONCEPTUALISATION OF IMPROVISATION IN ISRM ACTIVITIES

The researcher summarized all the units that were analyzed and interpretations drawn into **Table 45** below. **Table 45** (Extracted from **Table 31**) summarizes findings from analysis of all the ISRM units as follows.

Table 45. Numeric Summary of Conceptual density of Improvisation

Units of Analysis Activities related to;	Level	Number of instances of improvisation				Conceptual Density
		Collective Improvisation	Individual Improvisation	Process Improvisation	Product Improvisation	
1 Information Assets Access and Data Control	**Strategic**	*1*				1
	Tactical	*1*				1
	Operational	*1*		*2*		3
2 Information Security Architecture	**Strategic**	*1*		*1*		2
	Tactical	*2*				2
	Operational			*3*		3
3 Information Security Policies	**Strategic**	*1*	*1*			2
	Tactical			*2*	*1*	3
	Operational			*2*		2
4 Information Security Event Monitoring	**Strategic**			*2*	*1*	3
	Tactical		*2*	*4*		6
	Operational	*2*		*2*		4
5 IT Governance and Regulatory Compliance	**Strategic**	*4*			*2*	6
	Tactical	*2*	*1*			3
	Operational			*1*	*2*	3
6 Disaster Recovery and Business Continuity	**Strategic**	*2*				2
	Tactical	*1*		*1*		2
	Operational	*1*	*2*	*3*		6
		19	***6***	***23***	***6***	***54***

Table 45. can be interpreted by understanding the number of conceptual instances of *improvisation*, (denoted in numeric form) for each unit of analysis. The number of conceptual instances in each unit of analysis denotes **conceptual density** of *improvisation* for that unit.

Table 45 therefore shows *process improvisation* as being the most conceptually dense form of *improvisation* and more specifically in activities related to Event Monitoring. – **CLAIM 1.** (monitoring information security breaches and incidents). **Table 45** also shows that both *individual and product improvisation* were the least observed forms of *improvisation* in ISRM activities. – **CLAIM 2.** This conclusion was based on the conceptual density of both.

For easier representation of **Table 45, Figure 17** below was developed. **Figure 17** clearly shows that *process improvisation* is the most pronounced *improvisational* type in ISRM activities relating to Event Monitoring. This is because these activities are operational activities subject to unplanned changes, incidents and contingencies. These activities therefore comprise elements of flexibility. In contrast, *collective improvisation* is more pronounced in activities relating to IT Governance and Regulatory Compliance.-**CLAIM 3.** This is perhaps because IT Governance entails assigning decision rights jointly or collectively.

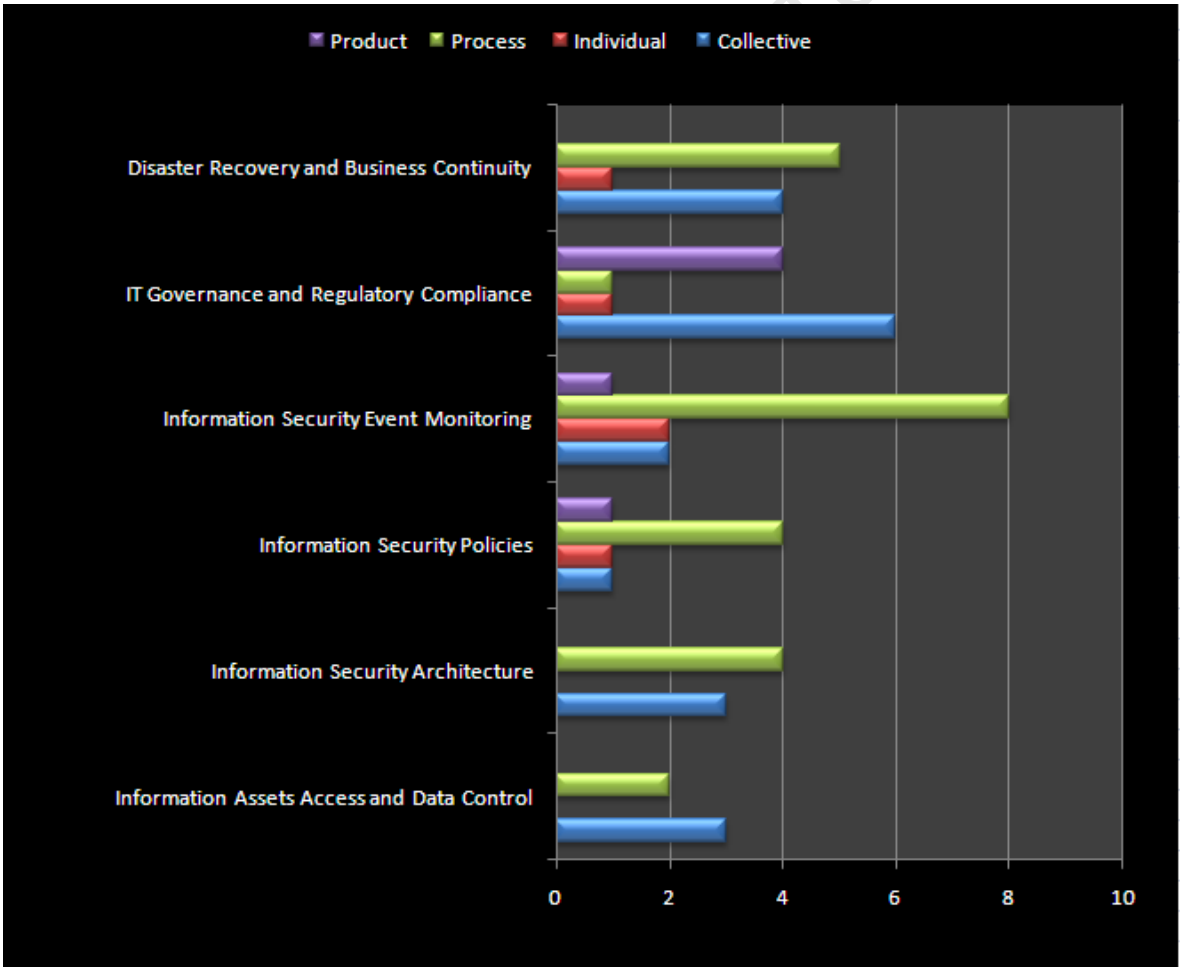


Figure 17. Summary of Conceptual Density of Improvisation in ISRM Activities

Analysis of ***Figure 17*** does not support the claim that *individual improvisation* is present in ISRM activities relating to assets control and information architecture and design.-**CLAIM 4.** Because *individual improvisation* concepts relating to these ISRM activities were not coded, it would be interpreted to mean that practitioners were hesitant to act as individuals in sensitive matters such as security of information assets.

7.8.1 Density of Types of Improvisation in ISRM

The researcher took a summary total of the various typologies of *improvisation* (*Process, Product, Individual* and *Collective*) and compared the number of conceptual instances (conceptual density). **Table 46** gives a numeric summary of the conceptual density as follows:

Table 46. Summary of Conceptual density of Improvisation

Level		Conceptual Density of types of improvisation *(in numeric form)*				Conceptual Density (Total)
		Collective Improvisation	Individual Improvisation	Process Improvisation	Product Improvisation	
Units of Analysis	Strategic	*9*	*1*	*3*	*3*	*16*
	Tactical	*6*	*3*	*7*	*1*	*17*
	Operational	*4*	*2*	*13*	*2*	*21*
	Total	*19*	*6*	*23*	*6*	*54*

The researcher then graphically represented this data in **Table 46** above to come up with **Figure 18**. It can be noted that **Figure 18** shows *process improvisation* as the most pronounced type of *improvisation* in ISRM activities. *Process improvisation* was also more pronounced at operational level as opposed to any other level.-**CLAIM 5.** Both *product* and *individual improvisations* were the least pronounced *improvisations* in ISRM activities. This can be interpreted to mean that information security practitioners would rarely opt to work or do things alone. Given alternatives, they seemingly would prefer to work or collaborate jointly with others. That is why *collective improvisation* seems to be much more pronounced than *individual improvisation*.- **CLAIM 6.** **Figure 18** also shows that there was a greater level of conceptual density of *collective improvisation* at strategic level.- **CLAIM 7.** This meant that joint consultation was valued greatly more-so at strategic level than any other level.

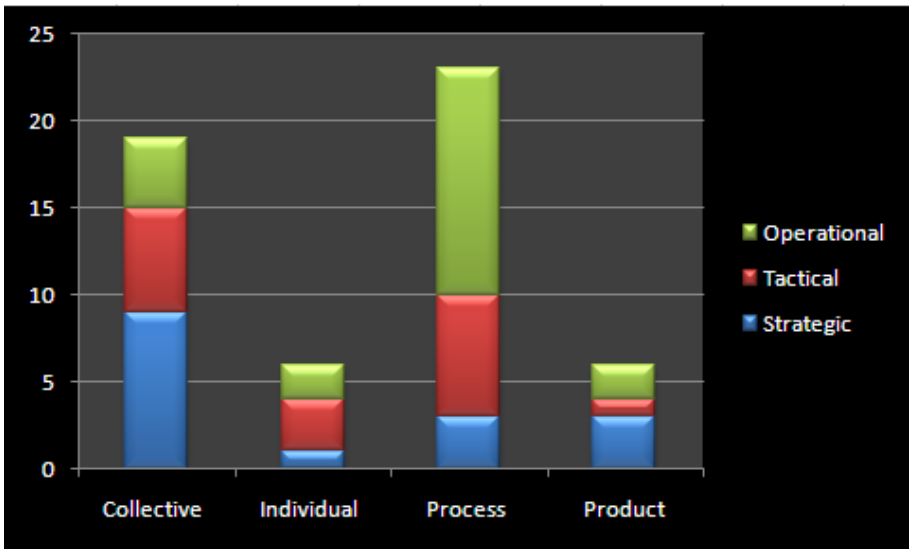


Figure 18. Summary of Conceptual Density of Types of Improvisation in ISRM Activities

7.8.2 Density of Improvisation at Various Organisational Levels

The researcher also wanted to know, at which organizational level (Strategic, Tactical and Operational), *improvisation* was more conceptual dense. Data extracted from **Table 31** and **Table 47** was then generated into a summary total of the various typologies of *improvisation* at the three levels.

Table 47. Summary of Conceptual density of Improvisation

Conceptual Density of Improvisation	**Organisational Level**			
	Strategic	**Tactical**	**Operational**	**Totals**
collective improvisation	*9*	*6*	*4*	*19*
individual improvisation	*1*	*3*	*2*	*6*
process improvisation	*3*	*7*	*13*	*23*
product improvisation	*3*	*1*	*2*	*6*
(Totals)	*16*	*17*	*21*	*54*

Figure 19 below is a graphical illustration of **Table 47** and shows that *improvisational* activities were more pronounced in operational activities and least pronounced in strategic activities. This can be explained as follows: *improvisation* by nature is expressive and this expressive nature is more pronounced in the routine day-to-day activities which are primarily

operational activities.-[CLAIM 8.] *Improvisation* is least pronounced in strategic activities because these activities are not regular and occur infrequently.-

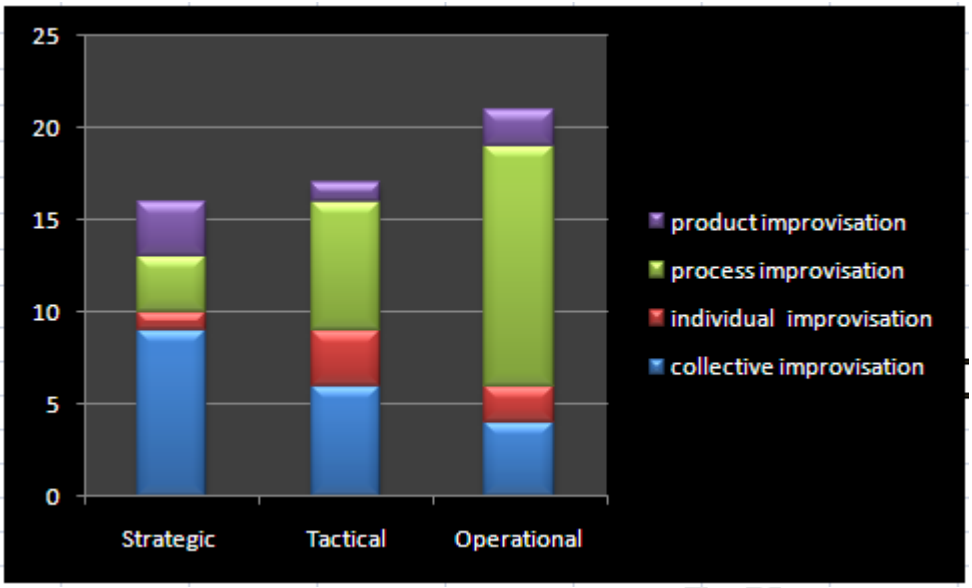


Figure 19. Summary of Conceptual Density of Improvisation at Organisational Levels

7.8.3 Density of Improvisation in Various ISRM Units of Analysis

Finally the researcher wanted to determine the conceptual density of *improvisation* and compare this data by unit of analysis. Data was also extracted from **Table 48** and **Figure 20** was generated.

Table 48. Summary of Conceptual density of Improvisation in Units of Analysis

Units of Analysis Activities related to;	Conceptual Density (Total)
1 Information Assets Access and Data Control	5
2 Information Security Architecture	7
3 Information Security Policies	7
4 Information Security Event Monitoring	13
5 IT Governance and Regulatory Compliance	12
6 Disaster Recovery and Business Continuity	10
TOTAL	54

Figure 20 below is a graphical illustration of **Table 48.** This figure shows that *improvisation was more conceptually dense* in activities relating to Event Monitoring and least pronounced in activities relating to information assets control.

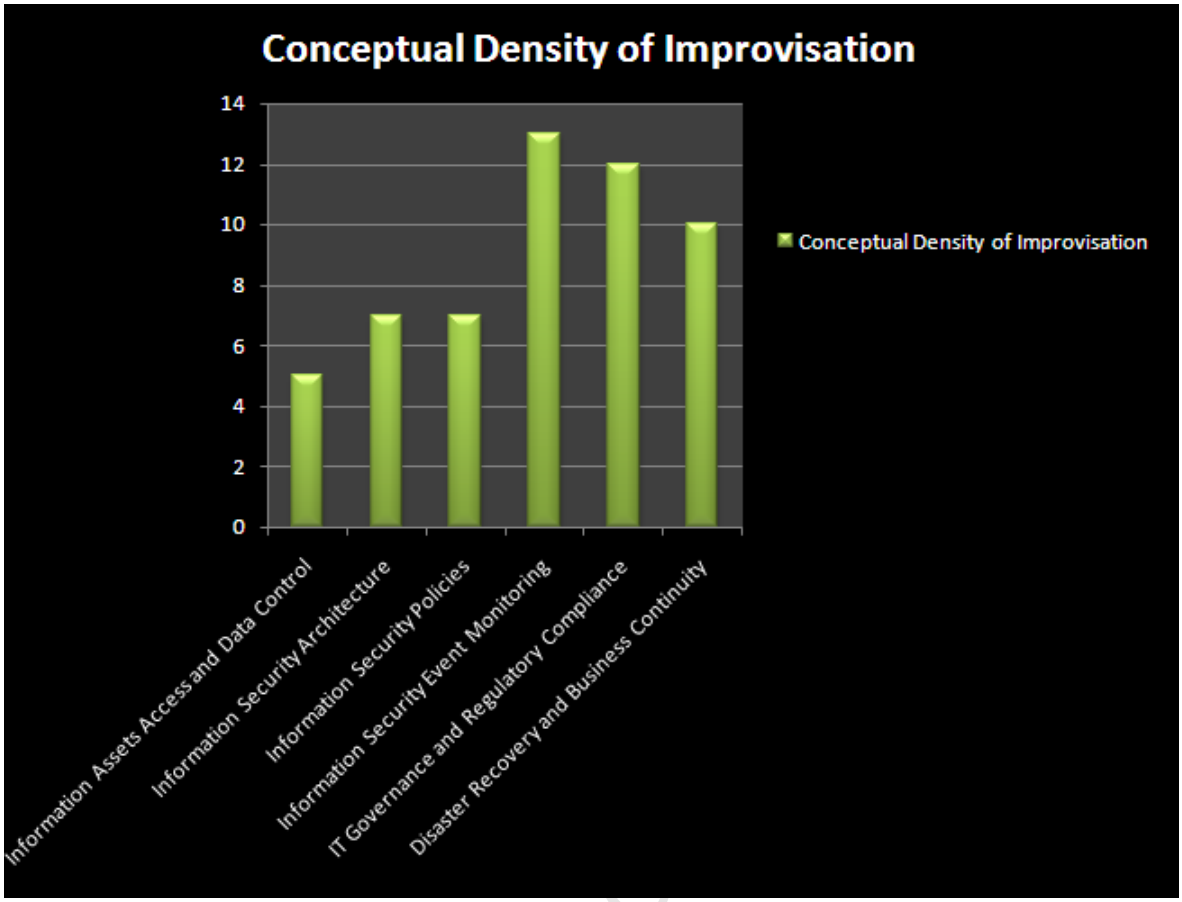


Figure 20. Summary of Conceptual Density of Improvisation in Various ISRM Activities

Figure 20 also shows that ISRM activities relating to IT Governance and Regulatory Compliance had the second most conceptually dense forms of *improvisations.*

A summary of conceptualization of *improvisation* in ISRM activities was carried out. This enabled the researcher to conclude and make the following statements or **knowledge claims <u>for this case</u>** about ***improvisation in ISRM activities***. The **knowledge claims** for this case stem directly from the premises and work done in the previous sections and are listed as follows:

a) Improvisation is generally manifested in ISRM activities and these manifestations occur in a variety of ways as follows:

1. The general trend was that *process improvisation* was a more conceptually dense form of *improvisation* than any other *improvisation*, and was generally evident in ISRM activities that related to Information Security Event Monitoring. *Process*

improvisation was also generally more evident in operational level ISRM activities as opposed to tactical or strategic ISRM level activities. **(CLAIM 1 and 5)**.

This can be interpreted to mean that operational level monitoring activities are continuously subject to unplanned changes, incidents and contingencies. These activities therefore comprise elements of flexibility and spontaneity.

2. The general trend was that *collective improvisation* was a more conceptually dense form of *improvisation* in ISRM activities relating to IT Governance and Regulatory Compliance and was generally more pronounced than *individual improvisation. Collective improvisation* was also generally more evident at strategic level. **(CLAIM 3, 6 and 7).**

   This can be interpreted to mean that because of the nature of risk, the information security practitioners would rarely opt to work alone or do things along.

3. The general trend was that *individual improvisation* was more pronounced at operational level and least pronounced at strategic level. Generally this form of *improvisation* was not observed in ISRM activities relating to assets control and information architecture and design **(CLAIM 4 and 8)**. This, however, may not always be the case in other organizations. *Individual improvisation* was also among the least conceptually dense forms of improvisation **(CLAIM 2)**.

   This can be interpreted to confirm the social institutions theory (Scott 2001) which suggests that social institutions impose diffusion from the top–down while actors from the bottom–up can individually engage in invention and negotiation although they would prefer not to do this alone.

4. The general trend was that, *product improvisation* was among the least *observed* form of *improvisation* in ISRM activities for this particular case study **(CLAIM 2)**.

   This can be interpreted to mean that product improvisation affects the substantive nature of new products with the tendency to exacerbate risk; this was to be avoided unless it was of paramount importance.

7.8.4 Holistic Conceptualisation of Improvisation in ISRM Activities

Findings by the researcher reveal that *improvisation* was more conceptually dense in Business Continuity activities, and more pronounced in the operational based activities of that unit. ISRM activities relating to Governance and Control also had an almost equivalent level of conceptual density of *improvisation*. However, *improvisation* was more pronounced in strategic activities relating to governance and control. The researcher has illustrated these finding in **Figure 21.**

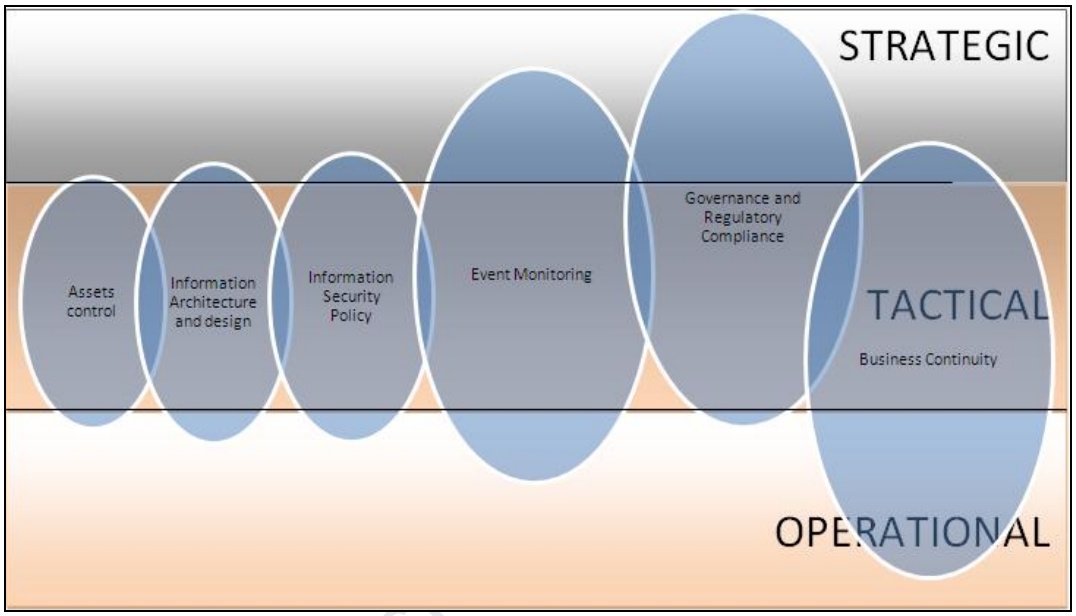


Figure 21. Holistic Conceptualisation of Improvisation in ISRM Activities at hierarchical levels

Figure 21 illustrates the 6 units of analysis that represent the distinct ISRM activities at the hierarchical levels of strategic, tactical and operational levels. These six distinct activities are oval "egg" shaped representations that overlap each other. The reason for the overlap is because in the real sense ISRM activities by nature overlap and usually are closely tied. It can be seen from **Figure 21** that conceptual density of *improvisation* was least exemplified in ISRM activities relating to assets control, information architecture and information security policy. Deeper insights reveal that the internalized knowledge of information security practitioners resulted in improvised acts relating to two important ISRM activities namely Business Continuity and Governance and Regulatory Compliance. What was happening was that the practitioners were expressing *improvisation* in settings that were non-routine and characterised by a minimal amount of supervision. It can be seen that in an ISRM such as

event monitoring which is often characterised by crisis and contingencies, the result is a greater conceptual density. In event monitoring, security incidents were disrupting or challenging the set order and required extemporaneous interventions (improvised action).

7.9 CHAPTER SUMMARY AND CONCLUSION

This discussions and interpretation chapter has demonstrated that the fusion (mixing) of paradigmatic approaches leads to understanding the, interesting and creative ISRM solutions. The chapter argued that to holistically understand these ISRM approaches by using the *Sensitizing Devic*, meant relying on understanding and interpreting the inventiveness and creativeness of practitioners who may or may not have been conscious of the philosophical assumptions belonging to alternative paradigms and approaches. This chapter has contended that advancement of *improvisational* knowledge in ISRM practices should come from explicating the holistic approach. This explicated knowledge would permit the understanding of creative solutions to practical problems employed by practitioners as they engage in the ISRM activities. The chapter's intention was to help practitioners become better aware of the assumptions and beliefs that they employ in their day-to-day activities. A better understanding of the conceptual framework developed and extended in this chapter is meant to lead practitioners to gain insights to creative solutions using the strengths of each approach. Without a systematic documentation of alternative approaches, *improvisation* would have escaped the attention of the practitioners.

