INFORMATION TECHNOLOGY AS A RISK MANAGEMENT TOOL: CASE OF NWPG (FINANCE DEPARTMENT)

By

Sehudi Terance Seletedi

Mini-dissertation submitted in partial fulfillment of the requirement for the Masters degree in Business Administration at the Graduate School of Business and Leadership of the North West University, Mafikeng Campus.

Supervisor: Prof. Nehemia Mavetera

TABLE OF CONTENTS

DECLARATION

I hereby declare that this research is my own work and efforts and that it has not been submitted anywhere for any reward. Where other sources of information have been used, they have been acknowledged.

Signature……..

Date……

ABSTRACT

This mini dissertation considers the Information Technology as a management tool: case of NWPG (Finance department). The dissertation reveals the perception of IT officials regarding the roles of IT portfolio, characteristics, success and Intervention that can be applied by IT management. Though the period of study is wide in scope, this research investigates those factors which contribute to IT as a risk management tool. The central focus is only those aspects that contribute to IT.

The dissertation also focusing on security controls which plays an important role as a main influence on risk management and is also vital to minimise business risk in fulfillment of the managements need for a going concern concept and how they can be implemented to address risks. Such security controls include formulated security policies and procedures that have to be complied with by all members of the organisation having access to all financial and other applications systems within that organisation. 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. Typically the system and information owners are responsible for changes to their IT systems.

The lack of security controls may lead to anyone within the organisation, acting as he or she deems fit. This can automatically lead to poor management decisions being made based on incomplete and inaccurate information created at the absence of access controls. Lack of security controls within a technological business environment enhances the possibility for fraudulent activities

Attention is also paid to the involvement of IT management staff that plays a vital and crucial role in IT planning processes that are designed by management that adequately includes operational resources to support the automated line business. It also includes the step process model that can help elevate the IT risk conversation to the appropriate business executive, aiding the decision making process regarding IT risk posture those steps are that you must identify and classify your IT asserts and once you have identify you can then assign controls to them and mitigate IT risk to acceptable levels. The other step is that you must remediate IT risk and you must also manage risk.

The Department of Finance in North-West Provincial Government has a legal responsibility to build risk management capacity in the public sector. Furthermore, The National Treasury has a legal responsibility to assist the Department of Finance in province in monitoring and addressing the systems of risk management in Provincial Departments and assisting with building risk management capacity in Provincial Departments. In executing its own mandate, The National Treasury takes acknowledgement of the mandate of the Provincial Treasury which is the Department of Finance as set out in the PFMA. It is also important to acknowledge the manner in which the legislation is written, sometimes it creates overlapping responsibilities for National Treasury.

Acknowledgement

I would like to express my sincere thanks to my supervisor: Professor Nehemiah Mavetera for his constant and constructive guidance throughout the study. Study group members of Group G and other MBA students who gave a hand, I say thank you very much.

- My family for the moral support, especially my mother Aus Meisie who tirelessly fought against the economic hurdles of this world to see her son attain the greatest gift of all, "Education".
- To my father (Seoposengwe Welmind Seletedi) who never lived to see the fruit of his advice and dedication.
- Gofaone my son, take this as your inspiration.

LIST OF FIGURES

List of figures.....Page

LIST OF TABLES

List of Tables.....Page

CHAPTER 1

RESEARCH PROPOSAL

1.1 Introduction

Valsamakis *et al* (2005:12) define risk management as a managerial function aimed at protecting the organisation, its people, assets and profits against the physical and financial consequences of risk. It involves planning, co-ordinating and directing the risk control and the risk financing activities in the organisation. Uncertainly about a situation can in most cases indicate the risk, which is the possibility of loss, damage or any other undesirable or unpleasant event. Almost any change, good or bad, poses some risk.

Security controls have a main influence on risk management and are vital to minimise business risk in fulfillment of the managements need for a going concern concept and how they can be implemented to address risks. Such security controls include formulated security policies and procedures that have to be complied with by all members of the organisation having access to all financial and other applications systems within that organisation. 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. Typically the system and information owners are responsible for changes to their IT systems.
Thus, they usually have to approve and sign off on changes to their IT systems (eg, system enhancement, major changes to the software and hardware). The system and information owners must therefore understand their role in the risk management process and fully support this process.

The lack of security controls may lead to anyone within the organisation, acting as he or she deems fit. This can automatically lead to poor management decisions being made based on incomplete and inaccurate information created at the absence of access controls. Lack of

security controls within a technological business environment enhances the possibility for fraudulent activities. This was a problem to be discovered within a big organisations such as government where white collar crime, committee through technology, brought most companies to collapse or running at deficits or even being liquidated. Other adverse effects that may contribute to the collapse of an organisation exposed to this type of an environment may be brought about by breach of government regulations by the staff unaware of the existence of such regulations, norms and any other measure governing the organisation.

1.2 Background and Context

The Department of Finance on North-West Provincial Government had to act beyond their budgetary constraints and they were loosing focus on their strategic plan. The idea was to provide good public service to its customers' and creditors' payment. It was a good one, the strategy to have it rolling was also good but the failure to the whole issue proved to have been brought by lack of management controls and poor management decisions. It appeared as if the work risk was far fetched to the management. During 2009/2010 financial year the forensic investigation by Price Waterhouse Coopers (PwC) discovered that the officials of the Department of Public works, Roads and Transport have been fraudulently enriching themselves with the funds of the government. The investigations were taken over by SAPS. Some of the officials were suspended, some were dismissed and those who were not found guilty were reinstated in their job situations.

The two-month audit, conducted in 2009 into tenders issued by the North-West Department of Public Works, Roads and Transport management directorate, led to the firing of the department's chief financial officer and chief director. The tender scandal, described by department's MEC as "shocking", saw the department spending its 2009/2010 financial budget of R525m in the first three months of the year and saw all of its three-year R1.5 billion medium-term expenditure framework budget being allocated apparently without following protocols.

The department's internal investigation into the awarding of the road tenders came after the departmental MEC was forced to borrow money from the National Treasury when it was discovered that in the first three months of the 2009/2010 financial year, the department had used "100 percent of its R525m budget". It was estimated that R1, 5bn allocated for road capital projects in the next period of three years for the medium-term expenditure framework had already been committed.

The managers responsible for business operations and IT procurement processes must take an active role in the risk management process. These managers are the individuals with the authority and responsibility for making the trade-off decisions essential to mission accomplishment. Their involvement in the risk management process enables the achievement of proper security for the IT systems, which, if managed properly, will provide mission effectiveness with a minimal expenditure of resources. The fraud was widespread in the Provincial Government after realising that there was serious implications and overpayments made to the the company which was awarded the tender to construct a road linking the town of Koster to Lichtenberg.

1.3 Problem Statement

In today's challenging global economy, business opportunities and risks are constantly changing. There is a constant need for identifying, assessing, managing and monitoring the organisation's business opportunities and risks. Risk management is a well-established philosophy; however, organisations are struggling to implement, embed and sustain a pragmatic Enterprise Risk Management solution that is robust, adds value and creates a balance between cost and reward.

The Department of Finance in North-West Provincial Government has a legal responsibility to build risk management capacity in the public sector. Furthermore, The National Treasury has a legal responsibility to assist the Department of Finance in province in monitoring and addressing the systems of risk management in Provincial Departments and assisting with building risk management capacity in Provincial Departments. In executing its own mandate, The National Treasury takes acknowledgement of the mandate of the Provincial Treasury which is the Department of Finance as set out in the PFMA. It is also important to acknowledge the manner

in which the legislation is written, sometimes it creates overlapping responsibilities for National Treasury.

.

The Department of Finance has capacity constraints; currently there is one official responsible for supporting all departments of risk management, making it difficult for the Department of Finance in fulfilling its mandate of monitoring and assessing the systems of risk management in provincial departments, assisting with building risk management capacity in Provincial Departments and enforcing the PFMA by implementing specific prescripts pertaining to risk management in Provincial Departments.

The Risk Management policies of some of the Provincial Departments are not reviewed annually to ensure continued relevance in the context of the department's aim and objectives. IT security program managers and computer security officers are responsible for their organisations' security programs, including risk management. Therefore, they play a leading role in introducing an appropriate, structured methodology to help identify, evaluate and minimise risks to the IT systems that support their organisations' missions. Information System Security Officer (ISSO) also acts as major consultants in support of senior management to ensure that this activity takes place on an ongoing basis.

The CFO's report in the department of finance in risk management indicates that Risk Management Unit in most Provincial Departments is not appropriately staffed in terms of the number of people and the skills and expertise required. The responsibilities for risk management have not been incorporated in the performance agreements for the relevant officials and there is no mechanism in place to communicate any changes to the business unit risk registers to the chief risk officer, the risk assessments are not regularly conducted and the risk management committees for some departments are not established and those that are established are not functional.

Risk management is the process that allows IT managers to balance the operational and economic costs of protective measures and achieve gains in mission capability by protecting the IT systems and data that support their organisations' missions. This process is not unique to the

IT environment; indeed it pervades in all areas of our daily lives. Take the case of home security, for example. Many people decide to have home security systems installed and pay a monthly fee to a service provider to have these systems monitored for the better protection of their property. Presumably, the home owners have weighed the cost of system installation and monitoring against the value of their household goods and their family's safety, a fundamental "mission" need.

The duties of the provincial department are set out in the Public Finance Management Act and Treasury regulation that the accounting officers should ensure that the risk assessments are conducted regularly to identify emerging risks of the department and a risk management strategy which must include a fraud prevention plan and must be used to direct internal audits efforts and priority and to determine the skills required of managers and staff to improve controls and to manage these risks. The Treasury regulation further states the accounting officers should ensure that the risk management strategy is clearly communicated to all officials to ensure that the risk management strategy is incorporated into the language and culture of the department.

The capacity problem in departments resulted in the lack of financial planning and control because departments were exceeding their budgets and/or incurred unauthorised expenditure, the creditors were paid late sometimes they were not paid, with the result that fruitless expenditure was incurred due to charges. The payments of invoices were duplicated, there was a serious abuse of the financial system; the commitments were not registered on the information system. They used incorrect allocations, the books of accounts were closed late and that made the department to have Auditor General's qualified report.

1.4 Research Aim and Objectives

1.4.1 Aims

1.4.1..1 To investigate Information Technology as a risk management tool in the department of Finance North West Provincial Government .

1.4.1.2 To determine emparically the skill level of IT employees.

1.4.2 Objectives

The objective of this study is to identify key learnings from successful Enterprise Risk Management. Implementations in risk management that could potentially be useful to other departments in developing and expanding on existing Enterprice Risk Management practices, and facilitate the preparation and practical implementation of Enterprice Risk Management in order to give assurance to all stakeholders that all potentially significant risks, are identified and managed.

1.5 Research Questions

- What is the importance and impact of Information Technology as a Risk Management tool in the Department of Finace?
- Are the employees in the department of Finance have skills to operate the financial systems and to perform those tasks to detect financial risk in the system?
- Is there any direct relationship between the job characteristics of Managers in the Information Technology directorate and their rate success or fuilure in Finance as a whole?

1.6 Importance/Significance of the Study

The importance of this study is to asses the relationship between the Information Technology and Risk Management in the Department of Finance and to investigate whether NWPG IT has an important role in Risk Management in all departments in North-West Province.

- Where specifically is the information processed and stored?
- What are the types of information storage?
- What is the potential impact on the organisation if the information is disclosed to unauthorised personnel?
- What are the requirements for information availability and integrity?
- What is the effect on the organisation's mission if the system or information is not reliable?
- How much system downtime can the organisation tolerate? How does this downtime compare with the mean repair/recovery time? What other processing or communications options can the user access?
- Could a system or security malfunction or unavailability result in injury or death?

The questionnaire endearvours to capture the opinions and perceptions of the respondents in respect of the effectiveness of Information Technology as a Risk Mananagement tool in the department and importance of qualifications in relation to success or failure in these jobs. The questionaire will be organised in a number of sections requiring of the respondents to indicate on a 5 point lickert scale, their perception on their jobs and how they personally feel about their jobs. The research process will consists of two distinctive phases that aim to determine how people describe, feel about their jobs as well as whether there is a definite relationship between their qualifications and being successful in their job. Members of management within the department will be surveyed on their opinions, their jobs and importance qualifications in relation to success or fuilure in these jobs by means of a self administered questionnaire.

1.7 Research Findings

The primary aim of this study is to assess the relationship between the position of certain academic qualifications and the degree of success with which these could be applied in any particular organisation to achieve its goal with reference to the Department of Finance in North-West Provincial government. By means of an investigation based on the hypothesis of this study, it is stated to verify this hypothesis data obtained. The evaluation of the report is partly based on the investigation. Departments are held resposible to make sure that they follow the right tendering procesess and make sure that after appointing a service provider it is their duty to monitor the smooth running of the project.

1.8 Conclusion

A successful risk management program will rely on the following:

- Senior management's commitment.
- The full support and participation of the IT team.
- 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 organisation.
- The awareness and co-operation of members of the user community, who must follow procedures and comply with the implemented controls to safeguard the mission of their organisation and
- An ongoing evaluation and assessment of the IT-related mission risks.

Active in risk management and fraud prevention is the consulting for a wide range of corporate, financial, educational and governmental clients. Its work involves risk analyses; risk financing reviews, including insurance and self-insurance and the development of risk management administration. Oganisations should consider projects on the use of captive insurance companies and co-ordinated captive and pooling studies for universities, railroads, hospitals, chemical companies, engineering firms, shipping companies and municipalities, among others.

Since the Department of Public Works, Roads and Transport has a problem, the Information Technology have to speed up the take over to enable it to increase security controls, promote the compliance and reduce the duplications and over payments as well as fraud prevention. Information Technology with an aid of forensic unit and internal auditors had to continue to render a quality service and commitment to the provincial departments.

This chapter described the research proposal and the problem statement. The following chapter which is Chapter 2, presents the literature review .

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

This chapter focuses on the literature reviewed for this study. The intergrated fit of the structure into strategy formulation and its implementation will be discussed. The purpose of this chapter is to do the findings and to gain better understanding of risk management procedures and examine on if Information Technology is used as a risk management tool in the North-West Provincial Government.

Most of the research from different schools recognises the factors that have the greatest influence on the implementation success. The articles discuss critical success factors in different dimensions as well as specifying which factors are important and how these factors are important. For this reason, we are researching critical success factors for effective risk management. We would like to prove that the critical success factors for effective risk management mentioned in the articles are not only true but also suitable for the department of finance in North-West provincial government.

2.2 Literature Review

This chapter presents the theories and articles relevant to the thesis topic of "Information Technology as a risk management tool: Case of Department of Finance". It is divided into the following two parts: Risk management and information technology success factors for risk management and this chapter helps the reader understand the basics of risk management and emphasises information technology as a critical success or a tool for effective risk management procedures.

Stoneburner *et al* (2005:04) argue that risk management is the process that allows IT managers to balance the operational and economic cost of protective measure and achieve gains in mission capability by protecting the IT systems and data that support their organisations' missions. This process is not unique to the IT environment; indeed it pervades decision-making in all areas of our daily lives. Take the case of home security, for example. Many people decide to have home security systems installed and pay a monthly fee to a service provider to have these systems monitored for the better protection of their property. Presumably, the home owners have weighed the cost of the system installation and monitoring against the value of their household goods and their family's safety, a fundamental "mission" need. The head of an organisational unit must ensure that the organisation has the capabilities needed to accomplish its mission.

Furthermore these mission owners must determine the security capabilities that their IT systems must have to provide the desired level of mission support in the face of real world threats. Most organisations have tight budgets for IT security; therefore, IT security spending must be reviewed as thoroughly as other management decisions. A well-structured risk management methodology, when used effectively, can help management identify appropriate controls for providing the mission-essential security capabilities.

Levitt, former chairperson of the US Securities and Exchange Commission, indicated that the average organisation of today is a complex enterprise engulfed by rapid technological change and fierce global competition. It is essential that risk be assessed on an ever-changing landscape as most major losses are as the result of a series of high impact but low likelihood events.

Stewart (2005:202) adds to the above by saying that risk is good and the point of risk management is not to eliminate all risks because that would also eliminate reward. The point is to manage risk by choosing where to place bets and where to avoid betting altogether. An organisation's security standards should establish a set of controls and guidelines to ensure that security procedures governing the use of the organisation's IT assets and resources are properly enforced and implemented in accordance with the organisation's goals and mission. Management plays a vital role in overseeing policy implementation and in ensuring the establishment of appropriate operational controls.

Operational controls, implemented in accordance with a base set of requirements (eg, technical controls) and good industry practices, are used to correct operational deficiencies that could be exercised by potential threat-sources. To ensure consistency and uniformity in security operations, step-by-step procedures and methods for implementing operational controls must be clearly defined, documented and maintained.

The King Report on Corporate Governance for South Africa - 2002, referred to as the King II Report (2007:73), pointed out the importance of a thorough understanding of the risks of the organisation in the pursuance of its objectives and together with the strategies employed to mitigate those risks. This is thus essential for a proper appreciation of a company's affairs by the board and stakeholders. This report also recommends enterprise-wide risk management strategies for all organisations because risk management is a holistic way to design, implement and manage capabilities for managing an organisation against risks that matters and to identify and plan for opportunities. This strategy includes but is not limited to the following risks: strategic risk, financial risk, security risk, information technology risk, operational risk, human resources risk and compliance risk, safety, health and environment risk.

Dickinson (2005:360) explained that the assertion of the enterprise-wide risk management (ERM) has emerged as a concept and as a management function within organisations since the mid-1990s. ERM is a systematic and integrated approach to the management of the total risks that an organisation faces. Its emergence can be traced to two main causes. Firstly, as a result of high profile organisation failures and preventable large losses and secondly, due to shareholder value models playing a greater role in strategic planning.
ERM became a prerequisite for successful and well-managed businesses. Over time, a business that cannot manage its key risks effectively will simply disappear.

According to the Deloitte Risk Intelligence Series (2006:3), risk is the potential for loss or the diminished opportunity for gain caused by factors that can adversely affect the achievement of an organisation's objectives. Organisations that focus solely on risk avoidance may survive but

rarely thrive; only those that intelligently manage risk taking as a means to value preservation and value creating will excel in today's risky yet opportunity-rich business environment.

Stoneburner *et al* (2005:32), explain that in implementing recommended controls to mitigate risk, an organisation should consider technical management and operational security controls or a combination of such controls, to maximise the effectiveness of controls for their IT systems and organisation. Security controls, when used appropriately, can prevent, limit or deter threat-source damage to an organisation's mission. The control recommendation process will involve choosing among a combination of technical management and operational controls for improving the organisation's security posture.

They also argue that the trade-offs that an organisation will have to consider, are illustrated by viewing the decisions involved in enforcing use of complex user passwords to minimise password guessing and cracking. In this case, a technical control requiring add-on security software may be more complex and expensive than a procedural control but the technical control is likely to be more effective because the enforcement is automated by the system. On the other hand, a procedural control might be implemented simply by means of a memorandum to all concerned individuals and an amendment to the security guidelines for the organisation but ensuring that users consistently follow the memorandum and guideline will be difficult and will require security awareness training and user acceptance.

Laudon and Laudon (2006:342) outlined that the information systems threat may come as a result of technical, organisational and environmental factors if there is a poor management decision. The threat may stem from internal users by introducing errors and accessing systems without authorisation. Intruders may also access organisations' data through networks by launching denial of service attack or software to disrupt organisational operation.

Chandra *et al* (2008:40) argue that the systems protection is vital since it prohibits unauthorised access and malicious attack to organisation's systems. This systems protection, if it is set correctly from onset, can ensure that the software assets such as application programs, the operating system and stored information are protected.

By not having proper information systems protection techniques in place, an unauthorised access to computer systems of organisations might cause dire consequences, in the sense that organisations hold valuable information.

Chandra *et al* (2008:54) pointed out that the valuable information stem from employees taxes, medical records and financial status of the organisations. To a large extent employees could be affected severely given the high rate of crime, especially fraught crime, whereby unauthorised access to employee's information could lead to intruders using that information to perform various illegal transactions.

Laudon *et al* (2011:270) on their opinion stated that many firms are reluctant to spend heavily on security because it is not directly related to revenue. However, protecting information systems is so critical to the operation of the business that it deserves a second look. Companies have very valuable information to protect. Systems often house confidential information about individual taxes, financial assets, medical records and job performance reviews. They can also contain information on corporate operation, including trade secrets, new products development plans and marketing strategies. Government systems store information on weapons systems, intelligence operations and military targets. These information assets have tremendous value and the repercussions can be devastating if they are lost or placed in the wrong hands. Most real systems are exposed to numerous sources of risk. Over the last two decades, the problem of ranking and prioritising these sources has challenged not only decision makers but the risk analyse community as well.

