

**A FRAMEWORK FOR IMPLEMENTATION OF INFORMATION SECURITY  
MANAGEMENT IN GOVERNMENT MINISTRIES, A CASE STUDY OF  
MINISTRY OF YOUTH AFFAIRS AND SPORTS, KENYA**

**BY**

**DICKSON O. GISIORA  
REG. NO. P56/60663/2010**

**A RESEARCH SUBMITTED IN FULFILLMENT FOR THE  
REQUIREMENT OF THE AWARD OF MASTER OF SCIENCE IN  
INFORMATION SYSTEMS.**

**UNIVERSITY OF NAIROBI**

**SUPERVISOR  
STEPHEN MBURU**

**JULY, 2012**

## **ABSTRACT**

Not only is Information Security Strategy crucial to protect information systems, but it is central to organization survival. Today's organizations depend on information for their survival. Specifically, organizations depend on the systems and controls in place that provide for the ongoing confidentiality, integrity, and availability of their data and information. Many organizations are ill-equipped to define their security goals, let alone to make an explicit connection between their security goals and the strategic drivers of the organization. Threats to organizational information and information systems are increasing in occurrence and in complexity and this emphasizes the urgency for organizations to learn how to better protect their information and information systems

Information security is subjective and contextual therefore, every organization's approach to a security strategy should be different and customized accordingly, because each organization has its own threats, risks, business drivers, and industry compliance requirements .

To improve the governance of IT and comply with regulatory demands, organizations are using best practice frameworks implement information security. One of these IT governance frameworks is COBIT (The Control Objectives for Information and related Technology). COBIT provides guidance on what could be done within an IT organization in terms of controls, activities, measuring and documentation. This framework is however generic and require specific knowledge in order to enable customization and use in a local scenario.

The research methodology that was adopted was a case study. The population of interest was officers in the Ministry of Youth Affairs and Sports working at the headquarters. Random sampling was used with targeted interviews to the officers in ICT department who are the custodians of Information systems in the ministry and the administration which provide policy guidelines for the ministry. Data was analyzed by the use of descriptive statistics such as frequency distribution tables, percentages, bar charts and pie charts.

The research established that the ministry faces a number of challenges in relation to implementing information security in today's environment. In as much as the ministry's top officials expressed firm commitment to implementing security in the ministry, there seemed to be no co-ordination between ministry staff and IT staff on the role of information which indicates a communication deficit.

The key recommendations include the need for management to fully recognize that Information Communication Technologies are a critical asset and which should be restricted to authorized/legal use only; Information Communication Technology is a Business Issue – not a technology issue and need to be aligned with priorities, industry-prudent practices and government regulations, and Information Communication Technologies are enterprise-wide business with associated risks, and therefore all staff should be involved in securing them. An implementation framework, The Control Objectives for Government Information Technologies (COGIT) was developed which the researcher recommended to government ministries as a reference model to Information security management.

# DECLARATION

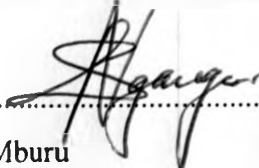
## BY CANDIDATE

I declare that this research is my own original work and to the best of my knowledge it has not been presented for a degree award in any other University.

Signed..........Date...*24/7/2012*.....  
Dickson O Gisiira  
P56/60663/2010

## BY SUPERVISOR

This research has been submitted with my approval as the University Supervisor.

Signed..........Date...*25/7/2012*.....  
Stephen Mburu  
Lecturer, School of Computing and Informatics  
University of Nairobi

## **ACKNOWLEDGEMENT**

I wish to acknowledge the professional guidance given to me by my supervisor Mr. Stephen Mburu whose support and encouragement enabled me to finalize the project on time, panelist Professor Okelo-Odongo, Samuel Ruhiu and Ms. Ronge whose contribution was invaluable to this project.

I also wish to acknowledge the support of my family, my wife Emma and daughter Prudence, and cooperation and assistance of my colleagues at work and in the Information System class of 2010 who motivated me to work hard to complete the project.

Lastly, I wish to thank my employer, The Ministry of Youth Affairs and Sports and my colleagues for giving me the opportunity and an ample time during which I have undertaken the course.

# TABLE OF CONTENTS

## Contents

Abstract.....	ii
Declaration.....	iv
Acknowledgement .....	v
Chapter one .....	9
1.1 Background of the study .....	9
1.2 Problem statement.....	10
1.4 Research Justification and Rationale .....	13
1.5 Scope and limitation of the Study .....	13
Chapter two.....	15
Literature Review .....	15
2.1 Introduction.....	15
2.2 Information Security Management .....	15
2.2.1 The importance of information security management.....	16
2.3 The CIA Model of Information Security Management.....	17
2.4 Contextualizing the Examination of Information Security.....	19
2.5 Measurement of Security Management .....	22
2.6 Policy as a foundation to security management .....	22
2.7 Security adoption rates of awareness.....	25
2.8 Compliance with Security.....	25
2.9 Information security management frameworks .....	26
2.10 Commercial standards for information security .....	27
2.10.1 ISO standards.....	27
2.10.1.1 ISO/IEC 27002:2005 (Code of Practice for Information Security Management) .....	27
2.10.1.2 ISO/IEC 27001:2005 (Information Security Management System - Requirements).....	28
2.10.1.3 ISO/IEC 15408 (Evaluation Criteria for IT Security) .....	29
2.10.1.4 ISO/IEC 13335 (IT Security Management).....	29

2.10.2	Payment card industry data security standard.....	30
2.10.3	COBIT .....	30
2.10.4	ITIL (or ISO/IEC 20000 series).....	31
2.11	Regulations related to information security .....	31
2.11.1	SOX .....	31
2.11.2	COSO.....	32
2.11.3	HIPAA .....	33
2.11.4	FISMA .....	33
2.11.5	FIPS .....	34
Chapter Three: .....		35
Research Methodology .....		35
3.1	Introduction.....	35
3.2	Research Design.....	35
3.4	Target Population.....	35
3.5	Sampling Design and Sample Size .....	35
3.6	Data Collection Procedures.....	36
3.7	Data Analysis and Presentation.....	36
Chapter Four .....		37
4.1	The Control Objectives For Government Information And Related Technologies (COGIT) .....	37
4.2	Planning and Organization.....	38
4.3	Organizational Security .....	38
4.4	Asset Classification and control.....	39
4.5	Personal security .....	39
4.6	Physical and environmental security .....	39
4.7	Communication and operation management .....	39
4.8	Access control .....	40
4.9	System development and maintenance .....	40
4.10	Business continuity management.....	40
Chapter Five: .....		41
Research findings and discussions.....		41

5.1	Introduction .....	41
5.2	Security Breaches .....	41
5.3	Levels of compliance to key business roles linked to IT .....	42
5.3.1	IT Planning and organization.....	43
	IT organization.....	45
5.4	Asset Classification and Control.....	47
5.5	Personal Security .....	48
5.6	Physical and environmental Security.....	49
5.7	Communication and operation management .....	50
5.8	Access Control.....	51
5.9	System Development and maintenance .....	52
5.10	Business Continuity Management .....	53
	Summary of the findings .....	55
	Chapter six .....	57
	Summary of research, outcomes and recommendations.....	57
6.1	Introduction.....	57
6.1	Security policy .....	57
6.2	Organizational security.....	59
6.3	Communication and operation management .....	60
6.4	Access control.....	61
6.5	Physical and environmental security. ....	62
6.6	Asset classification and control. ....	62
6.7	Information systems acquisition, development and maintenance. ....	63
6.8	Business continuity management .....	63
	Chapter Seven. ....	65
	Validated Control Objectives For Government Information Technology (COGIT).....	65
	References.....	70
	Appendix I .....	75
	Appendix II Interview Guide .....	4



# CHAPTER ONE

## 1.1 Background of the study

Information is an asset that, like other important business assets, is essential to an organizations business and consequently needs to be suitably protected. This is especially important in the increasingly interconnected business environment. As a result of increasing interconnectivity, information is now exposed to a growing number and a wider variety of threats and vulnerabilities (ISO/IEC 17799:2005). For this reason, many organizations nowadays implement various security policies in order to protect the organization. Also, to have a secure flow of information, organizations implement an information security framework, which helps the organization to identify the risks associated with the organization's information and ways to mitigate those risks.

The Government of Kenya is increasingly relying on formation Technology (IT) systems for essential operations including Human resource administration, financial operations and research. However the process of effectively implementing information security management in the government is challenging. The government consists of a mix of many factors ranging from administrative to political influence to compliance with the mandate of specific institutions in government. Consequently, unique and divergent demands are placed on securing and accessing IT systems. The aim of this project will be to determine the status of information security practices in the Ministry of Youth Affairs and Sports, and interrogate the Information security framework in place and the key issues and influencing factors surrounding the effectiveness of information security management practices and to find out what improvements can be made in the practices and hence develop an implementation framework that may be adopted

## 1.2 Problem statement

Today's organizations depend on information for their survival (Whitman & Mattord, 2004). Specifically, organizations depend on the systems and controls in place that provide for the ongoing confidentiality, integrity, and availability of their data and information (Krutz & Vines, 2004). According to Caralli (2004) many organizations are ill-equipped to define their security goals, let alone to make an explicit connection between their security goals and the strategic drivers of the organization. Schneier (2004) states that threats to organizational information and information systems are increasing in occurrence and in complexity and emphasizes the urgency for organizations to learn how to better protect their information and information systems

As information security become increasingly important to the continued success for businesses, many are seeking an appropriate security framework (Yhan, 2005). Information Technology systems have become increasingly critical to the smooth operation of organizations, and arguably the economy as a whole. The constantly evolving risks that preservation of information faces are exacerbated by the increasing frequency and sophistication of threats. A connection exists in society between the growing reliance on information systems and associated information. A requirement therefore exists for effective information security management to protect information systems from an escalating number of threats and risks. This is necessary in order to avoid major disruptions to services, as well as to protect organizations from loss, damage or modification of important data.

The dichotomy of social reliance on information is reflected in the fact that some components of society either inadvertently fail to stabilize, or in fact deliberately increase efforts to destabilize, the very information upon which they depend. This can occur through system user errors or malicious action taken by hackers and cyber criminals. As a result, one or more key characteristics of the confidentiality, availability or integrity of information may be compromised. Consequently, maintaining continuity in modern organizations ultimately relies on the preservation of information achieved through the process of applied information security.

The government has along with other organizations, adopted and embraced information systems and technologies in order to survive in a competitive environment. The ministry of Youth Affairs

and Sports is highly reliant on information to support its core activities and business operations. There is a dependence on activities associated with creating, using and sharing information for the ministry's core functions. It is currently operating three key systems that are the core of the functions namely, Youth Groups and Youth Polytechnics Information Management System, The Integrated Financial Management System, the Integrated Personnel Payroll system and the Government Human Resource Information System. The ever-present nature of information means that ministry is directly impacted by their reliance on, and use of, information technology resources, systems and information.

Information security is subjective and contextual (Canal, 2005), and according to Harris (2006), every organization's approach to a security strategy should be different and customized accordingly, because each organization has its own threats, risks, business drivers, and industry compliance requirements. This necessitates an approach that is suited to the ministry. It also necessitates an understanding of how information security 'fits', based on the structure and culture of the Ministry. Although technology itself is a major control applied to mitigate security risks, it is the management of security as a business function that determines ultimate success. The application of technology is most effective when aligned with the business goals.

Therefore, effective security depends on effective management. The need for effective information security management is therefore evidenced by a combination of factors. These include an increase in the reliance on electronic information, an increase in the events and activities that threaten the information that is relied upon, and the corresponding need for the application of controls to mitigate risks.

Research by Gartner and AMR (Haldar and Forsyth, 2004) conclude that many enterprises remain inadequately protected from security threats because of the perceived high cost of an effective security strategy that suits the organization's culture. The lack of focus on security strategy has led to an emphasis on products and technologies instead of a security strategy that incorporates security awareness, training, and policy and standards in an effort to develop a 'culture of compliance' towards information security.

An effective commitment to security requires that a process be in place that suits the culture of the organization (Leach 2003). Understanding the factors that add to compliance within this environment is multifaceted. The ministry environment contains a mix of corporate culture and the inadequacy of systems and inconsistently in applied policies and procedures.