CHAPTER EIGHT

This chapter gives a conclusion to the ISRM practices and draws on the new knowledge obtained and how this is evidenced in current contemporary setting. The chapter highlights the implications for the research findings to both practitioners and theorists. It is hoped that this concluding chapter positions this thesis as having served its purpose by showing how it has contributed both to theory and practice.

Table of Content
Chapter Eight

CHAPTER EIGHT: CONCLUSION

8.0 INTRODUCTION

This chapter concludes the research work carried out and shows why it was indeed necessary to carry out the research. The concluding chapter outlines the **rich insights** derived from the conceptualisation of *improvisation* in ISRM activities. As explained in this chapter, these insights have helped formulate a Meta level understanding of information security practitioners' ISRM activities and it is hoped that these insights will serve as an ideal platform for further theoretical development. Theory development that proceeds from this research, it is hoped, should be open for consideration of socio-contextual elements within information security risk management.

The chapter is divided into five sections. The first section discusses the accomplishments of this research. This section revisits the research problem statement and discusses how this was addressed. The second section discusses what this research means from a theoretical perspective. It gives implications for theory. The third section discusses what this research means to practice and to practitioners. It gives implications for practice. The fourth section outlines some of the limitations for this study. The last section wraps up the understanding of *improvisation* in ISRM activities. The researcher assesses his own work in this section and shows how this research has contributed to theory and practice. This last section proposes the establishment of criteria for accepting *improvisational* skills as genuine expressions that add value to the whole ISRM process.

8.1 ACCOMPLISHMENT: HOW THE RESEARCH QUESTIONS WERE ANSWERED

Revisiting the Research Questions

In order to successfully assess what was initially set out to be accomplished, the research questions are re-visited. The accomplishment of this research is measured against how the research questions are assessed against the research problem statement.

Revisiting the research questions addressed by this research, the following was main problem statement:

> ***How is improvisation manifested in Information Security Risk Management (ISRM) activities and how can improvisation in ISRM be conceptualised?***

This research was organised and structured in such a manner as to systematically allow the researcher to progress towards understanding how the problem statement listed above would be tackled. The problem statement raised issues about ISRM activities. The general idea was that *improvisation* had been manifested in organisations (Cunha et al. 1999); however, no research had ever been conducted to show *improvisation* in ISRM activities. It was therefore important to understand what ISRM was and what activities were inherent. The first sub-question raised was:

- *What ISRM activities are in an organisation and how are they carried out?*

The researcher conducted a literature review and established what these ISRM activities were. These have been discussed in detail in **Chapter 2, Section 2.4 (understanding ISRM). Chapter 2** unpacked the concept of information security risk and ISRM activities. This chapter enabled a clear understanding of the nature of risk and why certain ISRM activities are carried out to mitigate this risk. **Chapter 2** also suggested a predominant following by those who advocate the structured functionalist way of designing policies and frameworks devoid of contextualisation. This chapter introduced the technical and social issues pertinent to managing information security risk and placed significance on the need to further conceptualize this risk against the backdrop of emergent social contextual factors. The researcher believes this question was adequately addressed.

It was also important to consider another issue raised by the problem statement. This issue was the idea that *improvisation* is present in ISRM activities. How it was manifested was the general problem area requiring research. That was why the second sub-question was raised:

- *How is improvisation manifested in these ISRM activities in the organisation?*

The researcher embarked to understand and document the manifestation of *improvisation* generally by conducting an extensive literature review. *Improvisation* terminology was unpacked and the researcher identified the typology of *improvisation* as four distinct forms: *collective, individual, product* and *process.* The typology was found to be useful since it laid the foundation for the development of a preliminary model for conceptualisation. The model has been described in this research as the *Sensitising Device* **(Chapter 4, Section 4.5.2)**. The *Sensitising Device* was to be a useful lens in discovering *improvisation* in ISRM activities and was the first step towards understanding how *improvisation* is manifested in ISRM. The final step towards the actual manifestation was through the researcher's **knowledge claims** about the various manifestations of *improvisation* in ISRM activities. These knowledge claims are listed in **Section 7.8.3.** The researcher believes that by documenting these knowledge claims, this question was adequately addressed in this research.

It was also important to understand how *improvisation* could be conceptualised, what methodology would be suitable and what methods would be used to "unearth" this phenomenon at an organisational setting. That was why the following sub question was raised:

- *How can improvisation in ISRM be conceptualised**?***

Chapter 5 described in detail the methodology and the methods the researcher deemed suitable for accomplishing this. ***Some of the information obtained was by happenstance*** as opposed to well a calculated structure for obtaining information by using these stated methods. For instance, not all practitioners were able to attend scheduled interviews. Also, the large private sector organisation that accepted the case study research was not the organisation that was initially targeted for research. The initial organisation was a government organisation that dealt with large volumes of sensitive public data. This organisation proved

too sensitive for such a case study and this organisation declined the research. The upside of this was that the methods used, the organisation researched, and the data obtained ***still met the criteria for this research.***

Using the *Sensitising Device* as a lens, **Chapter 6** and **Chapter 7** embarked on the conceptualisation process for the organisation that accepted the research. While **Chapter 6** primarily dwelt on primary data analysis from this organisation, **Chapter 7** detailed document analysis and observations. *Improvisation* was found to manifest itself in various types (*collective*, *individual*, *process* and *product*) contextually and differently across the different units of analysis for this organisation. **Chapter 7** discussed in detail this manifestation of *improvisation* across the type, against the unit of analysis, and across the three organisational levels of *strategic*, *tactical* and *operational.*

Chapter 7 conceptualised *improvisation* in ISRM activities and embarked to establish meaning and impact of *improvisation* on ISRM outcomes. Although **Chapter 7** was limited to conceptualisation, contexts for understanding and exploring in-depth *improvisation* were incorporated into this chapter. The researcher believes that the conceptualisation of *improvisation* in ISRM activities was done in a manner that meets scientific rigour and adequately answers this question.

Finally it was important for the researcher to understand the context of *improvisation* in ISRM. Was it to be considered a good thing or a bad thing? It should be noted from the researcher's discussion that the disposition for *improvisation* to be a good thing was an acceptable proposition. That was why the following question was raised:

- *How is improvisation used as a foundation for Positive ISRM*

Insights obtained from this research constitute the idea that *improvisation* as a product of extemporaneous and creative thinking was evident in ISRM activities at all hierarchical levels of decision making (strategic, tactical and operational) and that this was indeed a positive thing. This research has embarked to justify this. The following sections therefore detail the positive aspect of *improvisation* in ISRM by understanding its implications to both theory and practice. The researcher believes that once these sections are explained in detail then this last question will be addressed. From a holistic perspective, the researcher notes that what was

initially set out to be accomplished in the form of a problem statement and research questions has indeed been accomplished by work done on all these chapters.

8.2 IMPROVISED ISRM ACTIVITIES: IMPLICATIONS FOR THEORY

A theoretical understanding of *improvisation* in ISRM emerged from the data collected, analysed and interpreted through interviews, observations and document analysis. While the researcher notes that this theoretical understanding is grounded in the data, it is also found to be supported by information security literature. What the information security literature has not as yet highlighted, however, is the ***potential positive benefit*** *improvisation* may induce in ISRM activities. This is the gap in literature that this theoretical framework has attempted to fill and is the basis for which a more general theory may be developed. Central to the framework was the inferred relationship between the various ISRM "**egg shaped"** activities which tended to overlap and of the **knowledge claims** about *improvisation* in ISRM.

As laid out in the knowledge claim, *improvisation* was manifest in ISRM activities and these manifestations occurred in different forms (see **Section 7.8.3**). Theoretically it follows that this research showed that practitioners were driven by extemporaneous and *improvised* decision-making within ISRM activities when activities were triggered by contingencies and emergent security incidents. As an implication to theory, this then is seen as a theoretical development in ISRM. ISRM is now endowed with this theoretical understanding.

8.2.1 Theoretical Framework: Demystifying "Pure organic structures" in ISRM

Another implication for theory is the new insights demonstrated by **knowledge claims**, which demystify early suggestions in literature that organisations need "pure organic structures" in ISRM (functionalism) to support complex actions. These organisations need structures characterised by rationality, coherence and amenability to computerization (Westrup 1996). By systematising differences among various information security practitioners' forms of managing information security risk, **knowledge claims** exhibited in this thesis suggests socio-contextual behaviour (incremetalism and functionalism as *improvisation*) as being of ***potential positive benefit.*** By doing so, the substantive framework reinforced the importance of *improvisation* in ISRM.

The *improvising* organisation is one that was seen by this research as endowed with information security practitioners who are ***socio-constructive agents***. In the *improvising* organisation, the research demonstrated that the gaps in **functionalism in ISRM** were filled by the agency of individuals, whose value and appreciation of *improvised* activities created avenues for continuous renewal of ISRM methods.

Also it is worth noting that the exploration of practical applications of ISRM activities has lead to the formulation of this theory. It should be appreciated that this theory reveals an important facet of information security risk practitioners. This theory in its simplicity can lead to a better conceptualization of practice. The following section shows why it is important to recognize *improvisation* in practice.

8.3 IMPROVISED ISRM ACTIVITIES: IMPLICATIONS FOR PRACTICE

By presenting examples where *improvisation* occurs and why certain *improvisations* served their purpose, the argument should be that improvisation gives strength to the decision making processes. In its various forms (*collective, individual, product* and *process*), improvisation should be encouraged in practice.

8.3.1 Improvisation Is Evident In ISRM Activities: Coping With This Fear

It can be seen that the sets of *improvisations* (*collective, individual, process* and *product*) presented in this research were essential and proved effective in ISRM processes. It can be seen that in general, however, *improvisations* proved **only** effective **provided** the practitioners were skilled enough, utilised the best available material and had a firm determination to achieve the intended purpose. It should therefore be suggested that so long as practice is endowed with practitioners who are capable of skilfully manifesting *improvised* acts, these acts should not be stifled, but made to flourish since they have been proven to be of value to ISRM. Practice should establish mechanisms to cope with the fear that various *improvisations* will override long nurtured functionalist structures. Various *improvisations* will actually give contextual meaning to these very functionalist structures.

8.3.2 Why Practitioners should not Attempt to Dilute Improvisation In ISRM Activities

Having no control over the outcome of interpretation and use of this research, the researcher is well aware that perhaps the findings would be construed as a way of highlighting '*what should not be happening'* in the information security environment. While there is reasonable justification for this assumption from a technical and natural science perspective, it should be noted that this assumption, when applied within the social sciences, poses sound theoretical conclusions i.e. '*this is what is meant to be happening'*.

These conclusions show that ***improvisation can lead to a rich and good ISRM practice.*** The researcher is of the opinion that it takes a discrete, bold, conscious step towards bridging this theory and practice. The need to encourage *improvisation* would be justified since:

- *Improvisation* offers information security practitioners and practices various ways to remain flexible and adaptive in turbulent situations;
- *Improvisation* allows for co-presence efficiency and effectiveness in detecting change and immediately taking advantage of this change.

The following sections list the possible benefits of *improvisation* as a rich and good ISRM practice:

8.3.3 Creativity Should Be All Inclusive

Practice through its organisational leaders (seen as managers of meaning and as catalysts of sense making, Weick 1993c) would be best advised to nurture creativity as a building block for various *improvisations.* Management should recognise the need to abandon stored procedural memory when faced with difficult tasks and be encouraged not to stifle the efforts of practitioners who are willing to *improvise* and to be creative while making use of their cognitive expressions.

Management of practice should be involved in as many information security practitioners' ISRM efforts as possible. This is because in emergency and crisis situations which impact the entire organisation, *improvisation* and creativity will thrive. This way management will have a first-hand encounter with this creativity and appreciate why practitioners have a:

- Willingness to forego formal functionalist approaches in favour of creatively acting in real time;
- Well-developed extemporaneous understanding of internal resources and the materials that are at hand;

It should be recognised that creativity should be accommodated in the planning, management and monitoring of information security risk within an organisation. Such an organisational culture that accommodates creativity should be open to:

1. The need for minimal structures for embellishing;
2. Re-assembly of and departures from routines;
3. Proficiency without structure.

8.3.4 Innovation and the Emergence of a Collective Mind

Practice should also be made aware of the emergence of and encourage a collective mind. This collective mind is also one of the building blocks for various *improvisations* in an organisation. This researcher has shown that collectively, teams will bear some responsibilities that individuals would be reluctant to take on. This finding is confirmed by Leede *et al.* (1999).

This research has also shown that collectively, teams will increase rates of innovation and/or solutions within the ISRM spectrum since collectively, teams are endowed with the ability to **rational-adapt** and to continuously innovate. This research finding is confirmed by Cunha and Cunha (2006). Practice should be encouraged to embrace *collective improvisation* as an expression of management culture and more specifically where there are greater bureaucratic measures which are less tolerant to collective creativity.

8.3.5 Organisational learning: Conceiving, Articulating, and Remembering.

The research has articulated the manner by which organisations staffed with skilled information security practitioners used various *improvisations* to thrive in challenging competitive contexts. Practice could benefit from this finding in the following manner:

The ability for information security practitioners to thrive in challenging circumstance is best conceived by understanding *improvisation* as a learning process. *Improvisational* skill would be encouraged when information security practitioners:

1. learn to develop a high degree of confidence in their skills to deal with non-routine events;
2. learn to develop competence at impromptu activities;
3. learn to be skilful at paying attention to their own performance and the performance of others while building on this new knowledge in order to keep the interaction going;
4. learn to maintain the pace and tempo at which others are extemporizing.
5. learn to focus on coordinating the contextual present (here and now) and not to be distracted by functionalism (structure/anticipation).

8.4 LIMITATION OF STUDY AND IDEAS FOR FUTURE RESEARCH

This section, while in no way attempts to qualify the research done, does make note of the limitations of the research.

8.4.1 Research Limitations

This research was described as a single case study from multiple situations or units of analysis. Quite rightfully, a single case study using non-pure grounded theory research techniques would not be expected to generate formal theory. However, while it is true that formal theory emerges over time (Glaser 1978) and with reflection (Strauss and Corbin 1998), this case study did in fact derive a conceptual abstraction of *improvisation* in ISRM activities in a novel way. The findings may not be generalisable nor may they pertain to other contextual and specific situations in other cases. This is rightfully understood and agreeable.

It will nevertheless remain feasible to generalize the methodology to an alternate phenomenon and an alternate case (this is discussed in **Section 8.5.5**). It would be interesting to see the results of this.

It should be noted that the conclusions and knowledge claims (see **Section 7.8.3**) for this study have been derived both inductively and deductively as explained in the previous sections. A limitation for this would be that this research would perhaps be construed as non-scientific in its analysis of data since it did not incorporate fully the deductive methods. A clear strength from this limitation is that the social scientists tell us that all human reasoning is a balance between deductive and inductive (Simon 1957). It could be argued that it is through inductive inference, based on our experience of the world, that we survive.

8.5 EVALUATION OF CONTRIBUTION

The following sections describe this research's contribution to literary work. This first part discusses some general areas the researcher felt this research contributed to literature and the second part consists of discussions about specific areas the researcher felt this research contributes to literature and practice.

As a matter of acknowledgement, this research initiated a way in which analysis from open coding of data and the identification of concepts of *improvisation* in ISRM enabled the researcher to capture deep insights on how the concepts and categories were and are related. The improvement of this theory should perhaps become evident over time when enough studies have been conducted to justify the proposal of a formal theory. Also, as a matter of acknowledgment, this research was an empirical attempt at conceptualising and validating *improvisation* in ISRM activities through the use of qualitative methods (i.e. hermeneutics). The in-depth case study allowed for the generation of concepts that represent issues previously perceived as *implicit* to the domain of ISRM (i.e. rational-adaption, *improvisation*, creativity) *as contrasted with the explicit* (ISO IEC 17799 standards, CobiT etc.) The objective was to reach an interpretive understanding of all these concepts (explicit and implicit) as a complete whole. The *Sensitising Device* was used as a lens for this.

8.5.1 Contribution in General

The researcher envisions a stage where this research work will be "constructed as important by the members of the scholarly community, relative to the accepted knowledge constituted in literature" (Locke and Golden-Briddle 1997).

The contribution this qualitative research can offer to information security practitioners is ***deep insights*** seen through detailed retrospective analysis, where the information security practitioners were without exception interested in the contextual ways of improving the ISRM techniques. Retrospectively, it should be acknowledged that this research provides ***rich and deep insights*** on the relationship the information security practitioners have with the emergent technology and the environment where they operate as social agents.

Barrett and Walsham (2004) list four specific areas of contribution that interpretive research work can be considered as making contribution to the scholarly community and practice. These are listed as follows:

- Structuring Intertextual Coherence
- Problematising Context for Contribution
- Positioning as Translating Interests
- Qualitative Generalisations as Contexts of Contribution

Each of these is discussed in turn in the following sections:

8.5.2 Specific Contribution: Structuring Intertextual Coherence

Lock and Golden- Briddle (1997) identified the process of structuring intertextual coherence as contributing to literary work for qualitative research. Intertextual coherence refers to the need for texts to establish contribution by re-presenting and organizing "*existing knowledge so as to configure a context for contribution that reflects the consensus of previous work*". Barrett and Walsham (2004) cite three suggested intertextual coherences as given by Lock and Golden- Briddle (1997).

a) ***Synthesized coherence:*** when manuscripts "*cite and draw connections between works and investigates streams not typically cited together to suggest the existence of the underdeveloped research areas*" (Barrett and Walsham 2004).
b) ***Progressive coherence:*** this indicates the "*networks of researchers linked by shared theoretical perspectives and methods working on research programs that have advanced over time*" (Barrett and Walsham 2004).
c) ***Non-coherence:*** refers to "*referenced works that are presented as belonging to a common research program but as linked by disagreements*" (Barrett and Walsham 2004).

The specific contribution envisioned by this research was that of achieving ***synthesized coherence*** i.e. by re-presenting and organizing existing knowledge about *improvisation* in a **novel** and unique way than was traditionally anticipated. This research work cited and combined works from social scientists like Ciborra C, (1994); Ciborra *et al.* (2000); Crossan and Sorrenti (1997); Cunha (2004); Cunha and Cunha (2006) who have conducted scholarly work about ***improvisation in jazz music*** with the more technical work in ***information security risk management*** from scholarly work by among others Baskerville (1991); Baskerville and Portougal 2003); Baskerville and Siponen (2002); Chambers *et al.* (2005) and Choobineh *et al.* (2007). This combination of scholarly work about *improvisation* and ISRM has *drawn connections between works and has investigated streams not typically cited together.*

The researcher exploited this *underdeveloped research area in a novel and interesting way.* The nature of this contribution was to configure a ***context for contributing to information security*** by in depth analysis of literature in IS risk management and the social sciences.

8.5.3 Specific Contribution: Problematising Context for Contribution

There are three ways of problematising an intertextual field that were identified by Lock and Golden- Briddle (1997). These three ways include:

a) Incompleteness: this is where it is claimed that the existing literature is not finished and that the present work further develops or specifies this.

b) ***Inadequacy:*** this is where it is claimed that the existing literature does not sufficiently incorporate different perspectives (relevant and important) and views to better understand the phenomena under investigation.

c) ***Incommensurability:*** this is where it is claimed not only that existing literature overlooks different and relevant perspectives but that claims in this literature are inaccurate.

The researcher problematised and provided locations and *raison d'etre* for the research efforts (Locke and Golden-Briddle 1997) by considering the present research in ISRM as being ***inadequate.*** By problematising contexts, this research showed that it is possible to independently integrate previous studies about *improvisation* (derived from the social and cognitive sciences) into the discipline of ISRM.

This is because research in ISRM has focused primarily in functionalism. The *raison d'etre* for this research therefore was that functionalist ISRM literature was inadequate, and this void was to be filled by looking at a more holistic socio-cognitive approach that also incorporated the incrementalist perspective. This fusion would be *improvisation.* It was the need to understand *improvisation* and find a method that allowed for its conceptualisation in ISRM that drove this research. This research showed that it remained possible to demonstrate that the theme of *improvisation* can establish a common framework of new knowledge into ISRM activities derived from information security practitioner insights. The intention of the researcher was an attempt to establish completeness, adequacy and commensurability of ISRM literature and *improvisation* literature (Barrett and Walsham 2004).

This research showed that it is possible to provide the existence of different levels of understanding and contexts when dealing with human behaviour in ISRM and providing a subjective understanding consistent with the everyday meanings and common sense notions which inhibit ISRM activities. This research showed it is possible to understand ISRM from the understanding bestowed by the practitioners themselves. The researcher feels that this research work is one step closer towards filling these gaps in ISRM literature.

8.5.4 Specific Contribution: Positioning as Translating Interests

Translation has been described by Barrett and Walsham (2004) as being the ongoing process by which the researcher attempts to have control over his/her knowledge claims through positioning texts in such a manner as to protect their stated contributions. It terms of positioning as translating interests, research work/articles in interpretive case studies can make a contribution when knowledge claims are accepted. It should be noted that knowledge claims are not always accepted and can be "black boxes" i.e. they are either accepted as unproblematic and uncontested or rejected (Barrett and Walsham 2004). Also important is that fact that the fate of the researcher's knowledge claim is always in the hands of later researchers/authors. In interpretive case studies, contributions as knowledge claims are always **soft facts.**

Drawing from Latour's (1987) work, there are strategies that interpretive researchers can use as positioning strategies i.e., strategies for "hardening" soft facts. These include:

a) ***Capitation:*** where the researcher leaves a margin of negotiation for each of the "*actors to transform it as he or she sees fit and to adapt it to local circumstances"*. Capitations recognise and provide a margin of negotiation in allowing later authors to translate their contribution while simultaneously recognising the need to retain subtle control (Barrett and Walsham 2004).
b) ***Framing:*** where the researcher carefully considers the audience. The aim of framing is to consider specific readership by carefully selecting words and anticipating readers' objections in advance (Barrett and Walsham 2004).
c) ***Staging:*** where researchers highlight what should be discussed, what is really interesting, and what is admittedly disputable (Barrett and Walsham 2004).
d) ***Stacking:*** where the research work draws on and extends evidence in supporting theories. In this strategy, researchers use their findings to move from specific instances to suggested applicability in the general field.

The researcher laid a series of **knowledge claims** (See **Chapter 7, Section 7.8**) that have been carefully considered and which the researcher feels he should be able to maintain a small element of control of. The researcher envisioned the contribution made to ISRM about

these knowledge claims and also the overall general research using the following positioning strategies:

- The research needed to **frame** discussions to particular audiences. The specific target audience for this research were people in the general profession of management of information security and also researchers interested in the field of information security risk management. The researcher feels that framing discussions to these target audiences has made some contributions.

- Need for **staging** which the particular audiences would find interesting. The research presented gaps in the literature that information security practitioners saw as being useful in exploring. These gaps provided ground for co-operation by information security practitioners in the dissemination of research information. The general contribution is that these information security practitioners will appreciate their own contribution in this research as seen from the eyes of this researcher.

- **Captation:** the researcher perceived that understanding *improvisation* as complementing ISRM functionalist approaches was an interesting way of looking at ISRM. The publication of some of the research work Njenga (2007); Njenga and Brown (2006a); Njenga and Brown (2006b); Njenga and Brown (2008) provided grounds for a warm reception of the work. Where there were objections or suggestions, these were incorporated in the main work. The main research work has also been done in such a way as to leave a margin of negotiation.