They furthermore argue that managing IT risk is part of running any business these days. Regardless of the business, understanding IT risk helps increase network security, reduce management costs and achieve greater compliance posture. Failure to identify, assess and mitigate IT risk sets the business up for serious security breaches and financial losses down the road. Those that think managing IT risk is the job solely of the IT staff are in for a big shock.

Companies make considerable investments in people; processes and technology to ensure their businesses run smoothly. Understanding the relationships and levels of risk among these vital assets is imperative if you want to increase network security, streamline compliance and reduce

overall IT costs. The challenge for most companies is to identify a repeatable process to identify, assess and remediate IT risk without interrupting their business activities.

Today's IT risk environment is more threatened than ever thanks to the growth in sophisticated malware attacks and security vulnerabilities, with Web 2.0 adoption adding new layers of IT risk. Regulations continue to increase, placing additional costs on organisations to meet these new requirements. Organisations need an intelligent approach when it comes to assessing IT risk and managing compliance.

The Information System Audits and Control Association (ISACA) has defined IT governance activities as consisting out of five focus areas and they are Strategic Alignment, Value Delivery, Resource Management and Performance Measurement.

2.3 IT risk at the board level

According to a 2009 survey of 280 audit committee members conducted by KPMG in conjunction with the National Association of Corporate Directors, IT risk is a key area of concern. Alarmingly, 45 percent said they are only somewhat satisfied with their oversight of IT risk and 42 percent said they are only somewhat satisfied with the quality of information they receive on IT risks. This shows a significant gap in the communication of risks between executive management and IT.

It's critical to the IT risk management process that executives are informed of threats and assist in assessing the business impact these risks pose and sign off on the risk position. Only when the IT and executives are aligned in the identification, assessment and remediation of IT risk can a company achieve higher levels of security and compliance.

Here is a simple four step process model that can help elevate the IT risk conversation to the appropriate business executive, aiding the decision-making process regarding IT risk posture as indicated in the 2009 survey of 280 audit committee members:

STEP 1: Identify

The first step is to identify and classify your IT assets down to which servers hold sensitive and confidential information. But, to determine which IT assets are most important, you need to first understand the core issues that concern the business stakeholders. Risks that need to be considered include:

- **Data Confidentiality**

There is a risk that confidential or sensitive information may be mishandled or made available to those who shouldn't have access to the data. In many regions, protection of sensitive information is required by law and is also addressed on an industry by industry basis through organisations such as the PCI Standards Council.

- **Data integrity risk**

This is incurred when the underlying data is unreliable because it is incomplete, inaccurate or otherwise suspect. The cause could be deliberate tampering or simple human error, be it improper error checking on form submissions or the inappropriate configuration of a transaction server.

Regardless of the cause, the impact to the business can be considerable, especially if the erroneous data is not discovered for some time. One of the most well-known IT risks in an organisation is availability. The short term loss of service due to IT systems failure has the potential to have a significant - and potentially long-lasting - impact on the daily operations of a business.

- **Relevance risk**

This type of risk is rarely considered but is one of the most common types we face. It has to do with not getting the right information to the right people, processes or systems at the right time. This often means that the right action is not taken or is taken too late.

- **Project risk**

Essentially, an investment or expense risk: the risk that an investment made in IT will fail to provide the expected value. Frequently, the real reason IT projects fail to meet their objectives is a lack of accountability and commitment.

So, what next?

First, identify your electronic assets. This requires scanning software that can inventory your network; non IP-addressable assets (such as people and processes) require automated surveys of the key organisational areas.

Second, map IT assets to specific business processes. By understanding what your organisation is trying to accomplish in the marketplace, you can establish what systems sustain that value.

In other words, you must build a complete picture of how your IT assets correlate with your business functions.

STEP 2: Access

Once you have identified your assets and the outstanding IT risks to the business you can then assign controls to them and mitigate IT risk to acceptable levels.

The only way to effectively manage growing data points is through the proper use of automation which typically focuses on gathering controls data for audit support. This results in the ability to assess the environment more frequently and has two main benefits:

- Find issues before they escalate into full blown projects; thereby control deficiencies can be remediated as part of daily operations, as opposed to project scale endeavours.
- Know where trouble spots are before the auditors arrive, demonstrating due care and that appropriate management controls are in place.

For too long, generating and providing reports to auditors has been treated as a disruption for IT operations. However, automation enables the production of meaningful and accurate reports

specifically tailored to meet auditor queries. It also reduces the amount of time spent collecting data and reporting on IT controls and instead allows the IT team to focus on how the organisation can make best use of its regulatory environment.

STEP 3: Remediate IT risks

A commonly overlooked part of the IT risk management process is the steps taken for remediation of detected deficiencies or vulnerabilities. There are three factors that mean organisations often have limited resources to address the risks they face every day capital, labour and time. By prioritising IT work upon the business impact and risk tolerances, organisations can make the best use of these scarce resources.

IT security teams need to think like a "traditional" business and demonstrate how specific remediation activities (and even bigger project-level investments) will impact the organisation's IT risk posture; thereby giving value for every penny spent. By assigning a business value to the remediation work, IT can show how the IT security spending has improved the organisation's compliance and security posture.

Once a value is assigned to control implementation and remediation activities, it must be tracked. Through consistent (automated) testing and reporting on changes made by the remediation efforts, the positive results of those activities become clear. Trends emerge that can be used to show the audit committee and other key stakeholders that you are exercising due care in responding to the shifting regulatory and threat landscape. In time, you can show that you are continually working toward a better managed risk programme.

STEP 4: Manage

The aim of the management phase is to make sure there is a common goal of operational and strategic visibility in compliance, IT risk and control environments. The main requirement is to get to know your business's numbers.

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

For IT risk, it may seem logical to start with metrics generated by IT or information security; however, this is not the whole picture. Look elsewhere in the business to see the impact of IT operations and effective security and compliance activities. Using the numbers generated by those business units ensures that your success aligns with theirs. This way, metrics for compliance and risk management are received in a language the stakeholders can understand.

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

Frequent measuring of IT risk indicators allows the organisation to spot trends, highlighting under- or over-performing areas of the enterprise. The organisation can then target areas that are underperforming and remediate well in advance of an audit to show that management has insight into those areas and is exercising due care. Once the data starts streaming in, continue to engage those parts of the business that have been tapped for that data. This showcases the value of high-quality IT risk management and provides a phenomenal platform from which to grow your influence and involvement in guiding IT risk decisions and improving your organisation's overall risk posture.

By assigning a value to the metrics you are tracking, you can build confidence within the business for your IT risk decisions. When pointing out high-risk areas to the stakeholders it is far better to avoid selling 'fear'. Instead, use solid metrics to build a stable base of credibility and business alignment that will pay dividends for years to come.

2.4 Limits and controls

Limits and controls represent the mechanism responsible for articulating and communicating an enterprise's risk appetite to different constituencies' senior management, business line management, traders and other risk takers, risk managers and operations personnel. Each limit represents a threshold or acceptable boundary within which permissible risk-taking activities may be pursued. Hence an enterprise's limit structure should be consistent with its overall business strategies and reflect the different types of risk-taking activities that are engaged in to execute these strategies. Limit setting in many institutions begins with a bottom- unprequisition for limits that are defined in the context of revenue and net income budgets prepared or set for each business unit. These limits requests are then evaluated and aggregated at the overall corporate level, usually by the enterprise-wide risk management function and presented by senior management to the board of directors for approval. The board-approved or delegated limits are then parcelled back to the various business units. Within the business units, limits are usually allocated to specific desks or traders at the discretion of the respective business unit heads. An institution's limit framework should include a combination of volume limits, risk sensitivity limits, portfolio level, value-at-risk (VaR) limits and stop-loss limits data and information systems.

Accurate, timely and comprehensive data together with robust, integrated information systems are an integral part of an effective risk management programme. The enterprise's risk management systems must have the ability to capture and measure key risks in a globally integrated manner. This implies that transaction and position data, counterparty information, real-time market data and modelling assumptions are appropriately captured in the system. Unfortunately, many institutions today are faced with the legacy of fragmented risk management systems that preclude an effective corporate-wide view of portfolio risks.

Once risk data have been transformed into meaningful risk management information, it must be delivered to different users in a fast, flexible, efficient and friendly manner. Speed of delivery is critical to monitor the enterprise's risk positions under rapidly changing market conditions. Flexibility is the key to allowing users to vary their views on data with respect to scope, contents,

frequency and format. Efficiency is necessary to minimise the drain on system and user resources. Finally, the user friendliness of risk management systems is vital to empower end-users to extract, evaluate and act upon risk information.

2.5 Classification of risks

Different enterprises are exposed to risks in different ways. For example, financial institutions may be much more prone to interest rate risk because of their lending activities compared with, say, manufacturing companies which make use of fixed interest rate debt. Importers and exporters, for example, are directly exposed to currency risk whilst those with no foreign dealings do not have this problem. Although the broad grouping of risk types will be similar for all enterprises, the classification of the risks into the broad grouping will differ from one enterprise to the next. In this regard, all risks can be grouped into two broad categories, namely speculative and event risks. Speculative risks are those risks that offer a chance of gain or loss. For example, a reduction in interest rates will be to the advantage of an enterprise that borrows money. However, an increase in interest rates will be to the detriment of that enterprise. Event risks, on the other hand, concern the possibility of loss only of an enterprise's plant and equipment due to a fire. The aforementioned lists of core business risks are not exhaustive and merely serve as examples of how the risks of enterprises may differ because of differences in the industries in which they operate as well as the individual characteristics of enterprises.

Operational risk is the exposure of an enterprise to have loss resulting from internal failures or shortcomings of people, processes and systems. There is always a human factor to consider in undertaking any business activity. The knowledge, experience, capability and reliability of the persons involved in all of the business processes are critical risk factors. People risks continue to be the major contributing factor in many dramatic failures and, despite the difficulties of measuring this kind of risk, it needs to be targeted in any programme aimed at improving risk management.

The following list serves as an example of people risks as outline in the Financial Services Authority 1999:

- Inexperienced, incompetent, unsuitable, negligent and/or maverick staff.
- Human error.
- A working culture creating low morale, high staff turnover, poor concentration.
- Low productivity and industrial action.
- Fraud and theft.
- Unauthorised and/or ill-informed decision making at all levels, particularly with
- Regard to business strategy, project management, change management, liquidity and outsourcing.

2.5.1 Processes

Process risk is the risk of a business process being inadequate and causing unexpected losses. This inadequacy includes execution errors due to flaws in the processes for example, if the exact procedure to be followed for a procurement order is not clearly set, the order may be delayed or even go missing due to certain steps in the process that are unintentionally being skipped.

Processes form part of the operations environment and therefore have a strong interactive relationship with people and systems. Any changes in processes affect people and systems. For example, if the accounting process is changed, it may alter the way in which people need to perform the different activities that are part of the process and this may also require the adaptation of the system used in the accounting process. People and systems, on the other hand, can also affect processes. For instance, the introduction of a new payment system in an enterprise may require processes to be changed to facilitate efficient operational performance.

Processes are also affected by external events such as legislation requirements that may change and therefore compel enterprises to follow different processes. The following are examples of processes in which the risk involved must be monitored and managed:

- The enterprise procurement process.
- The enterprise accounting process.

- The enterprise inventory management process.
- The staff appointment process.

Proactive risk management should address the risks relating to processes during, say, mergers, acquisitions and disposals, environmental changes, the implementation of new systems and the re-engineering of processes. Systems risks refer to the risks resulting from systems failures and they are therefore primarily based upon enterprises' reliance on technology. These days, most large enterprises are exposed to the risk of an interruption or slow-down in their computer systems. Client records are generally stored in digital format on computer systems, accounting and reporting is done via electronic systems and even the bulk of payments by customers to enterprises and vice versa, are made electronically.

The upshot of this is that enterprises are vulnerable to any disruption in the efficient functioning of systems and also to system obsolescence. For example, financial institutions find that computer software that facilitates the use of electronic banking by customers requires regular updating. This updating of the systems, financial institutions remain the targets of criminals who continuously attempt to disrupt and alter the systems to their own advantage, resulting in potential losses to the financial institutions. New technologies are often complex and therefore create uncertainty. The newer the technology, the greater the risk that it may not perform as expected. It is well known in the information technology profession that new systems often require modifications in order to function smoothly. Another aspect of new systems is that people's risks are involved in the sense that the new skills are required for the latest technologies. The learning of new technologies and the methods applied to operate them is often met with resistance by employees. Not only does this resistance need to be monitored and controlled but effective training programmes also need to be implemented. The following are examples of systems risks:

- Systems failures.
- Security breaches.
- Implementation failure.
- Insufficient systems capacity.

- Poor data integrity.

An enterprise can be exposed across all business areas to technology risk. Technology controls are therefore required throughout the enterprise to ensure that technology is protected against human error, data theft, equipment failure, fire, heat, water, smoke, corrosive fumes and so on.

2.6 Other important event risk concepts

Depending on their particular origin, event risks can be categorised as fundamental or particular risks.

Fundamental risks arise from losses that are impersonal in origin and consequence and originate in the economic, political or social interdependency of society. However, they may also arise from purely physical occurrences such as drought conditions occurring in Southern Africa.

Particular risks are losses that have their origin in discrete events which have an essentially personal cause. Such risks would, for example, be fire damage to a building or the explosion of a pressure tank. The reason for the distinction between particular and fundamental risks is to establish whether commercial insurance may be appropriate or available as a means of financing the consequences of such a risk. Losses arising from fundamental risks cannot be prevented, particularly by an individual. Frequently such losses are of a catastrophic nature and economic insurance cannot be made available to mitigate their effects.

2.7 Two other concepts which are closely related to event risks

2.7.1 Perils give rise to risks but are not risks in themselves. They can therefore be regarded as the source of loss. Typical examples of sources of losses are fires, explosions, earthquakes and storms.

2.7.2 The term "hazard"' relates to the environment surrounding the cause of loss. A container of flammable product, for example, produces a loss-causing environment which may give rise to a fire.

2.8 Trends Necessitating the Development of a Strategic Risk Management

The substantial costs of failure and the equally large benefits that accrue from a favourable risk-reward ratio highlight the importance of risk management in the enterprise. The need for a more integrated and holistic view of risk management is emphasised by the following trends that are changing the way enterprises create value:

2.8.1 Change

Barton *et al* (2002:3) outline that change today is no longer linear but exponential. The speed of change forces management in the New Economy to deal with a myriad of complex risks that have substantial consequences for their enterprises. Technology, the Internet, increased global supply chain competition, free trade and investment worldwide, complex financial instruments, deregulation of key industries, higher customer expectations, changes in organisational structures due to downsizing, re-engineering and mergers and more and larger mergers are but a few of the forces that create uncertainty in the New Economy. Collectively, these forces stimulate considerable change and create an increasingly risky and turbulent business environment. In his book, "The high risk society", Michael Mandel states: "Economic uncertainty is the price we must pay for growth." To be successful, enterprises must seek opportunities "where the forces of uncertainty and growth are the strongest''.

De Loach *et al* (2000:8) explain that the purpose of enterprise risk management is to make risk an active part of the business agenda with a balanced focus on the possible upside as well as downside effect of risk. Enterprises need to ensure that they are familiar with their greatest risks and opportunities in order to quickly adapt its strategies to capitalise on profitable growth opportunities and respond to competitive and other risks.

2.8.2 Globalisation

He furthermore said the disappearance of national boundaries and local market barriers results in intensified competition in terms of investors, customers, suppliers and even employees of enterprises. The explosive growth in international markets creates a multiple of market opportunities, some of which are short-lived and require enterprises to act quickly through streamlined risk taking and risk management processes.

Around-the-clock trading has resulted in many enterprises becoming increasingly internationally focused and taking on more exposures in different markets. This highlights the need to manage risks on an integrated rather than a regional basis. The increased volatility and interconnectivity of global markets have created a situation in which market and other events in one country or region affect markets in other parts of the world. The events on 11 September 2001 had a major effect on the stock market in USA as well as on other stock exchanges throughout the world. This growing interdependencies across markets, makes it necessary for enterprises to be able to assess the risk impact of interrelated market movements on their own portfolios of exposures.

2.8.3 Technology

Advances in information technology (IT) are powering the trend towards global operations. Information is more readily and rapidly available and is creating new alternatives and markets for employees, customers and investors to explore. Technology also enables enterprises' operations to grow in scope and assist with the transformation of business processes. Increased automation, extensive use of robotics and the discovery of new chemicals, treatments and processes, all spell potential new risks. Exponential change requires innovation and total solutions. Never-ending innovation gives rise to new risks that should be evaluated as soon as they occur without delay. The dangers of slipping behind and the rewards for getting ahead are apparent.

2.8.4 The increased value of intangible assets

Anderson *et al* 2001:26 said risk is on the rise as the boundaries of traditional business expand to include intangible ``new economy assets" or sources of value that are neither owned nor possible to be owned, such as knowledge, brands, relationships with employees, customers, suppliers, business partners and investors.

In the late 1970s, the book value of financial and physical assets on average equalled some 95 percent of market value. Today, it is 20 percent or less. The other 80 percent derives from intangible assets.

Increasing reliance on these assets that are not easily locked up or insured has made the value of enterprises more volatile and transformed the demands on risk management.

He furthermore outline that the increased concentration of risk resulting from extremely large buildings, manufacturing plants and organisations in general, causes individual values to change and potential liabilities to escalate dramatically. This compels enterprises to implement a proactive and integrated approach to risk management.

2.8.5 Increasingly accountable (and demanding) directors

Board of directors, CEOs and other senior executives are increasingly being held accountable for the creation, protection and enhancement of stakeholder value. Stakeholders increasingly want enterprises to identify and manage their business risks. More specifically, stakeholders want management to meet their earnings' goals. Risk management is a strategic tool that can increase profitability and smooth earning volatility, enhancing maximisation of shareholder wealth. In the past, directors were not directly involved in the day-to-day details of risk management because it was perceived as an operational management function. Perspective on risk management is changing, however, in response to the function's increasing capabilities in dealing with more strategic issues. In order to comply with these pressures, boards are searching for

more comprehensive, holistic techniques that give them greater confidence that their organisations are identifying, measuring, controlling and monitoring risk.

The emergence of new risk management tools and processes is an equally important driver for timely improvements in risk management and includes the following: Increasingly effective processes for risk identification.

New ways to identify risks associated with business activities are emerging. One of the most effective being ``risk-mapping'' which can be described as a process for identifying and prioritising risks so that improvement opportunities can be identified and appropriate risk management actions planned. The effective utilisation of risk management identification processes ensures the consistent and continuous identification of the full range of risk of the enterprise.

2.8.6 Increasingly effective measurement tools

Evolving tools such as RAROC (risk adjusted return on capital), ECAR (economic capital at risk) and VAR (value at risk) enable enterprises to ensure that returns are adequate for the risk undertaken and that capital is allocated optimally.

2.8.7 Increasingly effective information tools

Because of the development of computer technology and the Internet, information has become more readily available. Enterprises now have access to enterprise-wide resource planning systems such as those available from SAP or PeopleSoft and can source information worldwide.

2.8.8 Increasingly effective scenario analysis and planning

When considering the future, it is imperative for enterprises not to look at discrete forecasts but to consider the future as a range of possibilities. All possible outcomes should be considered,

identifying both potential risks and opportunities. This ``portfolio-based" view of the future is not only important for assessing business opportunities but also defines a value-added role for risk management. Identifying, understanding and managing the uncertainties an enterprise faces as it seeks to achieve its value creating objectives. All the aforementioned risk drivers and emerging risk management tools call for a new approach to assessing and managing risk. The ERM approach provides such a solution.

An introduction of information system Risk Management, May 31, 2006:10, SANS Institute 2007, outlined the following steps to be taken in IT Risk Management:

2.9 How Is Risk Managed?

Recall that the purpose of assessing risk is to assist management in determining where to direct resources. There are four basic strategies for managing risk: mitigation, transference, acceptance and avoidance. Each will be discussed below. For each risk in the risk assessment report, a risk management strategy must be devised that reduces the risk to an acceptable level for an acceptable cost. For each risk management strategy, the cost associated with the strategy and the basic steps for achieving the strategy (known as the Plan of Action & Milestones or POAM) must also be determined.