Security awareness is an important function, yet it is under-funded, under-represented and generally applied in an ad hoc process and in a reactive manner. Security awareness is therefore highly unstructured in most organizations and can be seen as operating on a spectrum ranging from either ignoring it, or developing according to a study conducted by Adams and Sasse (1999) on the compromises of security in relation to password management. One key factor which contributes to compromise in security is insufficient communication from security sections in organizations to users, which caused users to construct their own models of reality on possible security threats and the importance of security. All these are facts that the ministry is facing as it is applying Information Technology for day to day operations. The ministry operates in a unique economic and political environment that needs a balance to conduct its mandate. It therefore needs a specific Information security model that will work for it.

A range of best practices is applicable to information security management, including the growing maturity and consequential acceptance of well-regarded frameworks such as AS/NZS ISO 17799, CobiT, ITIL, COSO, ISO9002, Capability Maturity Model (CMM), Project in Controlled Environments (PRINCE), Managing Successful Programmes (MSP), Management of Risk (MoR), and Project Management Body of Knowledge (PMBOK), (ITGI, 2005) . Selection of various elements of disparate best practices can be aligned to suit the ministry; invariably the use of best practices needs to be applied in context to ministry needs.

The implementation of best practices tends to be costly and unfocused if treated as purely technical guidance. The most effective approach is to apply best practices starting at the business context. Implementation of best practices should therefore be consistent with the organization's business risk management and control framework (ITGI, 2005). The research therefore undertook to ascertain the extent to which the ministry is implementing information security and

come up with an implementation framework based on the COBIT maturity model and the ISO code of information security management that can be proposed to the ministry.

### **1.3 Aim and Objectives of the study**

The overall goal of the project was to determine the extent to which ministries implement Information security from whence develop a framework that can be suitably used by ministries to manage information security.

The specific objectives of the research were:

- i. To determine the current status of information security management practices in the Ministry of Youth Affairs and Sports
- ii. To identify key issues and influencing factors surrounding the effectiveness of information security management practices
- iii. Develop a customized security implementation framework that can be recommended to the ministry

### **1.4 Research Justification and Rationale**

There is a growing reliance on information and the importance of protecting information through security practices. The associated difficulties in the government environment with managing information security are a key aspect of this study. A significant outcome of the study for subsequent research is highlighted as the need to develop a framework for information security that can be adopted by the ministry so as to attain the Confidentiality, Integrity and Availability of information.

The cobit reference model was preferred because it is a well-known framework for IT governance improvement, risk mitigation, IT value delivery and strategic alignment maturity assessments and it provides descriptive operationalization. It contains all the processes, activities and documents needed to correctly represent all Information Technology Governance concerns.

### **1.5 Scope and limitation of the Study**

Research on Information Security Management generally addresses two areas; the technical computer security and non-technical security management, while some researchers span both areas (Baskerville & Siponen, 2002). This project addresses non-technical security aspect of the information security framework. The scope of the project focuses on two areas: IT Governance and Compliance and Policies and Procedures. The limitation of the project is highlighted as information security itself for which Information security necessitates that some information be kept confidential and therefore some data was not collected.

# **CHAPTER TWO**

## **LITERATURE REVIEW**

### **2.1 Introduction**

The approach to the literature review involved an initial in-depth study of available literature through a variety of sources. These sources include library books, journal articles, magazines, online books, information security whitepapers, conference proceedings and presentations, and a wide variety of other information security sources available from the Internet.

### **2.2 Information Security Management**

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. Information plays a crucial role in the day-to-day functioning of practically any organization. It is a vital asset that adds value to an organization and its business processes. In fact, it has been at the centre of business for decades. Companies are under an incredible amount of pressure from their competitors to perform in a global market. The information they possess is no longer only used by employees, but by customers and partners as well. These users expect continuous availability of, and instantaneous access to, organizational information (McAnally, P., DiMartini, B., Hakun, J., Lindman, G. & Parker, R., 2000).

This section will discuss the role of information and information security in an organization, showing why it is required along with other relevant aspects. It will as well discuss the three pillars on which information security rests. It will be shown how these pillars, namely confidentiality, integrity and availability, support the protection of organizational information. Specific reference will be made to the continuous availability of information.

### **2.2.1 The importance of information security management**

Information security requirements have gone through significant changes in the last few years. Before data processing equipment started to play such a crucial role, information was primarily protected through physical and administrative techniques. With the introduction of the computer, it became clear that automated tools were now needed to protect files and other important information. Another important change was the introduction of the distributed computing environment and the use of networks for information transmission (Stallings, 1995). Information and the business processes, systems and networks that use this information are extremely important to an organization. Protection of the information is essential to ensure that the business has a competitive edge and maintain cash flow and commercial image, while complying with legal requirements. Unfortunately, organizations are constantly faced with threats to their information. This information and Information Technology (IT) is playing a vital role in the world of business today and this importance of IT is rapidly growing (von Solms, 1999). IT and business are almost impossible to separate in today's technologically advanced world. This unique combination not only has the role of enhancing an organization's efficiency and effectiveness, but IT departments also take initiative in leading the organization into innovative industry structures and markets. (IBM Global Services, 2000). While technology is developing at an incredible pace, the need to secure systems is increasing just as rapidly. The increased use of computer systems and networks, especially the Internet, provides numerous opportunities for computer crime. (Halliday, Badenhorst & von Solms, 1996) Securing information and information systems is no longer only the responsibility of the IT department. The organization's senior management also has to take part in ensuring that effective security measures are in place to protect information. Management has to have a good understanding of the organization's situation concerning information security as well as the quality of the information security processes.

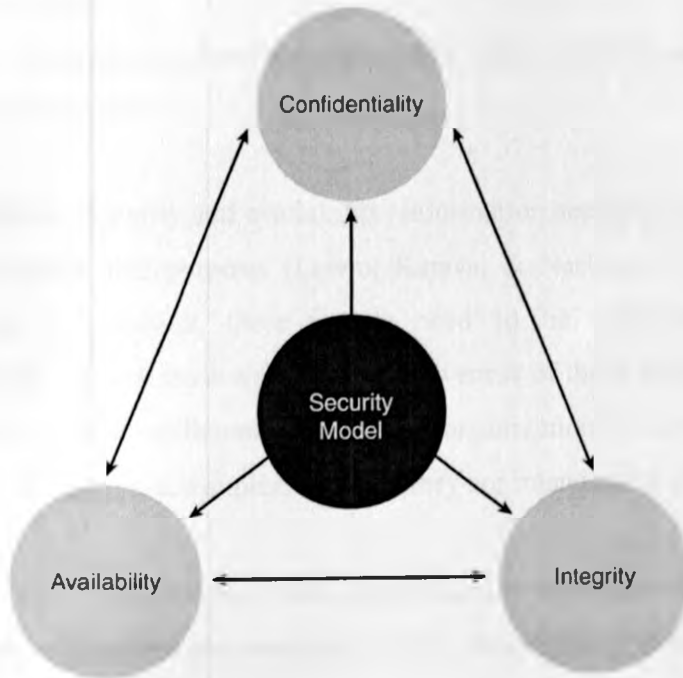
They should preferably understand how these processes relate to business management and the continuity of the organization (Eloff, Labuschagne, von Solms & Verschuren, 1999). The need for proper information security measures in all organizations cannot be questioned in today's day and age. Precisely what is meant by information security will be discussed next.



### 2.3 The CIA Model of Information Security Management

A simple but widely-applicable security model is the CIA triad; standing for Confidentiality, Integrity and Availability; three key principles which should be guaranteed in any kind of secure system. Whitson (2003) suggests that the major facets of security management are guaranteeing the confidentiality, integrity and availability of information (referred to as the 'CIA' model of security). The confidentiality, integrity and availability of security is a relatively commonly accepted 'model', whereby security can be viewed as involving a process to provide information with the CIA principles. Until recently, the CIA model models and frameworks, there lacks a commonly held view and practical implementation of a standard approach to the management of information security. It is almost as if organizations are caught somewhere between a technical CIA view of information security at one end, and true integration within corporate governance at the other end.

Fig 1: CIA model of information security



Applying the lack of consensus to the development of a practical conceptual framework for information security management thus becomes even more difficult, perhaps due in

part to the evolving uniqueness of requirements for different organizations. So while some authors agree loosely on the functions within security management (Siponen and Kajava, 1998; Andersen, 2001; Von Solms, 1999), actually applying information security functions effectively within the organizational context of the higher education sector is still a complex issue.

Information, as mentioned previously, is an important corporate asset, along with the systems and networks processing it. To ensure that an organization maintains its competitive edge, the information must be kept confidential, accurate and continuously available. Keeping this in mind, information security can therefore be classified as a combination of the following three factors (BS7799-1, 1999):

**Confidentiality** : Ensuring that those who are unauthorized to access information are prevented from doing so

**Integrity** : Ensuring that both the information and the methods by which it is processed, are accurate and complete

**Availability** : Ensuring that those users who have authorization to access information, are able to do so when required

To ensure confidentiality, integrity and availability, information security comprises mechanisms and procedures for exactly this purpose. (Leiwo, Kajava, & Nesland, 1994). To identify the appropriate technical mechanisms, three factors need to be considered. These are the functionality, assurance of correctness as well as effectiveness of these mechanisms. This means that such mechanisms should sufficiently protect an organization's information, be properly implemented and be effective in accomplishing what they are intended for (von Solms, 1999).

Besides identifying and implementing these mechanisms, organizations must furthermore educate users and other employees on issues, such as the importance of information security, the usage of information protection mechanisms, information classification and possible information risks. (Leiwo, Kajava, & Nesland, 1994). This will ensure sufficient protection of organizational information should any risks materialize.

Any information security risks could cause possible alteration, destruction, or disclosure of information, as well as a disruption in information processing. Information security provides

However, Harris further notes that until the 1980s the only computers available were mainframe computers which were, for the most part, self contained with no interconnection with extraneous computing systems (p. 17). She also states that during this time frame mainframe computers did not typically connect to other mainframe computers and that when there was a need for interconnection, it was done in a “crude fashion” for specific tasks (Harris, 2003, p. 18). At this point in time organizations did not fully depend on these systems for their survival and information security was merely an issue of securing the physical computer and its media, making sure the equipment was not stolen, damaged, or modified/. As information technology such as computer hardware equipment and software applications evolved, corporations increased their demand to harness the power and benefits of these technologies and thus become more dependent on them, notably so when personal

computers, or PCs, were introduced in the 1980s (Allen, 2002, p. 1). In the 1980s and 1990s the evolution and popularity of personal computers (PCs) in homes, businesses, and government agencies allowed for autonomous computing so that computers did not solely depend on one mainframe computer, but were now able to connect to multiple computers simultaneously via distributed, client-server computing architectures also known as networks (Allen, 2002, p. 1). Allen (2002), states that almost all organizations moved to the client-server or network model as it provided organizations the ability to sustain a visible business presence with other organizations, customers, partners, and suppliers (p. 1). Harris (2003) emphasizes that the popularity of PCs and networking for a larger audience caused computer technology to evolve rapidly in order to accommodate user demands for a variety of interfaces and applications; security and stability were not emphasized in the development of such the applications and operating systems (Harris, 2003, p. 18). Ultimately, what has emerged is the phenomenon known as the Internet, a labyrinth of computer networks boasting various degrees of security (or insecurity) attempting to access and share data [information] openly as well as clandestinely.

The evolution of information systems and information technology, according to Scheier (2003), will continue and will follow Moore’s law which predicts that the industry will double computing power of a microchip every 18 months and that the next generation of computing devices will be smaller faster, more available, and less expensive than ever before.

Increased importance of information security. Whitman & Mattord (2004) state that in today’s global markets, organizations of all types are dependent on and enabled by information

technology, which is the instrument that receives, stores, and transports information (p. 2). Harris (2003) emphasizes that public utilities, military defense systems, financial institutions, medical facilities, and every possible business sector are dependent on information technology. As a result, he points out that the level of dependence and the extent of integration that technology has attained in our lives makes information security a much more necessary and essential discipline to be addressed.

Ross et al. (2007) state the degree to which organizations have come to depend upon information and information systems to conduct routine and critical missions and business functions means that the protection of the underlying systems [and the information such systems host] is paramount to the success of the organization.