- **Stacking:** there was ample evidence of *improvisation*, from both the literature about organisational *improvisation* and the actual discovery of *improvisation* in ISRM activities. The fact that this was not the first research about *improvisation* in organisations revealed that the information security community showed an early interest about this phenomenon in relation to their discipline and profession. This research justified the presence of *improvisation* in ISRM and the Information Security domain as a contribution.

8.5.5 Specific Contribution: Qualitative Generalisations as Contexts of Contribution

When it comes to constructing qualitative generalisation as contexts for interpretive research contribution, it has been suggested that researchers/readers look for the ***content*** of contribution (Barrett and Walsham 2004). There are four types of generalisation for interpretive research identified by Walsham (1995). These include:

a) Development of concepts
b) Generation of theory
c) Drawing specific implications
d) Providing rich insights

This researcher discusses each of the points listed above in ways that justify contribution of this research work.

Development of concepts

This research used grounded theory techniques (open coding) to provide conceptual linkages between concepts. This research made conceptual linkages with a clear chain of analysis and discussions. The grounded theory techniques required concepts and categories to be tightly linked, while perceiving theoretical/conceptual density in terms of their properties. The research demonstrated the techniques of using the use of open coding process till theoretical saturation (Strauss 1987). *The researcher notes that the methods used for the development of concepts can be generalized and thus this research makes a contribution.*

Generation of theory

In general terms, this research used concrete, methodological choices as part of the overall analytical design of the research. The methodological choices made were in accordance with the problem statement raised and the research questions that followed. This research aimed at tightly linking these. Also the research at operational level developed theoretical concepts about *improvisation* which can be seen as valid in relation to this research. The choice of selecting information security practitioners in their various distinct departments as informants of primary data and the choice of selecting appropriate documents for review was in

accordance to the research objectives and problem statement. The data also produced and the interpretation can be seen as reflecting workmanship that is sound. *Although this theory may be perceived as context specific and therefore not easy to generalise, it remains possible to generalise the methodology and the methods towards theory generated by this research and this is to be seen as a contribution.*

Drawing specific implications

The specific implication drawn for this research was that the information security literature had not yet highlighted the ***potential positive benefit*** *improvisation* could induce in ISRM activities. *This is what this research has attempted to highlight and this is to be taken as a small contribution to the scholarly community in information security.*

Providing rich insights

One final contribution the researcher felt was of benefit to the broader scholarly community was that of providing ***rich insights*** to the scholarly community. The researcher presented some of the baseline ideas to practitioners in the industry and the scholarly community through peer reviewed publications (Njenga 2007; Njenga and Brown 2006a; Njenga and Brown 2006b; Njenga and Brown 2008). These publications were a necessary means of evaluating not only credibility of the work but of contributing additional insights to the community. The researcher's confidence in the research's contribution and insights was made possible by the following undertakings:

- Making informal conversations with information security practitioners of the host organization regarding interests in the setting being studied.
- Providing copies of a preliminary research finding to interested stakeholders and asking for written or oral commentary on the report.

8.6 FURTHER WORK

Ideally, the themes and knowledge claims about *improvisation in* ISRM activities presented in this research will assist future researchers in information security. The ideas presented here present a coherent substantive theory of how information security practitioners might approach this complex emergent area. The following suggestions for further work are offered:

- *The researcher has come up with a list of knowledge claims about improvisation in ISRM activities to which further work may be justified to prove or disprove these claims.*

- *This research did not explicitly address the role of improvisation as seen from a tacit knowledge perspective. Further work is needed to understand the role tacit knowledge play in terms of the development of shared meaning in ISRM activities. Tacit knowledge was briefly mentioned in the research.*

This research has aimed to providing an understanding of how *improvisation* is manifested in ISRM activities. As with all research, the utility of the framework for understanding *improvisation* in ISRM activities will be demonstrated by its uptake amongst the IS community and information security professionals. To conclude: from the richness and insights generated by this research, the reader may take comfort that the conclusions and knowledge claims have been derived from an intense validation and constant comparison of data (completing an inductive-deductive reasoning cycle). It is hoped that the research itself demonstrated both 'rigour and relevance' put forward as a requirement for IS research (Keen 1991). *In the end, the proposition should be noted that improvisation can be formally recognised and appreciated within ISRM.*

References

Adler, P. S., Goldofta B. and Levine D. I., (1999) “Flexibility verses Efficiency? A case Study Model of Changeovers in the Toyota Production System” *Organization Science* Vol. 10:1 pp. 43-68

Allan, G. (2003). “A critique of using grounded theory as a research method”, *Electronic Journal of Business Research Methods.* Vol 2:1 pp. 1-10

Barrett, F. J., (1998) “CODA: “Creativity and Improvisation in Jazz and Organizations: Implications for Organizational Learning”, *Organization Science* Vol. 9:5 pp. 650-622

Backhouse, J. and Dhillon, G. (1996), “Structures of responsibility and security of information systems”, *European Journal of Information Systems* Vol. 5:1 pp. 2-9.

Barrett, F. J., and Peplowski K., (1998) “Minimal Structures within a Song: An analysis of All of Me” *Organization Science* Vol. 9:5 pp. 558-560

Barrett, F.J., and Walsham (2004) “*Making Contribution from Interpretive Case Studies: Examining Process of Construction and Use*” Judge Institute of Management, University of Cambridge

Baskerville, R. (1988). “*Designing Information Systems Security”*. John Wiley & Sons, New York.

Baskerville, R. (2005) “Information Warfare: a comparative framework for Business Information Security”, *Journal of Information System Security*, Vol. 1:1 pp. 23-50

Baskerville, R. (1991), “Risk analysis: an interpretive feasibility tool in justifying information systems security”, *European Journal of Information Systems* Vol. 1 No. 2:1 pp. 121-30.

Baskerville, R. (1993) "Semantic Database Prototypes," *Journal of Information Systems*, Vol. 3:2, pp. 119-144.

Baskerville, R., and V. Portougal. (2003). “A Possibility Theory Framework for Security Evaluation in National Infrastructure Protection,” *Journal of Database Management*, Vol. 14:2 pp.1-13.

Baskerville, R. and Siponen, M. (2002), “An information security meta-policy for emergent organizations”, *Logistics Information Management*, Vol. 15:5 pp.337-46.

Baskerville, R., and Stage (1996) “Controlling prototype development through risk analysis. *MIS Quarterly.* Vol*.* 20:4 pp. 481–504.

Baumard, P., (1999) “*Tacit Knowledge in Organisations*”, London and Thousand Oaks: Sage.

Becker, J., and Niehaves B. (2007) “Epistemological perspectives on IS research: a framework for analysing and systematizing epistemological assumptions” *Information Systems Journal* Vol. 17 pp. 197-214.

Belgrad, D. (1998) "*The Culture of Spontaneity: Improvisation and the Arts in Post-war America"* The University of Chicago Press. Chicago/London.

Benbasat, I., Goldstein, D. K., and Mead, M. (1987) "The Case Research Strategy in Studies of Information Systems," *MIS Quarterly* Vol. 11:3 pp. 369–386

Bergeron, F, Buteau C and Raymond L (1991) "Identification of strategic information systems opportunities: applying and comparing two methodologies", *MIS Quarterly Vol.* 15:1 pp. 89–101

Blakley, B., McDermott, E., and Geer, D. (2001) **"**Information security is information risk management" *Proceedings of the 2001 workshop on New Security Paradigms* ACM Special Interest Group on Security, Audit, and Control, Cloudcroft, New Mexico

Birch, G.D.W. and McEvoy, N.A. (1992), "Risk analysis for information systems", *Journal of Information Technology*, Vol. 7, pp. 44-53.

Boland, R. J. (1991) "*Phenomenology: A Preferred Approach to Research in Information Systems," in Research Methods in Information Systems,* E. Mumford, R. A. Hirschheim, G. Fitzgerald, and A. T. Wood-Harper (eds.), North-Holland

Björck, F. (2004). "Institutional Theory: A New Perspective for Research into IS/IT Security". In *Proceedings of the 37th Hawaii International Conference on System Sciences (HICSS-37 2004),* 5-8 January 2004, Big Island, HI, USA: IEEE Computer Society.

Bourdieu, P., (1977) "*Outline of a theory of practice*" Cambridge UK: Cambridge University Press

Blakely, B., E. McDermott, and D. Geer. (2001). "Information Security is Information Risk Management," *Proceedings of the 2001 Workshop on New Security Paradigms* (Cloudcroft, NM, Sept. 10-13), New York: ACM Press pp. 97-104.

Brown, J. S. and Duguid, P. (1991) "Organisational Learning and Communities of Practice"; *Organisation Science*, Vol. 2 pp. 14-57

Browne H. K., Arbaugh W. A., McHugh J., Fithen W L., (2000) *A Trend Analysis of Exploitations*. http://www.cs.umd.edu/~waa/pubs/CS-TR-4200.pdf

Bryant, A. (2002), "Re-grounding grounded theory", *Journal of Information Technology Theory and Application*, Vol. 4:1,pp. 25-42.

Bunge, M. A. (1977) "*Treatise on Basic Philosophy Volume 3: Ontology I - The Furniture of the World",* Kluwer Academic Publishers, Dordrecht.

Burrell, G. and Morgan G. (1979) *Sociological Paradigms and Organisational Analysis*. Heinemann, London, U.K.

Burt, R., (1997) "The Contingent Value of Social Capital," *Administrative Science Quarterly* Vol. 42:2 pp. 339–365

Burton Group, (2005) Security and Risk Management Strategies*, "A Systematic, Comprehensive Approach to Information Security"*. Version 1.0
http://www.burtongroup.com/Content/doc.aspx?cid=644

Byrne, E., and Sahay S. (2007) "Generalisations from an interpretive study: The case of a South African community-based health information system" *South Africa Community Journal* Vol. 38 pp. 8-19

Carayon, P. and Kraemer. S. (2002) Macroergonomics in WWDU: What about computer and information system security? *Proceedings of the 6th International Scientific Conference on Work With Display Units – WWDU 2002* -- World Wide Work, at Berlin.

Carayon, P. and Smith, M.,J. (2000). "Work organization and ergonomics" *Applied Ergonomics* Vol 31 pp. 649-62.

Castano, S., Fugini, M., Martell, G., and Samarati, P. (1995). "*Database Security"*, Boston, MA: Addison- Wesley.

Cavusoglu, Hasan. (2004) "Economics of IT Security Management: Four Improvements to Current Security Practices" *Communications of the Association for Information Systems* Vol: 14:3

Chambers C., Dolske J., Iyer J., (2005) "*TCP/IP Security*" visited 19.07.2005
http://www.linuxsecurity.com/resource_files/documentation/tcpip-security.html

Chebrolu S., Abraham A., Thomas J.P. (2005) 'Feature deduction and ensemble design of intrusion detection systems'. *Computer and Security Journal*: Vol. 3 pp. 297.

Chickowski, E., (2007) "Information Security and Monitoring" *Processor,* Vol. 29:12 pp. 1-12, Available at www.processor.com

Choobineh, J., Dhillon, G., Grimaila, M.,R. (2007) "Management Of Information Security: Challenges And Research Directions" *Communications of the Association for Information Systems* Vol. 14:3 pp. 958-971

Ciborra, C, (1994) "The grassroots of IT and strategy". In *Strategic Information Systems: a European Perspective* (Ciborra C, Jelassi T, Eds), pp 3–24, John Wiley and Sons, Chichester, England

Ciborra, C. (1996) "The Platform Organization: Recombining Strategies, Structures and Surprises", *Organization Science* Vol. 7:2 pp. 103-108

Ciborra, C. (1999) *A theory of information systems based on improvisation*, in *Rethinking Management Information Systems* (Eds: W. Currie and R. Galliers), Oxford University Press, Oxford.

Ciborra, C.; Braa K.; Cordella A.; Dahlbom b.; Hanseth O.; Hepso V.; Ljungberg J.; Monterio E.; and Simon K. A. (2000) '*From Control to Drift'*., Oxford University Press, Oxford:

Cleveland, H., (1973) "Systems, Purposes and the Watergate" *Operations Research,* Vol. 21: 5 pp. 1019-1023

Creswell, J.W. (2003), "*Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*", 2nd ed., Sage Publications, Thousand Oaks, CA.

Crossan, M M., and Sorrenti M., (1997) "Making Sense of Improvisation" *Advances in Strategic Management* Vol. 14 pp. 155-180

Crotty, M., (1998), *The Foundations of Social Research: Meaning and Perspective in the Research Process*, Allen and Unwin

Cunha, M., P. (2004) “Management Improvisation” *FEUNL Working Paper No. 460.* Available at SSRN: http://ssrn.com/abstract=882455

Cunha, J. V. and Cunha, M. P. (2001) “Brave new (paradoxical) world: structure and improvisation in virtual teams” *Strategic Change* Vol. 10:6 pp. 337-347

Cunha, M.,P. and Cunha J., V. (2006) “Towards the Improvising Organisation” *Business Leadership Review* Vol. 3:4 pp. 1-6

Cunha, J. V. and Cunha, M. P. (2007) “Towards the Improvising Organisation” *Business Leadership Review – Association of MBA’s* Vol. 3:4 pp. 337-347

Cunha, M. P.; Cunha J. V.; and Kamoche, K (1999) “Organisational Improvisation; What When, How and Why “*International Journal of Management Reviews* Vol. 1:3 pp. 299-341.

Darke, P., Shanks, G. and Broadbent, M. (1998) “Successfully completing case study research: combining rigour, relevance and pragmatism” *Information System Journal*, Vol. 8:4 pp. 273-290.

Deetz, S. (1996) “Describing Differences in Approaches to Organization Science: Rethinking Burrell and Morgan and their Legacy,” *Organization Science* Vol. 7:2, pp. 191–207

Deming, W.E., (1986) “*Out of the Crisis*”, MIT Press, Cambridge, MA.

Denzin, N.,K. and Lincoln, Y.,S. (2003) “*Collecting and Interpreting Qualitative Material*”, (2nd ed.) Sage Publications, London.

Dey, I (1993) “*Qualitative Data Analysis”*, Routledge, London.

Dhillon, G. (1997) “*Managing Information Systems Security,* MacMillan Press LTD, United Kingdom.

Dhillon, G. (2001) “Violation of Safeguards by Trusted Personnel and Understanding Related Information Security Concerns”. *Computers and Security* Vol. 20:2 pp. 165- 172

Dhillon, G., (2007) "*Principles of Information Systems Security: text and cases*", John Wiley and Sons

Dhillon, G. and Backhouse, J. (2001) “Current Directions in IS Security Research: Toward Socio-organizational Perspectives,” *Information Systems Journal* Vol. 11: 2. pp.

Dhillon, G. and Moores, S. (2001) “Computer crimes: theorizing about the enemy within”. *Computers and Security* Vol. 20:8 pp. 715-723.

Doherty, N. F. (2006) “Aligning the information security policy with the strategic information systems plan. *Computers & Security* Vol. 25:1 pp. 55-63

Doherty, N. F., and H, Fulford. (2005) “Do Information Security Policies Reduce the Incidence of Security Breaches? An Exploratory Analysis,” *Information Resources Management Journal*, Vol. 18:4 pp. 21-39.

Doherty, N., Marples, C. & Suhaimi, A. (1999) "The relative success of alternative approaches to strategic information systems planning: An empirical analysis", *Journal of Strategic Information Systems* Vol. 8 pp. 263-283.

Dyer. J. S., and Sarin. R. K., (1982) 'Relative Risk Aversion' *Management Science* Vol. 28:8 pp. 875-886

Earl, M.,J. (1993) "Experiences in strategic information systems planning". *MIS Quarterly* Vol. 17:1 pp.1–24.

Earl, M., J. (1988) "Formulation of information systems strategies: Emerging lessons and frameworks". *Information Management: the Strategic Dimension* (Earl M, Ed), Claredon Press, Oxford.

Eisenhardt, K.,M. and Tabrizi B., N. (1995) "Accelerating Adaptive Processes: Product Innovation in the Global Computer Industry " *Administrative Science Quarterly*, Vol. 40:1 pp. 84-110

Eisenhardt, K.M. (1989) "Building Theories from Case Study Research," *Academy of Management Review* Vol. 14:4 pp. 532-550

Ein-Dor, P and Segev E (1978) "Organizational context and the success of management information systems". *Management Science* Vol. 24:10 pp. 1064–1077.

Eloff, J., and Eloff, M. (2003) "Information Security Management – A New Paradigm" *Proceedings of SAICSIT Conference* Pages 130 –136

ENISA (2006) "*Inventory of Risk Management/Risk Assessment methods and tools".* Accessed on 10 September 2006 http://www.enisa.europa.eu/rmra/rm_home.html

Ernst and Young, (2004) "Global Information Security Survey*". Tech News: "South African CEOs are getting more hands-on with information security issues"*
Available at;
http://estrategy.co.za/article.asp?pklArticleId=3290andpklIssueId=453andpklCategoryId=145

Farahmand, F., Navathe, S.,B., Sharp, P. and Enslow, P., H. (2003) "Managing Vulnerabilities of Information Systems to Security Incidents" *International Center for Electronic Commerce* (ICEC), ACM New York, USA

Feagin, J., Orum, A., and Sjoberg, G. (Eds.), (1991) "*A case for case study"*. University of North Carolina Press, Chapel Hill, NC.

Finne, T. (2000). "Information Systems Risk Management: Key Concepts and Business Processes," *Computers & Security* Vol. 19:3 pp. 234-242

Fitzgerald, B., and Howcroft D. (1998) "Towards Dissolution of the IS Research Debate: From Polarisation to Polarity" *Journal of Information Technology* Vol. 13:4 pp. 313- 326

Flyvbjerg, B., (2006) "Five Misunderstandings about Case Study Research" *Qualitative Inquiry* Vol. 12:2 pp. 219-245

Forno, R. and Baklarz R. (1999) '*The Art of Information Warfare'*: Insights into the knowledge warrior philosophy, Universal Publishers, MB, AU.

Furnell, S., Thuraisingham, B. and Sean, W. X. (2006) "Security Management, Integrity, and Internal Control in Information Systems*"*, *IFIP TC-11 WG 11.1 and W, G 11.5 Joint Working Conference* Vol. 193

Galbraith, J. (1977) '*Organisation Design'*, Addison-Wesley, Reading, Mass.

Galliers, R., D. (1987) "Information systems planning in the United Kingdom and Australia – a comparison of current practice". *Oxford Surveys of Information Technology* Vol. 4 pp. 223–255.

Glaser, B.G. (1978). "*Theoretical Sensitivity: Advances in the Methodology of Grounded Theory*". Sociology Press, California.

Glaser, B.G. (1992). "*Basics of Grounded Theory Analysis: Emergence Vs. Forcing*". Sociology Press: California.

Glaser, B., G. (2001). "*The Grounded Theory Perspective: Conceptualization Contrasted with Description"* (http://www.groundedtheory.com/soc14.html) Sociology Press, Mill Valley, Ca.

Glaser, B.G. & Strauss, A. L. (1967). "*The Discovery of Grounded Theory: Strategies for Qualitative Research*". Aldine Transaction: New Jersey.

Gonzalez, Jose J, and Agata Sawicka. (2002). "A Framework for Human Factors in Information Security". *Proceedings of the International Conference on Information Security (ICIS'02),* at Rio de Janeiro, Brazil.

Grover V. and Segars A., H. (2005) "An empirical evaluation of stages of strategic information systems planning: patterns of process design and effectiveness**"** *Information and Management* Vol. 42:5 pp. 761-779

Guba, E B & Lincoln, Y S (1994) "Competing Paradigms in Qualitative Research" In *Handbook of Qualitative Research,* ed. N K Denzin & Y S Lincoln, London.

Henning. E., (2002) "Teaching qualitative methodology for educational research: cultivating communities of deep learning practice*" Education as Change* Vol. 6:1 pp. 52-68

Henning. E., (2004) "*Finding your way in Qualitative Research*", Van Schaik Publishers, Pretoria.

Hirschheim, R. and Klein HK, (1989) "Four Paradigms of Information Systems Development" *Communications of the ACM*, Vol. 32:10 pp. 1199–1215.

Hirschheim R., Klein, H., and Lyytinen K. (1996), "Exploring the Intellectual Foundations of Information Systems," *Accounting, Management and Information Technologies,* Vol. 6:1 pp. 1–64.

Howard J., (1997) "*An Analysis Of Security Incidents On The Internet: 1989 – 1995*.– PhD thesis, Carnegie Mellon University.

Wiander, T., and Jarkko M. Holappa, J., M. (2006) "Theoretical framework of ISO 17799 compliant information security management system using novel ASD method". proceedings of the *IAEA Technical Meeting on Cyber Security of Nuclear Power Plant Instrumentation, Control and Information Systems",* 17-20, Idaho Falls, USA.

Hu, Q. Paul Hart, P., and Cooke, D. (2007) "The role of external and internal influences on information systems security – a neo-institutional perspective" *Journal of Strategic Information Systems* Vol. 16:2 pp. 153–172

Information Systems Audit and Control Association (2008). "*Board Briefing on IT Governance 2nd Edition"*. Conducted by IT Governance Institute (ITGI TM). ISACA.

ISO / IEC "ISO / IEC (2002) "Risk Management–Vocabulary" Guide 73, Guidelines for use in standards

ISO/ IEC (2005) Information technology -- Security techniques -- Information security management systems – Requirements available at http://www.iso.org/iso/catalogue_detail?csnumber=42103

IT Gov, (2000) "IT Governance: a Pocket Guide".-http://www.itgovernance.co.uk/it_governance.aspx

ITGI, (2003) "*Board Briefing on IT Governance*", 2nd Edition ITG Institute, http:// www.itgi.org

Jackson, W., (2006) "Time to focus on security, not compliance", *Government Computer News*, Vol. 25:8 pp. 28-40.

Kamoche, K.,N., Cunha, M.,P., and Cunha J., V. (2002) "*Organisational Improvisation*" Routledge, London.

Kaplan, B. and Maxwell, J. A (1994) "Qualitative Research Methods for Evaluating Computer Information Systems," in *Evaluating Health Care Information Systems: Methods and Applications,* J. G. Anderson, C. E. Aydin, and S. J. Jay (eds.), Sage, Thousand Oaks, CA. pp. 45–68.

Keen, P. G. W. (1991). "*Shaping the Future: Business Design through Information Technology"*. Harvard Business School Press, Boston, MA.

Kegan, D. L., (1971) "Organizational Development: Descriptions, Issues and Some Research Results" *The Academy of Management Journal*, Vol. 14:4 pp. 453-464

Killmeyer, J., and Tudor, K. (2006) "*Information Security Architecture*" CRC Press

Klein H. K., and Meyer M., (1999) "A Set of Principles for Conducting and Evaluating Interpretive Field Studies in Information Systems" *MIS Quarterly* Vol. 23:1 pp. 67-94

Kotulic, A.G. and Clark, J.G. (2004), "Why there aren't more information security research studies", *Information and Management,* Vol. 41:5 pp. 597-607

Krueger, R. A. (1989). "*Focus Groups: A Practical Guide for Applied Research".* Sage Publications, Newbury Park, CA.

Latour, B., (1987) "*Science in Action*" Harvard University Press, Cambridge, MA,

Lave, J., and Wenger, E. (199)."*Situated Learning: Legitimate Peripheral Participation*," Cambridge University Press, Cambridge, UK.