2.9.1 Mitigation

Mitigation is the most commonly considered risk management strategy. Mitigation involves fixing the flaw or providing some type of compensatory control to reduce the likelihood or impact associated with the flaw. A common mitigation for a technical security flaw is to install a patch provided by the vendor. Sometimes the process of determining mitigation strategies is called control analysis.

2.9.2 Transference

Transference is the process of allowing another party to accept the risk on your behalf. This is not widely done for IT systems but everyone does it all the time in their personal lives. Car,

health and life insurance are all ways to transfer risk. In these cases, risk is transferred from the individual to a pool of insurance holders, including the insurance company. Note that this does not decrease the likelihood or fix any flaws but it does reduce the overall impact (primarily financial) on the organisation.

2.9.3 Acceptance

Acceptance is the practice of simply allowing the system to operate with a known risk. Many low risks are simply accepted. Risks that have an extremely high cost to mitigate are also often accepted. Beware of high risks being accepted by management. Ensure that this strategy is in writing and accepted by the manager(s) making the decision. Often risks are accepted that should not have been accepted and then when the penetration occurs, the IT security personnel are held responsible. Typically, business managers, not IT security personnel, are the ones authorised to accept risk on behalf of an organisation.

2.9.4 Avoidance

Avoidance is the practice of removing the vulnerable aspect of the system or even the system itself. For instance, during a risk assessment, a website was uncovered that let vendors view their invoices, using a vendor ID embedded in the HTML file name as the identification and no authentication or authorisation per vendor. When notified about the web pages and the risk to the organisation, management decided to remove the web pages and provide vendor invoices via another mechanism. In this case, the risk was avoided by removing the vulnerable web pages.

2.9.5 Communicating Risks and Risk Management Strategies

Risk must also be communicated. Once risk is understood, risks and risk management strategies must be clearly communicated to organisational management in terms easily understandable to organisational management. Managers are used to managing risk, they do it every day. So presenting risk in a way that they will understand is key. Ensure you do not try to use "fear, uncertainty and doubt." Instead, present risk in terms of likelihood and impact. The more

concrete the terms are, the more likely organisational management will understand and accept the findings and recommendations.

With a quantitative risk assessment methodology, risk management decisions are typically based on comparing the costs of the risk against the costs of risk management strategy. A return on investment (ROI) analysis is a powerful tool to include in the risk assessment report. This is a tool commonly used in business to justify taking or not taking a certain action.

Managers are very familiar with using ROI to make decisions. With a qualitative risk assessment methodology, the task is somewhat more difficult. While the cost of the strategies is usually well known, the cost of not implementing the strategies is not, which is why a qualitative and not a quantitative risk assessment was performed. Including a management-friendly description of the impact and likelihood with each risk and risk management strategy is extremely effective. Another effective strategy is showing the residual risk that would be effective after the risk management strategy was enacted.

2.10 Risk mitigation options

The National Institute of standards and Technology July 2002 explains risk mitigation as a systematic methodology used by senior management to reduce mission risk. Risk mitigation can be achieved through any of the following risk mitigation options:

- **Risk Assumption.** To accept the potential risk and continue operating the NWPG IT system or to implement controls to lower the risk to an acceptable level.
- **Risk Avoidance.** To avoid the risk by eliminating the risk cause and/or consequence
- (eg, forgo certain functions of the system or shut down the system when risks are identified).
- **Risk Limitation.** To limit the risk by implementing controls that minimise the adverse impact of a threat's exercising vulnerability (eg, use of supporting, preventive, detective controls).

- **Risk Planning.** To manage risk by developing a risk mitigation plan and maintain controls.
- **Research and Acknowledgment.** To lower the risk of loss by acknowledging the vulnerability or flaw and researching controls to correct the vulnerability.
- **Risk Transference.** To transfer the risk by using other options to compensate for the loss, such as purchasing insurance. The goals and mission of an organisation should be considered in selecting any of these risk mitigation options. It may not be practical to address all identified risks, so priority should be given to the threat and vulnerability pairs that have the potential to cause significant mission impact or harm. Also, in safeguarding an organisation's mission and its NWPG IT systems because of each organisation's unique environment and objectives, the option used to mitigate the risk and the methods used to implement controls may vary. The "best of breed" approach is to use appropriate technologies from among the various vendor security products, along with the appropriate risk mitigation option and non technical, administrative measures.

2.11 Risk mitigation strategy

Senior management, the mission owners, knowing the potential risks and recommended controls, may ask, "When and under what circumstances should I take action? When shall I implement these controls to mitigate the risk and protect our organisation?"

2.12 Risk Mitigation Action Points

- This strategy is further articulated in the following rules of thumb, which provide guidance on actions to mitigate risks from intentional human threats:
- When vulnerability (or flaw, weakness) exists implement assurance techniques to reduce the likelihood of a vulnerability's being exercised;
- When vulnerability can be exercised apply layered protections, architectural designs and administrative controls to minimise the risk of or prevent this occurrence;
- When the attacker's cost is less than the potential gain apply protections to decrease an attacker's motivation by increasing the attacker's cost (eg, use of system controls such as

limiting what a system user can access and do can significantly reduce an attacker's gain);

- When loss is too great apply design principles, architectural designs and technical and non technical protections to limit the extent of the attack, thereby reducing the potential for loss.

2.13 Control categories

In implementing recommended controls to mitigate risk, an organisation should consider technical, management and operational security controls or a combination of such controls, to maximise the effectiveness of controls for their IT systems and organisation. Security controls, when used appropriately, can prevent, limit or deter threat-source damage to an organisation's mission.

The control recommendation process will involve choosing among a combination of technical, management and operational controls for improving the organisation's security posture. The trade-offs that an organisation will have to consider are illustrated by viewing the decisions involved in enforcing use of complex user passwords to minimise password guessing and cracking. In this case, a technical control requiring add-on security software may be more complex and expensive than a procedural control but the technical control is likely to be more effective because the enforcement is automated by the system.

On the other hand, a procedural control might be implemented simply by means of a memorandum to all concerned individuals and an amendment to the security guidelines for the organisation but ensuring that users consistently follow the memorandum and guideline will be difficult and will require security awareness training and user acceptance.

2.14 Technical Security Controls

Technical security controls for risk mitigation can be configured to protect against given types of threats. These controls may range from simple to complex measures and usually involve system architectures, engineering disciplines and security packages with a mix of hardware, software,

and firmware. All of these measures should work together to secure critical and sensitive data, information and IT system functions.

2.15 Supporting Technical Controls

Supporting controls are, by their very nature, pervasive and interrelated with many other controls. The supporting controls are as follows:

- Identification. This control provides the ability to uniquely identify users, processes and information resources. To implement other security controls (eg, discretionary access control [DAC], mandatory access control [MAC], accountability), it is essential that both subjects and objects be identifiable.
- Cryptographic Key Management. Cryptographic keys must be securely managed when cryptographic functions are implemented in various other controls. Cryptographic key management includes key generation, distribution, storage and maintenance.
- Security Administration. The security features of an IT system must be configured (eg, enabled or disabled) to meet the needs of a specific installation and to account for changes in the operational environment. System security can be built into operating system security or the application. Commercial off-the-shelf add-on security products are available. SP 800-30 Page 34
- System Protections. Underlying a system's various security functional capabilities is a base of confidence in the technical implementation. This represents the quality of the implementation from the perspective both of the design processes used and of the manner in which the implementation was accomplished. Some examples of system protections are residual information protection (also known as object reuse), least privilege (or "need to know"), process separation, modularity, layering and minimisation of what needs to be trusted.

The standard ISO/DIS 31000 "Risk management -- Principles and guidelines on implementation" states that once risks have been identified, they must then be assessed as to their potential severity of loss and to the probability of occurrence. These quantities can be either simple to

measure, in the case of the value of a lost building or impossible to know for sure in the case of the probability of an unlikely event occurring. Therefore, in the assessment process it is critical to make the best educated guesses possible in order to properly prioritise the implementation of the risk management plan.

The fundamental difficulty in risk assessment is determining the rate of occurrence since statistical information is not available on all kinds of past incidents. Furthermore, evaluating the severity of the consequences (impact) is often quite difficult for immaterial assets. Asset valuation is another question that needs to be addressed. Thus, best educated opinions and available statistics are the primary sources of information. Nevertheless, risk assessment should produce such information for the management of the organisation that the primary risks are easy to understand and that the risk management decisions may be prioritised. Thus, there have been several theories and attempts to quantify risks. Numerous different risk formulae exist but perhaps the most widely accepted formula for risk quantification is:

Risk = Rate of occurrence x The impact of the event.

Later research has shown that the financial benefits of risk management are less dependent on the formula used but are more dependent on the frequency and how risk assessment is performed.
In business it is imperative to be able to present the findings of risk assessments in financial terms. Robert Courtney Jr (IBM, 1970) proposed a formula for presenting risks in financial terms. The Courtney formula was accepted as the official risk analysis method for the US governmental agencies. The formula proposes calculation of ALE (annualised loss expectancy) and compares the expected loss value to the security control implementation costs (cost-benefit analysis).

2.16 Summary

In the quest for service excellence it is important to analyse every action in terms of how the government provides what the community or customer needs. It is believed that the devolution of power at appropriate levels can contribute greatly to improving service delivery levels. It will therefore be essential in the restructuring process to do the utmost to get away from old thinking

and not always base the new system on the old just for the sake of continuity. The government will have to be creative and imaginative to be effective. The structure established will have to be meaningful to the people they are meant to serve.

In view of the success that many organisations have achieved, it is certain that a great deal of what has been established in the past years will be retained and will indeed provide a sound and a solid foundation for the new generation structures or employers, the goal of restructuring is to provide a harmonious workplace where all workers are highly productive where if risk is identified it can be communicated and avoided before it even happens.

The chapter described the literature review and the following chapter which is chapter 3 presents research methodology and design.

CHAPTER 3

Research Methodologies and Design

3.1 Introduction

This chapter provides a variety of research methods and instruments used that will help to collect valid and reliable information from employees. In this chapter consideration will be a general practical orientation research parameters within which the data will be collected, research instruments as well as sampling design procedure for data collection and analysis. The primary aim of this study is to assess the relationship between the possesion of certain academic qualification and the degree of success with which these could be applied in any particular organisation to achieve its goal with reference to the Department of Finance. By means of an investigation based on the hypothesis of this study, it is stated to verify this hypothesis data that will be obtained. The evaluation of the report will be partly based on the investigation.

3.2 Meaning of Research

Reseach according to (Dane 1990:14), is a critical process for asking and attempting to answer questions that involve a questionair, an interview, an experiment and sometimes an entirely different method.

Kerlinger 1973 as quoted by (Dane 1990:4-5), indicates that it is a systematic controlled, emperical and critical investigation of hypothesis proportions about the presumed relationship among natural phenomena. As a process it is one of the tools used in pointing out the negative qualities of something and by examining all of its qualities, good, bad or indifferent.

3.3 Research Methodology

The reseach methodology presents the research design, the research environment, the research instrument, the data gathering procedure and the statical instrument. The researcher utilises the descriptive method of research in which questionnairs will be used to collect data to determine the variables that affect the IT as a Risk management tool in the Department of Finance.

3.4 Research Design

Brink and Wood (1998:100) state that the purpose of the research design is to provide a plan for answering the research question and is a "blue print action". It is the overall plan that spells out the strategies that the researcher uses to develop accurate objective and interprete information.

A quantitative, discriptive research design was chosen for this study in order to give a detailed description of IT as a risk management tool. The spcific questions addressed will generate knowledge, which will directly improve risk Management (Burns and Grove 1997:40).
According to Brink and Wood (1998:289), a discriptive survey design may be utilised to study characteristics in a population for the purpose of investigating probable solutions of a research problem.

The researcher actively tries to change the situation, circumstances or experience of participants, which may lead to a change in behaviour or outcomes for the participants of the study. Participants are ideally randomly assigned to different conditions and variables of interest are measured. The researcher tries to control the other variables in order to avoid confounds to causality. Therefore, experiments are often highly fixed even before the data collection starts.

In a good experimental design, a few things are of great importance. First of all, it is necessary to think of the best way to operationalise the variables that will be measured. Therefore, it is important to consider how the variables will be measured as well as which methods would be most appropriate to answer the research question. In addition, the statistical analysis has to be taken into account. Thus, the researcher should consider what the expectations of the study are as well as how to analyse this outcome. Finally, in an experimental design the researcher must think of the practical limitations including the availability of participants as well as how representative the participants are to the target population. It is important to consider each of these factors before beginning the experiment (Adèr *et al*, 2008).

3.5 Research Environment

The research study will be conducted at the Department of Finance, Information Technology directorate located at Garona Building, West Wing 1st Floor, IT Block.

3.6 Research Instrument

The researcher will be using a research made questionnaire, the questionnaire consists of number 1-5 as their choices, 1 means Strongly Disagree, 2 Disagree, 3 Neutral, 4 Agree, 5 Strongly Agree. The questionnaires will be distributed amongst the staff in NWPG IT. The first page is the letter to respondents; the second page contains part 1 which is the profile of the respondents, part 2 which is the area where the respondents were mostly exposed in his or her related working experience. Respondents are also encouraged to give any suggestion on what they think is important to empower their related working experience in the Department of Finance based on the respondents the researcher will be able to obtain sufficient answers based on the parameter given.

3.7 Target Population

The target population is the entire aggregation of respondents that meet the disignated set criteria (Burns and Grove 1997:236). The target population are the employees of NWPG IT in Finance Department. The total number of NWPG IT staff is 66 employees including those who are placed in the regions. The questionairs will be distributed only to 48 employees which constitutes 72% of the total Information Technology staff who are placed in head office in Garona building in Mmabatho. The questionnairs will be distributed to various sub directorates in NWPG IT which includes Management, Networking, Data Technolgy, Security and Help Desk.

3.8 Data Gathering

The researcher settled the study by making proposed problems that the researcher saw it with great importance to determine if IT is the management tool for risk management in the Department of Finance. The proposed problem was submitted to my research supervisor for the approval of a topic after which a letter of request was addressed to the director in IT asking for permission to allow the researcher to conduct a study.

After approval and obtaining the complete list of staff population, a Simple Random Sampling was utilised by the researcher for getting the sample wherein a researcher made a questionnaire that was formulated and subjected for corrections from experts. The researcher has located the respondents through the set of activity schedules in their offices. The researcher then will distribute questionnaires for the collection of data, after which the researcher had to collate and tally the gathered data. It was then interpreted with the use of statically tools tabulated, analysed and conclusion was drawn based from the result taken.

3.9 Informed Consent

Informed consent is a legal requirement before one can participate in a study (Brink *et al* 1998:200). After a full explanation of the nature of the study, participants were asked to give either a verbal consent for those who could not read or write or written consent of their willingness to participate in the study.

3.10 Summary

This chapter describes the research methodology and the ethical considerations. The following chapter, which is chapter 4, presents the data analysis and interpretation of findings.

CHAPTER 4

Data Analysis and Interpretation of Findings

4.1 Introduction

The methodology described in the previous chapter provided the baseline of data gathering in this chapter, the presentation of data is systematically linked to the format of the self developed questions attached in the appendix. The following will be used to analyse data, description of the sample, main results, discussion, presentation and interpretation of the results. This chapter will focus on the analysis and interpretation of data collected for this study.

According to De Vos *et al* (1998:203) data analysis entails that the analyst break down data into constituent parts to obtain answers to research questions and to test hypothesis. The analysis of research data does not in its own provide the answers to research questions. The purpose of interpreting data is to reduce it to an intelligible and interpretable form so that the relations of research problems can be studied and tested and conclusion drawn. On the other hand, when the researcher interprets the research result, he/she studies them for their meaning and implications.

sample, main results, discussion, presentation and interpretation of the results. This chapter will focus on the analysis and interpretation of data collected for this study.

4.2 Race

Table 4.2: Race of Respondents Distribution of sample

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	African	42	87.5	87.5	87.5
	Coloured	2	4.2	4.2	91.7
	Indian	1	2.1	2.1	93.8
	White	3	6.3	6.3	100.0
	Total	48	100.0	100.0	

Table 4.2 reflects race of the respondents and it indicates that africans are of higher precentage as compared to other races ,it is higher by 87.5% followed by 6.3% of whites, coloured are at 4.2% and indians being the lowest at 2.1%.

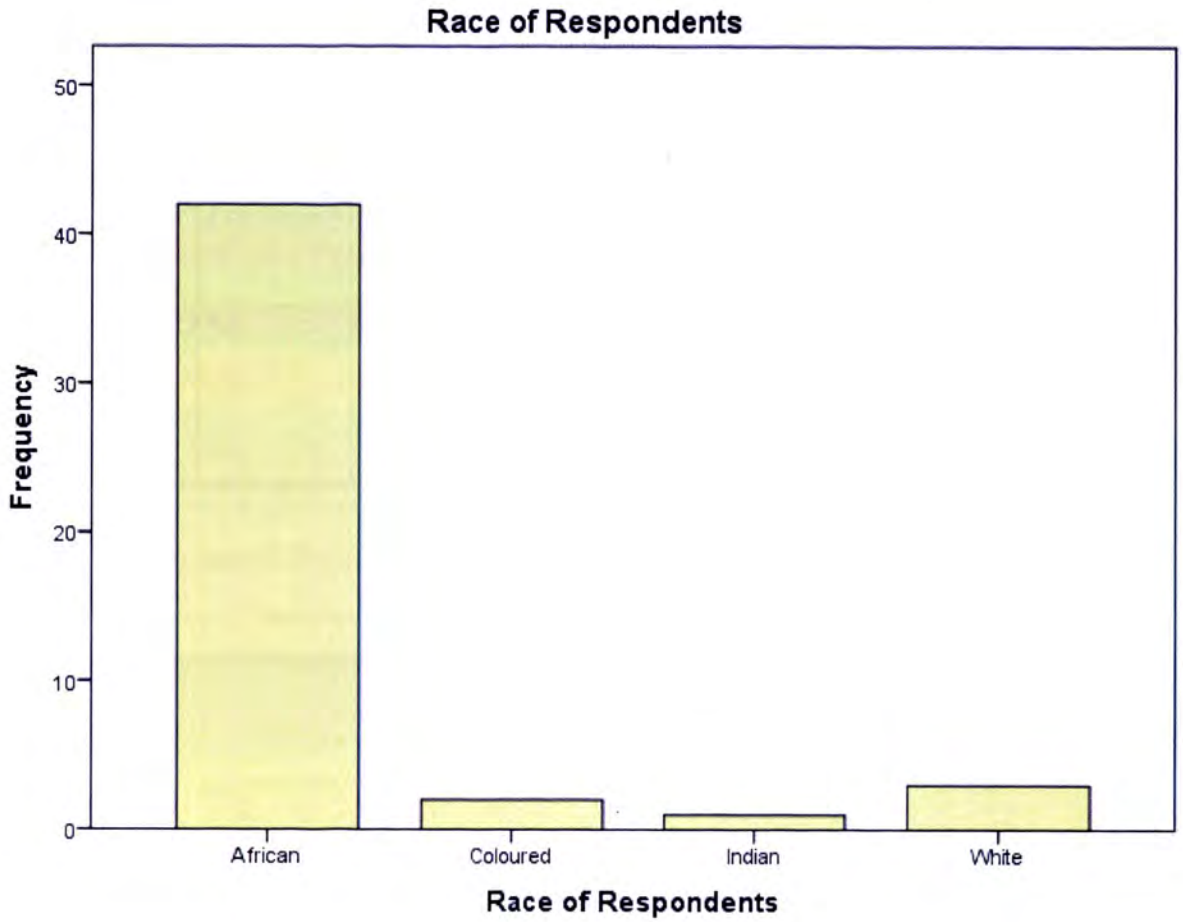

Figure 4.2 Race

According to Figure 4.2 above it is clear that in IT there are many Africans as compared to other races within the directorate. The graph shows 87% of Africans managed to respond to the questionnaires, 6.3 % were whites, 4.2% coloureds, 2.1% were Indians and all totaling to 100%.

4.3 Gender

Table 4.3: Gender of Respondents

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Male	30	62.5	62.5	62.5
	Female	18	37.5	37.5	100.0
	Total	48	100.0	100.0	

Table 4.3 shows that 62.5% of respondents are males and 37.5% are females.