The International Standards Organization (ISO) document ISO-27002 (2005) also emphasizes that information and the supporting processes, systems, and networks are important business assets and further emphasizes the importance of protecting an organization's information stating that "defining, achieving, maintaining, and improving

Information security may be essential to maintaining a competitive edge, cash flow, profitability, legal compliance, and commercial image"

Information systems and computer technology are also used to steal money, gain personal financial information, and steal individual identity. Some government agencies and organizations use what is called Information Warfare (Harris, 2003) to gather tactical information, intercept competitor's secrets, and in some cases cause destruction of the competitor's information (p. 21).

Warren and Hutchinson (2001) state that Information Warfare is concerned with damaging a country's National Information Infrastructure (NII) which they define as the physical and virtual backbone of an information society and includes at a minimum:

- Government networks (i.e., Executive and agency offices)
- Banking and financial network including stock exchanges, money transfers
- Public utility networks and Telecommunications
- Emergency services network (including medical, police, fire, and rescue)
- Private corporate and institutional networks
- Educational and research networks.

## **2.5 Measurement of Security Management**

The process of managing security needs a reference to ensure that all the necessary areas are being covered, and requires quantification to determine the level of security that is being implemented, identification of what is lacking and to track effectiveness of control measures (Martins and Eloff, 2001). A problem with not applying some type of management system to security is that it's likely to result in either too many controls or not enough controls being applied to areas within the organization. An ad-hoc approach to information security from a management standpoint, therefore, has the potential to be ineffective, and measurement becomes difficult. Measurement of the effectiveness of security is an important yet difficult process. In order to gain commitment from senior management, not only is it necessary to align security with business goals, but also to demonstrate that the application of security is effective to those goals, therefore having benefits that can be evaluated and measured.

The difficulty in evaluating the benefits of information security is considered one of the reasons for reluctance by senior management to invest in information security (Kankanhalli et al., 2003). May (2003) advocates that meeting the principles contained in standards can help measure and improve existing security processes and procedures. Obviously this would be accompanied by performing risk assessments and internal reviews.

## **2.6 Policy as a foundation to security management**

Higgins (1999) suggests that information security policy is a prerequisite to security management. Security policy is considered as being the foundation for applying information security within the organization. There is a high degree of consensus overall that effective information security management is dependent on the existence and practical application of security policy (Fulford and Doherty, 2003). Implementation of security policy is noted widely in literature as having a highly significant correlation to successful information security. The relationship between effective information security policy and an effective ISMS is also established within the literature (ECAR,2003).

According to Wood (2002) security policies are pivotal to enabling processes within the organization. Information security policy is increasingly critical to the continued operation of information systems and, as with other aspects of strategic importance, policy needs to be

addressed and driven at a high level within the organization. The open literature evidences a growing acknowledgement and emphasis on information security within organizations (Ernst and Young 2003, AusCERT 2003). Correspondingly there has been an associated increase in the uptake of security implementation measures, including development and deployment of security policies.

Dhillon looks at the requirement for organizations to address security through effective security policy, and suggests that policy adoption is very low, requiring more effective approaches. Baskerville and Siponen (2002) argue that an increasing trend towards 'emergent' organizations (those organizations experiencing significant structural and IT related change) has resulted in often federated and emergent policy with little guidance on how policies should actually be developed.

Information security should be provided as a service to enable the organization's priorities. As a service, however, it can be adversely affected by inappropriate application of security policy. This indicates that an effective development and implementation process is necessary. An effectively implemented security policy should not only indicate the required behavior from users but should also reflect the objectives of the organization so that users do not see it as a necessary evil (Hone and Eloff, 2002b). It should be done in a way that is relevant to the end users, be enforceable and appropriately reflect the direction of the organization. Security policy therefore plays a key role in providing direction for the organization on information security. Policy needs to be linked to an associated high level management commitment which, when combined with user awareness, gives an appropriate organizational context for the implementation of, and compliance with, information security.

Although policies tend to specify how the organization should operate, they are only relevant if they are implemented within supportive operational structures and actually complied with. To be meaningful, policies must provide individuals with an understanding of their responsibilities. Compliance completes the process. For these reasons security policy can be a difficult process. Policy must not only reflect security objectives but a number of other factors as well which are critical to the relevance, usefulness and applicability of the policy. These include relating policy

objectives to wider organizational objectives, having an appropriate development process for policy including content and structure, and encouraging compliance as well as providing mechanisms for enforcing policy. Processes for breaches of policy are also management.

Fulford and Doherty (2003) in their investigation on the application of information security policies in large organizations, noted the paucity of research on security policy aside from content focused research. The uptake of policy in terms of gaining top level management support and attaining compliance at all levels to policy is another major problem.

## **2.7 Security adoption rates of awareness**

Literature research indicates that effective information security awareness, either in some basic measurable fashion or as a fully developed structured program, is far from being widely implemented in many organizations. A survey conducted by Ernst and Young (2003) Global Information Security Survey found that only 35% of organizations surveyed had a formal information security awareness program in place, and that funding for awareness and training ranked as a low priority. In another global information survey conducted in 2002 of midsize and large firms, less than 50% of the 459 CIOs and IT Directors advised that they had a security awareness and training program in place (Kankanhalli et al., 2003).

The literature evidences that security awareness is an important function, yet it is under funded, under-represented and generally applied in an ad hoc process and in a reactive manner. Security awareness is therefore highly unstructured in most organizations and can be seen as operating on a spectrum ranging from either ignoring it, or developing interesting study conducted by Adams and Sasse (1999) on the compromises of security in relation to password management identified a number of contributing factors. Importantly, these included insufficient communication from security sections in organizations to users, which caused users to construct their own models of reality on possible security threats and the importance of security.

## **2.8 Compliance with Security**

A theme relating to awareness involves the concept of instilling into the organization a 'culture of compliance' towards information security (Furnell et al., 2000). The idea behind this is that the culture of the organization, which includes its values and norms of behavior, including descriptive and prescriptive behavior, its overarching policies, and higher level management support, results in a 'culture of compliance'. An organization with this type of culture has a level of compliance that is not only demonstrated from 'the top', but includes norms for security guidelines and practices that are invariably followed by all in the organization.



A culture of compliance in this case, would include an awareness of, followed by compliance with, information security policies, processes and guidelines, as part of its norms, values and culture. Compliance in this research will be based on the relationship between the ministry's security posture and, consequently, the policy security requirements and levels of compliance reflected at all levels of the ministry community through a 'culture of compliance'.

Research by Gartner and AMR (Haldar and Forsyth, 2004) conclude that many enterprises remain inadequately protected from security threats because of the perceived high cost of an effective security strategy that suits the organization's culture. The lack of focus on security strategy has led to an emphasis on products and technologies instead of a security strategy that incorporates security awareness, training, and policy and standards in an effort to develop a 'culture of compliance' towards information security. An effective commitment to security requires that a process be in place that suits the culture of the organization (Spurling, 1995; Leach 2003). Compliance in information security needs to be based on a balance between corporate security needs and yet remain supportive of work practices. The concept of creating a 'culture of compliance' within the ministry is a central point and is likely to be improved when the rationale for security requirements is understood.

## **2.9 Information security management frameworks**

A range of standards and frameworks has been developed in recent years that has helped shift the focus away from the previously narrow view of security (represented by the CIA model) to a wider framework). These types of frameworks take into account business perspectives, including not only a range of measures but also a focus on organizational structure, policy, and the capacity for measurement and certification.

An emerging concept leading from the development of these frameworks, and related to the application of management to information security, is the use of an 'Information Security Management System' (ISMS) based on recognized standards. An ISMS provides a management framework which the organization can reference, and is designed to meet the needs of the individual organization. Information Security Management Systems are in effect, an organizational framework for the operation of information security. The primary purpose of an

ISMS is concerned with the way, process or method in which information security is managed from an organizational perspective. From this perspective ISMSs are considered to be a helpful reference to the process of managing It follows that a key issue in relation to an ISMS is understanding the organizational requirements. Due to the nature of technology, organizational structures and processes as well as collaborative requirements in ministries, a flexible or dynamic solution is often required in an ISMS. Information security for universities in the future will therefore need to take into account organizational operations and context (Dhillon and Backhouse, 2000; Siponen and Kajava, 1998; Anderson, 2003).

## **2.10 COMMERCIAL STANDARDS FOR INFORMATION SECURITY**

### **2.10.1 ISO standards**

The International Organization for Standardization (ISO), established in 1947, is a non-governmental international body that collaborates with the International Electro technical Commission (IEC) and the International Telecommunication Union (ITU) on information and communications technology (ICT) standards. The following are commonly referenced ISO security standards:

#### **2.10.1.1 ISO/IEC 27002:2005 (Code of Practice for Information Security Management)**

ISO/IEC 27002:2005 (replaced ISO/IEC 17799:2005 in April 2007) is an international standard that originated from the BS7799-1, one that was originally laid down by the British Standards Institute (BSI). ISO/IEC 27002:2005 refers to a code of practice for information security management, and is intended as a common basis and practical guideline for developing organizational security standards and effective management practices This standard contains guidelines and best practices recommendations for these security domains: (a) security policy; (b) organization of information security; (c) asset management; (d) human resources security; (e) physical and environmental security; (f) communications and operations management; (g) access control; (h) information systems acquisition, development and maintenance; (i) information

security incident management; (j) business continuity management; and (k) compliance. among these 10 security domains, a total of 39 control objectives and hundreds of best-practice information security control measures are recommended for organizations to satisfy the control objectives and protect information assets against threats to confidentiality, integrity and availability.

### **2.10.1.2 ISO/IEC 27001:2005 (Information Security Management System - Requirements)**

The international standard ISO/IEC 27001:2005 has its roots in the technical content derived from BSI standard BS7799 Part 2:2002. It specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System (ISMS) within an organization. It is designed to ensure the selection of adequate and proportionate security controls to protect information assets. This standard is usually applicable to all types of organizations, including business enterprises, government agencies, and so on. The standard introduces a cyclic model known as the “Plan-Do-Check-Act” (PDCA) model that aims to establish, implement, monitor and improve the effectiveness of an organization’s ISMS. The PDCA cycle has these four phases:

- a) “Plan” phase – establishing the ISMS
- b) “Do” phase – implementing and operating the ISMS
- c) “Check” phase – monitoring and reviewing the ISMS
- d) “Act” phase – maintaining and improving the ISMS

Often, ISO/IEC 27001:2005 is implemented together with ISO/IEC 27002:2005. ISO/IEC 27001 defines the requirements for ISMS, and uses ISO/IEC 27002 to outline the most suitable information security controls within the ISMS.

ISO/IEC 27002 is a code of practice that provides suggested controls that an organization can adopt to address information security risks. These controls are not mandatory. There is therefore no certification for ISO/IEC 27002, but a company can be certified compliant with ISO/IEC 27001 if the management process follows the ISMS standard. There is a list of accredited

certification bodies that can certify an organization against the ISMS standard, which is maintained on the UK Accreditation Service website.

### **2.10.1.3 ISO/IEC 15408 (Evaluation Criteria for IT Security)**

The international standard ISO/IEC 15408 is commonly known as the "Common Criteria" (CC). It consists of three parts: ISO/IEC 15408-1:2005 (introduction and general model), ISO/IEC 15408-2:2005 (security functional requirements) and ISO/IEC 15408-3:2005 (security assurance requirements). This standard helps evaluate, validate, and certify the security assurance of a technology product against a number of factors, such as the security functional requirements specified in the standard.

Hardware and software can be evaluated against CC requirements in accredited testing laboratories to certify the exact EAL (Evaluation Assurance Level) the product or system can attain. There are 7 EALs: EAL1 - Functionally tested, EAL2 - Structurally tested, EAL3 - Methodically tested and checked, EAL4 - Methodically designed, tested and reviewed, EAL5 - Semi-formally designed and tested, EAL6 - Semi-formally verified, designed and tested, and EAL7 - Formally verified, designed and tested. A list of accredited laboratories as well as a list of evaluated products can be found on the Common Criteria portal<sup>13</sup>. The list of products validated in the USA can be found on web-site of the Common Criteria Evaluation and Validation Scheme for IT Security (CCEVS)

### **2.10.1.4 ISO/IEC 13335 (IT Security Management)**

ISO/IEC 13335 was initially a Technical Report (TR) before becoming a full ISO/IEC standard.