Lederer A., L. and Mendelow A., L. (1990) "The impact of the environment on the management of information systems" *Information Systems Research* Vol. 1:2 pp. 205–222

Lee, A. S. (1989) "A Scientific Methodology for MIS Case Studies," *MIS Quarterly* Vol. 13:1 pp. 33–52

Lee, A., S. and Baskerville, R., L. (2003) "Generalizing Generalizability in Information Systems Research" *Information Systems Research* Vol. 14:3 pp. 221-243

Leede J., Nijhof, A.,H., J. and Fisscher O, M. (1999) "The Myth of Self-Managing Teams: A Reflection on the Allocation of Responsibilities between Individuals, Teams and the Organisation" *Journal of Business Ethics* Vol. 21:2/3 pp. 203-215

Lewis J. and Ritchie J (2003) "*Qualitative Research Practise-A Guide for Social Science Students"* Sage Publications, London

Locke, K. and Golden-Briddle, K. (1997), "Constructing Opportunities for Contributions: Structuring Intertextual Coherence and Problematising in Organisational Studies", *Academy of Management Journal* Vol. 40:5 pp. 1023-1062

Luftman, J. and E.R. McLean (2004) "Key Issues for IT Executives"*, MIS Quarterly Executive* Vol. 3:2 pp. 89-104.

Mangham, Iain L. (1986), "*Power and Performance in Organizations: An Exploration of Executive Process"*. Basil Blackwell, Oxford.

Marion, R. (1999) "*The Edge of Organization: Chaos and Complexity Theories of Formal Social Systems".* Sage, Thousand Oaks, CA.

Maturana, H. R., and Varela, F..J.(1980) "*Autopoiesis and Cognition-The Realization of the Living,"* Dordrecht Reidel, Dordrecht.

McFadzean, E., Ezingeard J., and Birchall, D., (2007) "Perception of risk and the strategic impact of existing IT on information security strategy at board level" *Online Information Review Vol*. 31: 5 pp. 622-660

McGinn K. L. and Keros A. T., (2002) "Improvisation and the Logic of Exchange in Socially Embedded Transactions" *Administrative Science Quarterly*, Vol. 47:3 pp 442-473

Merriam-Webster Online Dictionary. (2009) Retrieved May 29, 2009, from http://www.merriam-webster.com/dictionary/methodology

Middleton G., (2006) "Security and Regulatory Activity*" Computer Business Review* Vol.17:5 pp. 32-34.

Miller, H.E. and Engemann, K.G. (1996), "A methodology for managing information-based risk", *Information Resources Management Journal,* Vol. 9:2 pp.17-24.

Miner A. S., Bassoff P. and Moorman C., (2001) "Organizational Improvisation and Learning: A Field Study" *Administrative Science Quarterly* Vol. 46:2 pp. 304-337

Minzberg H (1979) "*The Structuring of Organizations".* Prentice Hall International, United Kingdom.

Minzberg, H (1994) "*The Rise and Fall of Strategic Planning".* Prentice Hall International, United Kingdom.

Minzberg, H and Quinn J (1996) "*The Strategy Process: Concepts Contexts and Cases"*. Prentice-Hall Inc, NJ.

Mitnick, K. (2005) "*The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders and Deceivers"* John Wiley and Sons, Inc. New York, NY.

Mitnick. K., Simon, W., and Wozniak, S. (2002) "*The Art of Deception: Controlling the Human Element of Security"* John Wiley and Sons, Inc. New York, NY.

Miyake, N. (1997). "Constructive interaction and the iterative process of understanding" *Cognitive Science*" Vol. 10:2 pp. 151-177

Moorman, C., and Miner, A. (1998) "Organisational Improvisation and Organisational Memory," *Academy of Management Review* Vol. 23:4 pp. 698-723

Myers, M. D., (1997a) "Qualitative Research in Information Systems" *MIS Quarterly* Vol. 21:2 pp. 241-242.

Myers, M. D., (1997b). "Critical Ethnography in Information Systems" *Proceedings of the IFIP TC8 WG 8.2 international conference on Information systems and qualitative research Pennsylvania, US.* (pp. 276-300).

Neuman, P. G., (1995) "*Computer Related Risks*" The ACM Press,

National Institute of Standards and Technology (NIST): (2003) US Department of Commerce "*Risk Management Guide for Information Technology Systems*" Special Publication 800 -30
http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

Njenga, K., (2007). "Conceptualising Improvisation in Information Security Risk Management Activities", *(Doctoral Consortium) Proceedings of the 11th Pacific Asia Conference on Information* Auckland, New Zealand.

Njenga, K., and Brown, I., (2006a). On Improvisation: Framework For The Soft Approach to Managing Security Risk – South African Context, *Proceedings of the 3rd 2006 IT Governance International Conference 2006*, Auckland, New Zealand.

Njenga, K., and Brown, I., (2006b). Conceptualising the Influence of Tacit Knowledge in Security Risk Management Activities, *Proceedings of the 6th Conference on Information Security South Africa 2006*, Sandton, South Africa.

Njenga, K., and Brown, I.,(2008).Collective Improvisation: Complementing Information Security Frameworks with Self Policing, *Proceedings of the 7th Conference on Information Security South Africa June 2008*, Auckland Park, South Africa.

OECD Guidelines (2006) "*OECD Guidelines for the Security of Information Systems and Networks*" Available: http://www.oecd.org/dataoecd/16/22/15582260.pdf. Accessed on 24.8.2006

Office, US Government Accounting (1996) "*Information security*: *Computer attacks at department of defence pose increasing risks*," Tech. Rep. GAO/AIMD-96-84, U.S. Government Accounting Office.

Orlikowski, W. J., and Baroudi, J. J. (1991) "Studying Information Technology in Organizations: Research Approaches and Assumptions," *Information Systems Research* Vol. 2:1 pp. 1–28

Orlikowski, W.J. (1993), "CASE tools as organizational change: investigating incremental and radical changes in systems development", *MIS Quarterly,* Vol. 17:3 pp. 309-40.

Pandit, N., R. (1996) "The Creation of Theory: A Recent Application to the Grounded Theory Method" The Qualitative Report Vol. 2:4 pp. 1-15

Parker, D., B. (2002) '*Motivating the Workforce to Support Security Objectives':* A Long Term View*;* Fighting Computer Crime, A New Framework for Protecting Information, John Wiley and Sons 1998

Parker X., L. (2001) "Internal auditors need to develop an understanding of information security risk; discusses information security threats, risk assessment, monitoring and outsourcing": Institute of Internal Auditors; *Internal Auditor,* Vol. 58:1.

Parkinson, M. J. A. and Baker N.J. (2005) 'IT and Enterprise Governance', *Information Systems Control Journal*, Vol. 3 pp. 19-24

Peattie L., (2001) "Theorising planning: Some comments on Flyvbjerg's Rationality and Power" *International Planning Studies* Vol. 6:3 pp. 257-262

Peltier, T.R. (2001) "*Information Security Risk Analysis"* Auerbach, New York.

Perry L.T., (1991) "Strategic Improvising*: How to Formulate and Implement Competitive Strategies in Concert*" *Organisational Dynamics* Vol. 19:4 pp. 51-64

Polanyi, M. (1966) "*The Tacit Dimension"*, Routledge and Kegan Paul, London.

Power, R. (2000) "*Tangled Web: Tales of Digital Crime from the Shadows of Cyberspace"*. 1st ed. Indianapolis, IN

Pozzebon M., (2003) "*Conducting and Evaluating Critical Interpretive Research: Examining Criteria as a Key Component in Building Research Tradition*". HEC, Montreal

Premkumar, G. and King W., R .(1991) "Assessing Strategic Information Systems Planning". *Long Range Planning* Vol. 24:5 pp. 41–58.

Pyburn PJ (1983) "Linking the MIS plan with corporate strategy: An exploratory study" *MIS Quarterly* Vol. 7:2 pp. 1–14.

Raghunathan, B. and Raghunathan, T.,S. (1991) “Information systems planning and effectiveness: an empirical analysis”, *Omega* Vol. 19:2/3 pp. 125–135.

Raster, M. (1994) "Process architecture and information processing," in: *Process management* (in German), M. Gaitanides, R. Scholz, A. Vrohlings and M. Raster (eds.), Hanser, Carl, GmbH & Co., München u. a. pp. 123-142.

Reed, M. and D. L. Harvey (1992) ‘The New Science and the Old: Complexity and Realism in the Social Sciences’, *Journal for the Theory of Social Behaviour* Vol. 22:4 pp. 353–80.

Rodon, J. and Pastor, A. (2007) “Applying Grounded Theory to Study the Implementation of an Inter Organizational Information System.” *The Electronic Journal of Business Research Methods* Vol. 5:2 pp. 71 – 82

Rosenhead, J. and J. Mingers (2001a) “*Rational Analysis for a Problematic World Revisited*: *Problem Structuring Methods for Complexity, Uncertainty and Conflict”*. John Wiley and Sons, Chichester.

Rubin, H.J. and Rubin, I.S. (2005) “*Qualitative Interviewing: The Art of Hearing Data”. (*2nd Edition) Sage, Thousand Oaks, CA.

Rushton, K., (2005) “The UK Framework Governing Internal Control” SOX 404 in Canada: *An OpenForum British Columbia Securities Commission Morris J. Wosk Centre for Dialogue Vancouver, British Columbia;Available at http://www.bcsc.bc.ca/uploadedFiles/Rushton_SOX_2005-05-18.pdf*

South African Bureau of Standards (SABS) *Information Technology – Code of Practice for Information Technology Risk Management, SABS ISO/IEC 17799*.

Salmela, H., Lederer, A.,L. and Reponen, T. (2000) “Information systems planning in a turbulent environment” *European Journal of Information Systems* Vol. 9:1 pp. 3–15

Sambamurthy V, Zmud RW and Byrd TA (1994) “The comprehensiveness of IT planning processes: a contingency approach”. *Journal of Information Technology Management* Vol. 5:1 pp. 1–10.

Sarin, R. K., and Weber M., (1993) ‘Risk Value Models’: *European Journal of Operations Research* Vol. 70 pp. 135-149

Schneier, B. (2000) “*Secrets and Lies: Digital Security in a Networked World”.* John Wiley and Sons, Inc, New York.

Schon, D., (1983) “*The Reflective Practitioner: How Professionals Think in Action”*, Temple Smith, London.

Schultz E. (2005) “Security Views”: *Computers and Security,* Vol. 24:5 pp. 347-348

Schultze U., (2000) “A Confession Account of an Ethnography about Knowledge Work” *MIS Quarterly* Vol. 24:1 pp. 3-41

Scott, W.R., (2001) “*Institutions and Organizations”* Sage Publications, Thousand Oaks, CA

Segars, A. & Grover, V. (1999) Profiles of strategic information systems planning. *Information Systems Research* Vol. 10:3 pp.199-232

Segars, A., Grover, V. & Teng, J. (1998) Strategic information systems planning: Planning system components, internal co-alignment, and implications for planning effectiveness. *Decision Sciences*, Vol. 29:2 pp. 303-344.

Scott, W. R. (1987) "The adolescence of institutional theory," *Administrative Science Quarterly* 32:493-511.

Scribner, S. (1984) "Studying working intelligence". In B. Rogoff and J. Lave (Eds.), "*Everyday cognition: Its development in social context"*, Harvard University Press, Cambridge

Simon, H. A. (1957). *Models of man: Social and rational*. John Wiley and Sons, New York.

Siponen M., T. (2000) "A Conceptual foundation for organisational Information security awareness"; *Information Management and Computer Security journal* Vol. 8:1 pp.31-41

Siponen, M., T. and Kukkonen H.,O. (2007) "A Review of Information Security Issues and Respective Research Contributions" *The DATA BASE for Advances in Information Systems* Vol. 38:1 pp. 60-80

Smith, B. Brian, K. Microsoft Security Team (2003) "*Security Kit*": Microsoft Windows Security Resource Kit, Microsoft Press.

Stoneburger G., Coguen A., and Feringa A.; (2001). *Risk Management Guide for Information Technology Systems*. NIST – National Institute of Standards and Technology. Special Publication 800- 30. US Department of Commerce.

Straub, D.W. and Welke, R.J., (1998) 'Coping with Systems Risk: Security Planning Models for Management Decision Making', *MIS Quarterly*, Vol. 22:4 pp. 441-464.

Strauss, A. (1987) "*Qualitative Analysis for Social Scientists"*. Cambridge University Press, Cambridge, UK.

Strauss, A., and Corbin, J. (1990). "*Basics of qualitative research: Grounded theory procedures and techniques*". Sage Publications, Newbury Park, CA.

Strauss, A., and Corbin, J. (1998). "*Basics of qualitative research: Techniques and Procedures for Developing Grounded Theory*." Sage Publications, Newbury Park, CA.

Suchman, L. (1987) "*Plans and Situated Actions: The Problem of Human-Machine Communication",* Cambridge University Press, Cambridge, UK.

Parsons, T., (1949) "*Essays in Sociological Theory",* Free Press, Glencoe, Ill.

Thompson, M .E. and Von Solms R, (1997) "An effective information security awareness program Industry" , Proceedings of WG 11.2 and WG 11.1 of TCl I (IFIP): *Information Security for Small Systems to Management of Security Infrastructure*

Trauth, E.M. and Jessup, L.M. (2000), "Understanding computer-mediated discussions: positivist and interpretive analyses of group support system use", *MIS Quarterly,* Vol. 24:1 pp. 43-79.

Trcek, D., Trobec, R., Pavesic, N., & Tasic, J.F. (2007). “Information systems security and human behaviour”. *Behaviour & Information Technology*, Vol. 26:2, pp. 113-118.

Tudor J.,K. (2001) "*Information Security Architecture: An Integrated Approach to Security in the Organization*" AUERBACH; New York.

Urquhart, C. (1997), “Exploring analyst-client communication: using grounded theory techniques to investigate interaction in informal requirements gathering”, in Lee, A.S., DeGross, J.I. and Liebenau, J. (Eds), Information Systems and Qualitative Research, Chapman & Hall, London, pp. 149-81.

Vera, D. and Crossan M. (2004) “Theatrical Improvisation: Lessons for Organizations”, *Organization Studies*, Vol. 25:5 pp. 727-749

Vitale M., R., Ives, B., and Beath, C., M. (1986) “Linking information technology and corporate strategy: an organizational view”. *Proceedings of the Seventh International Conference on Information Systems* 15–17 Dec.

Von Solms, B., and Von Solms, R., (2004) “The 10 Deadly Sins of Information Security Management” *Computers & Security*, Vol. 23:5 pp 371-376

Von Solms, B, (2006). “Information Security – The Fourth Wave” *Computers & Security* Vol. 25:3 pp. 165-168

Von Solms B (2006) “ICT Risk Governance in a University Environment” *Proceedings of the Conference on Information Technology in Tertiary Education, Pretoria, South Africa, 18–20 September*

Von Solms B and Von Solms R (2005) ’From information security to…business security’? *Computer and Security Journal* Vol. 24:4 pp. 271-273

Vorster, A. & Labuschagne, L. (2006). A new comparison framework for information security risk analysis methodologies. *South African Computer Journal*. Vol. 37 pp. 98-106

Walker, G. Kogut, B. and Shan, W. (1997) “Social Capital, Structural Holes and the Formation of an Industry Network,” *Organization Science* Vol. 8:2 pp.109–125

Walsham, G. (1993) “*Interpreting Information Systems in Organisations*” John Wiley and Sons New York, NY.

Walsham, G. (1995) “Interpretive Case Studies in IS Research: Nature and Methods.” *European Journal of Information Systems* Vol. 4:2 pp. 74-81

Walsham, G. (2006) “Doing Interpretive Research” *European Journal of Information Systems,* Vol. 15 pp. 320-330

Webb G., R. (2006) ‘Planning to improvise: the importance of creativity and flexibility in crisis response’ *International Journal of Emergency Management*, Vol. 3:1 pp.66-72

Webb P., Pollard, C., and Ridley, G. (2006) "Attempting to Define IT Governance: Wisdom or Folly?" *Proceedings of the 39TH Hawaii International Conference on System Science* Hawaii, US.

Weber. E. U., and Milliman. R. A., (1997) "Perceived Risk Attitudes: Relating Risk Perceptions to Risky Choice" *Management Science* Vol. 43:2 pp. 123-144

Weick K.., (1993b) "*Organisational Redesign as Improvisation*," in G.P. Huber and H. W. Glick (Eds.), *Organisational Change and Redesign*, Oxford University Press, Oxford: (pp. 346-379).

Weick K., (1993c) "The Collapse of Sense making in Organisations: The Man Gluch Disaster" *Administrative Science Quarterly* Vol. 38 pp. 628-652

Weick, K. (1998) 'Improvisation as a mindset for organizational analysis', *Organization Science*, Vol. 9:5 pp. 543–555.

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

Weill, P., and Woodham, R. (2002) "Don't' Just Lead, Govern: Implementing Effective IT Governance *CISR Working paper, No 326.*

Welman C., Kruger F. & Mitchell B. (2007). "*Research Methodology*". Oxford University Press: South Africa.

Westrup, C., (1996) "Transforming Organizations through Systems Analysis: Deploying New techniques for Organizational Analysis," in *Information Technology and Changes in Organizational Work*, W. Orlikowski et al. (eds.) , pp.157-176.

Wheeler M., and Venter H.,(2006) *"* Change Management: A case study at the University of Pretoria", *Proceedings of the Conference on Information Technology in Tertiary Education (CITTE)* Pretoria, South Africa

Winkler, I. (2007) "*Zen and the art of information security*" Syngress Rockland, MA

Yates, J., and Orlikowski, W.J. (1992), "Genres of organizational communication: a structurational approach to studying communication and media", *Academy of Management Review*, Vol. 17:2 pp. 299-326.

Yin, R., K. (1994) "*Case Study Research, Design and Methods", (*2nd ed.) Sage Publications, Newbury Park, CA.

Yin, R., K. (2003) "*Case Study Research: Design and Methods"*, (3rd ed.) Sage Publications, Newbury Park, CA.

Yue, W. T., M. Cakanyildirim, Y. U. Ryu, and D. Liu. (2007). "Network Externalities, Layered Protection, and IT Security Risk Management," *Decision Support Systems*, Vol. 44:1 pp. 1-16.

Zuboff, S. (1988) "*In the Age of the Smart Machine",* Basic Books, New York.

APPENDICES

APPENDIX 1: INTERVIEW QUESTIONS DIRECTED TO INFORMATION SECURITY RISK PRACTITIONERS

General Questions

1. How does your organisation carry out ISRM activities in general?
2. How is the organisation structured, generally in terms of information security?
3. Who is responsible for information security needs for the organisation?
4. When do you ever delegate responsibilities?

Specific: Information Assets Access and Data Control

5. How does your organisation ensure accountability and confidentiality of information?
6. How do you make sure that information is not passed to unauthorised persons?
7. Who classifies sensitive information?

Specific: Information Security Architecture

8. What do you consider confidential information? What systems do you consider critical? How do you protect these systems?
9. How do you establish procedures/policies for information security architecture/design e.g. for password system?
10. What are the organisation's security roles and responsibilities were based on?
11. What sort of information security forums are there and what is the role of forums?

Specific: Information Security Policies

12. What criteria does the organisation use to determine and assign responsibilities for implementing information security policy?
13. Who plays a greater role towards helping define the organisation's information security needs and policy?
14. Do you ever follow procedures/policies when carrying out ISRM activities?
15. What established procedures/policies are there for accessing programmes/applications?
16. How do you co-ordinate your ISRM efforts? When is experience important in this co-ordination?
17. What assurances does the organisation have with regard to ensuring users are capable of applying information security policy and procedures?

Specific: Information Security Event Monitoring

18. How do you monitor the organisation's network systems? How do you use the intrusion detection systems?
19. Who monitors unauthorised system usage?
20. How do you respond to intrusions and incidents?
21. Who ensures and checks and monitors for the following? (a) dormant accounts; (b) antivirus updates; (c) shared files; (d) account lock out; (e) the use of regular passwords?
22. How do you respond to the monitoring process when carried out based on set standards specified when there are deviations?

Specific: IT Governance and Regulatory Compliance

23. Who influences compliance efforts? Who is responsible for IT Governance?
24. How do you rate your compliance efforts? What best practices are used?
25. Do you follow any guidelines? Is so which ones are they?

26. How does the organisation ensure the co-ordination of security controls are representative of the organisation's needs?
27. Are there times that users do not follow procedures?
28. What sorts of measures are taken to encourage a multi-disciplinary approach to information security?
29. Do you feel that policies and procedures tie you down in some way?

Specific: Disaster Recovery and Business Continuity

30. How do you ensure business continuity?
31. How do you conduct your disaster recovery exercises?
32. What happens if systems go down? How do you respond? Who co-ordinates these efforts?
33. Can you recollect on moments that reveal how you responded to emergency situations?