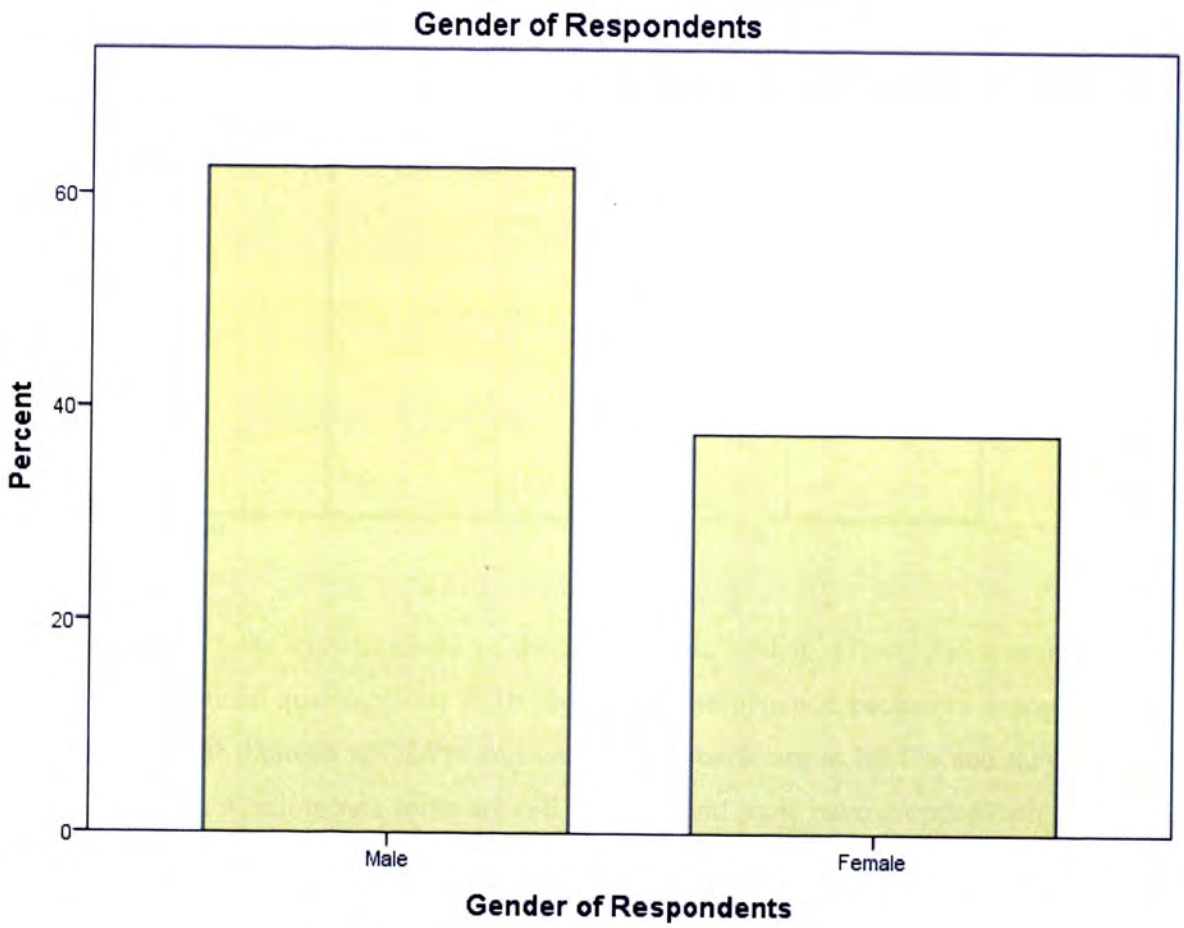

Figure 4.3: Gender of respondents

As per Figure 4.3 of gender respondents there are more males as compared to females in IT. The graph shows that there are 62.5% males and 37.5% females in IT who managed to respond to the questionnaires.

4.4 Qualifications

Table 4.4 : Qualifications of Respondents

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Post Graduate	5	10.4	10.6	10.6
	Bachelor Degree	8	16.7	17.0	27.7
	National Diploma	13	27.1	27.7	55.3
	Matric	21	43.8	44.7	100.0
	Total	47	97.9	100.0	
Missing	System	1	2.1		
Total		48	100.0		

Table 4.4 indicates the qualifications of the respondents, and it reflects the respondents who obtained post graduate qualifications at 10.6%, those who obtained bachelors degree at 17.0%, those with national diploma at 27.7% and those with matric are at 44.7% and they are at the highest percentage which means some are still studying and some have dropped their studies due to non financial assistance scheme like bursary in the department.

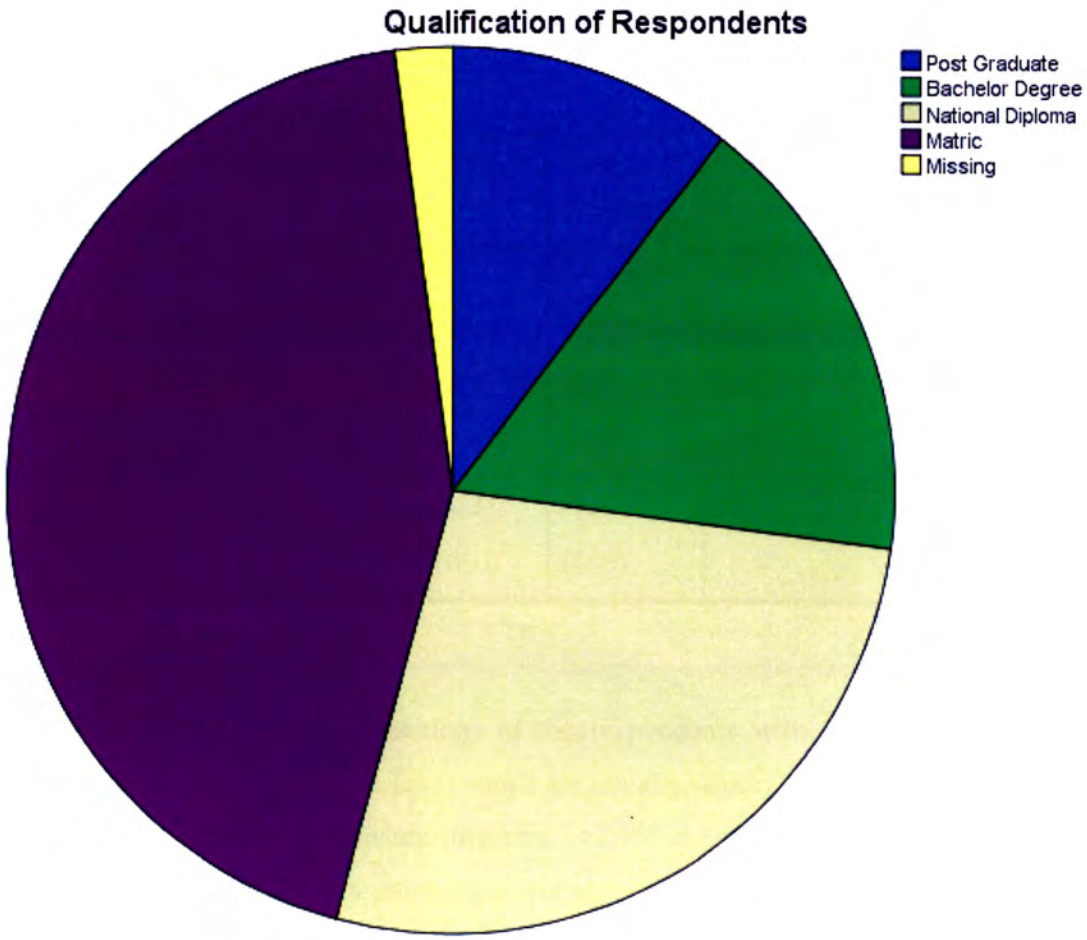

Figure 4.4 Qualifications

Figure 4.4 indicates the qualifications of respondents and with data gathered from the Table 4.4, it shows that there are 10.6% of staff that responded have post- graduate degrees,16.7% of staff have a bachelor's degree, 27.7% have a national diploma and 43.8% have a matric and the missing are those who have been given a questionnaire and did not return and that is only 2.1% as shown on the frequency table.

4.5 Job Function

Table 4.5 : Job Function

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Director	1	2.1	2.1	2.1
	Manager	2	4.2	4.2	6.3
	Supervisor	7	14.6	14.6	20.8
	Technical	23	47.9	47.9	68.8
	Other	15	31.3	31.3	100.0
	Total	48	100.0	100.0	

Table 4.5 indicates the job functions of the respondents with 2.1% of respondents being at director level,4.2% at manager level which are usually deputy dirctors and 14.6% at supervisory level and they are mostly assistant directors , 47.9% at technical level and other being at 31.3% and this represent the drivers ,messenger and secretaries in the directorate.

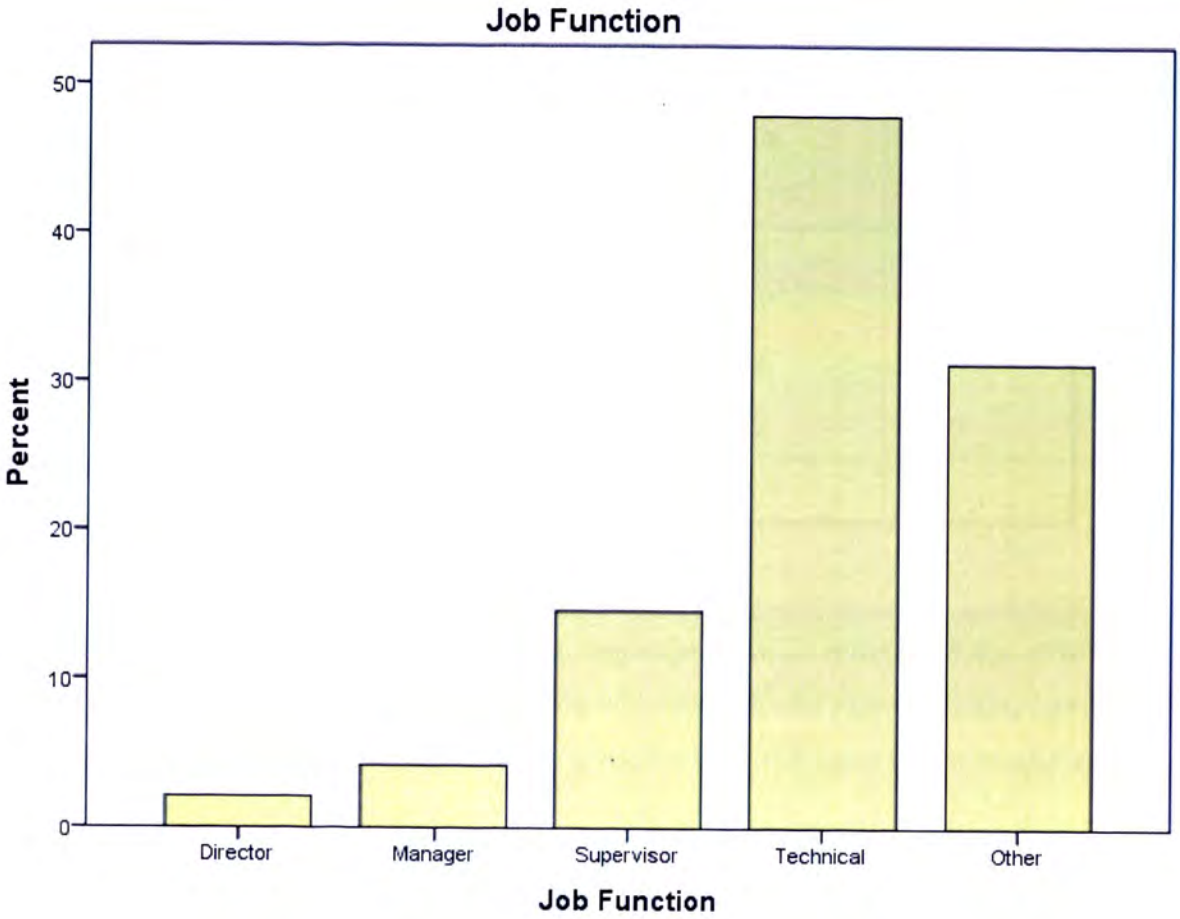

Figure 4.5: Job Fuction

According to Figure 4.5 of the job function there is a clear indication that 2.1% directors who are doing the functions of director and 4.2% of staff who are managers, 14.6% supervisors, 47.9% of staff who responded and are at technical level and 31.3% who fall in the category of other and those include the secretaries, drivers and messengers.

4.6 Work Experience

Table 4.6 : Work experience

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1.00	10	20.8	20.8	20.8
	2.00	17	35.4	35.4	56.3
	3.00	10	20.8	20.8	77.1
	4.00	11	22.9	22.9	100.0
	Total	48	100.0	100.0	

Table 4.6 reflects the work expirience of the respondents which reflects 35.4% of 6-10 years working experience, and 22.9% of respondents who have 16 and above working experience, 20.8 of respondents are at 11-15 years work experience and 20.8 again on those who are at 1-5 years of working expirience.

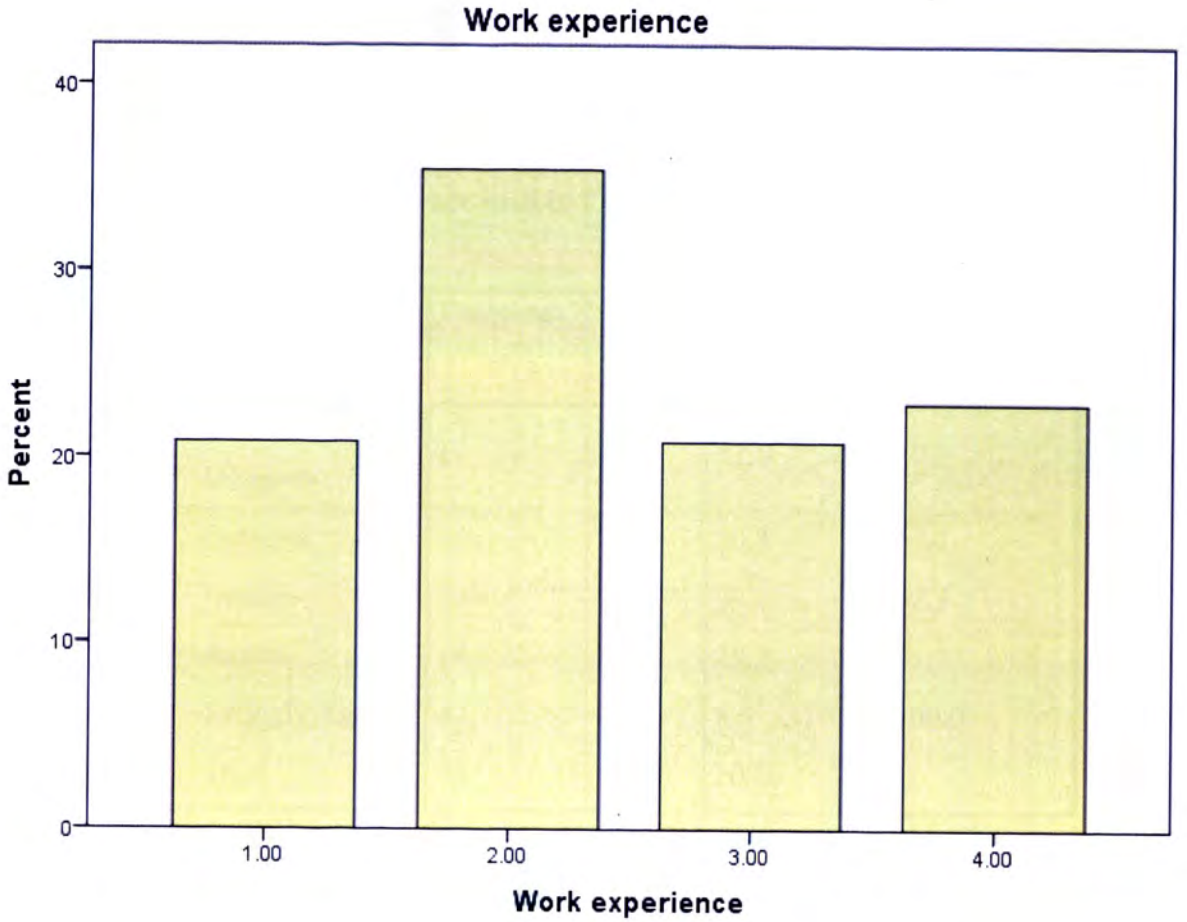

Figure 4.6: Work Experience

According to Figure 4.6 of the work experience of the respondents and the percentages shown on Table 4.7 we have 20.8% on the grouping of 1-5 and 35.4% of those who falls between 6-10 and 20.8% again of those who fall between 11-15 and 22.9% who are at 16 and above.

4.7 The role of IT portfolio in the department

4.7.1 Application and software used in IT

Table 4.7: Applications and software used in IT

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	6	12.5	12.5	12.5
	Disagree	10	20.8	20.8	33.3
	Neutral	14	29.2	29.2	62.5
	Agree	14	29.2	29.2	91.7
	Strongly Agree	4	8.3	8.3	100.0
	Total	48	100.0	100.0	

Table 4.7 reflects application software used in IT and if those applications and software have current licences,29.2% being the highest percentage strongly agree that there are current licences,12.5% strongly disagree, 29.2% are neutral again and 8.3% strongly agree.

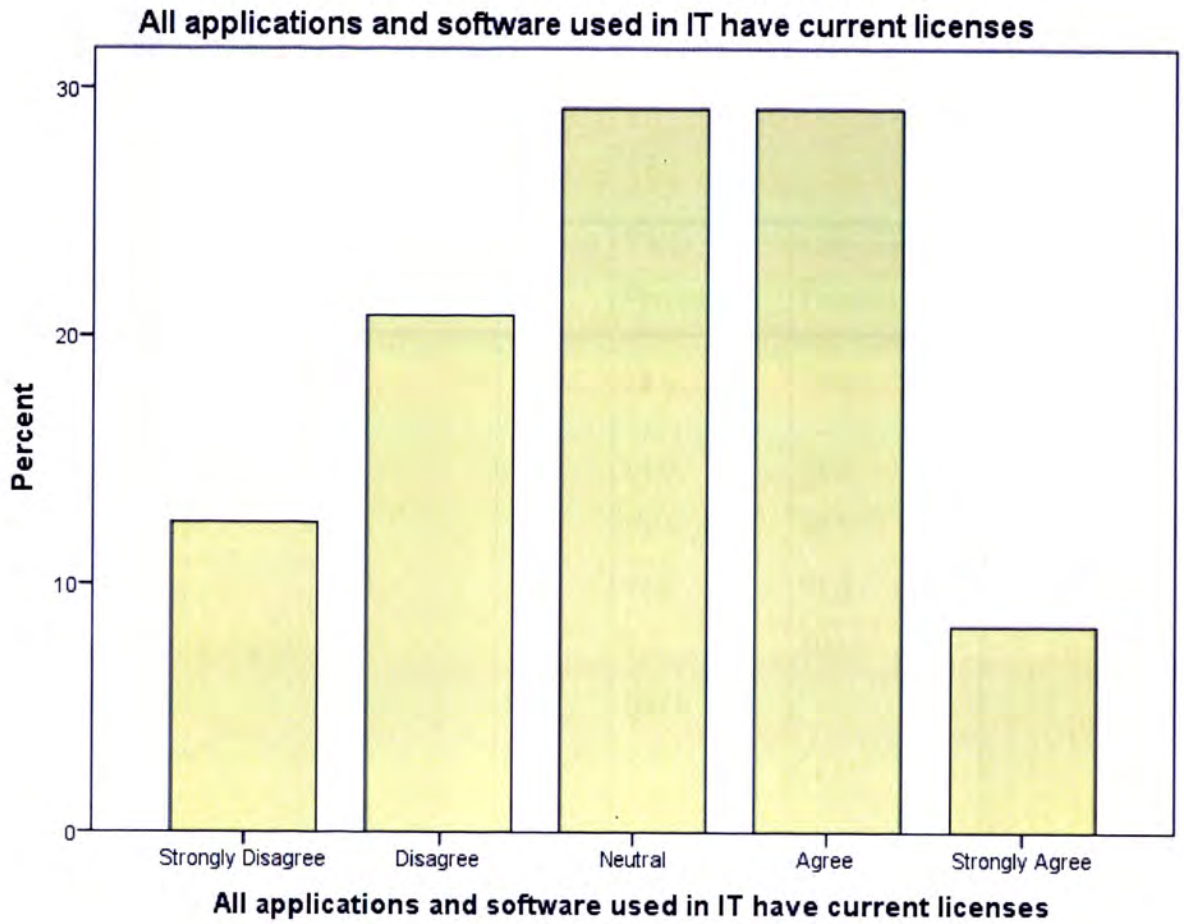

Figure 4.7 Application and software used in IT

As per Figure 4.7 there are respondents who agree, strongly disagree, be neutral, disagree and who strongly disagree that all the applications and software in IT have current licenses but the rating is not the same according to the frequency table. From the frequency table 4.9, the number of the respondents who are neutral and who agree are equal with the percentage of 29.2% and is the highest and the percentage of those who strongly agree is 8.3% and those who strongly disagree is 4%. But the overall observation indicates that the majority of the respondents agree that the current software and applications have current licences.