It consists of a series of guidelines for technical security control measures:

- a) ISO/IEC 13335-1:2004 documents the concepts and models for information and communications technology security management.
- b) ISO/IEC TR 13335-3:1998 documents the techniques for the management of IT security. This is under review and may be superseded by ISO/IEC 27005.
- c) ISO/IEC TR 13335-4:2000 covers the selection of safeguards (i.e. technical security controls). This is under review and may be superseded by ISO/IEC 27005.

- d) ISO/IEC TR 13335-5:2001 covers management guidance on network security. This is also under review, and may be merged into ISO/IEC 18028-1, and ISO/IEC 27033.

### **2.10.2 Payment card industry data security standard**

The Payment Card Industry (PCI) Data Security Standard (DSS) was developed by a number of major credit card companies (including American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International) as members of the PCI Standards Council to enhance payment account data security. The standard consists of 12 core requirements, which include security management, policies, procedures, network architecture, software design and other critical measures. These requirements are organized into the following areas:

1. Build and Maintain a Secure Network
2. Protect Cardholder Data
3. Maintain a Vulnerability Management Program
4. Implement Strong Access Control Measures
5. Regularly Monitor and Test Networks
6. Maintain an Information Security Policy

### **2.10.3 COBIT**

The Control Objectives for Information and related Technology (COBIT) is “a control framework that links IT initiatives to business requirements, organizes IT activities into a generally accepted process model, identifies the major IT resources to be leveraged and defines the management control objectives to be considered”. The IT GOVERNANCE INSTITUTE (ITGI) first released it in 1995, and the latest update is version 4.1, published in 2007. COBIT 4.1 consists of 7 sections, which are (1) Executive overview, (2) COBIT framework, (3) Plan and Organize, (4) Acquire and Implement, (5) Deliver and Support, (6) Monitor and Evaluate, and (7) Appendices, including a glossary. Its core content can be divided according to the IT processes.

COBIT is increasingly accepted internationally as a set of guidance materials for IT governance that allows managers to bridge the gap between control requirements, technical issues and business risks. Based on COBIT 4.1, the COBIT Security Baseline focuses on the specific risks

around IT security in a way that is simple to follow and implement for small and large organizations. COBIT can be found at ITGI18 or the Information Systems Audit and Control Association (ISACA) websites.

#### **2.10.4 ITIL (or ISO/IEC 20000 series)**

The Information Technology Infrastructure Library (ITIL) is a collection of best practices in IT service management (ITSM), and focuses on the service processes of IT and considers the central role of the user. It was developed by the United Kingdom's Office of Government Commerce (OGC). Since 2005, ITIL has evolved into ISO/IEC 2000021, which is an international standard within ITSM.

An ITIL service management self-assessment can be conducted with the help of an online questionnaire maintained on the website of the IT Service Management Forum. The self-assessment questionnaire helps evaluate the following management areas: (a) Service Level Management, (b) Financial Management, (c) Capacity Management, (d) Service Continuity Management, (e) Availability Management, (f) Service Desk, (g) Incident Management, (h) Problem Management, (i) Configuration Management, (j) Change Management, and (k) Release Management.

### **2.11 Regulations related to information security**

In addition to the various industry standards bodies and guidelines, certain regulated businesses, such as banking, may need to observe the regulations and guidelines specified by their own industry or professional regulatory bodies

#### **2.11.1 SOX**

After a number of high profile business scandals in the US, including Enron and WorldCom, the Sarbanes-Oxley Act of 2002 (SOX) was enacted as legislation in 2002. This act is also known as the “Public Company Accounting Reform and Investor Protection Act”. The purpose is to “protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes”. This regulation affects all companies listed on stock exchanges in the US. In section 404, the SOX requires “each annual report ...

contain an internal control report ... [that] contains an assessment of ... the effectiveness of the internal control structures and procedures of the issuer for financial reporting". As information technology plays a major role in the financial reporting process, IT controls would need to be assessed to see if they fully satisfy this SOX requirement.

Although information security requirements have not been specified directly in the Act, there would be no way a financial system could continue to provide reliable financial information, whether due to possible unauthorized transactions or manipulation of numbers, without appropriate security measures and controls in place. SOX requirements indirectly compel management to consider information security controls on systems across the organization in order to comply with SOX.

### **2.11.2 COSO**

The COSO (Committee of Sponsoring Organizations of the Treadway Commission) framework is a framework that initiates an integrated process of internal controls. It helps improve ways of controlling enterprises by evaluating the effectiveness of internal controls. It contains five components:

1. Control Environment, including factors like integrity of people within the organization and management authority and responsibilities;
2. Risk Assessment, aiming to identify and evaluate the risks to the business;
3. Control Activities, including the policies and procedures for the organization;
4. Information and Communication, including identification of critical information to the business and communication channels for delivering control measures from management to staff;
5. Monitoring, including the process used to monitor and assess the quality of all internal control systems over time.

The COSO framework and the COBIT framework described above are both used to satisfy compliance with SOX.

### **2.11.3 HIPAA**

The Health Insurance Portability And Accountability Act (HIPAA) of 1996 is a US law designed to improve the portability and continuity of health insurance coverage in both the group and individual markets, and to combat waste, fraud, and abuse in health insurance and health care delivery as well as other purposes. The Act defines security standards for healthcare information, and it takes into account a number of factors including the technical capabilities of record systems used to maintain health information, the cost of security measures, the need for training personnel, the value of audit trails in computerized record systems, and the needs and capabilities of small healthcare providers. A person who maintains or transmits health information is required to maintain reasonable and appropriate administrative, technical, and physical safeguards to ensure the integrity and confidentiality of that information. In addition, the information should be properly protected from threats to the security and integrity of that information, unauthorized uses, or unauthorized disclosure.

The full set of rules regarding adoption of the HIPAA standards for the security of electronic health information and privacy of personal health information can be found in US Department of Health and Human Services website.

### **2.11.4 FISMA**

FISMA stands for Federal Information Security Management Act, and is a part of the US E-Government Act (Public Law 107-347) that became legislation in 2002. It requires US federal agencies to develop, document, and implement an agency-wide programme to provide information security for the information (and information systems) that support the operations and assets of the agency. Some of the requirements include:

1. Periodic risk assessments of information and information systems that support the operations and assets of the organization
2. Risk-based policies and procedures designed to reduce information security risks to an acceptable level
3. Plans for providing adequate security for networks and information systems
4. Security awareness training to all personnel, including contractors



5. Periodic evaluation and testing of the effectiveness of the security policies, procedures and controls. The frequency should not be less than annually. Remedial action to address any deficiencies found to be properly managed.
6. A working and tested security incident handling procedure
7. A business continuity plan in place to support the operation of the organization.

### **2.11.5 FIPS**

The Federal Information Processing Standards (FIPS) Publication Series of the National Institute of Standards and Technology (NIST) is an official series of publications relating to standards and guidelines adopted and made available under the provisions of the FISMA<sup>30</sup>. FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems, is the first mandatory security standard laid down under the FISMA legislation. FIPS Publication 200, entitled “Minimum Security Requirements for Federal Information and Information Systems” is the second mandatory set of security standards that specify minimum security requirements for US federal information and information systems across 17 security-related areas. US federal agencies must meet the minimum security requirements defined in this standard by selecting appropriate security controls and assurance requirements laid down in NIST Special Publication 800-53 (Recommended Security Controls for Federal Information Systems). The 17 security-related areas include: (a) access control; (b) awareness and training; (c) audit and accountability; (d) certification, accreditation, and security assessments; (e) configuration management; (f) contingency planning; (g) identification and authentication; (h) incident response; (i) maintenance; (j) media protection; (k) physical and environmental protection; (l) planning; (m) personnel security; (n) risk assessment; (o) systems and services acquisition; (p) system and communications protection; and (q) system and information integrity.

## **CHAPTER THREE:**

### **RESEARCH METHODOLOGY**

#### **3.1 Introduction**

This chapter presents the methodology used in this research. Research methodology is a system of explicit rules and procedure upon which research is based and against which claims for knowledge are evaluated (Nachmias and Nachmias, 1996). It focused on the sources of data and their collection techniques, the sampling procedure to be adopted and tools for data presentation analysis and interpretation.

#### **3.2 Research Design**

The research design was a case study meant to investigate the information security management practices at the Ministry of Youth Affairs and Sports. A case study is an intensive analysis of an individual unit (e.g., a person, group, or event) stressing developmental factors in relation to context (wikipedia.org)

The COGIT, which is a derivative of COBIT information security framework will be used in this research as a reference to test the existing information security practices in the ministry.

#### **3.4 Target Population**

The target population was both managerial, technical and operational staff in the ministry using the various systems. The sample targeted officers from the key functional departments where systems are administered and used namely the ICT, The Accounts, Finance, Procurement and the Human Resource department. This sample was specifically be targeted because they were involved in the day to day operation and therefore are the ones who ensure compliance. Senior officers and administrators were also be targeted to shed light on policy direction and implementation.

#### **3.5 Sampling Design and Sample Size**

Random sampling design was used. The study involved a population of Eighty (80) officers drawn from functional departments in the ministry where the Information systems are used namely the ICT unit, the Accounts unit, the Finance unit, the Procurement unit, The Human Resource unit, Department of Youth Training and the Department of Youth Development and the Administration. Each of these groups interacts with the information in different levels and therefore it is envisaged that they have different views of information.

### **3.6 Data Collection Procedures**

The study used both primary and secondary data. Primary data was obtained through observation, interviews and self-administered questionnaires. Questionnaires contained both structured and unstructured questions. The closed ended questions enabled the researcher to collect quantitative data while open-ended questions enabled the researcher to collect qualitative data.

Secondary data was collected by use of desk search techniques from published reports and other publications. Secondary data was sourced from government's publications, reports, journals and policy documents. The study also involved face-to-face interviews with the officers using information systems and the administration so as to collect their views on Information security management procedures in the ministry.

### **3.7 Data Analysis and Presentation**

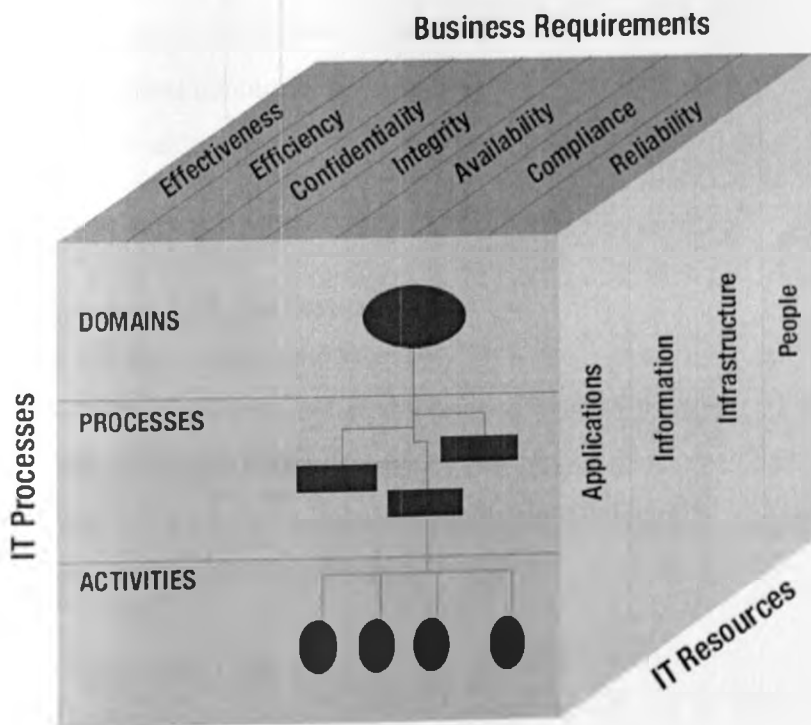
The data collected was analyzed using descriptive statistics. The data was summarized, coded and tabulated. Descriptive statistics such as means, standard deviation and frequency distribution were used to analyze the data. Data presentation was done by the use of percentages and frequency tables. Data was coded and entered into the Statistical Package for Social Sciences (SPSS) for analysis. SPSS was used to perform the analysis and it aided in organizing and summarizing the data by the use of descriptive statistics such as means, standard deviation and frequency distribution tables.

## CHAPTER FOUR

### 4.1 THE CONTROL OBJECTIVES FOR GOVERNMENT INFORMATION AND RELATED TECHNOLOGIES (COGIT)

The researcher constructed a derived model based on the cobit which was referred to as Control Objectives for Government Information Technology (Cogit). This is a customized model derived from the COBIT framework.