APPENDIX 2: OPEN CODING UNIT OF ANALYSIS ONE – INFORMATION ASSETS ACCESS AND DATA CONTROL

STEP 1 **Data Incidents** **(Transcribed Interviews)**	**STEP 2** **Context of Data Incident**	**STEP 3** **Researcher's memos** Determine Codes in vivo and other generated as underlined)	**STEP 4** **Level**	**STEP 5** **Concepts generated**	**STEP 6** **Categories** (See Section 4.4.1)
so we quickly had to make [create] a few more categories…so it doesn't just get as simple as you just having internet access ..and you don't get this.. [but rather] you having internet access and you belong to marketing…and you belong to IT [134]	Profiling users based on user activities was found to be critical. However, the nature of the observed profiling was most interesting. Multiple users had multiple requirements. The creation of extra categories outside of the normal categories was improvised–this had never been done before. i.e. new ways of defining categories that allowed for innovative information access.	***Classification and Control of Information Assets*** 2. Implies quick reaction in terms of profiling users and determining data security and classification levels based on information requirements	Operational Activity	**Quick reaction** to data access security levels	(Process) Improvisation
and we did and worked on exactly what they said.. and of course within the first few days.. of putting access controls in [the system]…we got hundreds and hundreds of calls…saying they couldn't get through.. they said that they wanted to go to selling sites.. whatever…and they couldn't go to see what was on hundreds of other sites [135]	The IT team improvised (employed automatic thinking towards) new control frameworks that guided the abuse of internet by users and helped place appropriate security controls to users.	***Accountability of information assets through access control*** 6. Implies being resourceful and providing reflexivity by placing data security controls	Operational Activity	**Being resourceful** in placing data access security controls	(Process) Improvisation

[134] C120-Appendix 10
[135] C119-Appendix 10

STEP 1 **Data Incidents** **(Transcribed Interviews)**	STEP 2 **Context of Data Incident**	STEP 3 **Researcher's memos** Determine Codes in vivo and other generated as underlined)	STEP 4 **Level**	STEP 5 **Concepts generated**	STEP 6 **Categories** (See Section 4.4.1)
it happens all the time…so in a lot of the applications and cases we have established that we don't have to give them that [admin] kind of access, but then there are I mean… it happens, … internet access…we used to talk about restricting internet access…obviously, but so far [for instance unlike] in [name withheld] America where they have a big database where they categorizing data… (internet restrictions) by but obviously in [back here] [136]	There is no clearly defined way of restricting user access by these practitioners so they formulate new ways of restricting based on their own understanding of security and that of the user's access requirements. In a sense, they improvised on information access	***Authorization process of Information facilities*** 1. Implies being imaginative in strengthening security controls on defined user roles and business security needs	Operational Activity	**Being imaginative** in data access security controls	(Process) Improvisation
in terms of safety of information, manipulating information, metadata around information and stuff like that [137] *The guy who heads up the department in respect to information system's intelligence is Peter Versfield…so we've go a whole department structured around data warehousing* [138]	Information is (in a data warehouse) is considered a high value assets. The security measures taken around information manipulation from the warehouse are structured around information system intelligence. The practitioners suggested that the activities they carried out revolving around securing information were emergent as the information and systems changed.	***Inventory Management and Information Asset Classification*** 1. Implies being practical in data/information assets classification and information intelligence ensuring information security	Strategic Activity	**Being practical** in data Structuring	(Collective) Improvisation

[136] C117-Appendix 10
[137] C59-Appendix 10
[138] C58-Appendix 10

STEP 1 **Data Incidents** **(Transcribed Interviews)**	STEP 2 **Context of Data Incident**	STEP 3 **Researcher's memos** Determine Codes in vivo and other generated as underlined)	STEP 4 **Level**	STEP 5 **Concepts generated**	STEP 6 **Categories** (See Section 4.4.1)
Coz, we had to do it… but in those groups…and what happens in the access aspect is that they can actually modify the database…and Derek is actually the one who approves this [139]	How systems are modified is often forced by exceptional circumstances such as users' information and data access demands. Such modification has to be balanced in such a way as not to compromise security while at the same time not to stifle business processes. In this case, the modification was improvised	***Authorization process for database modification*** 1. Implies that with limited options being quick witted in reacting to information database modifications	Operational Activity	**Being Quick - witted** in database modification	(Process) Improvisation

[139] C123-Appendix 10

APPENDIX 3: OPEN CODING UNIT OF ANALYSIS TWO - INFORMATION SECURITY ARCHITECTURE

STEP 1 **Data Incidents** **(Transcribed Interviews)**	**STEP 2** **Context of Data Incident**	**STEP 3** **Researcher's memos** Determine Codes in vivo and other generated as underlined)	**STEP 4** **Level**	**STEP 5** **Concepts generated**	**STEP 6** **Categories** (See Section 4.4.1)
and whether there is compliance you know considering security you know whether there are best solutions to match the technology platform… stuff like that [140]	The current architecture and technology platform (a fusion of many platforms) could not be matched with proposed policy compliance models so the nature of compliance had to be innovative based on the technology architecture, resulting to the process of compliance being improvised	***Compliance efforts and Information Architecture Specification*** 2. Implies being rational adaptive in ensuring compliant information architecture.	(Process) Improvisation	Tactical Activities	Being **rational adaptive** in determining compliant architecture
[The] middleware team...gives a human aspect to the way we design things...such that the whole way we design things is very middleware driven.. we've got a rich...middleware architecture [141]	The middleware team was socially driven with the social conditions permitting the middleware team to explore and discover new technical designs that interfaced between people, business processes and technology. Their discoveries were shaped by time and resources.	***Security Design requirements and Specifications*** 2. Implies lateral thinking by the middleware team charged with designing the security requirements of middleware architecture	(Process) Improvisation	Tactical Activities	**Lateral thinking** in designing middleware architecture
yes, but then it has to.. .it is going to be another workshop, to actually	Based on the feedback obtained, the practitioners were in the process of	***Information architecture requirements on Risk***	(Process) Improvisation	Tactical Activities	**Being imaginative** in

[140] C62-Appendix 10
[141] C66-Appendix 10

STEP 1 **Data Incidents** **(Transcribed Interviews)**	STEP 2 **Context of Data Incident**	STEP 3 **Researcher's memos** Determine Codes in vivo and other generated as underlined)	STEP 4 **Level**	STEP 5 **Concepts generated**	STEP 6 **Categories** (See Section 4.4.1)
realign our risk profile...to align with the corporate risk profile [142]	innovatively realigning the technology and operational risk profile with that of the corporate risk profile in ways not contemplated before.	1. Implies <u>being imaginative</u> by providing workshops for <u>reviewing structure and architecture.</u>			reviewing structure and architecture
there has been a lot…[of] good stuff that the[se] guys for instances like Etienne (Enterprise Risk]… they have done a lot of work… they have complied with every possible standard/ framework [143] *We have got the Architecture forum, which sits under Kevin Cricker… and uum. We also had a.. the stuff that I'm more involved in, in making sure that.. there is a compliance architecture in terms of business*[144]	A deeper enquiry revealed that although there was a feeling that compliance was achievable in every possible way, this was not the case. The practitioners did not realize that they filled their own compliance objectives by improvising in one form or another.	***Information Architecture Forum for Information Security*** 1. Implies <u>exceptionality</u> in applying implicit knowledge that <u>ensures architecture compliance</u>	(Collective) Improvisation	Strategic Activities	**Exceptionality** in compliant Architecture
so that's more in the area that I'm based in…all our designs… all the designs that the guys do have to go through the architecture forum…so the Architecture forum have to pull it apart	The technology and the design must always make business sense. In this case a large number of technologies coupled with a variety of designs, created an avenue for the forum to devise improvised solutions	***Information Architecture Design and Acceptance*** 1. Implies being <u>inventive in</u> vetting designs for <u>Information Architecture as</u> technology and designs are	(Collective) Improvisation	Strategic Activities	**Being inventive** in vetting Information Architecture designs

[142] C56-Appendix 10
[143] C9-Appendix 10
[144] C60-Appendix 10

STEP 1 **Data Incidents** **(Transcribed Interviews)**	STEP 2 **Context of Data Incident**	STEP 3 **Researcher's memos** Determine Codes in vivo and other generated as underlined)	STEP 4 **Level**	STEP 5 **Concepts generated**	STEP 6 **Categories** (See Section 4.4.1)
to see whether it makes sense from a technology point of view [145] *….Um to ensure that they comply with whatever policy and standards that they have devised or as defined by the board* [146]	that made business sense and that there is compliance	constantly vetted for rollout and use.			
well…that's actually where the mind set has to change…that's why the Information Security office used to be in IT…but now I'm actually reporting top Corporate governance board [147]	The unprecedented complexities of information security necessitated the creation of a seat in the board. The creation was also unprecedented, and aimed at facilitating compliance requirements.	***Architecture Compliance and Reporting Requirements*** 1. Implies the rational adaptive way of organisational restructuring to facilitate reporting requirements	(Collective) Improvisation	Strategic Activities	**Rational adaptive** Organisational restructuring
where we develop requirements specifications for reviewing the process.. we've got systems requirement specifications…doing all the system's stuff with the data…and then we've got integration specifications…in terms of how does this system send information to another system…or the middleware stuff…and	It was understood that the ideas for the development of compliant specifications, and system integrations were conceived as events unfolded. As new systems were introduced new ways and ideas were conceived on how to integrate these into the mainstream applications.	***Operational Procedures and Responsibilities*** 1. Implies being resourceful in developing home-grown holistic Information Architecture Integration solutions	(Process) Improvisation	Tactical Activities	**Being resourceful** in information Architecture Integration

[145] C61-Appendix 10
[146] C7-Appendix 10
[147] C12-Appendix 10

STEP 1 **Data Incidents** **(Transcribed Interviews)**	STEP 2 **Context of Data Incident**	STEP 3 **Researcher's memos** Determine Codes in vivo and other generated as underlined)	STEP 4 **Level**	STEP 5 **Concepts generated**	STEP 6 **Categories** (See Section 4.4.1)
all of that stuff has to go as either system's methodology [148]					

[148] C69-Appendix 10

APPENDIX 4: OPEN CODING UNIT OF ANALYSIS THREE - INFORMATION SECURITY POLICIES

STEP 1 **Data Incidents** **(Transcribed Interviews)**	**STEP 2** **Context of Data Incident**	**STEP 3** **Researcher's memos** Determine Codes in vivo and other generated as underlined)	**STEP 4** **Level**	**STEP 5** **Concepts generated**	**STEP 6** **Categories** (See Section 4.4.1)
what they did was… they took the notebooks…they gave those new notebooks to people…and they gave the old notebooks that people had that were still on working conditions to other people [149]	Policy dictated that the old laptops be replaced by new ones. The old could not be used as their warranty had lapsed and it could be expensive to maintain them. A way was devised and the practitioners improvised by rotating the old with new to control costs. This had never been done before.	***Information Security Policy Co-ordination*** 2. Implies <u>being ingenious</u> in situations resulting from <u>limited resources</u>	Tactical Activity	**Being ingenious** on Information Security Policy	(Collective) improvisation
and most of them.. they cant even document all that stuff [150]	The lack of documentations of some of the critical activities done, provided clear motivation for some activities to be improvised as there were no explicit guidelines to follow upon.	***Accountability and Reporting of Information incidents*** 2. Implies unexpected incidents where practitioners <u>lack of documentation have</u> to be <u>imaginative</u> in their contextual activities providing grounds for improvisation.	Tactical Activity	**Being imaginative** with policies when none	(Process) improvisation

[149] C99-Appendix 10
[150] C79-Appendix 10

STEP 1 **Data Incidents** **(Transcribed Interviews)**	STEP 2 **Context of Data Incident**	STEP 3 **Researcher's memos** Determine Codes in vivo and other generated as underlined)	STEP 4 **Level**	STEP 5 **Concepts generated**	STEP 6 **Categories** (See Section 4.4.1)
so that was the real challenge in terms of getting...their minds [my mind] to change…nobody wants to be [held responsible]…[151] *it was perfect…when they actually saw the CobiT…exception results…they actually came to like. It… coz we are here to* [152]	One practitioner took it upon himself to convince the rest in an innovative manner about the benefits of CobiT. He was faced with time pressures of CobiT implementation, so as a matter of improvising in the situation, he rolled out a preliminary compliance filing report which was 'tweaked' favorably on the user's side, and immediately there was buy-in.	***Co-operation and training on Information Security policy*** 1. Implies lateral thinking to change existing mind-sets and thus motivation of <u>training on policies</u> to users.	Tactical Activity	**Lateral thinking** on information security policies	(Individual) improvisation
Well most of the times we…try and keep us much structure as we can but most of the time that we do…people don't follow the right procedures…[for instance] logging in a call the structure, would be broken by uuh them [IT USERS] coming straight to us…because there is obstruction at the border and they need to go through…and obviously to them it is a great thing…because I mean they are willing to [jump levels] and would do what ever they need	Time pressures, uncertainties, break-down, downtimes are all factors that influence 'on-the-spur' decision making and improvisation. In this particular case, the designed structures inhibited normal business processes, and the practitioners had to devise and improvise using their skills on 'how to get stuff across the border'.	***Policy on Access, Classification and Control of information*** 1. Implies being quick-witted to understand and instruct on procedure so that things are done according to plan	Operational Activity	**Being quick-witted** on Information Security policies	(Process) Improvisation

[151] C37-Appendix 10
[152] C38-Appendix 10

STEP 1 **Data Incidents** **(Transcribed Interviews)**	STEP 2 **Context of Data Incident**	STEP 3 **Researcher's memos** Determine Codes in vivo and other generated as underlined)	STEP 4 **Level**	STEP 5 **Concepts generated**	STEP 6 **Categories** (See Section 4.4.1)
to do to get their stuff across the border [153]					
and obviously now when we reflect on it…[policy] it has not been too bad on business, but now when we hit certain areas, is that we have to make some kind of adjustments… because there are so many applications out there…and the thing is that, to be working…these needs to run on the administration rights of the machine [154]	Implementing policies was seen as producing some stability in processes. However, with emergent applications, the stability was hampered. The implementation was interactive with many applications with unique improvised approaches.	***Policy on Incident Management Procedures*** 1. Implies conceptual understanding of environmental changes and hence being rational adaptive on <u>policies</u> towards business processes 2. Implies emergent and numerous applications in the market making practitioners overwhelmed	Strategic Activities	**Rational adaptive** on Information security policies	(Collective) Improvisation
and those kind of things…and…so we actually made provisions, that we could do it..[amend policy] when we looked at the group policy…on administration rights issues [155]	In this instance, the 'thinking' about making provisions and the actual 'doing it', i.e. amending group policy, comprised the ingredients for improvisation	***Policy on Change Management*** 1. Implies that circumstances could arise that make it necessary to <u>be inventive</u> on <u>policy</u> and make <u>amendments as deemed fit.</u>	Tactical Activity	**Being inventive** policy amendments	(Process) improvisation
we could give those users…whatever…administration rights on the machine centrally..	This particular case called for circumventing policy that restricted the issuance of administrative rights (full	***Policy on Change Management*** 1. Implies that for practitioners to achieve	Operational Activity	**Creativeness** on applying Information Security Policies	(Process) improvisation

[153] C126-Appendix 10
[154] C137-Appendix 10
[155] C138-Appendix 10

STEP 1 **Data Incidents** **(Transcribed Interviews)**	STEP 2 **Context of Data Incident**	STEP 3 **Researcher's memos** Determine Codes in vivo and other generated as underlined)	STEP 4 **Level**	STEP 5 **Concepts generated**	STEP 6 **Categories** (See Section 4.4.1)
but [only] if we could manage those users who got admin rights on the machine…so that was on the agenda then…we didn't want to [156]	access to computer resources) which posed as security risk, in the hope that such rights would be properly controlled and managed. The thinking then was that users needed these rights.	required objectives this may call for creativeness on applying policies			

[156] C139-Appendix 10

APPENDIX 5: OPEN CODING UNIT OF ANALYSIS FOUR - INFORMATION SECURITY EVENT MONITORING

STEP 1 **Data Incidents** **(Transcribed Interviews)**	**STEP 2** **Context of Data Incident**	**STEP 3** **Researcher's memos** Determine Codes in vivo and other generated as underlined)	**STEP 4** **Level**	**STEP 5** **Concepts generated**	**STEP 6** **Categories** (See Section 4.4.1)
Which increases the admin side which increases everything else, but in the long run it is probably [felt] it is the right thing to do [157] *well… what you see… well what happens is that it is all about saving money* [158]	The downside for implementing innovative measures and controls for information security was the increased costs, with which the practitioners were not comfortable though deemed necessary.	**Monitoring Equipment Placement and Protection** 2. Implies even though there are security control implementation challenges for ensuring robust security posture the practitioners have to be practical about it	Operational Activity	**Being practical** on Security controls Implementation	(Process) improvisation
so there are those little things…that we do just to help us and to help the business.. coz its those quick little things that…we need to do better [159]	Through continuous internal control assessments, the practitioners appreciated that they were not operating at optimally and would continually open up to new ways of improving controls, discovering novel purposes and accomplishing desired objectives.	**Monitoring Security incidents and requirements** 2. Implies being reflexive and being quick-witted in dealing with internal controls	Operational Activity	**Being quick-witted** in Internal control	(Process) improvisation

[157] C122-Appendix 10
[158] C104-Appendix 10
[159] C96-Appendix 10

STEP 1 **Data Incidents** **(Transcribed Interviews)**	STEP 2 **Context of Data Incident**	STEP 3 **Researcher's memos** Determine Codes in vivo and other generated as underlined)	STEP 4 **Level**	STEP 5 **Concepts generated**	STEP 6 **Categories** (See Section 4.4.1)
so I mean yeah.. everyday... I mean , it would be actually be.. it would be too easy if people followed procedure....coz notebooks [things] break everyday… I mean...we just had a big change…and that was it…we just bought some extra amount of notebooks and that was it [160] *I mean they also…in doing it… I mean.. they are also creating a more mobile environment where people also can work…with that...so for those people that are... I mean....if a person has got a broken notebook…then they cant work…you see?… so I mean they had to do something…and we've been trying to…giving them little injections with these notebooks to keep them going…know what I mean?* [161]	Practitioners were always weary of users who did not follow procedure, creating security risk, damage etc. Being exposed to these situations practitioners became spontaneous to changes, re-altering routines to accommodate this indifference to procedure, sometimes employing improvised guidelines.	**Monitoring Security incidents and requirements** 1. Implies being inventive to information system planning methods	Strategic Activity	**Being inventive** in Information systems planning methods	(Process) improvisation
changing the mouse… then changing this… I mean some of them…these people have	With limited resources practitioners had to improvise with the tools at hand and work needed to be done	**Monitoring Equipment Placement and Protection** 1. Implies creativeness in	Tactical Activity	**Creativeness** in Determining system resource	(Product) improvisation

[160] C97-Appendix 10
[161] C106-Appendix 10

STEP 1 Data Incidents (Transcribed Interviews)	STEP 2 Context of Data Incident	STEP 3 Researcher's memos Determine Codes in vivo and other generated as underlined)	STEP 4 Level	STEP 5 Concepts generated	STEP 6 Categories (See Section 4.4.1)
got…notebooks that has got a mouse in it and they've got a keyboard in it…and they've got it attached to a monitor…because they don't have a PC [162] *because the monitor is not working…the mouse isn't working...and the keyboard isn't working…so* [163]		determining system resource requirements		requirements	
I'd say a lot because...the whole way that.. we do run…from a WAN [view]…we run Microsoft and all that…but the way the things are put together.. and that's the difference…every one is running Microsoft stuff.. and every one has got databases…everyone's got users…and everyone's got PCs and servers…but it is the way [164]	The practitioners admit that although they use applications similar to those found in any other organization, the way they design and integrate these is innovative. There is improvisation within the context of using off-the-shelf applications and running business processes.	**Monitoring Operational Procedures and responsibilities** 1. Implies being ingenious and contextual in they way practitioners design and integrate systems	Operational Activity	**Being ingenious** in designing and integrating Systems	(Product) improvisation
[We carried out] particular checks around [form] abuse…which forms part of our information security requirements to ensure confidentiality and integrity	Although there were explicit guidelines on how security checks were to be done, in some instances, innovation was applied in the checking mechanism that guaranteed confidentiality and	**Monitoring Security incidents and requirements** 1. Implies being practical in the way information risk checks are carried out.	Operational Activity	**Being practical** in carrying out information security risks	(Collective) improvisation

[162] C107-Appendix 10
[163] C108-Appendix 10
[164] C83-Appendix 10

STEP 1 **Data Incidents** **(Transcribed Interviews)**	STEP 2 **Context of Data Incident**	STEP 3 **Researcher's memos** Determine Codes in vivo and other generated as underlined)	STEP 4 **Level**	STEP 5 **Concepts generated**	STEP 6 **Categories** (See Section 4.4.1)
basically at more or less operational level [165]	integrity of information. The innovative ways these checks were done were not explicit in any framework although they achieved their purpose.			checks	
[name withheld] … it's the way…the applications…and the people that use them…everyone's uses are a bit…different… so…[name withheld] uses are quits different from [name withheld] uses…because they've got different applications running on the servers…and they've got probably different ways of logging in [166]	The combined skills of practitioners and the technology makes for novel use of technology in the monitoring user activities in ways not experienced elsewhere, with high level of reflexivity that influence routines.	**Monitoring application usage** 1. Implies acknowledgment of <u>being original within</u> the <u>context of using different application</u>	Operational Activity	**Being original** in the context of using different applications	(Process) improvisation
and we've configured those things together and we've come up with 'IBAS' which stands integrated business architecture solutions [167]	The practitioners devised a hybrid methodology that fuses other methodologies since the architecture and components used differs with other organizations. The understanding of the system processes has necessitated this.	**Monitoring processes and application integration** 1. Implies <u>being resourceful</u> in configuring systems as, <u>home grown solutions</u> (IBAS).	Tactical Activity	**Being resourceful** in configuring systems	(Process) improvisation

[165] C5-Appendix 10
[166] C84-Appendix 10
[167] C75-Appendix 10

STEP 1 **Data Incidents** **(Transcribed Interviews)**	STEP 2 **Context of Data Incident**	STEP 3 **Researcher's memos** Determine Codes in vivo and other generated as underlined)	STEP 4 **Level**	STEP 5 **Concepts generated**	STEP 6 **Categories** (See Section 4.4.1)
yeah what they are trying to do… holistically… what they have been trying to do… the business process …it is all based on the criticality of the business process…and what's important and what's not [168]	The laying down and prioritizing based of criticality of systems and security risk posture, has produced innovative ways of balancing process risk exposure. In this case, the holistic examination was never done before.	**Monitoring processes and application integration** 1. Implies lateral thinking in understanding what is important and determining risk in the emergent business processes at any given time	Tactical Activity	**Lateral thinking** in determining business process risk	(Collective) improvisation
I put a huge enterprise around that…I picked all the main applications and put them on a spreadsheet [169]	The background to this exercise was that no one had previously examined each application against process criticality. The fact that a simple spreadsheet was used to achieve this displayed a level of innovation and improvisation.	**Monitoring Application Classification Guidelines** 1. Implies ingenious personal initiative to catalogue critical business processes in the aim of identifying risk in use of critical applications.	Tactical Activity	**Being ingenious** in identifying risk in applications	(Individual) improvisation
Communicating aims?…and…and also…they must like… as you say…'assessing the risk'…if the machine is out of warranty and it is a tier one applications it is going to be down for some time and… the	Without proper resources due to breakdown, the situation motivated variations of how the processes were going to run, and the assessment of risk in such instances. The variations gave a high need to improvise.	**Monitoring and assessing application risk** 1. Implies being capable in performing risk assessments based on criticality of systems (I tier) and the down-time.	Operational Activity	**Being capable** in performing risk assessment	(Process) improvisation

[168] C149-Appendix 10
[169] C51-Appendix 10

STEP 1 **Data Incidents** **(Transcribed Interviews)**	STEP 2 **Context of Data Incident**	STEP 3 **Researcher's memos** Determine Codes in vivo and other generated as underlined)	STEP 4 **Level**	STEP 5 **Concepts generated**	STEP 6 **Categories** (See Section 4.4.1)
vendor might say come tomorrow…then you might get parts from uumm, I don't [170]					
sure, I mean I haven't really worked anywhere else.. i wouldn't be able to say so much….I mean…our actions.. we base it on the criticality of the application…obviously…uum.. experience…obviously if the heat comes from the executives and that kind of thing ... we know which applications are critical and which and which are not [171]	The pressures from the executives and senior management often catalyse creative and incremental changes to the applications, and in the long run, the improvised actions forced by these pressures create change that is difficult to articulate.	**Monitoring and assessing application risk** 1. Implies <u>being practical</u> in <u>risk analysis</u>	Operational Activity	**Being practical** in risk analysis	(Process) improvisation
so Derek run certain exception reports and actually reported the behavior [172]	Without preparation and sufficient resources, exception reports were generated	**Exceptional reporting** 1. Implies <u>getting by</u> on security <u>checks and assessments</u>	Tactical Activity	**Getting by on** security checks and assessments	(Individual) improvisation

[170] C115-Appendix 10
[171] C144-Appendix 10
[172] C6-Appendix 10

APPENDIX 6: OPEN CODING UNIT OF ANALYSIS FIVE - IT GOVERNANCE AND REGULATORY COMPLIANCE

STEP 1 **Data Incidents** **(Transcribed Interviews)**	**STEP 2** **Context of Data Incident**	**STEP 3** **Researcher's memos** Determine Codes in vivo and other generated as underlined)	**STEP 4** **Level**	**STEP 5** **Concepts generated**	**STEP 6** **Categories** (See Section 4.4.1)
yes and when I developed that spreadsheet and showed it to the management…it was [an eye opener]…I was like jeez… I mean it was like we were focusing on applications [that were not critical] [173] *so they actually have to adjust…I mean the big guys.. the executives… committee,…whatever…so we gave them all the facts and figures…all the notebook stuff* [174]	This was an instance when planning and action were occurring together in a synthesized 'real-time' strategy. The management took note of the innovative ideas of the practitioner planner and approved of them.	***Technical Compliance Checking*** 2. Implies <u>inventive in planning and checking</u> measurement tools to achieve <u>compliant technology</u>	Tactical Activity	**Being inventive** in developing measurement tools	(Individual) improvisation
yes but …like I said…had we not adopted CobiT at the board level, we would have made it far more difficult [to implement], but … and the challenge being the audit report [175]	Prior to this, CobiT was the accepted and understood framework at board level, so an innovative way was proposed to use the same tool in IT security governance, which was	***Compliance and System Audit Control*** 2. Implies <u>being inspired</u> to adopt CobiT tool and fit this with processes that ensured information compliance and <u>monitoring international standards</u>	Strategic Activity	**Being inspired** to ensure best compliance methods	(Product) improvisation