4.8 Production servers

Table 4.8: Production server

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	5	10.4	10.6	10.6
	Disagree	7	14.6	14.9	25.5
	Neutral	11	22.9	23.4	48.9
	Agree	20	41.7	42.6	91.5
	Strongly Agree	4	8.3	8.5	100.0
	Total	47	97.9	100.0	
Missing	System	1	2.1		
Total		48	100.0		

Table 4.8 reflects production servers, it is the indication of if production servers, appliactions and supporting software are physically located in the data center. The respondents have responded in the following onder, 41.7% agree,22.9% are neutral,14.6% disagree,10.4% strongly disagree, 8.3% agree.

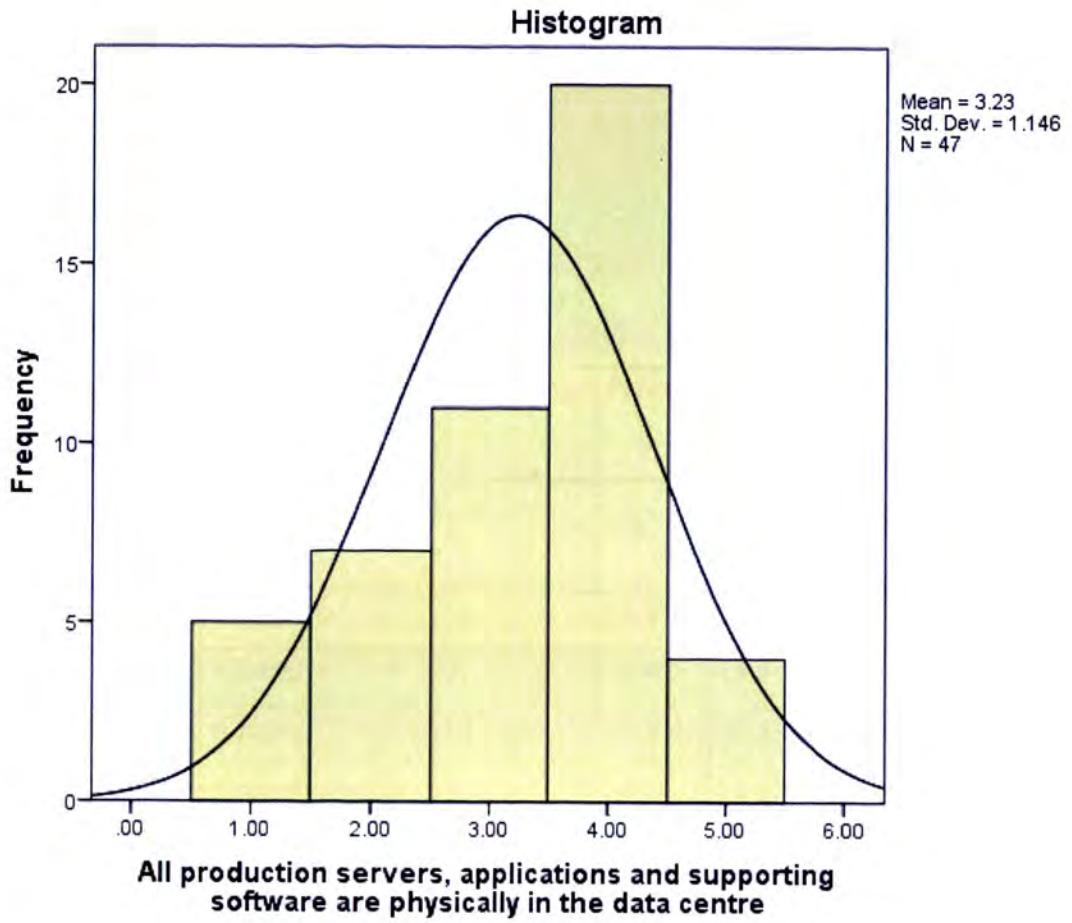

Figure 4.8 All production servers, applications and supporting software are physically in the data centre

According to Figure 4.8 the data indicates the value of the mean being equal to 3.23% and the standard deviation of 1.146% with the total number of respondents amounting to 47 and there was one answer missing from the respondent. As per Table 4.8 we can see how the respondents have responded to whether all the application and supporting software are physically in the data center and the highest percentage is of those respondents who agree with 41.7% and they are followed by those who are neutral with 22.9% and being neutral give a clear picture of the respondents are in between, they are actually not sure. The total percentage of those who disagree are 14.6% and those who strongly disagree are equal to 8.3%. You may find that the lowest groups of those who strongly disagree are that staffs who are technical or who are on

management because they work directly with the servers, applications and supporting software while managers manage them.

4.9 Contacts in case of emergency

Table 4.9: Contacts in case of Emergency

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	3	6.3	6.3	6.3
	Disagree	11	22.9	22.9	29.2
	Neutral	9	18.8	18.8	47.9
	Agree	18	37.5	37.5	85.4
	Strongly Agree	7	14.6	14.6	100.0
	Total	48	100.0	100.0	

Table 4.9 is the reflection of wether the respondents know what to do ,whom to contact in case of fire, accident, and inappropriate physiacl access. The respondents have responded in the following order, 37.5% of respondents agree, 22.9% disagree,18.8% of the respondents are neutral, 14.6 strongly agree and 6.3 strongly disagree.

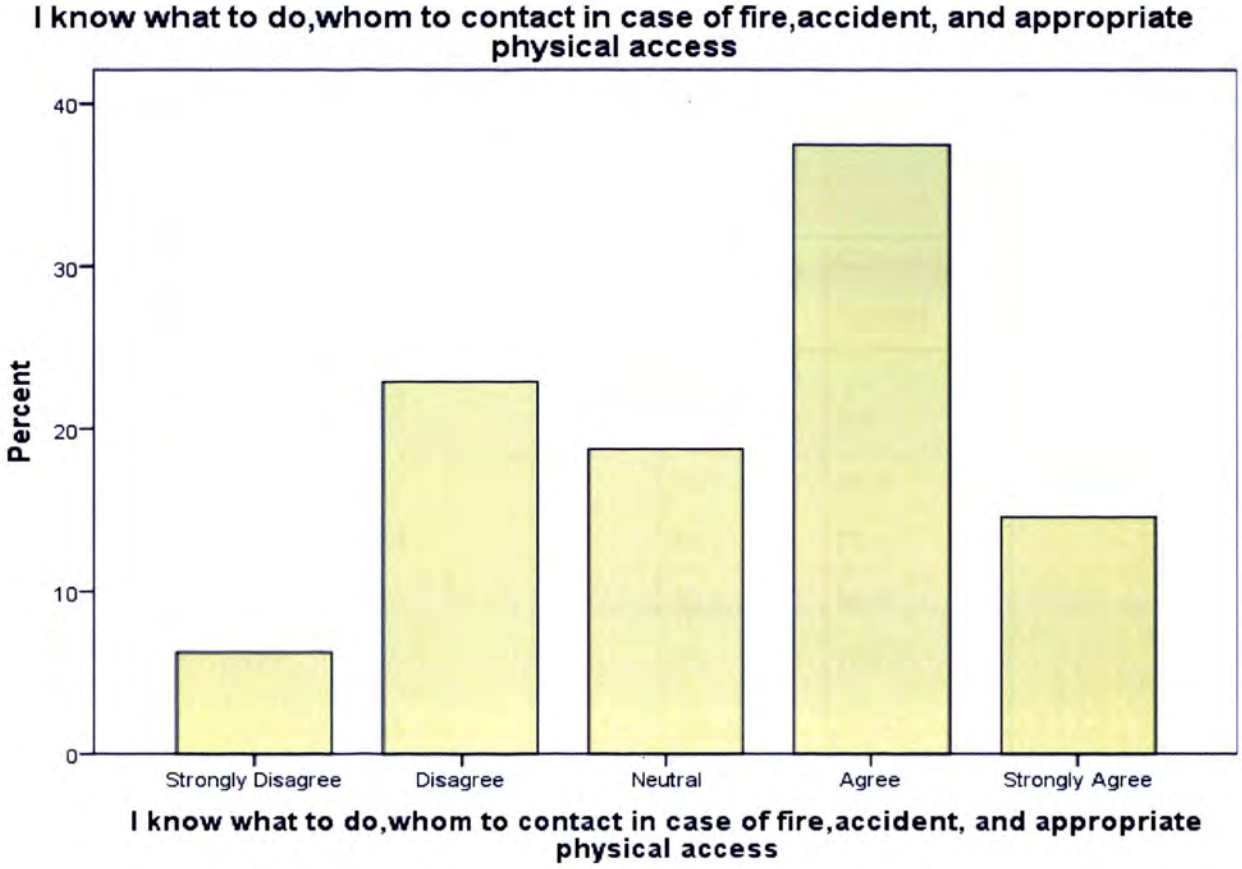

Figure 4.9 reflects who to contact in case of fire,accident,and appropriate physical access

According to Figure 4.9 it is clear that the majority of the respondents agree that they know who to contact in case of fire. During an accident it is revealed on Table 4.9 that the percentage of those who agree are 37.5% followed by 22.9% of those who disagree and 18.8 % of those who are neutral, 14.6% of those who strongly agree 6.3% of those who strongly disagree.

4.10 Success of IT management

4.10.1 Communication Process

Table 4.10: Communication Process

		Frequency	Percent	Valid Percent	Cumulative Percent
Value	Strongly Disagree	12	25.0	25.0	5.0
	Disagree	11	22.9	22.9	47.9
	Neutral	14	29.2	29.2	77.1
	Agree	10	20.8	20.8	97.9
	Strongly Agree	1	2.1	2.1	100.0
	Total	48	100.0	100.0	

Table 4.10 indicates if whether there is a process to communicate new policies and procedures to the staff and if training is provided when needed.The respondents have responded in the following order,29.9% disagree,29.2% are neutral, 25% strongly disagree, 20.8% agree and only 2.1% strongly disagree.

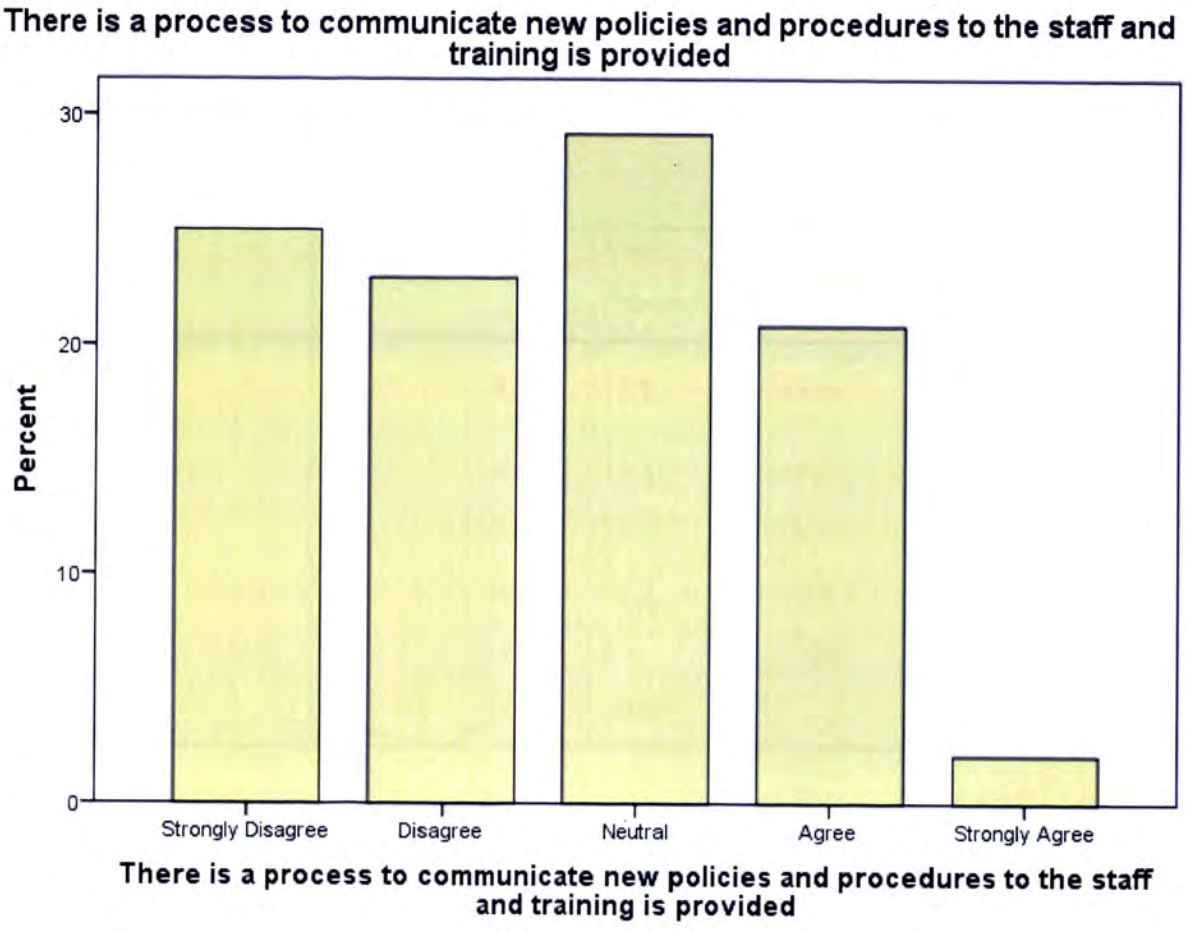

Figure 4.10 Communication of new policies

Figure 4.10 indicates that the highest number of respondents are neutral with the percentage of 29.2 with the percentage data taken from the frequency table, in their response that indicate that there are processes to communicate new policies and procedures to the staff and training is provided, they are followed by those who strongly disagree with the percentage of 25.0 and that gives the clear indication that if there are those processes that might only be known by managers and directors and they don't communicate them because that is also followed by the respondents who disagree with the percentage of 22.9 and those who agree is 20.8% followed by those who strongly agree with 2.1%.

4.11 The legal, regulatory and policy requirement.

Table 4.11: Legal, Regulatory and Policy requirement

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	9	18.8	18.8	18.8
	Disagree	6	12.5	12.5	31.3
	Neutral	18	37.5	37.5	68.8
	Agree	14	29.2	29.2	97.9
	Strongly Agree	1	2.1	2.1	100.0
	Total	48	100.0	100.0	

Table 4.11 reflects the legal,regulatory and policy requirement relative to the delivery of automated servicein IT. The respondents have responded in the following order,37.5% are neutral,29.2% agree, 18.8% strongly disagree, 12.5% disagree and only 2.1% strongly agree.

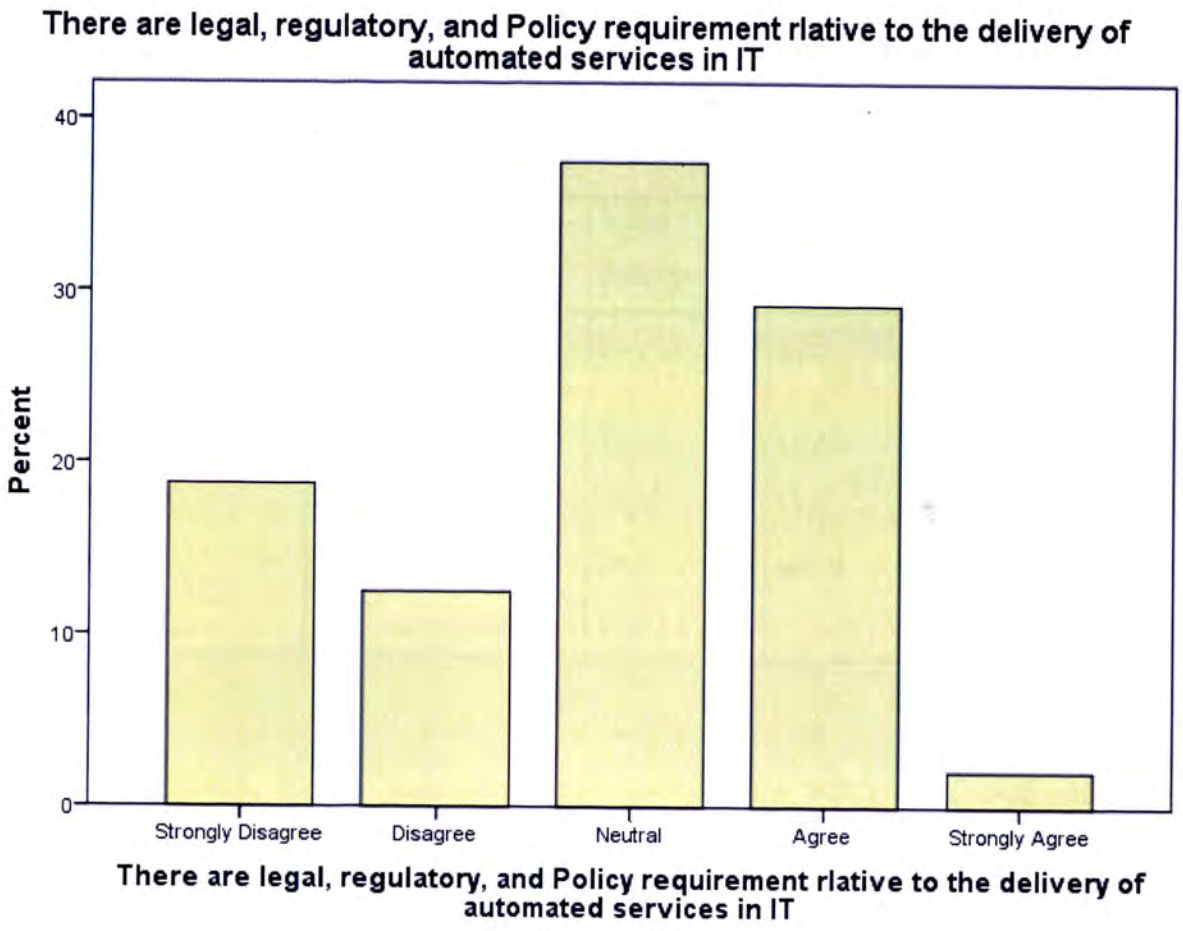

Figure 4.11 The legal, regulatory and policy requirement.

According to Figure 4.11 most of the respondents are not sure and Table 4.11 shows the percentage of 37.5 which is the highest and those respondents who are neutral and they are followed by those who agree with the percentage of 29.2 and 18.8 of those who strongly disagree and that might be because of lack of communication and training when new policies are implemented as indicated in graph 4.16 that, 12.5% of those who disagree and 2.1% of those who strongly agree.

4.12 Demonstration of compliance with applicable standards

Table 4.12: Compliance and Applicable standards.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	13	27.1	27.1	27.1
	Disagree	6	12.5	12.5	39.6
	Neutral	17	35.4	35.4	75.0
	Agree	12	25.0	25.0	100.0
	Total	48	100.0	100.0	

Table 4.12 reflects if the respondents can demonstarte compliance with applicable standards,Legal and regulatory requirements implemented in IT. The table shows the following results,35.4% of the repondents who are neutral, 27.1% strongly disagree, 25% agree and 12.5% disagree.