The COBIT framework explains how IT processes deliver the information that the business needs to achieve its objectives. This delivery is controlled through 34 high-level control objectives, one for each IT process, contained in the four domains. The Framework identifies which of the seven information criterion (effectiveness, efficiency, confidentiality, integrity, availability, compliance and reliability), as well as which IT resources (people, applications, technology, facilities and data) are important for the IT processes to fully support the business objective. The figure below shows the COBIT framework.



The researcher customized the COBIT model to suit the government functions and IT objectives to form the Control Objectives for Government Information Technologies, (COGIT). The four domains in COBIT namely, Planning and organization, Acquisition and Implementation; Delivery and support; and Monitoring.

The researcher came up with nine processes that are related to IT security function in the government namely;

- IT planning and organization
- Organizational security
- Asset classification and control
- Personal security
- Physical and environmental security
- Communication and operation management
- Access control
- System development and maintenance
- Business continuity management

Thirty activities under the under the nine processes were identified as follows;

**The activities under the processes are as follows;**

#### **4.2 Planning and Organization**

- Definition of Roles and responsibilities.
- Availability of documented information security policy
- Staff awareness of security policy
- Staff education and training on information security

#### **4.3 Organizational Security**

- Responsibility for information security (hierarchy in the organization)
- Availability of expertise on information security,
- Authorization for use of Information Systems

#### **4.4 Asset Classification and control**

- Ability for the organization to locate all assets (including software, hardware, staff and services )
- Ability to control local and remote access
- Knowledge of staff know what to do with information with regard to its storage, usage, archiving, back-up and destruction

#### **4.5 Personal security**

- Knowledge of staff on procedure in case of incidents
- Training of staff on basic security of information e.g. locking of computers etc.
- Availability of formal disciplinary process for employees who have violated security policies

#### **4.6 Physical and environmental security**

- Knowledge of existence of high valuable portable goods e.g. laptops
- Appropriateness of physical and environmental security procedures in place to prevent interference with business premises and information systems
- Staff who travel with portable computers are aware of the risk relating to theft and the potential liability through compromised data
- Visitors to the organization are always escorted around the building and are never left to wander on their own
- Servers are maintained in air conditioned , fire retardant power conditioned secure facilities

#### **4.7 Communication and operation management**

- In the event of equipment failure, theft or a site disaster, data backup and storage would enable the organization to retrieve information with minimal business interruptions
- If Systems are updated/upgraded according to a structured plan and not in an ad-hoc fashion

- In the event of a security incident, there is a procedure which clearly define what to do and who to call for assistance
- If Antivirus systems are up-to date and in the event of a virus outbreak, we could be able to prevent our systems as best as possible
- If Systems are adequately protected by our internet service providers (ISP) security and / our own firewalling systems
- Appropriateness of mechanisms in place to authenticate users logging into our systems

#### **4.8 Access control**

- Levels of control of access .. E.g Users if may log on/ gain access to our systems without being formally registered by their own user accounts
- Password management.... If a password management system is in place which specifies the frequency of password changes as well as minimum password complexity e.g. password must be changed after every two weeks with X characters
- If the organization controls access to information via access control policy which specifies which users have access to what data
- If there is a mechanism to ensure processing facilities are only used for authorized business purposes

#### **4.9 System development and maintenance**

- Mode of acquisition of systems
- Ability of systems to provide audit trails

#### **4.10 Business continuity management**

- If the organization has business continuity plans which specifies who must take what action and what has to be done to ensure that the ministry can continue functioning in the event of a disaster such as fire/ floods
- If there is a nominated person in the ministry who is responsible for BCM
- If security policies have been reviewed within the last year.

## CHAPTER FIVE:

### RESEARCH FINDINGS AND DISCUSSIONS

#### 5.1 INTRODUCTION

This chapter presents a detailed discussion of the research findings in an attempt to achieve the objectives of the study. Data was analyzed through two main ways: Quantitative analysis by making use of statistical techniques and by qualitative analysis.

The researcher was able to collect 76 questionnaires out of the 80 that were administered. First, the researcher wanted to know the perception of the respondents towards Information Security management and hence the question if they consider information security management as an issue that the government should be concerned with. 73.3% of the respondents strongly agreeing with the statement and 26.3% agree. None of the respondents was undecided or disagreed.

**Table 1 : Perception of staff towards Information Security Management**

	Frequency	Percent
Strongly agree	56	73.7
Agree	20	26.3
Total	76	100.0

#### 5.2. SECURITY BREACHES

The researcher further wanted to know, if in the last one year, the respondents had experienced any Information Security breaches.

Table 2 below shows the respondents to the various security breaches.

Security Breaches	Yes	%	No	%	Not responded	%
Inadvertent breach ( e.g. user accidentally deletes file or changes computer configurations)	24	31.6	40	52.6	12	15.8
Deliberate attack (e.g. hacker, disgruntled staff gains access , deleting or stealing data)	28	36.8	32	42.1	16	21.1
Asset theft	24	31.6	32	42.1	20	26.3



Equipment failure	56	73.7	8	10.5	12	15.8
Back up failure	28	36.8	28	36.8	20	26.3
Data theft	8	10.5	48	63.2	20	26.3
Site disaster	12	15.8	44	57.9	20	26.3
Copyright infringement (e.g. staff copying pirated software)	12	21.1	36	47.4	24	31.6
Compliance (e.g. passing of information to unauthorized people)	8	10.5	48	63.2	20	26.3

The above data confirms that in the past one year, most of the respondents had experienced some information security breaches which to the opinion of the researcher is consequential. Information being an asset to the institution, it is important that it be treated like the other high value assets for example money. In an optimal situation, there are not supposed to be any security breach as it could lead to direct losses to the institution. 31.6% of the respondents indicate that there has been accidental loss of data/configurations, 36.8 % indicate that there has been a deliberate attack to information resources. This comes in the wake of a recent hacking activity to the Kenya government websites, [www.xxxx.go.ke](http://www.xxxx.go.ke).

A whopping 73.7% indicate that there have been equipment failure, while 36.8 indicate that there have been back up failure. Other breaches, namely data theft, site disaster, copyright infringement and unauthorized passing of information account for lesser breaches, but can be of monumental effects if they happen on critical operations of the ministry.

### 5.3 Levels of compliance to key business roles linked to IT

The researcher set to find out the perceived level of compliance to the key business roles that are linked to IT. The respondents were supposed to assess the level of compliance by indicating if they Strongly agree, agree, are undecided, disagree or strongly disagree to the maturity statements of the nine processed that the researcher identified namely : IT planning and organization; Organizational security; Asset classification and control; Personal security; Physical and environmental security; Communication and operation management; Access control; System development and maintenance and Business continuity management

Maximum points (5) were be assigned to the parameter “strongly agree” and the least (0) to the strongly disagree. An average of the respondents was be calculated, which in turn will be

computed using the COBIT metrics to give the COBIT score. All the COBIT scores were added to show the maturity level of that particular IT goal.

### 5.3.1 IT Planning and organization

The objective provide management direction and support for information security in accordance with business requirements and relevant laws and regulations. Management should set a clear policy direction in line with business objectives and demonstrate support for, and commitment to, information security through the issue and maintenance of an information security policy across the organization.

#### Findings

**Table 3: IT planning and organization**

<b>IT Planning and organization</b>	<b>Strongly agree</b>	<b>Agree</b>	<b>Undecided</b>	<b>Disagree</b>	<b>Strongly Disagree</b>
Roles and responsibilities for information security in the ministry are well defined e.g. someone is responsible for back-ups, registering users on the system, planning against disaster, liaising with service providers	4	32	8	24	4
We have a documented information security policy	0	20	20	28	4
Staff are aware of security policy	0	12	12	40	8
All staff are given adequate and appropriate information security education and training	0	12	4	36	16
Staff are well informed as to what is considered to be acceptable and unacceptable usage of information systems e.g. e-mail and internet conduct	0	16	4	44	8
<b>Total</b>	<b>4</b>	<b>92</b>	<b>48</b>	<b>152</b>	<b>40</b>
Total Number/Total respondents/Number of objectives	0.01	0.25	0.12 6	0.4	0.10
Maturity score	0.05	1	0.37 8	1.2	0.1

Maturity level for Security Policy is 2.7.

The key finding is that there is no formal, documented security policy in existence at. During interviews, some staff assumed a policy was in place, due to their understanding that security

was only about passwords. However, at a global view, the e-government policy is available that the ICT unit has adopted to its use.

The data shows that 52.94 % agree and that roles and responsibilities for information security have been well defined, but 61.53 % (disagree and strongly disagree) indicate that there is either no documented information security policy or it does not exist at all. 76.47 % indicate that staff are not given appropriate information and security training. 76.47 % also indicate that they are not adequately informed on what is considered to be acceptable and unacceptable usage of information systems.

This therefore implies, according to the maturity model that IT strategic planning is understood by IT management, but is not documented. IT strategic planning is performed by IT management, but only shared with business management on an as needed basis. Updating of the IT strategic plan occurs only in response to requests by management and there is no proactive process for identifying those IT and business developments that require updates to the plan. Strategic decisions are driven on a project-by-project basis, without consistency with an overall organization strategy. The risks and user benefits of major strategic decisions are being recognized, but their definition is intuitive.

### **Key Issues Surrounding Security Policy**

For policy to be effective, several attributes were noted as being required. These include senior management support, appropriateness of policy to the organization, awareness of policy and its meaning, and available procedures for implementation. The major themes stemming from this area are several. Development of policy in terms of the actual writing of policy, coverage of policy and how policy should be constructed were raised as issues. The appropriate context for policies, including business requirements down to the low level procedures for policies appeared to often be 'missing links' for final implementation of policy.

An analysis of these issues concludes that several factors contribute to policy ineffectiveness. Firstly and foremost, ensuring and monitoring compliance with security policy is difficult. Secondly, the process of policy development itself does not ensure that policies are going to be supported by the government. Policies can often be information and direction, as well as high

level organizational direction (Hone and Eloff, 2002a). The information security policy should be written in a way that is completely user focused.

It should be noted however that developing security policy solely on information security international standards has some shortcomings (Baskerville and Siponen, 2002). Firstly, these standards do not take into account that organizations differ, and therefore security requirements will differ.

## IT organization

Table 4: IT Organization

Section B: IT Organization		Strongly Agree	Agree	Undecided	Disagree	Strongly disagree
	A director (or equivalent) member of staff has a responsibility for information security	4	40	8	12	8
	Expertise on information security is available and where not, external advice is sought	2	36	12	12	8
	Third party (outsider) access to our information system requires approval by a senior manager	16	24	28	4	0
	<b>Total</b>	24	100	48	28	16
	Total Number/Total respondents/Number of objectives	0.1 0	0.4 4	0. 21	0.13	0. 07
	Maturity score	0.5	1.7 6	0. 63	0.26	0. 07

### Maturity for IT organization is 3.22

The data shows that 61 % agree that a director or equivalent has the responsibility over information security management. Many of the respondents also agree that expertise on information security is available and where not, it is sought. The data also shows that approval is always sought from senior management for outsiders to access information.

It was revealed in the interviews that overall responsibility for security management often defaults to technical administrators or security officers with insufficient authority or knowledge of the ministry's higher objectives. This is often due to information security being seen as 'IT Security' instead of 'Information Security'. Although this is a seemingly slight difference it is

one that differentiates between a perception of 'it's an IT problem' and a perception of 'it's a business problem'. Information security strategies developed under these circumstances tends to lack ownership and stakeholder collaboration, and can result in important objectives not being considered properly, particularly business goals. Further, adopting this approach does not address enforceability or maintenance of policy.

There is an implicit understanding of the need for of an IT organization; however, roles and responsibilities are neither formalized nor enforced. The IT function is organized to respond tactically, but inconsistently, to customer needs and vendor relationships. The need for a structured organization and vendor management is communicated, but decisions are still dependent on the knowledge and skills of key individuals. There is an emergence of common techniques to manage the IT organization and vendor relationships.

As noted by Hone and Eloff (2002a), difficulties are also associated with this process in that they do not truly reflect the culture of the organization. An end result of this is that they do not result in a document that effectively provides relevant direction for information security in the organization. This is a key issue as a theme emerging from data analysis indicated that the relevant issues were more associated with engaging people in information security management.