[173] C53-Appendix 10
[174] C109-Appendix 10
[175] C45-Appendix 10

STEP 1 **Data Incidents** **(Transcribed Interviews)**	STEP 2 **Context of Data Incident**	STEP 3 **Researcher's memos** Determine Codes in vivo and other generated as underlined)	STEP 4 **Level**	STEP 5 **Concepts generated**	STEP 6 **Categories** (See Section 4.4.1)
	done with minimal implementation challenges				
So in line with that.. approach it was a good idea that the strategy that I'm formulating made it so much easier to adopt [CobiT] [176]	Sometimes, as in this specific case, strategic thinking called for an acceptable framework to be followed that serves long term security interests. Not all were in support so there had to be means to devise ways to allow the acceptance of CobiT	***Compliance and System Audit Control*** 1. Implies rational adaptive as part of strategic thinking	Strategic Activity	**Rational adaptive**	(Individual) improvisation
so you've got a methodology…so basically all of this stuff that comes out …goes through the architectural forum…for scrutiny [177]	The architecture forum collectively scrutinizes every proposal and methodology and finds best fit. The forum draws on cognitive, affective, technical and social resources in an improvised way.	***Security Reviews*** 1. Implies creativeness on the process of implementing methodologies	Strategic Activity	**Creativeness** in Implementing methodologies	(Collective) improvisation
in terms of how we…have been meeting certain compliance requirements in terms of ECT Act [178] *or any other critical ACT in line with*	The practitioners were honest about the methods engaged in meeting compliance requirements. They suggested that these methods were reflexive to the point of minimal	***Compliance with information protection legislation and IT Governance*** 1. Implies exceptionality and reflexive ways of meeting regulatory requirements such as ECT Act.	Strategic Activity	**Exceptionality** in meeting regulatory requirements	(Collective) improvisation

[176] C20-Appendix 10
[177] C70-Appendix 10
[178] C29-Appendix 10

STEP 1 **Data Incidents** **(Transcribed Interviews)**	STEP 2 **Context of Data Incident**	STEP 3 **Researcher's memos** Determine Codes in vivo and other generated as underlined)	STEP 4 **Level**	STEP 5 **Concepts generated**	STEP 6 **Categories** (See Section 4.4.1)
*all the information reporting and all this … do we all **** play* [179]\ *YES.. a lot of ACTS have been…introduced… but…I don't think they have been tested yet….so we want to comply to the bear minimal* [180]	compliance. The contradiction here is that there is both intention to comply and not to comply. The reason being resources and motivation.				
but I still have a role to play in terms of compliance [181] *my approach, my strategy… is that was that we excel on the CobiT framework.. the principles of confidentiality…integrity and availability* [182] *if you look at the CobiT core systems there are certain modules that relate to theses core requirements* [183]	The notion of Human Agency posits that humans are free to enact technologies the way they wish to. The role played by this practitioner in meeting technical compliance requirements is the agent of compliance making the compliance process the product of novel consequences. (thinking and action)	***Compliance with information protection legislation and IT Governance*** 1. Implies getting by in terms of compliance requirements with the help of a champion or role player to oversee the framework compliance process.	Strategic Activity	**Getting by in** using the compliance framework	(Individual) improvisation
Do you know CobiT processes? the 34 processes [in CobiT]? Once you adopt CobiT, there are certain levels of every	The CobiT framework as envisioned is generic and has left the practitioners to imagine new forms	***Compliance with information protection legislation and IT Governance***	Strategic Activity	**Managing** Frameworks	(Product) improvisation

[179] C30-Appendix 10
[180] C31-Appendix 10
[181] C35-Appendix 10
[182] C15-Appendix 10
[183] C16-Appendix 10

STEP 1 **Data Incidents** **(Transcribed Interviews)**	STEP 2 **Context of Data Incident**	STEP 3 **Researcher's memos** Determine Codes in vivo and other generated as underlined)	STEP 4 **Level**	STEP 5 **Concepts generated**	STEP 6 **Categories** (See Section 4.4.1)
process that you have to accept. There is high, low and medium [184] *from the CobiT exception results they actually saw from the lower….extreme they actually saw from the level of reporting, you know, the approaches…on the low and medium…they were all…4 to 5* [185]	of its application, to which the practitioners have appropriated some features for purposes other than previously envisioned. This has lead to the innovative application of CobiT.	1. Implies managing the framework against the targeted processes to achieve best practice/expectations			
I think frameworks can be deceiving… we actually incorporate 3 frameworks…we incorporate the overall framework, to govern the enterprise architecture solution distribution which is basically the Zachman Framework. [186] *but if you look in the Zachman's framework and you go right down to….the system's design.. basically those three of the Zachman's Framework.. then there is the CobiT and ITIL… are the ones that come into play in governing mostly the IT… processes…uum.. so we have an over-*	This observation has motivated the practitioners to creatively deviate from requirements that dictate unquestionable observance of frameworks, to that of tailoring frameworks to fit needs (Zachman's Framework).	***Compliance with information protection legislation and IT Governance*** 1. Implies lateral thinking in understanding frameworks and selecting alternative options and creative solutions	Strategic Activity	**Lateral thinking** in applying frameworks	(Product) improvisation

[184] C40-Appendix 10
[185] C39-Appendix 10
[186] C73-Appendix 10

STEP 1 **Data Incidents** **(Transcribed Interviews)**	STEP 2 **Context of Data Incident**	STEP 3 **Researcher's memos** Determine Codes in vivo and other generated as underlined)	STEP 4 **Level**	STEP 5 **Concepts generated**	STEP 6 **Categories** (See Section 4.4.1)
encapsulating…methodology…which is the Zachman's Framework [187]					
The Zachman framework consists of rows across (which are ITIL, CobiT) but the same principles are applied because there has to be an understanding of the business process for all the different areas [188] *to suit their environment...more than it does anywhere else…so everywhere its just the gaps around…what you need.. I mean…ITIL and CobiT…are great frameworks but…its impossible to* [189]	The creation and modification of a fusion framework allows for reflexivity. The framework shows a paradoxical existence between change and stability. The change stemming from use of existing frameworks, with stability maintaining security posture in business processes.	***Compliance with information protection legislation and IT Governance*** 1. Implies being ingenious in fusing frameworks of ITIL, CobiT simultaneously where applicable	Operational Activity	**Being ingenuous** in Fusing Frameworks	(Product) improvisation
Now in terms of the high, we were getting 2 to 3 security, but in terms of the lower and medium we were getting 4's to 5's [190] *So we got certain maturity requirements *** which we met ..and some which we had to improve on.. and then the focus* [191]	As part of the understanding of what was being said, it was noted that the human agency (Practitioners) and the technical and material agency (CobiT) were operating in dialectic and emergent fashion, whereby the resulting maturity requirements were influencing the practitioners, and the practitioners activities aimed to achieve certain results. This lead	***Security Reviews of IT Application Systems*** 1. Implies creativeness on the part of practitioners when customising maturity requirements	Tactical Activity	**Creativeness** on customising Maturity requirements	(Product) improvisation

[187] C74-Appendix 10
[188] C76-Appendix 10
[189] C85-Appendix 10
[190] C41-Appendix 10
[191] C19-Appendix 10

STEP 1 **Data Incidents** **(Transcribed Interviews)**	STEP 2 **Context of Data Incident**	STEP 3 **Researcher's memos** Determine Codes in vivo and other generated as underlined)	STEP 4 **Level**	STEP 5 **Concepts generated**	STEP 6 **Categories** (See Section 4.4.1)
so it sort of made my job so much more easier, but now when I talk to them around these components, you know immediately the guys want to go for 4's…targeting a maturity level of 4 [192]	to creativity.				
yes it was a dream come true…[laughter] as the security [maturity] levels of CobiT… are brilliant…when you give a presentation on that and you say look here guys…if you have managed 31 of the requirements…maturity level number 4's [193] *yes 4' and 5's…you certainly felt that you would attempt higher say 3 or 4 … after 3 …. So it is manageable and practicable* [194]	There was a complex interplay between the practitioners and how CobiT was implemented with intangible by-products being produced such as confidence, acceptance and reflexivity, all occurring in an improvised fashion.	***Security Reviews of IT Application Systems*** 1. Implies the process <u>managing framework implementation</u> to the level of user acceptance requires creativity	Operational Activity	**Managing** Framework implementation	(Product) improvisation
and the irony is… and I've got to give them credit for it…they've been doing a lot of work, but they've probably been focusing on the wrong way [195] *Maybe our risk profile has got to be*	The practitioners consulted with each other and realized without the clear feedback that they were obtaining based on the risk profile, they needed to re-think CobiT as they were implementing it, and improvise on the risk-profile while	***Review of Risk*** Implies <u>getting by</u> with the framework implementation process, without an explicit <u>approach to risk</u>	Strategic Activity	**Getting by** in the framework Implementation	(Product) improvisation

[192] C43-Appendix 10
[193] C47-Appendix 10
[194] C48-Appendix 10
[195] C54-Appendix 10

STEP 1 **Data Incidents** **(Transcribed Interviews)**	STEP 2 **Context of Data Incident**	STEP 3 **Researcher's memos** Determine Codes in vivo and other generated as underlined)	STEP 4 **Level**	STEP 5 **Concepts generated**	STEP 6 **Categories** (See Section 4.4.1)
entirely different…from the CobiT one…maybe we have to re-look our risk profile too…right? maybe that area that CobiT say's is high…maybe low [196]	obtaining feedback from both the model and users				

[196] C55-Appendix 10

APPENDIX 7: OPEN CODING UNIT OF ANALYSIS SIX - DISASTER RECOVERY AND BUSINESS CONTINUITY

STEP 1 **Data Incidents** **(Transcribed Interviews)**	**STEP 2** **Context of Data Incident**	**STEP 3** **Researcher's memos** Determine Codes in vivo and other generated as underlined)	**STEP 4** **Level**	**STEP 5** **Concepts generated**	**STEP 6** **Categories** (See Section 4.4.1)
to give to the people …that they gave…and got the ones that [were] broken…they had to think quick...and make that kind of a judgment… [197]	Practitioners were initially not thought of as being rational when they re-issued old laptops to ensure processes continued to run but no one could predict that their quick judgment would later prove useful	***Business Continuity management Process*** 2. Implies being quick-witted in unpredictable and unexpected circumstances in information decision making	Strategic Activity	**Being quick-witted** in decision making	(Collective) improvisation
and it all boils down to budgeting.... now they didn't budgets for it … so they had to justify why…they had to do it… so that was the main kind of thing [198]	The efficient operation of Processes were hampered when laptops broke, creating a need for extra resources. With limited resources, an innovative budget (justification) was generated	***Business Continuity Planning Framework*** 1. Implies being resourceful in ensuring business continuity and limited budgets overruns	Operational Activity	**Being resourceful** and ensuring business continuity	(Process) improvisation
yes and categorised… them because those are the items…that we specifically focus on, particularly from a disaster recover and also business continuity…the BM5 security and the components so the initial aim was building an	While building a secure architecture around data classification, observation of discourse revealed that this particular planner embraced approaches characterized by individual creative capacities and reflexivity.	***Business Continuity Planning Framework*** 1. Implies managing risk by analysing data classification	Operational Activity	**Managing** data classification	(Individual) improvisation

[197] C103-Appendix 10
[198] C105-Appendix 10

STEP 1 **Data Incidents** **(Transcribed Interviews)**	STEP 2 **Context of Data Incident**	STEP 3 **Researcher's memos** Determine Codes in vivo and other generated as underlined)	STEP 4 **Level**	STEP 5 **Concepts generated**	STEP 6 **Categories** (See Section 4.4.1)
architecture around the data classification [199]					
Well this is how we draw their attention…when it goes down…well…we tell…them "we told you not to [rely on] this business tool [200]	The strength of the business continuity process particularly in this case was that there was not enough to simply point out "we told you so" but rather that this practitioner demonstrated the ability to adopt and improvise under situations of uncertainties.	***Continuity on Critical Operations*** 1. Implies **being inspired** particularly from uncertainties caused by system downtime	Operational Activity	**Being inspired** resulting from system downtime	(Individual) improvisation
mmhhh..I think …our main thing here is to keep basically… I mean we have a lot of good uses in policies when it comes to keeping the system going…so certain time we do have to do what we have to do to keep them [systems] going…and sometimes we don't…know if it is the right thing to do [201]	It was observed that at times practitioners did not have concrete directions for how to do things. In such situations they would do whatever it took, to avoid system downtime. Their skills and knowledge made their activities amenable to complex variations and transformations that mitigated systems downtime.	***Business Continuity Measures*** 1. Implies being rational adaptive when faced with challenges to maintain system uptime.	Tactical Activity	**Rational adaptive** in maintaining system uptime	(Process) improvisation

[199] C52-Appendix 10
[200] C130-Appendix 10
[201] C124-Appendix 10

STEP 1 **Data Incidents** **(Transcribed Interviews)**	**STEP 2** **Context of Data Incident**	**STEP 3** **Researcher's memos** Determine Codes in vivo and other generated as underlined)	**STEP 4** **Level**	**STEP 5** **Concepts generated**	**STEP 6** **Categories** (See Section 4.4.1)
And that's when they normally start...start taking notice of uuhmm maybe we should actually do this in a different way.. I mean we have a whole...middle tier uuuh...application integration system...that does this kind of things….that makes you do all the right kind of stuff… but uuuhmm for simple things like uuhhm..email its amazing that uummh..the email being down [202]	When systems (email) goes down and creates a crisis, the practitioner was not dictated to on how to handle the crisis but rather operated in an environment where reflexivity was encouraged to which the success of the response was laid in unscripted activities.	***Decision Making Procedures and Communication arrangements*** 1. Implies quick reaction in crisis situations (email system downtime)	Operational Activity	**Quick reaction** in preventing email system downtime	(Collective) improvisation
so those kind of things is hard to… because.. they do it because…they are under a lot of pressure...at the time.. and those kind of things [203]	Certain activities were pointed out that by nature entailed a lot of pressures (environmental, or organizational). The pressures give rise to activities that are carried out in non-routine and unexpected ways.	***Decision Making Procedures and Communication arrangements*** 1. Implies exceptional performance when working under tremendous pressure	Operational Activity	**Exceptionality**	(Individual) improvisation
correct…something will always happen [204]	With the use of technology, order in not always guaranteed and there was acknowledgement by practitioners that that was the case. With that in mind, their activities were certainly not scripted and were bound to reflect the emergent nature of	***Disaster scenarios and critical operations*** 1. Implies being innovative in disaster planning noting that uncertainties occur	Strategic Activity	**Being innovative** in disaster planning	(Collective) improvisation

[202] C131-Appendix 10
[203] C132-Appendix 10
[204] C133-Appendix 10

STEP 1 Data Incidents (Transcribed Interviews)	STEP 2 Context of Data Incident	STEP 3 Researcher's memos Determine Codes in vivo and other generated as underlined)	STEP 4 Level	STEP 5 Concepts generated	STEP 6 Categories (See Section 4.4.1)
	these changes, creating situational based behavior and improvisation.				
[Knowing things like] how…long you've been here? know what … I mean…a lot of it is in based on experience…and just knowing what is important and what's not… and we sit…and we put together our plan…for next year… ere..a lot of them don't know what the application…is running on [205]	The type of planning postulated by practitioners goes beyond the normal mandate and considers individual skill areas, experience and expertise which calls for reflexivity and not rigidity and structure.	***Decision Making Procedures and Communication arrangements*** 1. Implies lateral thinking guided by experience is critical to making important decisions in risk management	Strategic Activity	**Lateral thinking** in Risk Management	(Collective) improvisation
than on the low level ones…so… and we also know that…like if we get a call on a Saturday…for something that is down…. don't worry…we will look at it on a Monday...since it is not a high level one...but if you get a call for something that you know is high level you will come in [206]	The practitioners revealed that they were reflexive in prioritizing responses to crisis and ambiguity.	***Decision Making Procedures and Communication arrangements*** 1. Implies being quick-witted in responding to crisis making disaster planning activities reflexive	Strategic Activity	**Being quick witted** in disaster planning	(Collective) improvisation

[205] C145-Appendix 10
[206] C147-Appendix 10

STEP 1 **Data Incidents** **(Transcribed Interviews)**	STEP 2 **Context of Data Incident**	STEP 3 **Researcher's memos** Determine Codes in vivo and other generated as underlined)	STEP 4 **Level**	STEP 5 **Concepts generated**	STEP 6 **Categories** (See Section 4.4.1)
no…they have their own little...monitoring tools monitoring the network… we have the monitoring tools monitoring the users..(Microsoft users)…so we actually have two…we have the small…one….I'm not sure what's its called and then we have the big one…called the Microsoft operations Manager (MsOM) [207] *The small one.. we find its quite nice….reflexive.. because its quick.. easy…and it can monitor.. say you need something.. now.. it can do it for you now……and then we can move it on to the other one…as an additional kind of monitoring...in a different kind of way* [208]	One way the practitioners have shown reflexivity in incident monitoring is by considering the use of computer technology tools as supplementing their work, and not as the driving force. That means they exercise choice in what to use and when, particularly in prioritizing responses and incident recovery needs.	***Recovery time monitoring and objectives*** 1. Implies <u>being resourceful</u> over choice and priority over use of computer technology tools that help in <u>incident monitoring</u>	Operational Activity	**Being rational adaptive** in Incident monitoring	(Collective) improvisation
well, to tell you the…well…we've always had both…its always been the kind of thing that its just easier…coz	The practitioners have realized the potential of working with more than one monitoring tool in a reflexive realistic manner and not	***Recovery time monitoring and objectives*** 1. Implies <u>being innovative</u> in the use	Operational Activity	**Being innovative** in Incident	(Collective) improvisation

[207] C91-Appendix 10
[208] C92-Appendix 10

STEP 1 **Data Incidents** **(Transcribed Interviews)**	STEP 2 **Context of Data Incident**	STEP 3 **Researcher's memos** Determine Codes in vivo and other generated as underlined)	STEP 4 **Level**	STEP 5 **Concepts generated**	STEP 6 **Categories** (See Section 4.4.1)
we actually use the one…to monitor...and seek…and give us a better clearer indication of…if the things that are up or down...it gives you a nice green, red or orange.. know what I mean…? Very simple[209]	rigidly following original intentions which could be overstated. This means creativity is not impeded.	of different technologies and combining in new ways to achieved optimal <u>incident monitoring</u> objectives		Monitoring	
its probably more critical…for [name withheld] . to have a lot more systems being up…because every one relies on them.. .see what I mean [210]	In this case, practitioners expressed great dependency on technology to run operations within the backdrop of crisis situations. i.e. system downtime. A realistic planning mechanism expressed was one that considered not technical solutions but social solutions which account for ingenuity and creativity.	***Recovery time monitoring and objectives*** 1. Implies managing system uptime	Operational Activity	**Managing** system uptime	(Collective) improvisation
Well… it is kind of working at the moment...its just that it is a bit slow… at the moment [211]	System testing on speed or slowness, as potential risk areas, were activities expressed by practitioner. The reflexivity demonstrated by practitioners was in exercising the choice of either accepting a status quo of the system or intervening in	***Business Continuity Measures*** 1. Implies getting by as practitioner relying on technology to run business processes	Operational Activity	**Getting by**	(Collective) improvisation

[209] C93-Appendix 10
[210] C128-Appendix 10
[211] C129-Appendix 10

STEP 1 **Data Incidents** **(Transcribed Interviews)**	STEP 2 **Context of Data Incident**	STEP 3 **Researcher's memos** Determine Codes in vivo and other generated as underlined)	STEP 4 **Level**	STEP 5 **Concepts generated**	STEP 6 **Categories** (See Section 4.4.1)
	the system to mitigate the risk.				

APPENDIX 8 - HIGH LEVEL QUESTIONNAIRE

ANSWERED BY A SENIOR SECURITY MANAGER

General Risk

Researcher's Memo's

Security Policy and Management

1. What do you base (document or other) your organisation's security roles and responsibilities on?

Our roles and responsibilities are based on providing the preservation of confidentiality, integrity and availability. ***Confidentiality*** – ensuring that accessibility is only for those authorised. ***Integrity*** – safeguarding of accuracy and completeness of information. ***Availability*** – ensuring authorized users have access to information.	**(NIST SP 800-30) System and Information Owners.** The system and information owners are responsible for ensuring that proper controls are in place to address integrity, confidentiality, and availability of the IT systems and data they own. **(Octave 2003)** By using the OCTAVE approach, an organization makes information-protection decisions based on risks to the confidentiality, integrity,

2. Have you documented your organisation's security roles and responsibilities?

Our organisations security roles and responsibilities are documented in the [name withheld] Corporate Information Security Policy.	**(NIST SP 800-30) Document Review**. Policy documents (e.g., legislative documentation, directives), system documentation (e.g., system user guide, system administrative manual, system design and requirement document, acquisition document), and security-related documentation (e.g., previous audit report, risk assessment report, system test results, system security plan5, security policies) can provide good information about the security controls used by and planned for the IT system.

3. Between your employees and third parties, who plays a greater role in terms of helping define your security needs and policy?

There is an equal level of contribution in balancing the needs of the company and those advised by third parties.	**(Octave 2003)** OCTAVE is self-directed, meaning that people from an organization assume responsibility for setting the organization's security strategy. The technique leverages people's knowledge of their organization's security- related practices and processes to capture the current state of security practice within the organization

4. Are there instances you may feel that there lacks commitment by employees regarding certain clauses in the security policy?

Adherence to the e-mail usage policy seems to be disregarded by many users.	**(SP 800-30) 3.2.1 Threat-Source Identification** a situation and method that may accidentally trigger a vulnerability. **Vulnerability:** A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.

5. Do you feel liberated or constrained by security policy?

I feel that the policy provides both a liberating and constraining feeling insofar that you are aware of the parameters within which you have to work.	**(Octave 2003)** OCTAVE is self directed, requiring an organization to manage the evaluation process and make information-protection decisions

6. What mechanisms are used to communicate security policy to employees?

We use our Intranet, Imbizo. Information days, regular e-mails are posted as reminders of the policy.	(**Burton Group 2003**) Promoting appropriate security awareness requires a program of written policies, training, incentives, penalties, and continuous reminders. As described in the *Security and Risk Management Strategies* overview, "Concepts and Definitions," simple memos such as "no privilege without identity," as well as zero tolerance can be used to promote awareness

Contractual Terms

7. Do you use contractual terms and conditions to specify your employees or third party information security responsibilities? Are you aware of any breaches?

Contractual terms are very clearly defined and there have been breaches which have resulted in litigation.	**(Burton Group 2003) Legal** processes provide input to risk management and compliance1 assessment personnel. Legal issues associated with contracts, vendors, contractors, employees, and other personnel and entities must be intimately involved with the enterprise risk-management process. Legal issues play a leading role in risk transfer and risk avoidance.

8. Do all new employees and third party users sign confidentiality or nondisclosure requirements before you allow them to use sensitive information?

As part of letter of acceptance of employment, staff are made aware of the requirements of the policy.	**(Burton Group 2003) Personnel security** starts with the hiring process and goes throughout the lifecycle of the interaction of the individual and the enterprise. This discipline addresses pre-employment screening and disciplinary action, as well as giving personnel proper guidance, periodic reassessments, and management controls.

Information Security Forum

9. Do you have a management forum that you utilise to implement, review, assign roles and approve your information security policy? Who are the designated persons?

There is a joint approach between IT and Corporate Governance, with the IT Risk and Continuity Manager being the designated person in IT.	**(Octave 2003)** When applying OCTAVE, a small team of people from the operational (or business) units and the information technology (IT) department work together to address the security needs of the organization, balancing the three key aspects illustrated in Figure 1: operational risk, security practices, and technology.