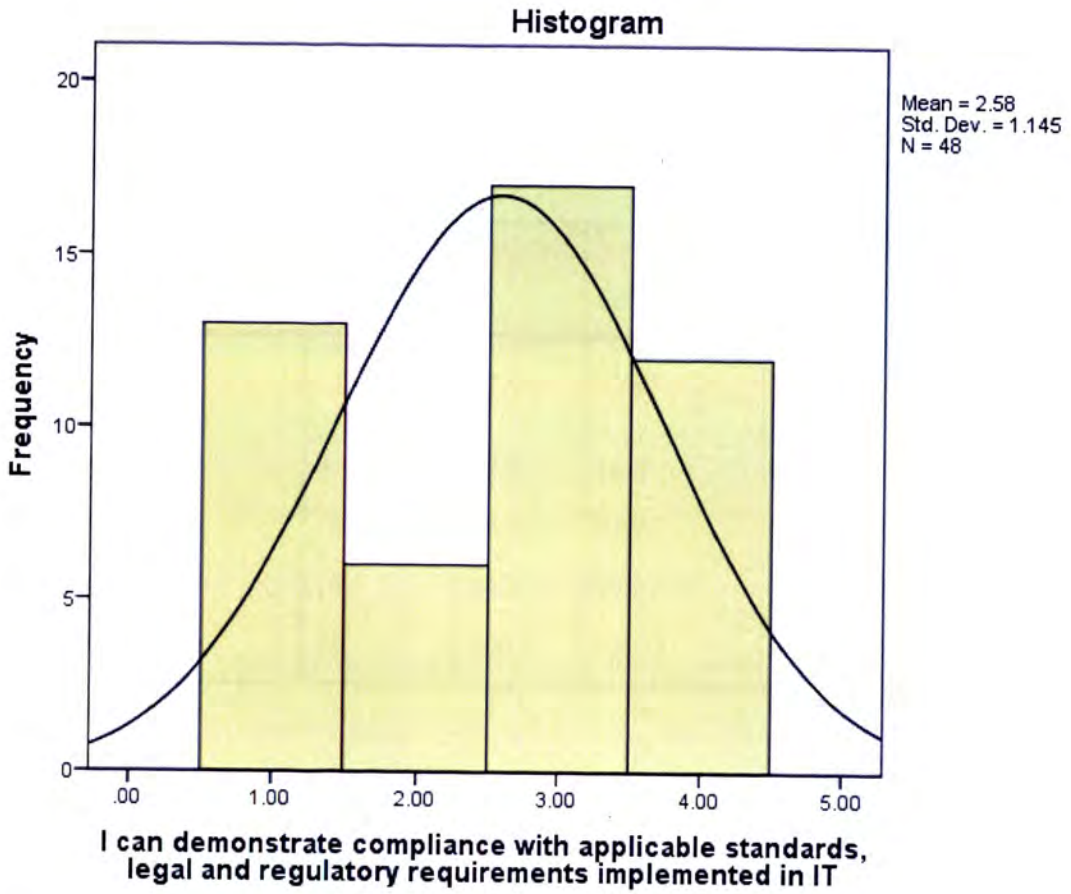

Figure 4.12 Demonstration of compliance with applicable standards

The data on Figure 4.12 shows the mean of 2.58% and the standard deviation of 1.145% with a total number of respondents of 48. Our data is normal distributed, hence the graph 4.20 shows 35.4% of the respondents who are neutral can demonstrate compliance with applicable standards legal and regulatory requirements implemented in IT, followed by 27.1% who strongly disagree with that statement and 25.0% agree while 12.5 disagree.

4.13 IT planning process designed.

Table 4.13 : IT planning process

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	11	22.9	22.9	22.9
	Disagree	9	18.8	18.8	41.7
	Neutral	14	29.2	29.2	70.8
	Agree	14	29.2	29.2	100.0
	Total	48	100.0	100.0	

Table 4.13 shows that there is an IT planning process that are designed by management that are adequately includes operational resources to support the automated line business and 29.2% of respondents are neutal,29.2% agree,18.8%disagree and 22.9% strongly disagree.

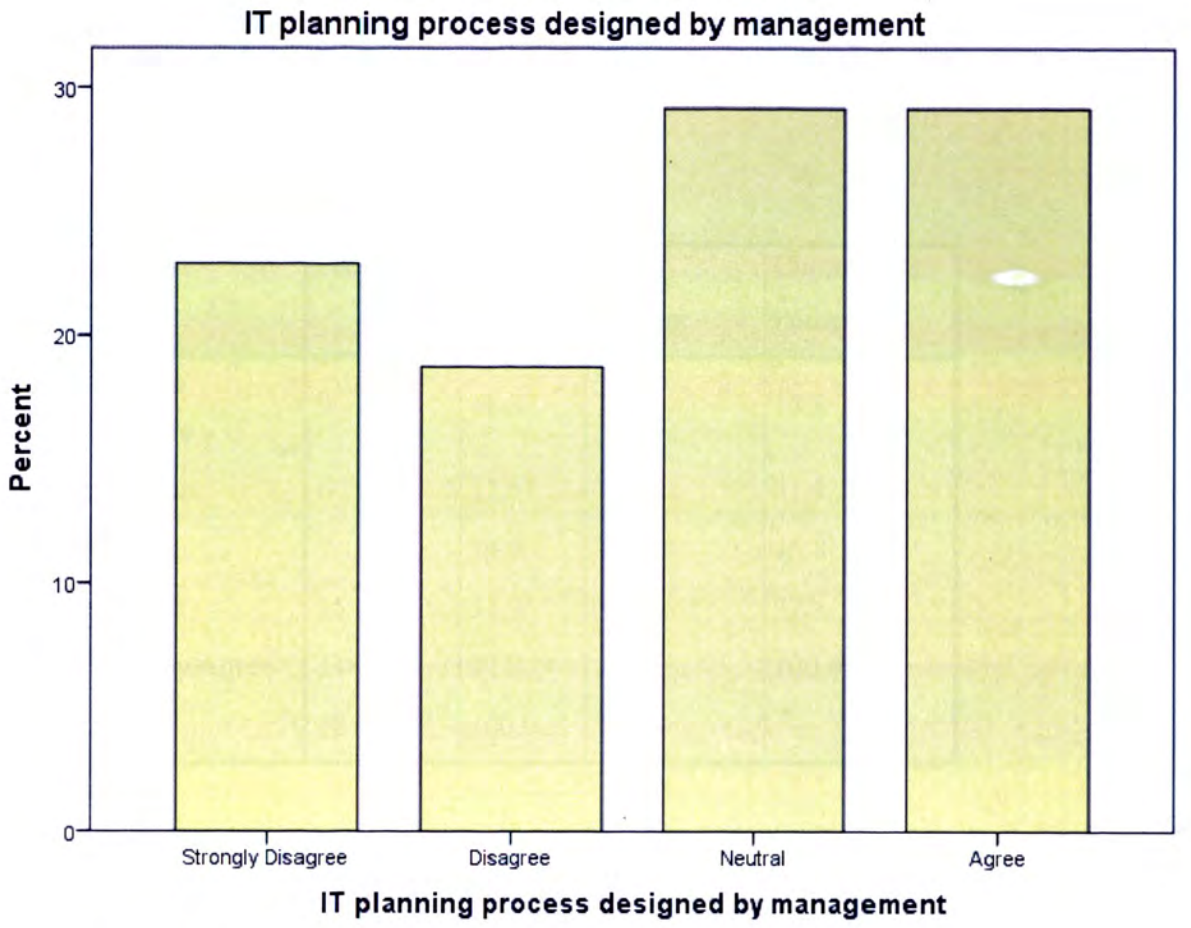

Figure 4.13 IT planning process designed.

Figure 4.13 shows that the respondents who are neutral and those who agree are equal with the percentage of 29.2 respectively followed by those who strongly disagree with 22.9% and the percentage of those who disagree is 18.8%.

4.14 Intervention that can be applied by IT management

4.14.1 Backup strategy

Table 4.14: Backup strategy

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	9	18.8	18.8	18.8
	Disagree	6	12.5	12.5	31.3
	Neutral	7	14.6	14.6	45.8
	Agree	15	31.3	31.3	77.1
	Strongly Agree	11	22.9	22.9	100.0
	Total	48	100.0	100.0	

Table 4.14 indicates if there are backup startegies developed for continuity of automated services should the department have an IT system failure. 31.3% of the respondents agree,22.9% strongly agree, 18.8% strongly disagree, 14.6% are neutral, 12.5% disagree.

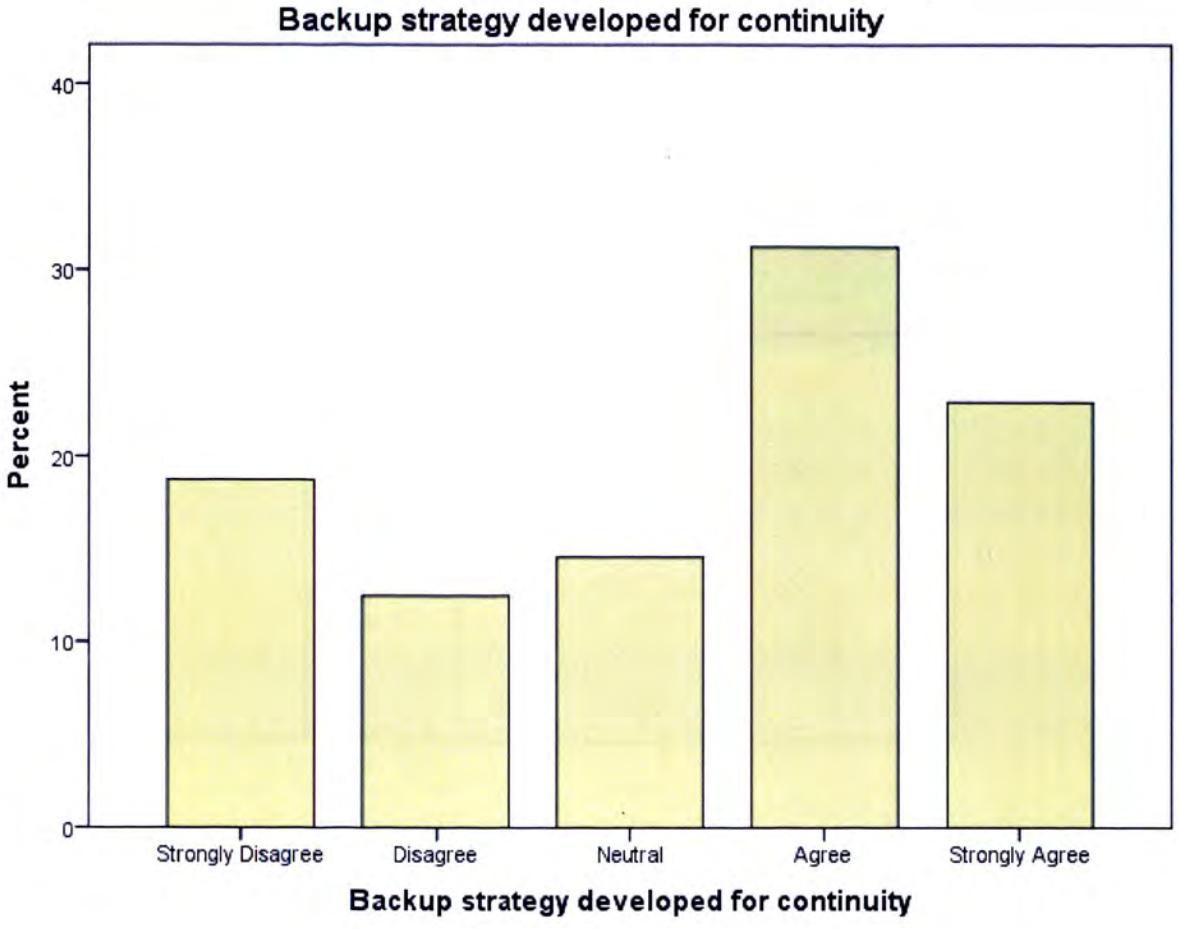

Figure 4.14 Backup strategy

According to Figure 4.14 the highest graph of 31.3% has also indicated in Table 4.14 that the respondents who agree that there is a backup strategy developed for continuity of automated services, should the department have IT system failure and that is followed by 22.9% of the respondents who strongly agree. This is followed by 18.8% of those who strongly disagree and 14.6% of those who are neutral and 12.5% of those who agree and that shows that the majority of the respondents are aware that there is a backup strategy developed. It is just that communication is poor according to the observation of the respondents.

4.15 IT system failure

Table 4.15: Results in case of IT system failure.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	7	14.6	14.6	14.6
	Disagree	2	4.2	4.2	18.8
	Neutral	3	6.3	6.3	25.0
	Agree	20	41.7	41.7	66.7
	Strongly Agree	16	33.3	33.3	100.0
	Total	48	100.0	100.0	

Table 4.15 indicates if an IT system failure result in a newsworthy event,Wide spread will be communicated to the users via global e-mail by IT personnel. 41.7% agree,33.3% strongly agree, 14.6% strongly disagree,6.3% are neural and 4.2% of the respondents strongly disagree.

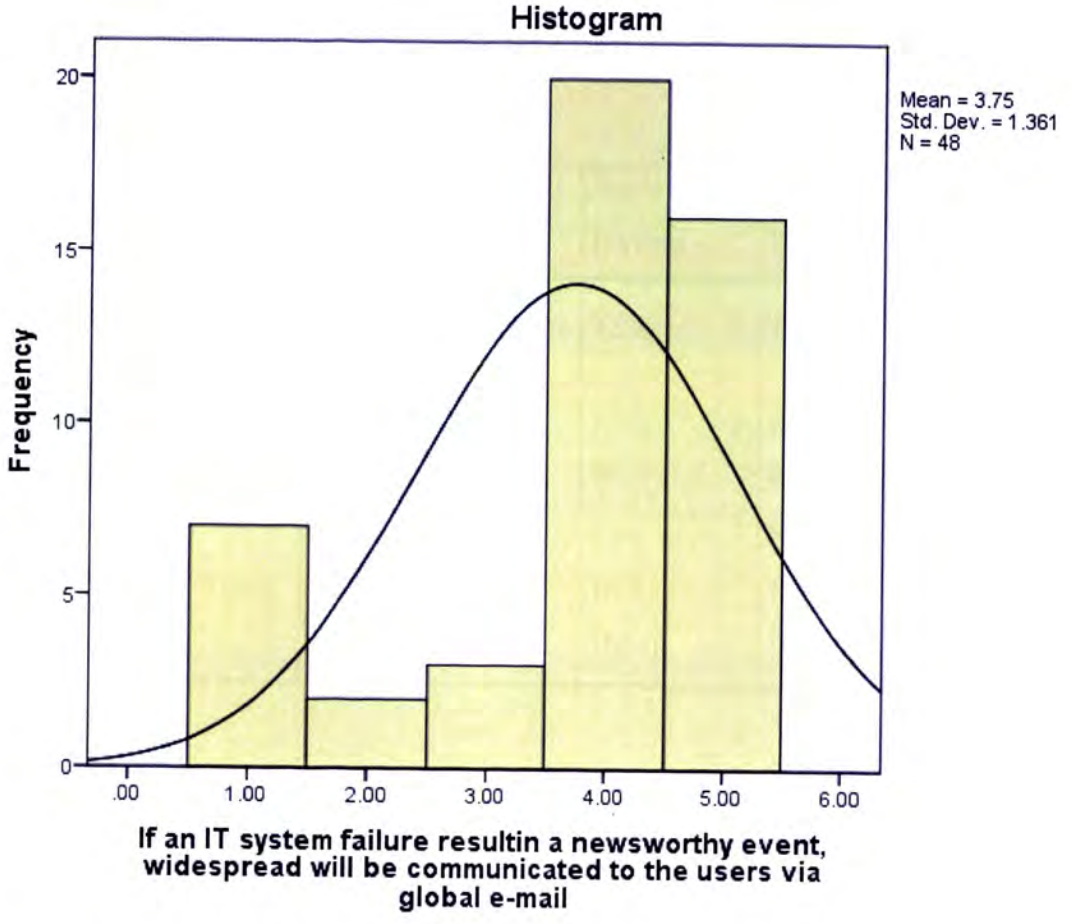

Figure 4.15 IT system failure

The data on the Figure 4.15 shows the value of the mean of 3.75% and the standard deviation value of 1.361% with a total number of 48 respondents and the graph is skewed to the right hence the Table 4.16 shows that the numbers of respondents who agree are at a very high level with 41.7%, followed by 33.3% who strongly agree and 14.6% who strongly disagree and 6.3% of those who are neutral with 4.2% of those who disagree and you may find that those few respondents who strongly disagree are those who do not have access to e-mails as this widespread is communicated via electronically.

4.16 Secured Infrastructure

Table 4.16: Secured infrastructure

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	6	12.5	12.5	12.5
	Disagree	5	10.4	10.4	22.9
	Neutral	6	12.5	12.5	35.4
	Agree	22	45.8	45.8	81.3
	Strongly Agree	9	18.8	18.8	100.0
	Total	48	100.0	100.0	

Table 4.16 shows that there are infrastructure (password,PC,Firewalls,Network policies,Procedures and hardware,Software) that are protect the information asserts(data integrity,confidentiality,availability) been developed,Implemented and communicated.45.8% of the respondents agree,18.8% strongly agree,12.5% are neutral,12.5% strongly disagree and 10.4% disagree.

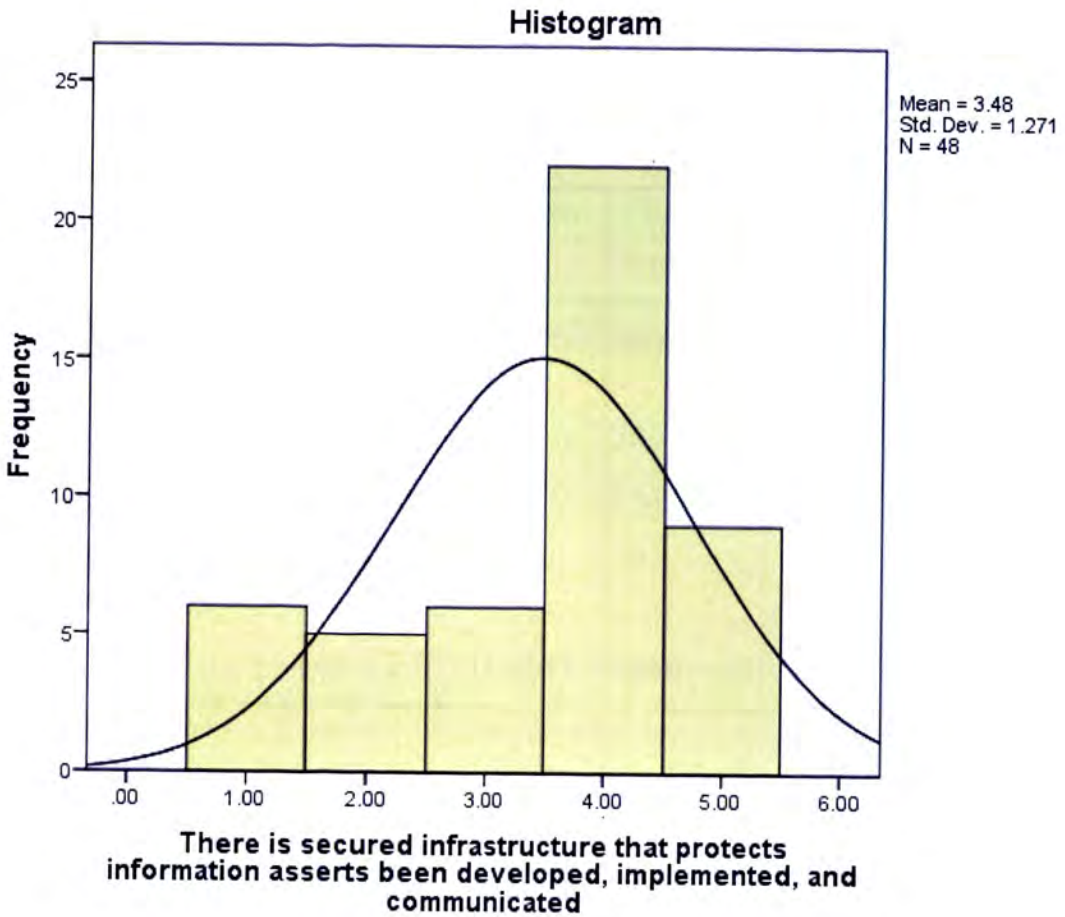

Figure 4.16 Secured Infrastructure

According to Figure 4.16 the data on the graph shows the mean value of 3.48% and the standard deviation value of 1.271% with the total of 48 respondents hence the frequency table 4.27% shows that 45.8% of the respondents who agree that there is secured infrastructure that protects information asserts been developed, implemented and communicated 18.8% of respondents strongly agree while 12.5% of those who are neutral are equal to those who strongly disagree and 10.4% disagree to that statement. The majority of the respondents agree so we can say that the few who fall below neutral might be lacking training or need a workshop.