Overally, the data tends to indicate that the processes are defined. roles and responsibilities for the IT organization and third parties exist. The IT organization is developed, documented, communicated and aligned with the IT strategy. This is consistent with existing information of the implementation of the e-government strategy in all ministries.

## 5.4 Asset Classification and Control

**Table 5: Asset Classification and Control**

<b>Asset classification and control</b>	<b>Strongly Agree</b>	<b>Agree</b>	<b>Undecided</b>	<b>Disagree</b>	<b>Strongly disagree</b>
We can identify and locate all assets (including software, hardware, staff and services ) used in information handling	8	24	20	20	0
We control local and remote access to our information assets adequately	0	40	16	16	0
Our staff know what to do with information with regard to its storage, usage, archiving, back-up and destruction	0	20	28	8	0
<b>Total</b>	8	84	64	44	0
Total Number/Total respondents/Number of objectives	0.0 1	0.25	0.1 2	0.4	0
Maturity score	0.0 5	1	0.3 6	0.8	0

### **Maturity: 2.21**

The findings show the awareness of the need to protect and control the physical computing environment is recognized and evident in the allocation of budgets and other resources. Environmental controls are implemented and monitored by the operations personnel. Physical security is an informal process, driven by a small group of employees possessing a high-level of concern about securing the physical facilities. The facilities maintenance procedures are not well documented and rely upon the best practices of a few individuals. The physical security goals are not based on any formal standards and management does not ensure that security objectives are achieved.

## 5.5 Personal Security

Table 6: Personal security

Section D Personal security		Strongly Agree	Agree	Undecided	Disagree	Strongly disagree
	Staff are aware that security incidents must be reported to management immediately	24	16	16	16	0
	Staff have been trained to secure their computers at all times when moving from their work stations e.g. locking and logging off their computers when going to tea break or lunch	8	20	8	24	16
	There is a formal disciplinary process for employees who have violated our security policies and practices	0	20	20	24	8
	<b>Total</b>	32	56	64	64	24
	Total Number/Total respondents/Number of objectives	0.21	0.36	0.42	0.42	0.15
	Maturity score	0.6	1.44	1.26	0.84	0.15

### Maturity 4.21

The data shows that staff are generally aware that security incidents must be reported, though staff have not been trained adequately on security management. A formal process has not been put in place to ensure that violations to information security are taken seriously. The data however shows that this area, standards are well enforced.

There is an emerging understanding that IT risks are important and need to be considered. Some approach to risk assessment exists, but the process is still immature and developing. The assessment is usually at a high-level and is typically applied only to major projects. The assessment of ongoing operations depends mainly on IT managers raising it as an agenda item, which often only happens when problems occur. IT management has not generally defined procedures or job descriptions dealing with risk management.

Discussions on this area of security awareness highlighted that awareness raising activities are not well structured. Awareness is raised predominantly by occurrence of incidents rather than a

structured, targeted program of activities. Although the ministry engages in security awareness activities, these tend to be along the lines of bulletins, emails etc and are neither comprehensive nor targeted in their approach, or cannot in any way be described as active campaigns.

## 5.6 Physical and environmental Security

Table 7: Physical and environmental security

<b>Section E: Physical and environmental security</b>	<b>Strongly Agree</b>	<b>Agree</b>	<b>Undecided</b>	<b>Disagree</b>	<b>Strongly disagree</b>
Our organization contains high value portable goods or stock	20	32	8	12	0
We have appropriate physical and environmental security procedures in place to prevent interference with business premises and information systems	12	40	4	16	0
Staff who travel with portable computers are aware of the risk relating to theft and the potential liability through compromised data	16	24	12	16	4
Visitors to our organization are always escorted around the building and are never left to wander on their own	16	24	12	16	4
Our servers are maintained in air conditioned , fire retardant power conditioned secure facilities	8	28	16	8	12
<b>Total</b>	<b>72</b>	<b>148</b>	<b>52</b>	<b>68</b>	<b>20</b>
Total Number/Total respondents/Number of objectives	0.1 8	0.38	0.1 3	0.17	0.0 5
Maturity score	0.9	1.52	0.3 9	0.34	0.0 5

### Maturity Level 3.2

The table above shows that the ministry contains high value and portable goods, and to a large extent, staff consider are aware of the risks involving data loss. It further shows that visitors are not left to loiter around and to a large extent, they think that servers are maintained in good conditions.



## 5.7 Communication and operation management

**Table 8: Communication and operation management**

<b>Section F: Communication and operation management</b>						
		Strongly Agree	Agree	Undecided	Disagree	Strongly disagree
	We are confident , that in the event of equipment failure, theft or a site disaster, our data backup and storage would enable us to retrieve our information with minimal business interruptions	12	16	20	20	4
	Our systems are updated/upgraded according to a structured plan and not in an ad-hoc fashion	4	20	32	12	4
	In the event of a security incident, procedure clearly define what to do and who to call for assistance	4	16	8	24	0
	We are confident that our antivirus systems are up-to date and in the event of a virus outbreak, we could be able to prevent our systems as best as possible	4	24	16	16	12
	Despite being connected to public networks, we are confident that our systems are adequately protected by our internet service providers (ISP) security and / our own firewalling systems	4	24	24	16	4
	Appropriate mechanisms are in place to authenticate users logging into our systems	4	36	24	8	0
	<b>Total</b>	32	136	124	96	24
	Total Number/Total respondents/Number of objectives	0.07	0.29	0.27	0.21	0.05
	Maturity score	0.35	1.16	0.81	0.42	0.05

### **Maturity 2.79**

The organization is fully aware of the key role that IT operations activities play in providing IT support functions. In addition, the organization communicates the need for co-ordination between users and systems operations. Budgets for tools are being allocated on a case-by-case basis. IT support operations are informal and intuitive. There is a high dependence on the skills and abilities of individuals. The instructions of what to do, when and in what order, are not documented. There are no operating standards and no formal operator training exists. Management does not measure the meeting of schedules by IT operations or analyze delays.

## 5.8 Access Control

**Table 9: Access control**

<b>Section G: Access control</b>	<b>Strongly Agree</b>	<b>Agree</b>	<b>Undecided</b>	<b>Disagree</b>	<b>Strongly disagree</b>
Users may log on/ gain access to our systems without being formally registered by their own user accounts	4	12	28	20	8
A password management system is in place which specifies the frequency of password changes as well as minimum password complexity e.g. password must be changed after every two weeks with X characters	0	12	40	20	0
Our organization controls access to information via access control policy which specifies which users have access to what data	0	36	16	20	0
We ensure that information processing facilities are only used for authorized business purposes	8	28	8	24	4
<b>Total</b>	12	88	92	84	12
Total Number/Total respondents/Number of objectives	0.03	0.28	0.30	0.27	0.03
Maturity score	0.15	1.12	0.9	0.54	0.03

### **Maturity 2.74**

The researcher found out that management is aware of the benefits of controlling the IT configuration but there is implicit reliance on technical personnel knowledge and expertise. Configuration management tools are being employed to a certain degree, but differ among platforms. Moreover, no standard working practices have been defined. Configuration data content is limited and not used by interrelated processes, such as change management and problem management.

## 5.9 System Development and maintenance

Table 10: System development and maintenance.

Section H: system development and maintenance		Strongly Agree	Agree	Undecided	Disagree	Strongly disagree
	Our systems tend to be bought in , either as off the shelf products or customized systems outsourced from developers	4	20	28	12	4
	We are aware that systems need to provide audit trails so that usage of the system and data input /changes may be audited	8	28	16	16	0
	<b>Total</b>	12	48	44	28	0
	Total Number/Total respondents/Number of objectives	0.07	0.31	0.28	0.18	0
	Maturity score	0.35	1.24	0.84	0.36	0

### Maturity 2.79

The findings indicate that there is no formally defined acquisition and implementation methodology, but requirements tend to be defined in a similar way across the business due to common practices within IT. Solutions are identified informally based on the internal experience and knowledge of the IT function. The success of each project depends on the expertise of a few key IT individuals and the quality of documentation and decision making varies considerably.

## 5.10 Business Continuity Management

Table 11: Business continuity management

Section I: business continuity management	Strongly Agree	Agree	Undecided	Disagree	Strongly disagree
We have business continuity plans which specifies who must take what action and what has to be done to ensure that the ministry can continue functioning in the event of a disaster such as fire/ floods	12	10	10	2	0
There is a nominated person in the ministry who is responsible for managing business continuity processes	0	16	10	6	0
Our security measures have been reviewed within the last year.	4	8	8	8	0
<b>Total</b>	16	34	28	16	0
Total Number/Total respondents/Number of objectives	0.1 4	0. 29	0. 24	0.14	0
Maturity score	0.7	1. 16	0. 72	0.28	0

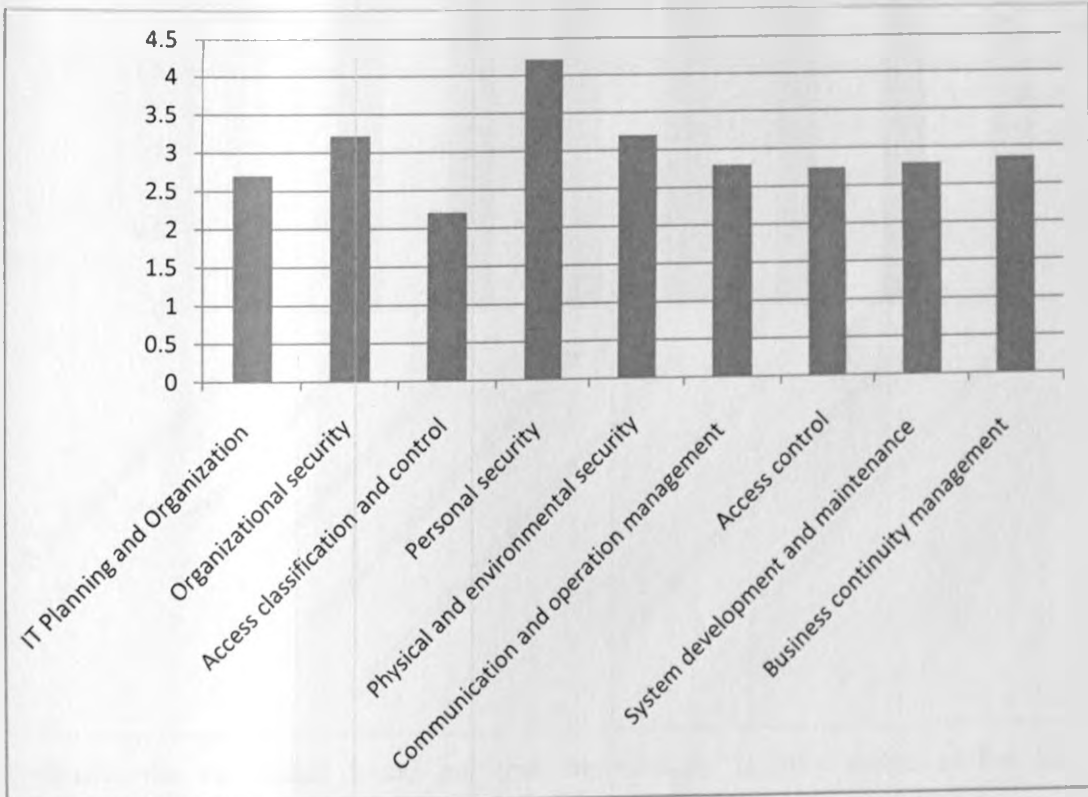
### Maturity 2.86

The researcher found out that the management recognizes a need to collect and assess information about monitoring processes. Standard collection and assessment processes have not been identified. Monitoring is implemented and metrics are chosen on a case-by-case basis, according to the needs of specific IT projects and processes. Monitoring is generally implemented reactively to an incident that has caused some loss or embarrassment to the organization. Monitoring is implemented by the information services function for the benefit of other departments, but is not implemented over IT processes. Process definition and monitoring measures follow traditional financial, operations and internal control approaches, without specifically addressing the needs of the information services function.