10. When was the last time your organisation promoted the importance of information security to its employees through e.g. workshops?

A formal notification was done a year ago, “Security Awareness Week”. This done in the form of an internal competition with staff having to answer certain aspects of the policy.	**(Burton Group 2003) Personnel Security** includes personnel related principles and concepts such as security awareness, roles, clearances, ethics, separation of duty, and appropriate use of information and facilities. Personnel security must address employee and contractor lifecycles such as hire-transfer-terminate.

11. Who is mandated to review and evaluate information security incidents?

The IT Risk and Continuity Manager.	**(Burton Group 2003)** Top management typically takes responsibility for decisions about deterrence, while project management adapts the protection system, and project teams, operations, and users undertake prevention, detection, and response. **(NIST SP 800-30)** IT security program managers and computer security officers are responsible for their organizations' security programs, including risk management.

12. How often are reviews and approvals of information security policies conducted? Who conducts them?

Reviews of the policies are conducted by both our internal and external auditors. These reviews are held annually.	**(Burton Group 2003) Auditing** processes are conducted by internal and external auditors to verify compliance with policies, standards, regulations, and other requirements. Internal auditors provide critical feedback for management at all levels, while external auditors perform an independent verification that internal auditors are doing their jobs properly.

13. Are there moments when information security methods, techniques or initiatives not entirely supported by designated persons of authority? If so, are there special considerations as to why this maybe the case?

Due to the design of certain of our systems, it becomes impractical to fully apply all our security policies particularly with regard to access to data. As a result hereof full application of the policies are not always fully supported.	**(Octave 2003)** The team develops an organization-wide protection strategy focused on improving the organization's security practices as well as mitigation plans to reduce the important risks to critical assets.

14. How does the forum (if any) assist in the promotion of the importance of information security?

We ensure that we place security awareness on our balanced scorecard.	**(NIST SP 800-30)** A successful risk management program will rely on…(1) senior management's commitment;… (4) the awareness and cooperation of members of the user community, who must follow procedures and comply with the implemented controls to safeguard the mission of their organization;

15. How often are information security incidents reported to the forum (if any)?

They are reported as they occur or are detected by our external service providers who monitor our network activity. We have a monthly meeting to analyse incidents received.	**(Burton Group 2003)** The sensors provide feedback by observing behaviors and reporting them to audit services and repositories for long-term orientation and analysis, to security management services and repositories for tactical orientation, and to detection services for real-time orientation. Detection services then feed policy decision points or security management services that determine responses to the current situation, and act by passing control to actuators in the resources or control services to perform the necessary actions.

Co-ordination of Security Implementation

16. Who co-ordinates the implementation of security controls?

The technical component resides within TEG (technology enablement group) as they respond to the policies and procedures provided by the IT Risk and Continuity management.	**(NIST SP 800-30)** A successful risk management program will rely on…(3) the competence of the risk assessment team, which must have the expertise to apply the risk assessment methodology to a specific site and system, identify mission risks, and provide cost effective safeguards that meet the needs of the organization;

17. Who distributes information security roles and responsibilities throughout your organisation?

It is a joint activity of Corporate Governance and IT.	**(Burton Group 2003)** Senior management and the enterprise security team develop security objectives and a security posture for managing risks. Risk prioritization, objectives, and posture then drive policies, which drive security governance of people, organizations, processes, and technologies. Policies also determine the roles for

18. How does your organisation ensure that the co-ordination of security controls by members are representative of the organisation's needs as well as the need of the employees?

The intent of our policies is to offer our organisation the necessary protection , but also to provide the assurance of the protection of the integrity of the individuals who use the system.	**(Burton Group 2003) Governance** of the security structure must ensure that the security organizational model fits the enterprise organization structure, and that the organization's structure and policies provide adequate resources, chains of command, and appeals or exceptions processes to allow reasonable coordination mechanisms for risk management.

Information Security Infrastructure

19. When did you last feel necessary to establish a management framework that controls your organisation's implementation of information security?

This was undertaken last year with the inclusion of Information Security into Business Intelligence competency.	**(Burton Group 2003)** A framework is both a vehicle for understanding the overall security approach and an inventory of the applicable technologies, which remain the primary concern of Burton Group's in-depth coverage.

20. When did you last have to access external expert help/opinion to information security?

We have an on-going relationship with an external service provider to hold regular consultations of market trends with security.

(Burton Group 2003) External auditors verify compliance with policies, standards, regulations, and other requirements by performing an independent verification that internal auditors are doing their jobs properly. External audits may be required for legal or other reasons.

21. Have you recently felt a need to revamp your internal information security expertise? If so why?

No.

(NIST SP 800-30) As changes occur in the existing IT system environment infrastructure and organizational policies, introduction of new technologies), the IT security practitioners must support or use the risk management process to identify and assess new potential risks and implement new security controls as needed to safeguard their IT systems (e.g., expansion in network connectivity, changes to the existing.

22. Who is designated to monitor changes in information security standards and methods?

The IT Risk and Continuity Manager

(NIST SP 800-30) IT security trainers or security/subject matter professionals must understand the risk management process so that they can develop appropriate training materials and incorporate risk assessment into training programs to educate the end users.

23. Have you had incidents where there was conflict of opinion between your internal experts and external experts in relation to information security policy?

I would not regard it as conflict, rather a variance of views in terms of company needs and external stringent adherence to best practices.	**(NIST SP 800-30)** A risk assessment report should not be presented in an accusatory manner but as a systematic and analytical approach to assessing risk so that senior management will understand the risks and allocate resources to reduce and correct potential losses.

Information Security Responsibilities

24. What measures have you taken to encourage a multi-disciplinary approach to information security?

By regular communications with the broader [name withheld] community we have heightened the need for corporate response to security.	**(Octave 2003)** When applying OCTAVE, a small team of people from the operational (or business) units and the information technology (IT) department work together to address the security needs of the organization, balancing the three key aspects illustrated in Figure 1: operational risk, security practices, and technology.

25. How do you carry out the security process of information assets control?

All requests for access are done via application which is authorised by the relevant executive, with final authorization given by the IT Risk and continuity manager.	**(NIST SP 800-30)** An organization's security standards should establish a set of controls and guidelines to ensure that security procedures governing the use of the organization's IT assets and resources are properly enforced and implemented in accordance with the organization's goals and mission. Management plays a vital role in overseeing policy

26. Kindly specify the security roles and responsibilities that are distribute amongst the various users and services.

Roles are specifically split into two areas, technical response and the process, procedures and people element.	**(Burton Group 2003) Knowledge** arms key people with the long-term understanding required to perform their security roles. The enterprise must instill appropriate levels of knowledge in systems administrators, data owners, system and application designers, management, and administrators.

27. Is there delegation of security responsibilities between asset owners?

Delegation, yes, in terms of recommendation levels of access.	**(Burton Group 2003)**Top management typically takes responsibility for decisions about deterrence, while project management adapts the protection system, and project teams, operations, and users undertake prevention, detection, and response.

Information Security Advisers

28. How does your organisation co-ordinate your information security knowledge base and experience?

We use our own experiences and solicit the expertise of outside agencies such as Gartner, etc.	**(Octave 2003)** OCTAVE is self-directed, meaning that people from an organization assume responsibility for setting the organization's security strategy. The technique leverages people's knowledge of their organization's security- related practices and processes to capture the current state of security practice within the organization.

29. Has your organisation identified an ‘in-house’ information security advisor or champion?

Yes, it is a joint role filled by the IT Risk Manager and our Telecommunications Architect and specialist.	**(NIST SP 800-30)** Risk management is a management responsibility. This section describes the key roles of the personnel who should support and participate in the risk management process; Senior management, Chief Information Officer, System and Information Owners, Business and Functional Managers, IT security program managers.

30. How does the ‘in-house’ information security advisor help your organisation to make information security decisions?

We present to the organisation’s potential breaches of security and offer solutions thereof.	**(Burton Group 2003)** Risk management is not a one-size-fits-all proposition. For example, some enterprises only establish protections on a risk-justified, case-by-case basis, but others raise their protective baseline to a level dictated by assumed standards of due care in a particular industry before undertaking risk analyses.

31. Does the ‘in-house’ information security advisor have access to external security experts and advisors? Please specify who.

Yes, we primarily use [name withheld] .	**(NIST SP 800-30)** Appropriate persons (in-house personnel or external contracting staff) who have the appropriate expertise and skill-sets to implement the selected control are identified, and responsibility is assigned.

32. Has the information security advisor ever been asked to assess security problems, threats and vulnerabilities and investigate security incidents or breach?

Yes	**(NIST SP 800-30)** Appropriate persons (in-house personnel or external contracting staff) who have the appropriate expertise and skill-sets to implement the selected control are identified, and responsibility is assigned.

33. Does the information security advisor have access to th organisation's management personnel?

Yes	**(Octave 2003** Self direction is one of the principles of OCTAVE. The concept of self direction means that people inside the organization are in the best position to lead the evaluation and make decisions.

34. Are there times the security advisor is not consulted in case of security incident or breach?

None of which I'm aware.	**(Octave 20003)** There is more than one set of activities that can produce the outputs of OCTAVE; for this reason, a unique set of activities is not specified. The outputs define the outcomes that an analysis team must achieve during the evaluation

Other Organisations

35. Do you have a co-operative relationship with law enforcement authorities?

Dependent on the nature of the security breach eg fraud we would have a cooperative arrangement with SAPS	**(NIST SP 800-30)** IT-related risks arise from legal liability or mission loss due to— 1. Unauthorized (malicious or accidental) disclosure, modification, or destruction of information 2. Unintentional errors and omissions 3. IT disruptions due to natural or man-made disasters 4. Failure to exercise due care and diligence in the implementation and operation of the IT system.

36. Does your organization maintain a relationship with other organisations that could help it cope with incidents and breaches?
(regulatory bodies, CERT, information service providers, telecomm operators etc)

Yes, we are also members of a special interest group hosted by [name withheld]	**(CobiT)** Business process owners bear the final responsibility for the information technology as deployed within the confines of their business process. Of course, they will make use of services provided by specialised parties like the traditional IT department or the third party service provider.

37. Does your organisation belong to security groups and associations (CERT etc)?

As above.	**(CobiT)** Business process owners bear the final responsibility for the information technology as deployed within the confines of their business process. Of course, they will make use of services provided by specialised parties like the traditional IT department or the third party service provider.

38. How does your organisation ensure that confidential information is not accidentally passed on to any unauthorised person in or out of the organisation?

We do this by developing access hierarchies and permissions.	**(Octave 20003)** By using the OCTAVE approach, an organization makes information-protection decisions based on risks to the confidentiality, integrity, and availability of critical information-related assets. All aspects of risk (assets, threats, vulnerabilities, and organizational impact) are factored into decision making, enabling an organization to match a practice-based protection *strategy* to its security risks.

Independent Security Reviews

39. When did you last conduct an independent review of your information security policy?

One is currently being conducted by our external auditors as part of an annual process.	**(CobiT) Monitoring** All IT processes need to be regularly assessed over time for their quality and compliance with control requirements. This domain thus addresses management's oversight of the organisation's control process and independent assurance provided by internal and external audit or obtained from alternative sources.

40. Did this review find consistency between policy and practise?

There were certain inconsistencies highlighted from the last review and these were addressed and remedied.	**(CobiT)** CobiT also is useful in helping auditees evaluate and strengthen internal controls. There is a tremendous benefit for them to be better prepared for upcoming audits. Being aware of the review criteria means that auditees are aware of the control practices recommended for the IT processes. CobiT's organisation makes it easy for the auditee to relate to and interpret auditors' requests for information and subsequent recommendations.

41. Did this examination reveal effectiveness of security policy?

Yes	**(CobiT)** CobiT also is useful in helping auditees evaluate and strengthen internal controls. There is a tremendous benefit for them to be better prepared for upcoming audits. Being aware of the review criteria means that auditees are aware of the control practices recommended for the IT processes. CobiT's organisation makes it easy for the auditee to relate to and interpret auditors' requests for information and subsequent recommendations.

42. What assurances do you have that the independent policy reviewers have the necessary skills and experience?

They come recommended from service provider used	**(CobiT)** Using the CobiT control objectives as a basis for assessing IT audit and auditor skill requirements, effective and timely training can be provided to ensure that the audit can be performed successfully.

Job Description

43. What criteria have you used to assign the responsibilities for implementing your information security policy with regard to job description?

Relevant experience in an IT environment. Clear understanding of Information Security Extensive knowledge of IT strategies, best practise processes and standards. Thorough working knowledge of analysis and design methodology and modelling techniques	**(CobiT)** Each [auditor's] education, training and experience in IT is characterized based on these three skill sets: B**asic Understanding:** Broad knowledge of an IT process, purpose, objectives and goals. W**orking Knowledge: d**emonstrated ability to identify internal control strengths and weaknesses within an IT process. **Expert Knowledge:** Ability to design and use computer assisted audit techniques to identify, evaluate and correct internal control weaknesses.

44. Have you found it necessary to have a specific job description assigned responsibility for protecting specific information assets or is such assignment relative and contextual?

Yes	**(NIST SP 800-30) Assign Responsibility**: Appropriate persons (in-house personnel or external contracting staff) who have the appropriate expertise and skill-sets to implement the selected control are identified, and responsibility is assigned.

Training

45. What assurances does your organisation have with regard to ensuring users are aware of information security threats and concerns?

We ensure that knowledge is kept current by the subscription to the relevant professional bodies and the attendance of conferences and seminars	**(NIST SP 800-30)** Conduct security awareness and technical training to ensure that end users and system users are aware of the rules of behavior and their responsibilities in protecting the organization's mission.

46. What assurances does your organisation have with regard to ensuring users are capable of applying information security policy and procedures and in minimising security risks?

Whilst there are no absolute assurances, we believe that adherence to the Security policies would lend itself to that assurance.	**(NIST SP 800-30)** Conduct security awareness and technical training to ensure that end users and system users are aware of the rules of behavior and their responsibilities in protecting the organization's mission.

Security Incidents

47. How does your organisation monitor security incidents?

This is done by means of both internal and external monitoring of both data access and network activity. Internet usage is also very closely monitored and measured.	**(Burton Group 2003)** Behavior, identity, method, and other contexts may be jointly monitored to detect threats or to determine access rights. **(Octave 2003)** *Monitor* the action plans for schedule and for effectiveness (This activity includes monitoring risks for any changes.)

48. How has your organisation tried to minimise the damage caused by information security incidents?

By the application of access policies, use of Firewalls, message filtering, etc.	**(NIST SP 800-30)** An organization's security standards should establish a set of controls and guidelines to ensure that security procedures governing the use of the organization's IT assets and resources are properly enforced and implemented in accordance with the organization's goals and mission.

49. Do you have a formal or informal reporting procedure for security incidents?

Yes, Incidents are generally reported to IT Risk management or via our External Service provider through their network monitoring mechanism.	**(NIST SP 800-30)** Reviews of the history of system breakins; security violation reports; incident reports; and interviews with the system administrators, help desk personnel, and user community during information gathering will help identify human threat-sources that have the potential to harm an IT system and its data and that may be a concern where a vulnerability exists.

50. How does your organisation determine that all or most of the critical security incidents are reported?

There is a formal meeting held monthly, however if serious breaches are detected, emergency meetings are convened. There are also automated alerts prompting us of potential threats, specifically external threats.	**(NIST SP 800-30)** In most organizations, the network itself will continually be expanded and updated, its components changed, and its software applications replaced or updated with newer versions. In addition, personnel changes will occur and security policies are likely to change over time. These changes mean that new risks will surface and risks previously mitigated may again become a concern. Thus, the risk management process is ongoing and evolving.

51. How does your organisation assure itself that the reporting procedures for security incidents have been correctly followed?

Formal reports have to be forwarded to the IT leadership team and a Risk Matrix is maintained and included in the Monthly Board report.	**(CobiT)** Reports are issued on the outcomes of IT activities, which are measured against the various practices and controls, and the cycle begins again.

52. How does your organisation ensure that it has learnt from such events?

By regular security reviews.	**(CobiT)** Management needs to identify the most important activities to be performed, measure progress towards achieving goals and determine how well the IT processes are performing.

53. How do you ensure that people report observed information security weaknesses?

Whilst nothing formal is in place, we depend on the various competencies within the organisation report potential breaches.	**(NIST SP 800-30)** People prefer to address the threat/vulnerability pairs as observations instead of findings in the risk assessment report.

Knowledge Management

54. Does your organisation maintain a repository of all incidents reported, mechanisms for monitoring and quantifying types of security incidents?

Yes.	**(Burton Group 2003)** Another goal of the systematic, comprehensive approach to information security is to secure the systems, applications, and repository technologies that contain content or information. This should be done through a combination of covering approaches implemented in security infrastructure solutions, and by appropriately deploying controls within the assets themselves

55. Have you noted instances of recurring incidents?

Most corporates are faced with constant hacking and intrusion attempts.	**(Burton Group 2003) Behavior** is a characteristic of people (as threats, potential threats, users, customers, etc.) and organizations. Security posture, security controls, and security processes such as awareness seek to assure desired behavior and limit undesired behavior.

56. How does your organisation ensure that by learning about the security incidents reported on there is improvement on information security and information security policy?

Incidents are prioritised and “red flagged”. The “red flag” incidents become part of the audit report with the required management response.	**(Burton Group 2003)** Through conscious, systematic, and continuous development and documentation, procedures should control who makes decisions and under what circumstances, and policy should dictate the overall governance structure at a strategic level.

Technology Risk

Passwords, Firewalls and Encryption

57. How does your organisation determine, and quantify risk relative to the machines particularly if these derive services from the central servers?

Risk quantification is determined by the criticality of data on specific servers.	**(NIST SP 800-30) When a vulnerability can be exercised →**apply layered protections, architectural designs, and administrative controls to minimize the risk of or prevent this occurrence.

58. What does your organisation consider as confidential information and how is this protected?

Any information that would , if made accessible to the wrongs persons, negatively impact the brand, is regarded as confidential.	**(Burton Group 2003) Confidentiality:** Prevent intentional or unintentional unauthorized or inappropriate disclosure of information.

59. How secure do the computers have to be particularly if these are connected to the internet or the company's network?

We ensure that the level of security on these computers/servers would offer the company the necessary protection.	**(Burton Group 2003) Use control:** Ensure and verify appropriate use of information and IT systems by authorized personnel, prevent inappropriate use by authorized personnel, and prevent use by unauthorized personnel.

60. How often does your organisation monitor the following;
(a) dormant accounts,
(b) the use of regular passwords, (c) shared files,
(d) account lock out (e) antivirus updates?

This monitoring is done on a regular basis by our Active Directory administrators.	**(NIST SP 800-30) Identification.** This control provides the ability to uniquely identify users, processes, and information resources. To implement other security controls (e.g., discretionary access control [DAC], mandatory access control [MAC], accountability), it is essential that both subjects and objects be identifiable.

61. Do you require encryption of confidential information when it is transmitted or stored electronically?

Yes, specifically pertaining to all debit and credit card transactions	**(NIST SP 800-30) Protected Communications.** In a distributed system, the ability to accomplish security objectives is highly dependent on trustworthy communications. The protected communications control ensures the integrity, availability, and confidentiality of sensitive and critical information while it is in transit. Protected communications use data encryption methods (e.g., virtual private network, Internet Protocol Security [IPSEC] Protocol), and deployment of cryptographic technologies (e.g., Data Encryption Standard [DES], Triple DES, RAS, MD4, MD5, secure hash standard, and escrowed encryption algorithms such as Clipper) to minimize network threats.

62. What are your password requirements for user and system accounts?

User sign-ons are unique to each user and passwords are required to alpha/special character/numeric format and a 30 day expiry lifespan	**(NIST SP 800-30) Access Control Enforcement.** Data integrity and confidentiality are enforced by access controls. When the subject requesting access has been authorized to access particular processes, it is necessary to enforce the defined security policy (e.g., MAC or DAC).

63. Are firewalls used to prevent unauthorized access connections from external networks and computer systems to internal networks?

Yes	**(Burton Group 2003)** Organizations should deploy firewalls and antivirus protections, and not allow users to surf the Web while logged into spyware-susceptible root or Windows Administrator accounts. They should also consider the Generally Accepted Information Security Principles (GAISP) outlined by the Information Systems Security Association (ISSA) and other security best practices.

64. Are your network and computer systems monitored for network intrusions?

Yes	**(NIST SP 800-30)** Detection controls warn of violations or attempted violations of security policy and include such controls as audit trails, intrusion detection methods, and checksums. **Intrusion Detection and Containment.** It is essential to detect security breaches (e.g., network break-ins, suspicious activities) so that a response can occur in a timely manner. It is also of little use to detect a security breach if no effective response can be initiated.

APPENDIX 9 - OBSERVATION ON DISASTER RECOVERY EXERCISE

OBJECTIVE: TO MONITOR ACTIVITIES WHILE A DISASTER RECOVERY EXERCISE IS TAKING PLACE

Location and Venue

There was a particular instance when the organisation organised a disaster recovery test office in two locations, one which was 19 km from the organisation's headquarters. The researcher was invited to observe the activities that were carried out in the disaster recovery process.

Disaster Recover Process and Activities

In the disaster recovery process, the researcher did not become part of "the furniture" but went to the scene to explore issues that would reveal more about the phenomenon of improvisation. The researcher intended exploring ways that he would collect data.

An observation protocol/ schedule was designed prior to going to the site and the researcher used it to record what was observed.

	Site Location : Continuity South Africa (CSA) Pinelands- 19 Kilometres from Head office	
	Access to this site is restricted and every one is issued a temporary access ID.	
Start 9: 00 am	1. Equipment testing	**Notes** Disaster Recovery Site has **12** PC's**.** There were also 6 personnel manning PC's each with a designate duty.
	2. Data testing	At this stage the development area Switch (a virtual section in the database designated for testing data) had earlier been switched off, meaning the activities were delayed.

	Site Location : Continuity South Africa (CSA) Pinelands- 19 Kilometres from Head office	
	Access to this site is restricted and every one is issued a temporary access ID.	
9:30 am	1. Isolation of Development Area 3 Disaster recovery Manager Leaves after making the call 4 The rest of the 5 people seem busy concentrating on 1 particular PC. 8 Unix systems link up to the main frame. 9 Select data date and time. Restore data based on selected data and time 10 Restore from back-ups brought using the main frame channel.	For the Disaster recovery process to continue, the Development Area Switch had to be switched on again. (This usually takes time due to formal procedures being followed). Apparently the development team were unaware of the timing of the disaster recovery date. To address this, the Disaster Recover Manager made frantic calls back to the Office. After the call, he leaves the venue. In a matter of time the area was switched on. At this stage, another person enters the secure room. Soon after the Disaster Recover Manager comes back again. He explains that on normal occasions there are 2 tests of this nature once a year. **Manifest file** A manifest file (a check list) of the recovery procedures is produced. It documents the steps to be followed in the recovery process.
10:00am	4 Review of Manifest file 5 Unix environment goes live for recovery. 6 Back-ups selected for	There is a Data Analysts who sits and observes everything. The Analyst seems to give instruction to the *CSC personnel about the recovery process. The four essential items to be checked in the back-ups include; • The back-up date • Return Number

	Site Location : Continuity South Africa (CSA) Pinelands- 19 Kilometres from Head office **Access to this site is restricted and every one is issued a temporary access ID.**	
	recovery.	• Seal number • Container number While one person reads the manifest file, the other types the instructions in the UNIX environment. * *Computer Science Corporation (CSC) have been sub-contracted to handle the mainframe capability although the equipment is owned by [name withheld] .*
10:30	1 Two servers restored successfully	At this time 2 servers have been restored successfully, the time taken being 30 minutes. Information from these two contains server information about the following; Food Server P670 Textile Server P 670 RMS Server P570 FDS/TMS Server P650 ECS/APPWORX Server P650 QUEST Server P615 The reason given for the quick recovery by the teams is that they have done this more than once and have internalised the process. It was noted that no documentation is being taken.
11:00AM	10.8 Tivoli Storage Manager (TSM) 10.9 Windows restored personnel take over.	The Tivoli Storage Manager Application reconstructs the restored data from the UNIX Application (flat files) into formats recognised by the windows Application system. There is a connection initiated between these two systems to tunnel data using TELNET protocol.
CONCLUSION Key notes;		

Site Location : Continuity South Africa (CSA)

Pinelands- 19 Kilometres from Head office

Access to this site is restricted and every one is issued a temporary access ID.