4.17 IT management staff

Table 4.17: IT management staff

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	10	20.8	20.8	20.8
	Disagree	6	12.5	12.5	33.3
	Neutral	7	14.6	14.6	47.9
	Agree	14	29.2	29.2	77.1
	Strongly Agree	11	22.9	22.9	100.0
	Total	48	100.0	100.0	

Table 4.17 indicates if the IT management staff are considered directly resposible and accounatble if elements within the automated system failed. 29.2% agree, 22.9% strongly agree, 20.8% strongly disagree, 14.6% are neutral and 12.5% disagree.

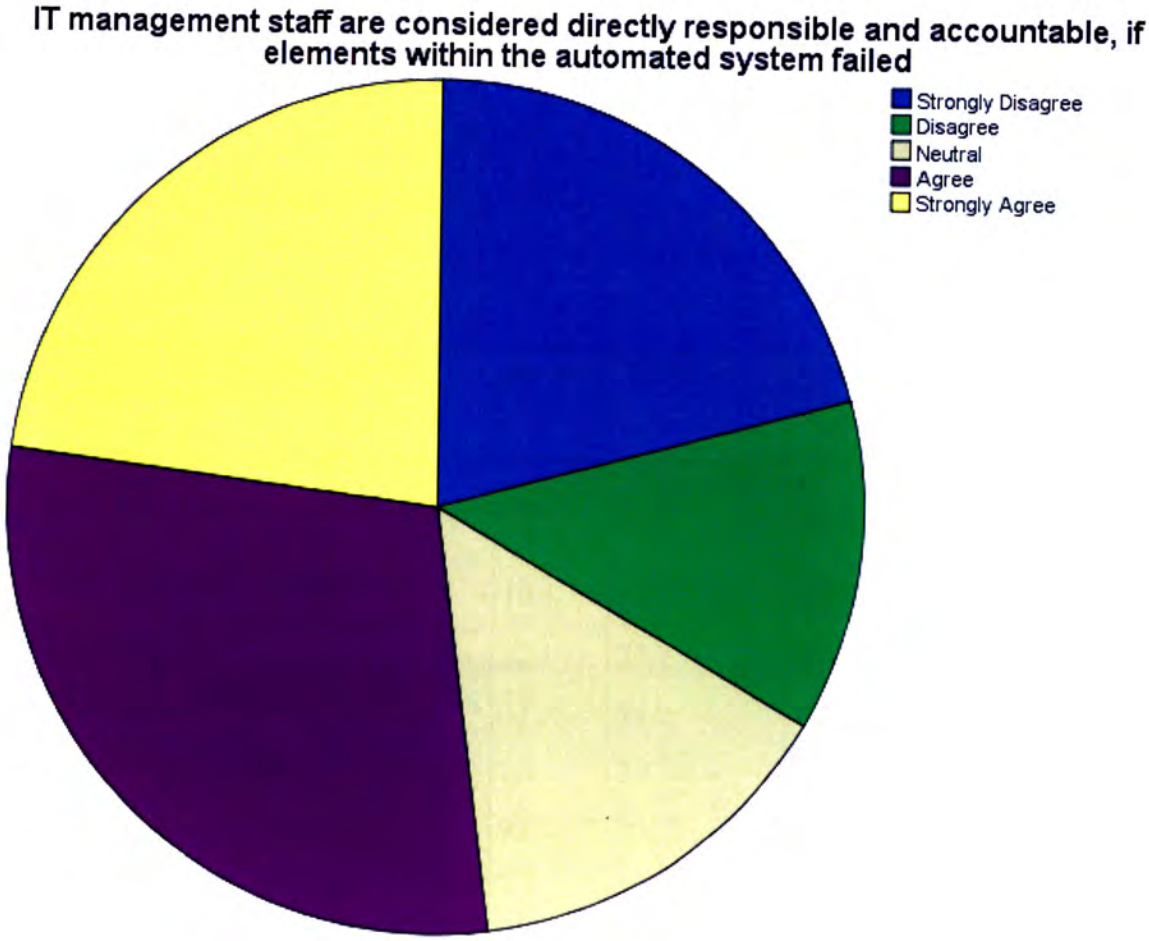

Figure 4.17 IT management staff

As per Figure 4.17 the chart shows a large number of respondents who agree that IT management staff are considered directly responsible and accountable, if elements within the automated system failed, the percentage of those who agree is 29.2 followed by those who strongly agree with 22.9% and 20.8% of the respondents strongly disagree and 14.6% is neutral with 12.5% of those who disagree.

4.18. The characteristics of IT managers.

4.18.1 Risk including IT risks

Table 4.18: Risk, including IT risks

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	12	25.0	25.5	25.5
	Disagree	5	10.4	10.6	36.2
	Neutral	13	27.1	27.7	63.8
	Agree	16	33.3	34.0	97.9
	Strongly Agree	1	2.1	2.1	100.0
	Total	47	97.9	100.0	
Missing	System	1	2.1		
Total		48	100.0		

Table 4.18 reflects the risk including IT risk, and if they are communicated by management in terms of their impact on business.34% agree, 27.7% neutral,25.5% strogly disagree, 10.6% disagree while 2.1% strongly disagree.

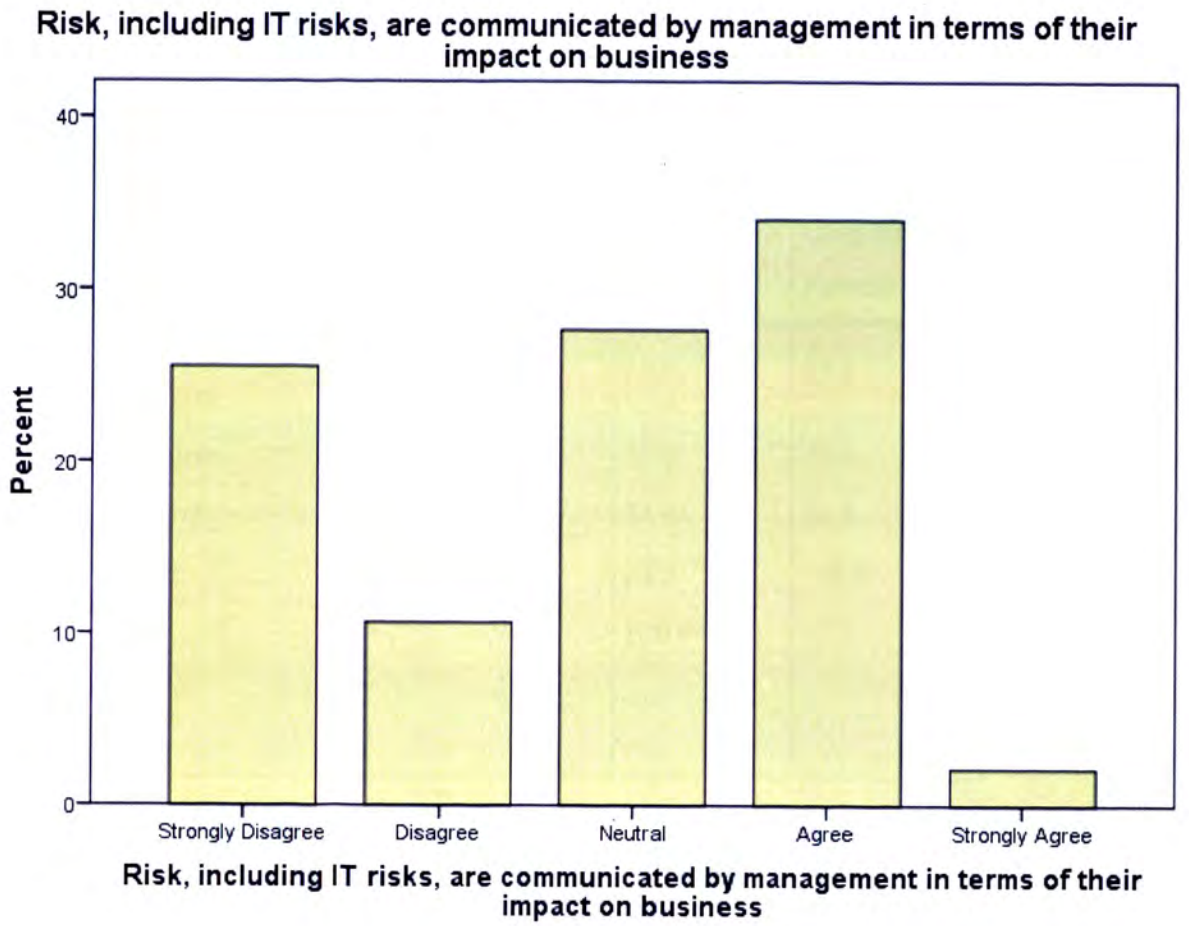

Figure 4.18 Risk including IT risks

As per Figure 4.18 above shows the respondents who agree with 33.3% followed by 27.1% of those who are neutral 25.0% are those who strongly disagree and 10.4% disagree and the lowest is 2.1% of those who strongly agree.

4.19 Business process approach

Table 4.19: Business process approach

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	14	29.2	29.8	29.8
	Disagree	5	10.4	10.6	40.4
	Neutral	16	33.3	34.0	74.5
	Agree	12	25.0	25.5	100.0
	Total	47	97.9	100.0	
Missing	System	1	2.1		
Total		48	100.0		

Table 4.19 indicates 97.9% of respondents of if there is a business process approach to risk management technology and the table shows the results as follows, 34% are neutral, 29.8% strongly disagree, 25.5% agreeand 10.6% disagree.

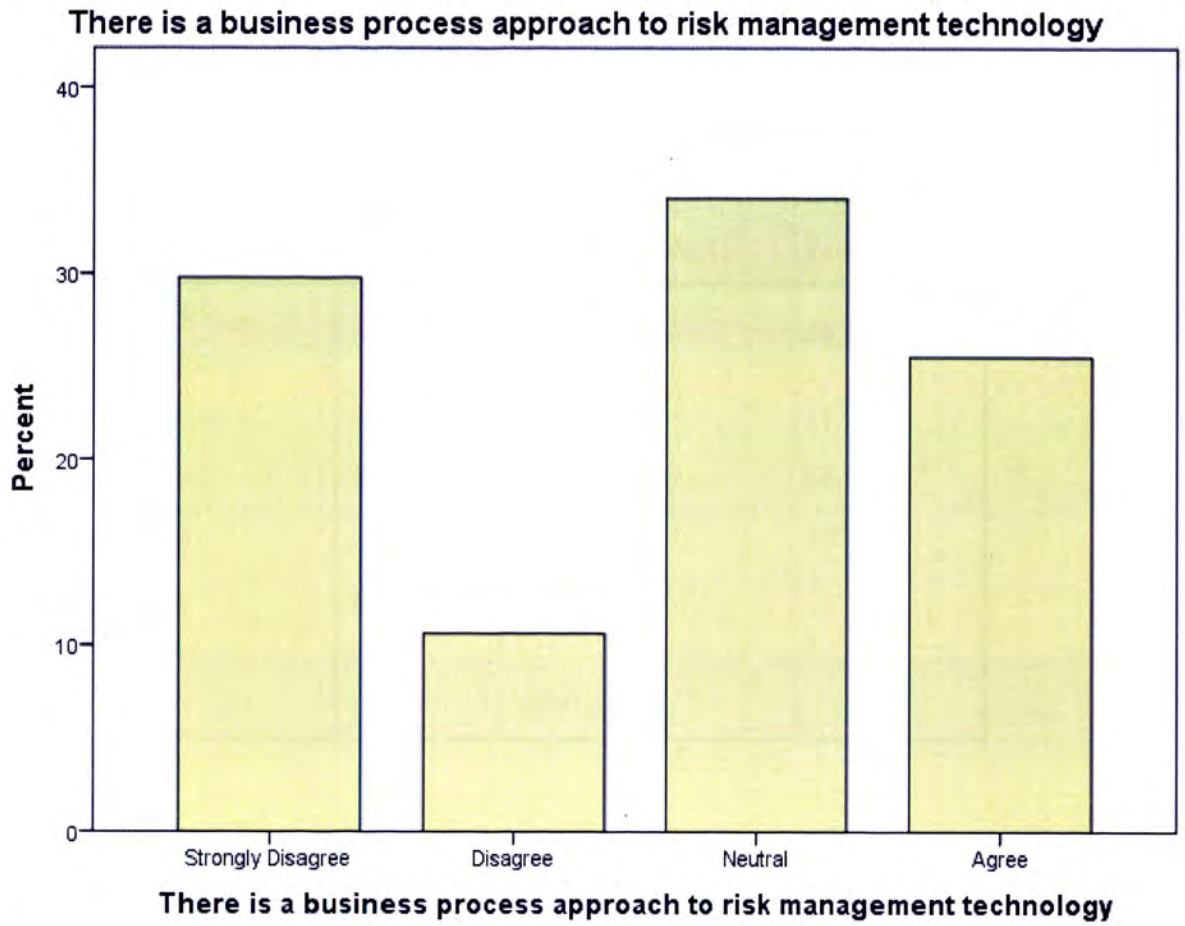

Figure 4.19 Business process approach

According to Figure 4.19 the respondents who are neutral are higher than the others with 33.3% followed by those who strongly disagree with 29.2% and 25.5% of those who agree and 10.4% of those who disagree. The graph shows that the majority of the respondents are not showing if there is a business process approach to risk management technology and that is followed by the respondents who strongly disagree. That means somewhere you may find that the risk management technology business process approach is not well communicated.

4.20 Procedures for checking professionals

Table 4.20: Procedure for checking professionals' credentials

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	18	37.5	38.3	38.3
	Disagree	6	12.5	12.8	51.1
	Neutral	8	16.7	17.0	68.1
	Agree	15	31.3	31.9	100.0
	Total	47	97.9	100.0	
Missing	System	1	2.1		
Total		48	100.0		

Table 4.20 shows that 97.9% respondents on whether there is a procedure in the department for checking professionals credentials, backround and references in the department.The table shows that there is 38% of respondents who strongly disagree, 31.9% agree, 17% are neutral and 12.8% disagree.

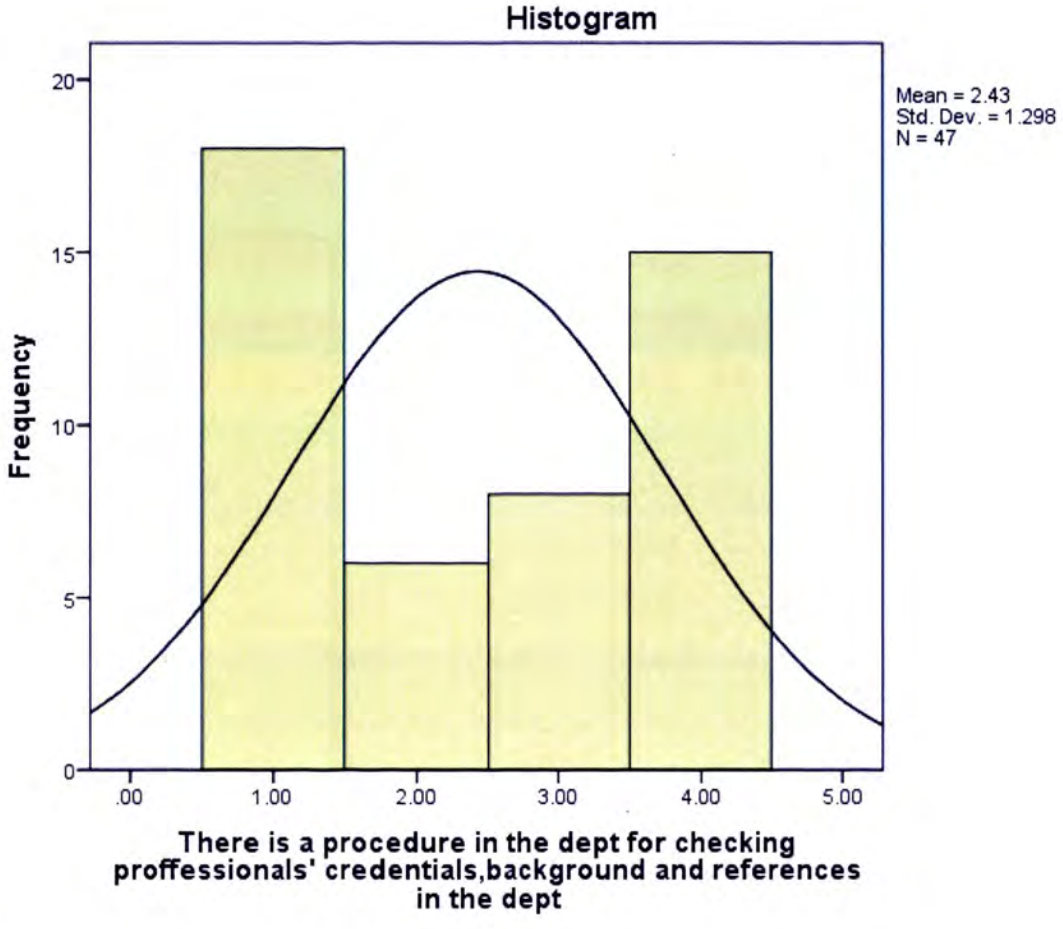

Figure 4.20 Procedures for checking professionals

As per figure 4.20 the data shows the mean value of 2.43% and the standard deviation of 1.298% with a total number of 47 respondents which means one has not responded and our data is slightly skewed to the left hence the frequency table 4.35 shows clearly that the respondents which carries a high percentage are those who strongly disagree with 37.5%, followed by 31.3% of those who agree. This might show that the respondents believe that risk management is not properly managed as they strongly disagree that there is a procedure in the department for checking professionals. 16.7% of the respondents are neutral while 12.5% disagree.

4.21 Operational Support for risk management

Table 4.21 : Operational support for risk management

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	16	33.3	34.0	34.0
	Disagree	1	2.1	2.1	36.2
	Neutral	16	33.3	34.0	70.2
	Agree	14	29.2	29.8	100.0
	Total	47	97.9	100.0	
Missing	System	1	2.1		
Total		48	100.0		

Table 4.21 reflects 97.9% of total respondents while 2.1% of respondents are missing.The table shows that 34% of the respondents are neutral, onother 34% are those who strongly disagree, 29.2% agree and 2.1% disagree.

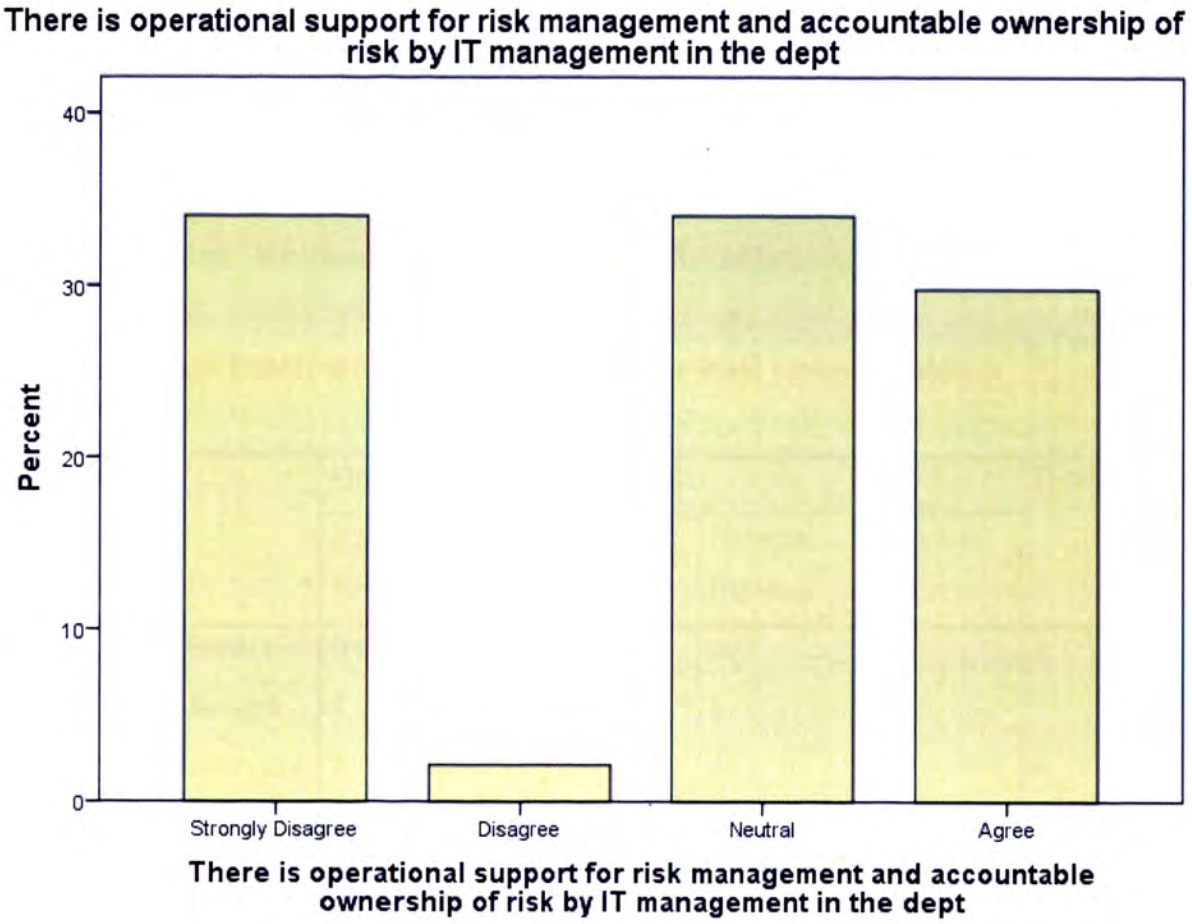

Figure 4.21 Operational Support for risk management

According to Figure 4.21 the respondents who are neutral are equal with 33.3% with those who strongly disagree that there is operational support for risk management and accountable ownership of risk by IT management in the department of finance, 29.8% agree while 2.1% disagree and the other 2.1 percent is missing.