**Table 12 Summary of all the processes**

IT Processes	COBIT Score
IT Planning and organization	2.7
Organizational security	3.22
Asset classification and control	2.21
Personal security	4.21
Physical and environmental security	3.2
Communication and operation management	2.79
Access control	2.74
System development and maintenance	2.79
Business continuity management	2.86
<b>Average</b>	<b>2.96</b>

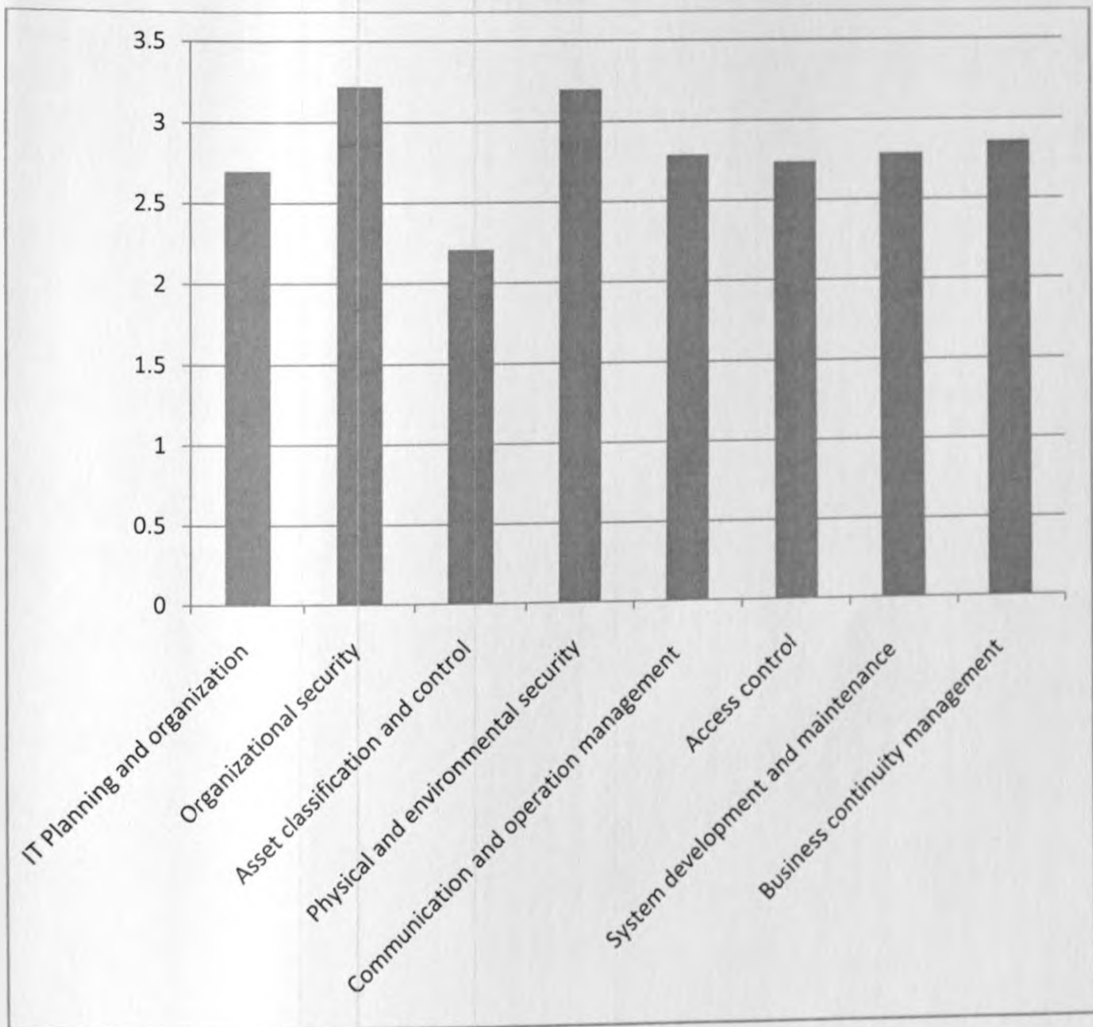
The graph below shows a representation of the interrelationship between all the nine processes as per the researcher's model.



## Summary of the findings

From the findings, the researcher found out that the area of asset classification and control is the poorest in all the processes investigated. Personal security scores the highest. This can be attributed to the fact that the government still approaches Information security in the traditional way where it emphasizes on physical aspects of information as opposed to the logical ones.

The standard deviation for the data in the graph is 0.579. However, when the process that scores highest, personal security is removed, the standard deviation is 0.338. The researcher deduced that this could be an outlier and therefore do not show the true picture. The graph below shows the relation of all the other processes when the personal security has been removed.



Overall, the researcher found out that the ministry is fully aware of the key role that Information technology activities play in providing support for its core functions. In addition, the ministry communicates the need for co-ordination between staff and IT staff.

The results of this research indicate that the ministry faces a number of challenges in relation to implementing information security in today's environment. The ministry's top officials expressed firm commitment to implementing security in the organization and solid intentions to secure the business and its operations, and this commitment has served the ministry well.

The researcher however notes that there is need to align policies and priorities across many different decision makers representing a broad mix of government, security and IT stakeholders.

During the business and operations analysis, the researcher noted that there was a complacent feeling from some management and staff about the security risks and liabilities at customer.

## **CHAPTER SIX**

### **SUMMARY OF RESEARCH, OUTCOMES AND RECOMMENDATIONS**

#### **6.1 Introduction**

This Chapter presents the results arrived at from the analysis of the data. The conclusions reached are also discussed and presented in this chapter. The Chapter also incorporates the various suggestions and comments given by the various officers during interviews and in the filled questionnaires. The research findings have been summarized alongside the objectives of the study, and the Control Objectives for Government Information Technologies as customized by the researcher. Conclusions have been drawn from the study and the actionable recommendations are also given.

#### **6.1 SECURITY POLICY**

The key finding is that there is no formal, documented security policy in existence at. During interviews, some staff assumed a policy was in place, due to their understanding that security was only about passwords. However, at a global view, the e-government policy is available that the ICT unit has adopted to its use.

A mixed understanding of security and of security policies and procedures amongst the staff and management observed would certainly be solved by a session or workshop on security awareness. The top management need to review security risks in relation to their division and responsibilities.

ISO-27002 states that the objective of an information security policy is to provide management direction and support for information security in accordance with business requirements and relevant laws and regulations. Management should set a clear policy direction in line with business objectives and demonstrate support for, and commitment to, information security through the issue and maintenance of an information security policy across the organization (ISO-27002, 2005).



Information security policies according to Harris (2003) are high-level and are not necessarily technical in nature. They are drafted and put to use in order to protect the organization's assets by ensuring that mechanisms are established to protect organizational assets' confidentiality, availability, and integrity. She states that having an information security policy in place can also reduce legal liability by following the concept of due care and due diligence (Harris, 2003, p. 793).

They must also specify the penalties for unacceptable behavior and define an appeal process. A standard is a more detailed statement of what must be done to comply with policy. Practices, procedures, and guidelines explain how employees are expected to comply with policy (Whitman & Mattord, 2004,).

Immediate action should be taken to cascade and implement a comprehensive information security policy that will define and communicate the management's commitment to information security to the entire organization.

Management at all levels should actively support security within the organization with clear direction, demonstrated commitment, and explicit acknowledgement of information security responsibilities. Control includes:

- clear direction and visible support for information security initiatives, including providing appropriate resources for information security controls;
- coordination of information security efforts across the organization, including designation of information security officer(s) and committee(s);
- assuring formulation, review and approval of appropriate organization-wide information security policy;
- periodic reviews of the effectiveness of information security policy, including external review as appropriate, and updating of the policy as needed; and
- appropriate management controls over new information facilities, systems and capabilities.

## 6.2 ORGANIZINAL SECURITY.

This element is defined by ISO-27002 (2005) as the establishment of a management framework for information security within the organization. The role of organizational management with regards to information security according to ISO-27002 is to:

- ensure that information security goals are identified, meet the organizational requirements, and are integrated in relevant processes;
- formulate, review, and approve information security policy; review the effectiveness of the implementation of the information security policy;
- provide clear direction and visible management support for security initiatives;
- provide the resources needed for information security;
- approve assignment of specific roles and responsibilities for information security across the organization;
- initiate plans and programs to maintain information security awareness; ensure that the implementation of information security controls is coordinated across the organization (ISO-27002, 2005, p. 9).

ISO-27002 (2005) states that management should actively promote and support information security within the organization through: clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities. The researcher recommends that all information security responsibilities should be clearly defined in the following ways:

- Information security activities should be co-ordinated by representatives from different parts of the organization with relevant roles and job functions.
- A management authorization process for new information processing facilities should be defined and implemented.
- Appropriate contacts with relevant authorities should be maintained.
- Appropriate contacts with special interest groups or other specialist security forums and professional associations should be maintained.
- organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes, and procedures for information security)

should be reviewed independently at planned intervals, or when significant changes to the security implementation occur.

- Identification of risks related to external parties Control The risks to the organization's information and information processing facilities from business processes involving external parties should be identified and appropriate controls implemented before granting access.

### **6.3 COMMUNICATION AND OPERATION MANAGEMENT**

The researcher found out that there is need to better coordinate communications and workflow across many diverse IT and security operations groups. The objective of this control is to ensure the effective operation and security of information processing facilities such as data centers, network and/or security operations centers.

According to Harris (2003), the Communications and Operations Management element of information security strategy pertains to everything that takes place to keep a network, computer systems, applications, and environment up and running in secure and protected manner. She states that communication networks and computing environments are “evolving entities and require continual and day-to-day maintenance (p. 753).

ISO-27002 states that in order to provide consistency and predictability of information security operations, operating procedures should be documented, maintained, and made available to all users who need them. ISO-27002 recommends that documented procedures should be prepared for system activities associated with information processing and communication facilities, such as computer start-up and close-down procedures, backup, equipment maintenance, media handling, computer room and mail handling management, and safety.

Projections of future capacity requirements should be made, to reduce the risk of system overload. The operational requirements of new systems should be established, documented, and tested prior to their acceptance and use. Harris (2003) states that products should always be evaluated for the level of trust and assurance they provide and that there be an agreed upon and documented procedure for evaluating products and components of a data communications network and information system (Harris, 2003, p. 757). Software and information processing facilities, following ISO-27002, are vulnerable to the introduction of malicious code, such as computer viruses, network worms, Trojan horses, and logic bombs. ISO recommends that all

users of information systems should be made aware of the dangers and ramifications of malicious code. Managers should, where appropriate, introduce controls to prevent, detect, and remove malicious code and control mobile code (ISO-27002, 2005, p. 42). An essential part of the ongoing management of information security operations is ensuring that information is backed up and can be restored reliably (Harris, 2003, p. 559). ISO-27002 recommends that a backup policy should be developed and that back-up copies of information and software should be taken and regularly tested in accordance with such a policy. ISO-27002 emphasizes that adequate back-up facilities should be provided to ensure that all essential information and software can be recovered following a disaster or media failure and that appropriate operating procedures should be established to protect documents, computer media (e.g.tapes, disks), input/output data and system documentation from unauthorized disclosure, modification, removal, and destruction. (ISO-27002, 2005, p. 42). Electronic mail (Email) communication is a critical and integral component of organization's today and yet it is an insecure communications media in that it can be easily intercepted and fraudulently modified (Harris, 2003, p. 763). ISO-27002 suggests that information exchange, such as email, should use encryption wherever possible and that all network systems that support the relaying of email and information be monitored and configured with appropriate levels of access control (ISO-27002, 2005, p. 42).

#### **6.4 ACCESS CONTROL.**

Proper access control, as stated by Harris (2003), should be included in an information security strategy to control a user's as well as software's ability to view or modify information and access or communicate with a component of an information system. Access control policy and mechanisms should ultimately manage the flow of information between users and information systems as well as intercommunication between disparate information systems (Harris, 2003, p. 867).

The following elements of access control which need to be addressed in an information security strategy through policies, standards, and documented procedures in Access Control Policy

- User access management
- Network Access Control

- Operating System Access Control
- Software Application access Control
- Information Access Restriction (i.e., database, file and folder access control)

### **6.5 PHYSICAL AND ENVIRONMENTAL SECURITY.**

The objective of Physical and Environmental Security is to prevent unauthorized physical access, damage, and interference to the and information. Critical or sensitive information processing facilities should be housed in secure areas, protected by defined security perimeters, with appropriate physical security barriers and physical entry controls. They should be physically protected from unauthorized access, damage, and interference. The protection provided should be commensurate with the identified risks and are intended to mitigate natural and environment threats.

The Physical and Environmental Security element of an information security that should be address physical site design and layout, environmental components, emergency response readiness, training, physical access control, intrusion detection, electrical power and fire protection. Physical and Environmental Security mechanisms protect people, data, equipment, systems, and the facility itself should be put in place.