- It should be noted that the Personnel using TSM are not knowledgeable with UNIX hence had to wait until UNIX restoration is complete then they can take over. Each person seems to know what to do.
- There is also distinct organisation with each specialised role player.
- There was an instance when a lap-top (there is no policy in place about bringing personal lap-tops into the recovery site, anyone can bring their own) was plugged into the wrong net-work and this seems to have affected the recovery of data perhaps corrupting portions of it. The entire recovered data had to be trashed and the whole process repeated again. The reason was the one user wanted to read email in the live environment. (Using another switch).

DISCUSSION

The researcher developed field notes while conducting informal interviews to complement observation with data. This process shed light on the various parts of the inquiry. The advantage of this process was that the whole exercise was able to assist the researcher mentally organise and fit in specific pieces of information that would not have been obvious through interview only.

The fact that preliminary observation showed that many activities were conducted with formal guidelines and were complemented by experience was ample evidence to suggest that the official corporate security risk policy document was hardly given any consideration.

There was an initial belief that improvisation as a potential for action latent in most if not all human activities would be evident in these units of analysis. The general assumptions made were that when the security risk practitioners improvised within these units of analysis, this activity was an existential act, which on a basic level could be understood via a qualitative assessment.

Site Location : Continuity South Africa (CSA)

Pinelands- 19 Kilometres from Head office

Access to this site is restricted and every one is issued a temporary access ID.

The idea was to get practitioners to recollect on areas of innovation and improvisation that involved initiating processes based on previous experience and activities. These activities would then be compared with the other structure methodologies and frameworks explicitly drawn. Once the comparison has been made, they would attempt to extract revelations of new processes and thus methods of doing things. The analysis of the units would enhance learning which in turn would help generate new insight and knowledge acquisition.

APPENDIX 10 - OPEN CODING FROM TRANSCRIBED INTERVIEWS

Interviewee	Comment #	DATA-SETS (Compartmentalised Transcripts)
EK	C1	to get people to change their mind-set to doing things in a formalised manner you could bring informal
	C2	Ok basically just to put into context… my role as opposed to Derek's role… Derek's role is more operational, is strategic…
	C3	while performing IT governance…my role is more from a strategic ensuring that direct management confidence is facilitated
	C4	management confidence is facilitated if you talk of IT Risk Management…that can be incorporated as part of the Information Security Risk Strategy…
	C5	Particular checks around [form] abuse…which forms part of our information security requirements to ensure confidentiality and integrity basically at more or less operational level
	C6	so Derek will run certain exception reports and actually report the behaviour….
	C7	Um to ensure that they comply with whatever policy and standards that they have devised or as defined by the board
	C8	of the challenges…that we have as….*** .is that the academic part of it differs from reality….and the practical implementation
	C9	there has been a lot… good stuff that the guys for instances like Etienne (Enterprise Risk]… they have done a lot of work… they have complied with every possible standard/ framework..
	C10	... but when it comes to the practical implementation at operational level…by the *… would require so much in training…to actually bridge that gap….
	C11	most people . you know…actually in the retail environment the challenge is…the bottom line…[profits]…
	C12	well…that's actually where the mind set has to change…that's why the Information Security office used to be in IT…but now I'm actually reporting top Corporate governance board..…
	C13	well…yes.. so here is no longer…as part of the corporate governance model..
	C14	um. I'm actually now sitting there now…not in IT…

	C15	my approach, my strategy… is that was that we excel on the CobiT framework.. the principles of confidentiality…integrity and availability
	C16	if you look at the CobiT core systems there are certain modules that relate to theses core requirements
	C17	so those core systems are…part of my approach.. they cover…operational.. and strategy…
	C18	the framework can be the requirements can actually * measurement. because in the CobiT framework of the things that we did was we did a ****
	C19	So we got certain maturity requirements *** which we met ..and some which we had to improve on.. and then the focus
	C20	So in line with that.. approach it was a good idea that the strategy that I'm formulating made it so much easier to adopt
	C21	.. since when they had adopted CobiT it made my work…so much easier.. so I don't have to try to explain to them about CobiT…
	C22	the executive were already familiar with it… they bought into it…and they already put it into working…
	C23	it came from the board…
	C24	no… I'm the group information security officer…
	C25	I think it was top-down…like I said corporate governance used to be.. previously at [name withheld] into various components of corporate governance…
	C26	like we would have legal…we would have retailing and others… now legal forms part of corporate governance… internal audit forms part of corporate governance…and IT security and also Risk Management
JC	C27	But we would have Risk Management at a granular level, within IT security corporate governance…specifically in the ****compliance part of it …so where do we meet? The compliance requirement …
	C28	: operationally, IT Governance would still be there. They still have a major role to play…but you know from a compliance perspective
	C29	in terms of how we…have been meeting certain compliance requirements in terms of ECT Act
	C30	or any other critical ACT in line with all the information reporting and all this … do we all **** play
	C31	YES.. a lot of ACTS have been…introduced… but…I don't think they have been tested yet….so we want to comply to the bear minimal

	C32	there was the initial; buying… [of the idea/ my position].. because when people think of information security…and me being the .. coz they could see me coming through the door [and go] "ooh here is Audit coming again…".
	C33	I used to be the Audit Manager before…I took on this position…there was the mind set change- I had to change…
	C34	then I had to change… [since] I'm not Audit…I'm more on a consultative role now…
	C35	but I still have a role to play in terms of compliance…
	C36	but I [now] not here to follow up on people …
	C37	so that was the real challenge in terms of getting...their minds [my mind] to change…nobody wants to be [held responsible]… but then they saw…the CobiT compliance filing [report] part of it..
	C38	it was perfect…when they actually saw the CobiT…exception results…they actually came to like. It… coz we are here to…
	C39	from the CobiT exception results they actually saw from the lower….extreme they actually saw from the level of reporting, you know, the approaches…on the low and medium…they were all…4 to 5….
	C40	Do you know CobiT processes? the 34 processes [in CobiT]? Once you adopt CobiT, there are certain levels of every process that you have to accept. There is high, low and medium.
	C41	. Now in terms of the high, we were getting 2 to 3 security, but in terms of the lower and medium we were getting 4's to 5's.
	C42	and theses are the components that I'm focusing on in terms of confidentiality, availability and integrity
	C43	so it sort of made my job so much more easier, but now when I talk to them around these components, you know immediately the guys want to go for 4's…targeting a maturity level of 4…
	C44	you get a buy in immediately…
	C45	yes but …like I said…had we not adopted CobiT at the board level, we would have made it far more difficult, but … and the challenge being the audit report

	C46	that was coming …through which was highlighting certain risks…but the fact that this CobiT Implementation] was coming directly from the top…you know we always focused on reliance on the subject…I'm telling you…
	C47	yes it was a dream come true…[*laughter*] as the security [maturity] levels of CobiT… are brilliant…when you give a presentation on that and you say look here guys…if you have managed 31 of the requirements…maturity level number 4's
	C48	yes 4' and 5's**…**you certainly felt that you would attempt higher say 3 or 4 **…** after 3 …. So it is manageable and practicable
	C49	it is actually putting more resources but then, on the items that are high risk…putting much more focus on… on those area
	C50	… the high risk is more on the direct Risk management side, risk profiling, then the other one is…the information architecture, it think it is **AI5** or something around data classification and application technicality…
	C51	I put a huge enterprise around that…I picked all the main applications and put them on a spreadsheet,
	C52	yes and categorised… them because those are the items…that we are specifically to focus on, particularly from a disaster recover and also business continuity…the **BM5** security and the components so the initial aim was building an architecture around the data classification…
	C53	yes and when it developed that spreadsheet and showed it to the management…it was [an eye opener]…I was like jeez… I mean it was like we were focusing on applications [that were not critical]…
	C54	and the irony is… and I've got to give them credit for it…they've been doing a lot of work, but they've probably been focusing on the wrong way..
	C55	Maybe our risk profile has got to be entirely different…from the CobiT one…maybe we have to re-look our risk profile too…right? maybe that area that CobiT say's is high…maybe low
	C56	yes, but then its has to.. .its going to be another workshop, to actually realign our risk profile...to align with the corporate risk profile
	C57	maybe that area which I thought that CobiT
EV	C58	The guy who heads up the department in respect to information system's intelligence is [name withheld] …so we've go a whole department structured around data warehousing…

	C59	in terms of safety of information, manipulating information, metadata around information and stuff like that..
	C60	We have got the Architecture forum, which sits under [name withheld] … and um. We also had a.. the stuff that I'm more involved in, in making sure that.. there is a compliance architecture in terms of business processes
	C61	and supporting systems.. so that's more in the area that I'm based in…all our designs… all the designs that the guys do have to go through the architecture forum…so the Architecture forum have to pull it apart to see whether it makes sense from a technology point of view
	C62	and whether there is compliance you know considering security you know whether there are best solutions to match the technology platform… stuff like that..
	C63	So the architecture forum.. is up to date with that..
	C64	That's um [name withheld] …they have got a big, big data warehouse department .,
	C65	Security and Confidentiality integrity, That's [name withheld] . but security is also part of data warehouse so there are overlaps with Peter Versfild..** extends to reports and what information can be used…sometimes the reports are online…there is a combination..
	C66	there is a middleware team...that gives a human aspect to the way we design things...such that the whole way we design things is very middleware driven.. we've got a rich...middleware architecture
	C67	that is handled in the architectural forum...If you look at this model over here…um you will see the business process… the supporting applications, we've got all the information supporting the application..
	C68	then we've got the hardware and operating systems which we call the infrastructural components…as a whole solution...all of this has to support the business process...and so all these things we first look at the systems development life cycle…
	C69	where we develop requirements specifications for reviewing the process.. we've got systems requirement specifications…doing all the system's stuff with the data…and then we've got integration specifications…in terms of how does this system send information to another system…or the middleware stuff…and all of that stuff has to go as either system's methodology...
	C70	so you've got a methodology…so basically all of this stuff that comes out …goes through the architectural forum…for scrutiny

	C71	but working with these things we also do pa*n reviews so we actually scrutinise each specification and we go through detailed.. analysis.. through...specifications
	C72	There is also this job in this area… which is part of the architectural
	C73	I think frameworks can be deceiving… we actually incorporate 3 frameworks…so we incorporate three frameworks... we incorporate the overall framework, to govern the enterprise architecture solution distribution which is basically the Zachman Framework.
	C74	but if you look in the Zachman's framework and you go right down to….the system's design.. basically those three of the Zachman's Framework.. then there is the CobiT and ITIL… are the ones that come into play in governing mostly the IT… processes…um.. so we have an over-encapsulating…methodology…which is the Zachman's Framework
	C75	and we've configured those things together and we've come up with '**IBAS**' which integrated business architecture solutions.
	C76	The Zachman framework consists of rows across (which are ITIL, CobiT) but the same principles are applied because there has to be an understanding of the business process for all the different areas
GA	C77	yeah so I mean…basically. we have… I mean there is a lot of…millions of processes ..in IT that run… so I mean from our side we also have a lot and there are certain systems that are …up at night and there are certain systems that run running during the day
	C78	and its just me being an old timer being bogged with SLA's and OLA's all those kind of things…coz I mean…those documents are whatever…
	C79	and most of them.. they cant even document all that stuff…
	C80	yes I think in a lot of areas it is like that…I mean…unless you work in call centres and that kind of stuff…so a lot of stuff that is,… is worked at from intellectual capital over the years…I mean someone probably in finance…who does the books or whatever…and they get rid of him or whatever…
	C81	like that…they bring in someone new…yes...he might be a CPA or whatever…but he does not have experience…but the
	C82	**:** I mean he doesn't know how the company works…because thing are forever changing…so.. its those… things…and er.. it's not his fault…know what I mean… and it would take him a long while…probably just to catch up…

	C83	I'd say a lot because...the whole way that.. we do run…from a WAN ***[view]…***we run Microsoft and all that…but the way the things are put together.. and that's the difference…every one is running Microsoft stuff.. and every one has got databases…everyone's got users…and everyone's got PCs and servers…but it the way..
	C84	[name withheld] … it's the way…the applications…and the people that use them…everyone's uses are a bit…different… so…[name withheld] uses are quits different from [name withheld] uses…because they've got different applications running on the servers…and they've got probably different ways of logging in
	C85	to suit their environment...more than it does anywhere else…so everywhere its just the gaps around…what you need.. I mean…ITIL and CobiT…are great frameworks but…its impossible to
	C86	Well…The impact on that.. I know really … would be that the whole import and export business is based on..this… um email system…and uh its is not really down.. but too….slow at the moment…like 2 hours slow..but the eventuality is that there is going to be um uh a massive impact on the…business
	C87	so it ***[the continued communication operation]*** shouldn't be based on the business kind of procedure…
	C88	I'd say the users probably tend to feel it more than we do…I mean a lot of stuff we do we do tech reasons ***[for the proper running of the system]*** … I mean we restrict what they can do…what they can install…and what they can mess around with… but ultimately the machine is a [name withheld] company machine…and they need to do the work…they have been to do.. so we give them access to do…that..
	C89	But I'd say on our side and from the tools point of view and that kind of stuff…we have most of the tools that we need and we use most of the generic stuff.. but the stuff that we feel that we really …really need , we do kind of budget for that and we do get it…so we budget for the
	C90	… I don't know…we haven't got that many....fancy tools... we use mostly generic stuff.. but its those little things that make our lives easier…like the little ***monitoring [network]*** tools…besides the big ones.. ooh..we…run the big..operations manager…(Microsoft Operations Manager).

	C91	no…they have their own little...monitoring tools monitoring the network… we have the monitoring tools monitoring the users..(Microsoft users)…so we actually have two…we have the small…one….***I'm not sure what's its called***r and then we have the big one…called the Microsoft operations Manager (MsOM).
	C92	The small one.. we find its quite nice….reflexive.. because its quick.. easy…and it can monitor.. say you need something.. now.. it can do it for you now.……and then we can move it on to the other one…as an additional kind of monitoring...in a different kind of way…
	C93	well, to tell you the…well…we've always had both…its always been the kind of thing that its just easier…coz we actually use the one…to monitor...and seek..and give us a better clearer indication of…if the things that are up or down...it gives you a nice green, red or orange.. know what I mean…? Very simple…
	C94	but the other one…usually gives you more information…the more technical…stuff on the technical side… so the one, would be geared more to the operating.. the operators…who get to see the lights…and stuff…and also have a quick feel on the…kind of things…people need
	C95	the other one the Microsoft operations manager might sort of take the operators much time.. coz it is sort of complicated….to work. With...than the other one..
	C96	so there are those little things…that we do just to help us and to help the business.. coz its those quick little things that…we need to do better…
	C97	so I mean yeah.. everyday... I mean , it would be actually be.. it would be too easy if people followed procedure....coz notebooks ***[things]*** break everyday… I mean...we just had a big change…and that was it…we just bought some extra amount of notebooks and that was it...
	C98	that was it.. the board or whatever that said…460 notebooks or whatever.. and that was it…
	C99	**:** that was it…but what they did was… they took the notebooks…they gave those new notebooks to people…and they gave the old notebooks that people had that were still on working conditions to other people…
	C100	now you have … and we didn't buy notebooks for about three years… now you have five year, six year old notebooks…

	C101	yeah...with no warranty and they are going to break… its just a matter of time…and so now they had to re-look that whole thing…they did.. .. it took a bit.. a couple…
	C102	about a whole month however.. and they decided that they are going to buy and extra amount more…
	C103	to give to the people that they gave…and get the ones that are broken…they had to think quick...and make that kind of a judgment…they had to..
	C104	well… what you see… well what happens is that it is all about…saving money…
FR	C105	and it all boils down to budgeting.... now they didn't budgets for it … so they have to justify why…they had to do it… so that was a main kind of thing…
	C106	I mean they also…in doing it… I mean.. they are also creating a more mobile environment where people also can work…with that...so for those people that are... I mean....if a person has got a broken notebook…then they cant work…you see?… so I mean they had to do something…and we've been trying to…giving them little injections with these notebooks to keep them going…know what I mean?.
	C107	changing the mouse… then changing this… I mean some of them…these people have got…notebooks that has got a mouse in it and they've got a keyboard in it…and they've got it attached to a monitor…because they don't have a PC…
	C108	because the monitor is not working…the mouse isn't working...and the keyboard isn't working…so…
	C109	so they actually have to adjust…I mean the big guys.. the executives… committee,…whatever…so we gave them all the facts and figures…all the notebook stuff…
	C110	including the new ones as well…the ones that were breaking…
	C111	you have to***…[laughter]…*** keep working…you see a lot of time… with the planning it is the main thing…because the business gives ***[priority]…*** obviously for certain projects…so that's where IT can get its money from
	C112	. or we can ***[for that matter]*** for hardware and stuff like that … then there is capacity and replacements which comes from our budget…
	C113	and that's how we get actually our money… because we basically.. so ***[if]*** its simple…if they don't give us the money and they basically want to grow.. by ***[say]*** 50% we cant…

	C114	so they…and.. and… we don't…normally don't bank a lot from our capacity and replacement money…ah so we do kind of get more of less something …from my side…coz they do cut it a little bit…
	C115	Communicating aims?…and…and also…they must like… as you say…'assessing the risk'…if the machine is out of warranty and it is a tier one applications its going to be down for some time and… the vendor might say come tomorrow…then you might get parts from um, I don't
	C116	know…Jo-burg…and if Jo-burg haven't got a part then you have to get parts from.. wherever.. States..***[US]..*** so we might as well wait…and that's all fine.. if they accept the risks…
	C117	it happens all the time…so in a lot of the applications and cases we have established that we don't have to give them that [admin] kind of access, but then there are I mean… it happens, … internet access…we used to talk about restricting internet access…obviously, but so far ***[for instance unlike]*** in ***[name withheld]*** America where they have a big database where they categorising data… (internet restrictions) by but obviously in ***[back here]***
	C118	[name withheld] you need access to retailing and selling sites.. coz that's the business they are in.. and there is also other sites that pop up all the time…aaah… whatever they are researching on…or whatever…at the time…and…it was kind of easy at the beginning because we gave them a list in and told them to choose the categories they said that they wanted internet access on..
	C119	and we did and worked on exactly what they said.. and of course within the first few days.. whatever…putting it ***[list]*** in ***[the system]***…we got hundreds and hundreds of calls…saying they couldn't get through.. they said that they wanted to go to selling sites.. whatever…and they couldn't go to see what was on hundreds of other sites…
	C120	so we quickly had to make ***[create]*** a few more categories…so it doesn't just get as simple as you just having internet access ..and you don't get this.. ***[but rather]*** you having internet access and you belong to marketing…and you belong to IT…
	C121	coz IT needs to download certain things like codes…and that kind of stuff…
	C122	Which increases the admin side which increases everything else, but in the long run it is probably *[felt]* it is the right thing to do…

	C123	**:** Coz, we had to do it… but in those groups…and what happens in the access aspect is that they can actually modify the database…and [name withheld] is actually the one who approves this…
BN	C124	hmmm..I think …our main thing here is to keep basically… I mean we have a lot of good uses in policies when it comes to keeping the system going…so certain time we do have to do what we have to do to keep them [systems] going…and sometimes we don't…know if it is the right thing to do..
	C125	So a lot of the times, is ah.. we try and structure as much as we can but obviously things may fall outside the structure…um.. I'd say…
	C126	Well most of the times we…try and keep us much structure as we can but most of the time that we do…people don't follow the right procedures…***[for instance]*** logging in a call the structure, would be broken by uh them [IT USERS] coming straight to us…because there is obstruction at the border and they need to go through…and obviously to them it is a great thing…because I mean they are willing to [jump levels] and would do what ever they need to do to get their stuff across the border
	C127	so sometimes we perceive that the thing is not actually as important as something else sitting around that needs more priority…so a lot of [reasons] people break structure would be varied as much as they use email… because they rely on the email system for instance if you make email in the business [primary] basis of your communication system… and system can go down…
	C128	its probably more critical…for [name withheld] ..to have a lot more systems being up…because every one relies on them.. .see what I mean…
	C129	Well… it is kind of working at the moment...its just that it is a bit slow… at the moment…
	C130	Well this is how we draw their attention…when it goes down…well…we tell…them "we told you not to ***[rely on]*** this business tool"…
	C131	And that's when they normally start...start taking notice of uuhmm maybe we should actually do this in a different way.. I mean we have a whole...middle tier uh...application integration system...that does this kind of things….that makes you do all the right kind of stuff… but um for simple things like um..email its amazing that um..the email being down..

	C132	so those kind of things is hard to… because.. they do it because…they are under a lot of pressure...at the time.. and those kind of things..
	C133	correct…something will always happen..
	C134	Yooh…um.. yes, sure.. um…what would I say? I mean, this time we just went through a new desk-top kind of structure...now, and our policy was in place…
	C135	that no one was going to have any administration rights to the machines…
	C136	that no one was going to be able to install these third-party…[applications] whatever…
	C137	and obviously now when we reflect on it…***[policy]*** it has not been too bad on business, but now when we hit certain areas, is that we have to make some kind of adjustments… because there are so many applications out there…and the thing is that, to be working…these needs to run on the administration rights of the machine…
	C138	and those kind of things…and…so we actually made provisions, that we could do it***..[amend policy]*** when we looked at the group policy…on administration rights issues…
	C139	we could give those users,…whatever…administration rights on the machine centrally.. but [only] if we could manage those users who got admin rights on the machine…so that was on the agenda then…we didn't want to…
	C140	because obviously this could cause some problems…installing stuff.. those kind of things..
	C141	we had actually had to give them…we try to narrow it down a lot…we also try to give them…and make sure that they are not running an extra link to the applications they don't normally need…
	C142	the ones they don't normally use…[though] we just cant try to just stop them running the applications [they don't need], but we now don't want them to do that…
	C143	I um I mean …you make the.. I mean a decision whatever.. um..
	C144	sure, I mean I haven't really worked anywhere else.. I wouldn't be able to say so much.…I mean…our actions.. we base it on the criticality of the application…obviously…um.. experience…obviously if the heat comes from the executives and that kind of .. coz we know which applications are critical and which and which are not…

	C145	how…long you've been here…we know what … I mean…an lot of it is based on most of the things…in… in whatever…is based on…a lot of it is based on experience…and just knowing what is important and what's not… and we sit…and we put together our plan…for next year… ere..a lot of them don't know what the application…is running on…
	C146	we… need to say like ***[for instance]*** they are running out of disks …and.. I don't know.. er the box ***[notebook]*** is 5 years old…and it means now… the warranty…and this is the stats.***[statistics]*** … it is kind of like under-performing…but we tend to focus more on the high level ones….
	C147	than on the low level ones…so… and we also know that…like if we get a call on a Saturday…for something that is down…. don't worry…we will look at it on a Monday...since it is not a high level one...but if you get a call for something that you know is high level you will come in…
	C148	and a lot of that is just based… on… you know… that.. I mean you have to know…the whole..
	C149	yeah what they are trying to do… holistically… what they have been trying to do… the business process …it is all based on the criticality of the business process…and what's important and what's not…