4.22 Cross Tabulation

The objective of this section is to test the relationship between independent and dependent variables as well as the strength of those relationships. In this section the objective is to test for significant association between variables such as qualifications and job functions and each individual question. Such analysis will show meaningful tendencies at the individual item level.

Table 4.23 : Job Function * Qualification of Respondents Cross Tabulation

		Qualification of Respondents				Total
		Post Graduate	Bachelor Degree	National Diploma	Matric	
Job Function	Director	0	1	0	0	1
	Manager	1	1	0	0	2
	Supervisor	2	1	1	2	6
	Technical	0	4	8	11	23
	Other	2	1	4	8	15
Total		5	8	13	21	47

According to Table 4.24 above there is a cross tabulation where two variables were measured against each other and the variables used are the qualification of the respondents against the job function of the respondents. It shows on the table above that there is only one director who possesses a bachelor's degree and one manager who possess a post graduate degree and one manager who hold a bachelor's degree.

In the supervisory level there are two supervisors who hold post graduate degrees and one with a bachelor's degree and one with a national diploma.

Technically we have two post graduates, one bachelor degree, four national diplomas and eight with matric. There are others who fall in the category of other and those who have two post graduates, 1 bachelor's degree, four national diplomas and eight with matric.

Table 4.24 : Job Function * Work experience Cross-tabulation

		Work experience				Total
		1- 5 Years	6 -10 Years	11 - 15 Years	16 - Above	
Job Function	Director	1	0	0	0	1
	Manager	0	0	1	1	2
	Supervisor	0	1	1	5	7
	Technical	5	11	3	4	23
	Other	4	5	5	1	15
Total		10	17	10	11	48

As per Table 4.25 there are two variables used and they are the job functions of the employees against their work experience. In the table we can see that at director level we have one director who has work experience of 1-5 years, one manager who has 6-10 years, one with 11-15 and four with 16 and above.

At supervisory level we have one supervisor with 6-10 years working experience, one with 11-15 years 5 with 16-above. Of those who are technical, we have five who are at 1-5 years, eleven of those who fall between 6-10, three of them are at 11-15 and four who are at 16-above.

There are those who fall in the category of other and four who fall between 1-5 years, five who are at 6-10, another five between11-15 years and one between 16 and above.

4.25 Summary

This chapter discussed the data analysis and interpretation, with the use of graphs, frequency tables, descriptions and inferential statistics. The demographic information provided background information on the respondents and factors that influenced their level of knowledge and choice of infant feeding methods.

Chapter 5, which is the next chapter, concludes the findings of the study, discusses its limitations and makes recommendations for practice and further research.

Chapter 5

Summary, Recommendation and Conclusion

The purpose of this chapter is to summaries the study that was conducted. Included in this summary are a review of the purpose of the study, a restatement of the research questions, the research methodology used and a summary of study results discussion and conclusion.

5.1 Summary

5.1.1 Purpose of the study

The purpose of the study was to determine from the literature the nature and scope of Information Technology's impact and to determine empirically the skill level of IT employees.

The survey results showed on the cross tabulation Table 4.24 that there is only one director who possesses a bachelor's degree and one manager who possess a post graduate degree and one manager who hold a bachelor's degree. This is a clear indication that we there is a shortage of qualifications in management.

5.2 Findings and discussions of results: Research Questions

To investigate the importance and impact of Information Technology as a Risk Management tool in the Department of Finace.

The survey results in Figure 4.19 indicate 33.3% of operational support for risk management in the department and Figure 4.20 reveals 25.0% of respondents who agree that risk including IT risks are communicated by management in terms of their impact on business.

Investigate if the employees who are operating the financial systems have enough skills to perform those tasks to detect financial risk in the system.

The survey results in Figure 4.22 reveals that, there is a strong disagreement of 33.3% of respondants who disagree that there is an operational support for risk management and accountable ownership of risk by IT management, and also disagree that there is a direct

relationship between the job characteristics of Managers in the Information Technology directorate and their rate success or fuilure in the department of Finance.

5.3 Research Methodology

The researcher used the quantitative, descriptive research methodology to collect data from officials who are working in the department of Finance Information Technology Directorate in North-West Provincial Government. Data collected from the survey respondents represent their perception regarding the roles of IT portfolio, characteristics, success and intervention that can be applied by IT managers. The staff who did not submit their questionaires were reminded via e-mail and most of them were technicians who are field workers. The questionnaires were only distributed to the NWPG IT officials who are based in Garona building and not distributed to the IT officials who are working in the regions and the regions compose of Rustenburg, Klerksdorp, Potchefstroom, Lichtenburg and Vryburg but in case the researcher continues with his studies after completion of MBA the employees who are working in the regions and all directorates within the department of Finance will be involved. Respondents completed their questionnaires that addressed their perception regarding characteristics, success, interventions that can be applied and failures (Appendix B). Questionnaires were analysed using Stastical tool, Statical Product and Service Solutions (SPSS).

5.4 Results

Table 4.7 provides data relating to distribution process by IT officials regarding the role of IT portfolio in the department; IT portfolio includes IT personnel, computers, hardware, software etc. The data shows that 29.2% of respondents are neutral and 29.2% again agree that there are current licences for the software used and 12.5% strongly disagree. This is the indication that the majority of the respondents are aware of the current licences that are used in the department.

There are few respondents who disagree and 41.7% agree that all production servers, applications and supporting software are physically located in the data center. 37.5% also agree that they know the personnel who must be contacted in case of emergency. This is a clear

indication that the IT portfolio in the department especially IT directorate plays an important role.

The success of IT management is indicated on Figure 4.10. It shows that most of the respondents disagree that there is a success of IT management, 29.2 % is neutral followed by 25.0 % who strongly disagree and the research cannot depend on the neutral respondents because neutral is the indication that the respondent is not sure of his or her option. That means there is a poor communication of new policies and procedures, 29.2% agree that there is a need of legal, regulatory and policy requirement relative to the delivery of automated service in IT directorate.

Section D of the questionnaire contained four questions (8-11) that asked the respondents about the intervention that can be applied by IT management in case of emergency in the department. It is clear as indicated by 31.3% of respondents that agree that there is backup strategies developed for continuity of automated services, should the department have IT failure and 45.0% of respondents agree that there is secured infrastructure that protects the information asserts been developed, implemented and communicated, 18.8% percent strongly agree and only 12.5% strongly disagree.

According to Table 4.18, 29.2% strongly agree that IT management staff are considered directly responsible and accountable if elements within the automated system failed, and 29.2% of the respondents agree with that statement.

Section E of the questionnaire contained four questions (12-15) that asked the respondents about the characteristics of IT management and they are focusing on risk management in IT. Figure 4.19 indicate that 33.3% agree that risk including IT risk are communicated by management in terms of their impact on business and it is followed by 27.1% of respondents who are neutral about that statement and 25.0 % strongly disagree.

According to Figure 4.20 33.3% of the respondents are neutral about the statement that says there is a business process approach to risk management technology and that is followed by 29.2% of respondents who strongly disagree and 25.0% who agree.

Figure 4.23 reveals the data that shows the results of the respondents on operational support for risk management, it indicates that 33.3% of the respondents strongly disagree that there is

operational support for risk management and accountable ownership of risk by IT management in the department. It is followed by 29.25 of those who agree and another 33.3% is neutral.

5.5 Discussion

These findings indicate that the IT official's perception regarding roles of IT portfolio, rate of manager's success, interventions that can be applied and characteristics of IT managers are not the same but the majority indicate a positive perception. These study indicated that there are policies and procedures that are implemented but the questionaire revealed that those policies are not communicated because you may find that only few respondents agree or strongly agree that this policies acommunicated.

It it is clear from the response that it is only management who responded positively about policies which means that managers do not give reaction to their subordinates because implementation of policies are discussed at management meetings, so it is the duty of the managers to give feedback to their subordinate about this policies, and these results in poor communication in the IT department. It is clear that IT is a risk management tool in Finanace as indication of respondents strongly agree that there is operational support for risk management and IT management is held accountable ownership of risk and they are also responsible and accountable if elements within the automated system fails.

There is a clear indication of IT as a role plays of risk management in the department of finance we can see that there are secured infrastructure that protects the information asserts been developed, implemented and communicated and there is also a backup strategy developed for continuity of automated services should the department have an IT failure.

5.6 Recommendations

Based on the findings of this study to examine the perception of officials in IT regarding the roles of It portfolio, characteristics, success, intervention that can be applied by IT managers. The findings reveal that management and subordinates or officials below management level hold different perceptions.

It is clear that there are policies, procedures and planning processeses that adequately includes operational resources to support the line business are designed by IT management to manage risk but these operational resources are not communicated. My take on this matter is that the change management must conduct workshops about policies in the department, they must inform the staff as a whole and not as a selected staff and inform them about all applications and software that are used.

Further research will be conducted.

REFERENCES

Adèr, H.J. & Mellenbergh, (G.J.with contributions by D.J. Hand). 2008: *Advising on Research Methods: A consultant's companion. Huizen, the Netherlands:* Johannes van Kessel Publishing.

Burton,R. Borge, O. 2002, *Strategic Organisational Diagnostic and Design.*The dynamic of Fit.p80-92

Chandra,S.T. Freedberg,M.A. and Abrams.R.2011: *The American Journal of Gastroenterology.* 102.p279-282.

Communications of the Association for Information Systems, Volume 26, Article 13, November 2010

David Hillson; Ruth Murray-Webster (30 March 2007): *Understanding and Managing Risk Attitude.* Gower Publishing, Ltd.. ISBN 978-0-566-08798-1. Retrieved 17 April 2012.

Delloit. 2007: *The risk intelligent chief audit executive.* Risk Intelligence Series, 5:p1-7.

Deloach William Scott, Maria M. Carcia and Rosario F. Licata.2010:*Jornal of Agent-Oriented Software Engeneering.*Volume 4,no 3, p244-249.

.

Dickinson, G. 2005: *Enterprise risk management: Its origins and conceptual foundation.* Geneva Papers on Risk & Insurance - Issues & Practice, 26(3): 360-366. July.

Duden.D and Geaglone.P, 2006: For Risk Managers – *Enterprise Risk Systems Compared, Risk & Insurance Technology Magazine*

Searchcio.2008: *Business process* [Online]. Available from: http://searchcio.techtarget.com/sDefinition/0,,sid182_gci1088467,00.html Accessed:02/08/2008].

Risk management for IT systems [online].Available from: http://www.isaca.org/Knowledge-Center/Risk-IT-IT-Risk-Management/Pages/Risk-IT1.aspx?

Risk IT, *Framework for management of IT Related Business* [Online]: Available from: http://www.isaca.org/Knowledge-Center/Risk-IT-IT-Risk-Management/Pages/Risk-IT1.aspx?gclid=CJvFqtLzvLMCFcrItAodJHIA7g.

IT Governance Institute,2007:*Cobit 4.1 Expert* [Online].Available from: http://www.isaca.ch/files/ Cobit Framework.pdf[accessed:25/07/2008].

IT Governance Institute.2008:*Cobit-control objectives for information and related* [Online].Available from http://en.wikipedia.org/wiki/Risk_management.

Johann Moouton.2001:*How to succeed in your Master's & Doctoral Studies*. A South African Guide nd Resource Book.p145-152 , 1st Edition.

Kenneth Laudon & Jane Laudon. 2011: *Essentials of Management Information Systems,*9th Edition,p277-280.

King II Report on *Corporate Governance for South Africa* see Institute of Directors in South Africa.

Levitt,S. Kessler,R. Daniel,K. 1999: *Statical Modeling,Cacisal Inference and Social Science*.Discussion Paper NCJ 176365 Washington.D.C : Bureau of Justice Statistics.

Louis Cohen , Lawrence Manion and Keith Morrison, 2000: *Research Method in Education* 6th Edition,p345-355.

MEC. Loisa Mabe, 2011. *Department of Finance Budget Speech.* http://www.nwpg.gov.za/Documents/Speeches/MEC%20SPEECH%2011%20MTEF%20(EPRE)%20-%2008%20March%202011_1.pdf

Merylyn, W.Wood, J. Pamla. B. 1997: *Advance Design Nursing Research* 2nd Edition.p389-398.

Burns.N,Grove .S .2010: *Building Evidence Practice* 3rd Edition,p448-460.

Nelleke Bak, 2004: *Completing your thesis*, A practical Guide, 1st Edition,p320-345.

North-West Provincial Departments: 2009-2011 *Risk Management Strategic Support Plan.*

North West University Manual for Post Graduate Studies, January 2010

Randall F.Young, University of Texas, *Emperical Evaluation of Information Security Planning and Intergration*

Shough, R. 2007. Deloitte. *The Evolving Nature of Risk Management* 10th Southern African Internal Audit Conference., 1 - 29. August

Steward, T.A: 2005: *Managing risk in the 21st Century.* Fortune. 7 February, 2012.

Stoneburner G, Goguen ,and Feringa A. 2005: *Risk Management Guide For Information Technology Systems,* P133-139.

United States Environmental Protection Agency (April 2004). *General Risk_Management Program Guidance* . United State Environmental Protection Agency.

Valsamakis, A.C. Vivian , R.W. & Du Toit , G.S. 2005: *Risk management*: *managing enterprise risks*. 3rd Edition. Sandton: Heinemann Higher.P180-202.

APPENDIX A

Letter of Request to distribute questionnaires

The Chief Director
Department of Finance
Information and Technology Directorate
North West Provincial government
Private bag x 2060
Mmabatho
2745

Dear Sir

REQUEST TO DISTRIBUTE A QUESTIONAIR IN IT AS A REQUIREMENT TO FULLFILL MY MBA PROGRAM

I hereby duly request a permission to distribute a survey questionnaire to IT officials in order for my fulfillment of my Master of Business Administration. My topic is "Information Technology as a risk Management: Case of North-West Provincial Government (Finance).

If you have any comment or concern you are free to contact my supervisor who is, Professor Nehemia Mavetera at 018-389 2143 or e-mail him at Nehemia.Mavetera@nwu.ac.za

Hope you find all in order.

Regards,

Terance Seletedi

APPROVED/NOT APROVED

Mr. Mohamed Haffejee (Acting Chief Director)

APPENDIX B

DEMOGRAPHICAL BACKGROUND

Please mark with an X in the appropriate box

1. Race

1.1	African	
1.2	Coloured	
1.3	Indian	
1.4	White	

2. Gender

2.1	Male	
2.2	Female	

3. Job Function

3.1	Director	
3.2	Manager	
3.3	Supervisor	
3.4	Technical	
3.5	Other	

4. Qualifications

4.1	Post Graduate	
4.2	Bachelor Degree	
4.3	National Diploma	
4.4	Matric	

5. Work Experience in Years

5.1	1-5	
5.2	6-10	
5.3	11-15	
5.4	16 -above	

The following questions ensure the role of IT portfolio in the department.
Please indicate the extent to which you agree with each statement by putting an X in the appropriate box

1. All applications and software used in IT have current licenses.

1.Stongly Disagree	2.Disagree	3.Neutral	4.Agree	5.Strongly agree

2. All production servers, applications and supporting software are physically located in the data center.

1.Stongly Disagree	2.Disagree	3.Neutral	4.Agree	5.Strongly agree

3. I know what to do, whom to contact in case of fire, accident and inappropriate physical access.

1.Stongly Disagree	2.Disagree	3.Neutral	4.Agree	5.Strongly agree

The following questions ensure rate of success of IT management

4. There is a process to communicate new policies and procedures to the staff and training is provided if necessary.

1.Stongly Disagree	2.Disagree	3.Neutral	4.Agree	5.Strongly agree

5. There are legal, regulatory and Policy requirement relative to the delivery of automated services in IT.

1.Stongly Disagree	2.Disagree	3.Neutral	4.Agree	5.Strongly agree

6. I can demonstrate compliance with applicable standards, Legal and regulatory requirements implemented in IT.

1.Stongly Disagree	2.Disagree	3.Neutral	4.Agree	5.Strongly agree

7. There is IT planning process that is designed by management that adequately includes operational resources to support the automated line business.

1.Stongly Disagree	2.Disagree	3.Neutral	4.Agree	5.Strongly agree

The following questions ensure the intervention that can be applied by IT management in case of emergency in the department.

8. There is a backup strategies developed for continuity of automated services should the department have an IT system failure.

1.Stongly Disagree	2.Disagree	3.Neutral	4.Agree	5.Strongly agree

9. If an IT system failure result in a newsworthy event, wide spread will be communicated to the users via global e-mail by IT personnel.

1.Stongly Disagree	2.Disagree	3.Neutral	4.Agree	5.Strongly agree

10. There is a secured infrastructure (password, PC, Firewall, Network policies, Procedures and hardware, Software) that protect the information asserts (data integrity, confidentiality, availability) been developed, implemented and communicated.

1.Stongly Disagree	2.Disagree	3.Neutral	4.Agree	5.Strongly agree

11. IT management staff are considered directly responsible and accountable if elements within the automated system failed.

1.Stongly Disagree	2.Disagree	3.Neutral	4.Agree	5.Strongly agree

SECTION E

The following questions ensure the characteristics of IT managers

12. Risk, including IT risks, are communicated by management in terms of their impact on business

1.Stongly Disagree	2.Disagree	3.Neutral	4.Agree	5.Strongly agree

13. There is a business process approach to risk management technology.

1.Stongly Disagree	2.Disagree	3.Neutral	4.Agree	5.Strongly agree

14. There is a procedure in the department for checking professionals' credentials, background and references in the department.

1.Stongly Disagree	2.Disagree	3.Neutral	4.Agree	5.Strongly agree

15. There is operational support for risk management and accountable ownership of risk by IT management in the department.

1.Stongly Disagree	2.Disagree	3.Neutral	4.Agree	5.Strongly agree

APPENDIX C

ABBREVIATION TABLE

LIST OF ABREVIATIONS AND ACRONYMS

1. CFO.....Chief Financial Officer
2. DAC.....Discretionary Access Control
3. ECAR.....Economic Capital At Risk
4. ERM.....Enterprise ResourceManagement
5. HTML.....Hypertext Markup Language
6. ID.....Identity Document
7. ISACA.....Information System Audit And Control Association
8. ISSO.....Information System Security Officer
9. IT .....Information Technology
10. MAC..... .....Mandatory Access Control
11. NWPG.....North West Provincial Government.
12. PFMA.....Public Finance Management Act
13. POAM.....Plan Of Action And Milestone
14. RAROC..... .....Risk Adjusted Return On Capital
15. ROI.....Return On Investment
16. SPSS.....Statical Product and Service Solutions
17. PWC.....Price Water Coopers
18. VAR.....Value At Risk