### **6.6 ASSET CLASSIFICATION AND CONTROL.**

The ministry needs to know what assets need to be secured and therefore an information security strategy should identify all assets and document the importance of these assets. The asset inventory should include all information necessary in order to recover from a disaster, including type of asset, format, location, backup information, license information, and a business value.

Whitman & Mattord (2004) state that proper information security via risk identification begins with the classification and identification of assets where each information asset is identified, categorized, classified, and a value is assigned. They state that this process is important in order assure that the most valuable information assets are given the highest priority and are secured. The implementation of specific information security controls may be delegated by the owner or responsible party as appropriate but the owner still remains responsible for the proper protection of the assets (ISO-27002, 2005, p. 19). ISO-27002 also emphasizes that owners or responsible

parties should be identified for all assets and that they be given the responsibility for the maintenance of appropriate information security control.

## **6.7 INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT AND MAINTENANCE.**

Information security policy and controls should be put in place that address the acquisition, development, and maintenance of information systems. Because organizations depend on operating systems, infrastructure, business applications, off-the-shelf software, services, as well as in-house developed applications, there must be a defined policy governing and controlling the planning, procurement, and implementation of such information technology. ISO-27002 also state that “security requirements must be identified at the requirements phase of a project and should be justified, agreed, and documented as part of the overall business case for an information

## **6.8 BUSINESS CONTINUITY MANAGEMENT**

Business Continuity Management (BCP) is a complex and quickly evolving element of information security management and is difficult to define. Business Continuity management can be defined as a “holistic management process that identifies potential impacts that threaten an organization and provides a framework for building resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value creating activities” (Honour, n.d.). He adds

that Business continuity is also “the management of recovery or continuity in the event of a disaster” as well as the “management of the overall program through training, rehearsals, and reviews, to ensure the plan stays current and up to date”

ISO-27002 (2005) articulates that the overall objective of the information security aspects of business continuity management is to counteract interruptions to business [organizational] activities and to protect critical business process from the catastrophic effects of “major failures” of information systems or disasters [natural and man-made].

The goal is to “ensure their timely resumption” and should provide controls to continuously identify and reduce risks, confine the consequences of damaging incidents, and ensure that information required for business processes is readily available (p. 95).

The consequences of exploited threats such as disasters, security, failures, loss of service, and service availability, according to ISO-27002 (2005), should be addressed in a business continuity plan that includes information security as an integral of the entire business continuity process.

Harris (2003) concurs and affirms that main goal of business continuity is to resume organizational functionality and business as quickly as possible and that the overall plan should cover all organizational elements, identify critical service and functions, provide

All business continuity plans, whether for natural disasters, man-made hazards, or work stoppages, must do the following:

- Define essential business functions to be performed if operations are partially or completely shut down.
- Contain personnel contact information and incident notification procedures.
- Be maintained in the designated plan repository. (A copy must always be stored at an accessible off-site location or in a fireproof container.)
- Be protected as restricted information.
- Provide plan access to all individuals who have a need to know.
- Be reviewed and updated as necessary at least every 6 months.
- Be exercised yearly to test both the accuracy and completeness of the documentation as well as the reasonableness of the plan.
- Be revised in response to the Lessons Learned Report issued following an exercise.

The researcher further recommends that the ICT and Ministry disaster recovery projects be overseen by the Business Continuity Management Board, that a clear remit and timeline prioritize this work and that any mitigation requiring capital investment be appropriately prioritized.

## **CHAPTER SEVEN.**

### **VALIDATED CONTROL OBJECTIVES FOR GOVERNMENT INFORMATION TECHNOLOGY (COGIT)**

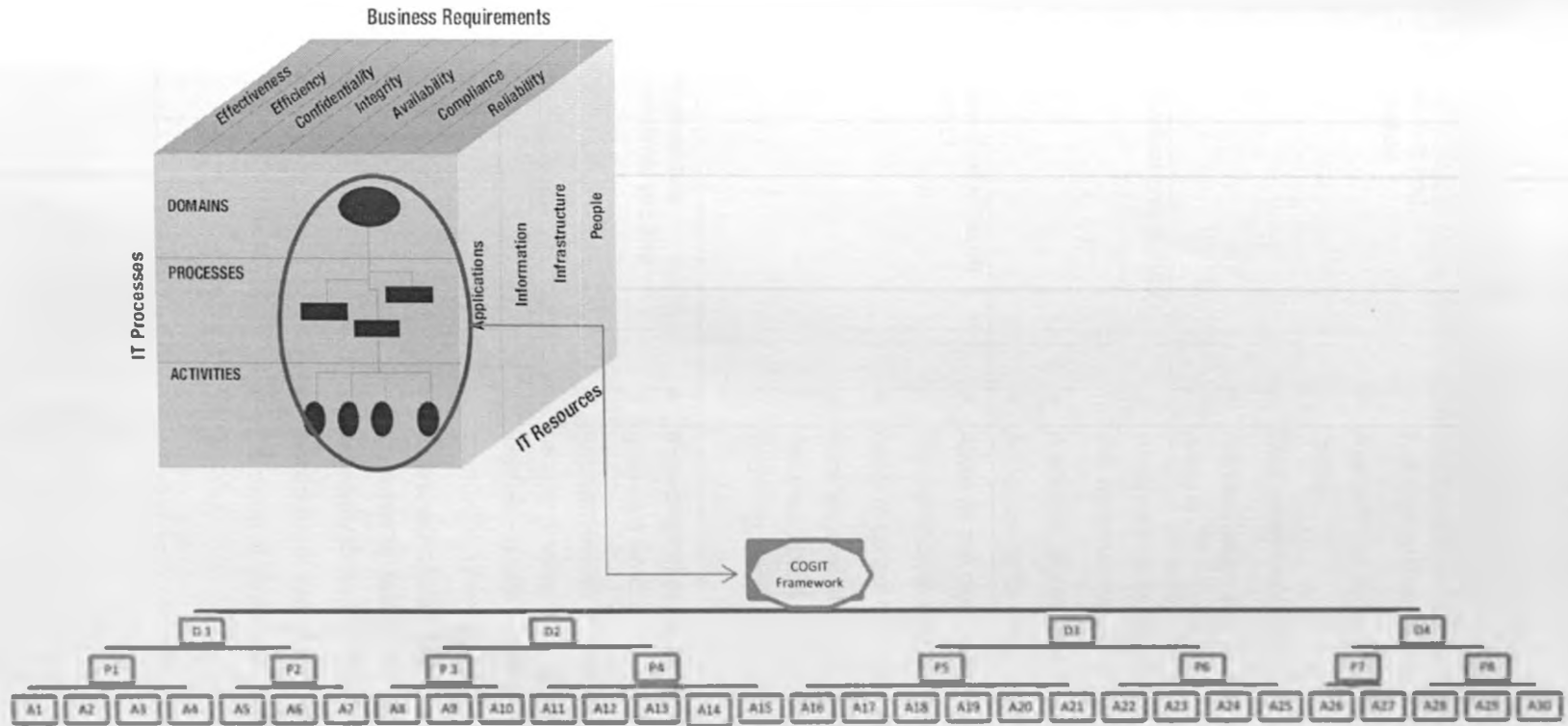
The researcher proposes a framework for information Security measures based on eight processes and thirty activities. The Control Objectives for Government Information Technologies (COGIT) is a derivative of the COBIT model. It covers a broad spectrum of areas in IT governance which are included in the four domains as per the COBIT framework, these are: D1: Plan and organize, which highlights the organizational and infrastructural form, D2: Acquire and implement which covers identifying IT requirements, acquiring and implementing IT within the government's current business processes, D3: Deliver and support which focuses on the delivery aspects of the IT, and D4: Monitor and evaluate that deals with a ministry's strategy in assessing the needs of the government, meets the objectives of the government and compliance with the regulatory requirements. However, while COBIT defines 34 processes in the four domains, COGIT specifies only eight processes that are relevant to government requirements.

Control is approached by looking at the information necessary to support the government business objectives. Information is then the result of the combined application of IT-related resources that need to be managed by IT processes. Each process summarizes several activities which can be used to design an appropriate control task

The figure below shows the Cogit framework



# The COGIT Framework



The matrix below shows details of all the activities and Processes.

	Process	Activities
D1	P1. Planning and Organization	<ul style="list-style-type: none"> <li>• Definition of Roles and responsibilities</li> <li>• Availability of documented information security policy</li> <li>• Staff awareness of security policy</li> <li>• Staff education and training on information security</li> </ul>
	P2. Organizational security	<ul style="list-style-type: none"> <li>• Responsibility for information security (hierarchy in the organization)</li> <li>• Availability of expertise on information security.</li> <li>• Authorization for use of Information Systems</li> </ul>
D2	P3 Asset Classification and Control	<ul style="list-style-type: none"> <li>• Ability for the organization to locate all assets (including software, hardware, staff and services )</li> <li>• Ability to control local and remote access</li> <li>• Knowledge of staff know what to do with information with regard to its storage, usage, archiving, back-up and destruction</li> </ul>
	P4. Physical and Environmental security	<ul style="list-style-type: none"> <li>• Knowledge of existence of high valuable portable goods e.g laptops</li> <li>• Appropriateness of physical and environmental security procedures in place to prevent interference with business premises and information systems</li> <li>• Awareness of staff of the risks relating to theft and the potential liability through compromised data especially those travelling with IT portable devices</li> <li>• Monitoring of visitors who access the ministry</li> <li>• Condition of server room and other data repository facilities</li> </ul>

	Process	Activities
D3	P5. Communication and Operation management	<ul style="list-style-type: none"> <li>• In the event of equipment failure, theft or a site disaster, data backup and storage would enable the organization to retrieve information with minimal business interruptions</li> <li>• If Systems are updated/upgraded according to a structured plan and not in an ad-hoc fashion</li> <li>• In the event of a security incident, there is a procedure which clearly define what to do and who to call for assistance</li> <li>• If Antivirus systems are up-to date and in the event of a virus outbreak, we could be able to prevent our systems as best as possible</li> <li>• If Systems are adequately protected by our internet service providers (ISP) security and / our own firewalling systems</li> <li>• Appropriateness of mechanisms in place to authenticate users logging into our systems</li> </ul>
	P6. Access Control	<ul style="list-style-type: none"> <li>• Levels of control of access ... E.g Users if may log on/ gain access to our systems without being formally registered by their own user accounts</li> <li>• Password management.... If a password management system is in place which specifies the frequency of password changes</li> <li>• If the organization controls access to information via access control policy which specifies which users have access to what data</li> <li>• If there is a mechanism to ensure processing facilities are only used for authorized business purposes</li> </ul>

	Process	Activities
D4	P7. System development and maintenance	<ul style="list-style-type: none"> <li>• Mode of acquisition of systems e.g. off shelf or developed</li> <li>• Ability of systems to provide audit trails</li> </ul>
	P8. Business Continuity Management	<ul style="list-style-type: none"> <li>• If the organization has business continuity plans which specify who must take what action and what has to be done to ensure that the ministry can continue functioning in the event of a disaster such as fire/ floods</li> <li>• If there is a nominated person in the ministry who is responsible</li> <li>• If security policies have been reviewed within the last year.</li> </ul>

## REFERENCES

1. Adams, A. and Sasse, M., (1999) Users are not the Enemy. *Communications of the ACM*, Vol. 42, No. 12, pp. 41-46.
2. Anderson, J. (2003) Why We Need a New Definition of Information Security. (Webdocument). URL: [http://www.ida.liu.se/~TDMM32/projekt/tdmm32\\_group12.pdf](http://www.ida.liu.se/~TDMM32/projekt/tdmm32_group12.pdf)
3. Anderson, P.W., (2001), Information Security Governance, Information Security Technical Report, Vol 6, No. 3, pp. 60-70.
4. AusCERT (2004) Report: 2004 Australian Computer Crime and Security Survey. (Web Document) URL: <http://www.auscert.org.au/render.html?it=2001>
5. BS7799-1. (1999). Information security management – Part 1: Code of practice for information security management. London: British Standards Institution
6. Caruso, J., (2003), Information Technology Security: Governance, Strategy and Practice in Higher Education, Educause Centre for Applied Research (ECAR).
7. Dhillon, G. (2003). Data and information security. *Journal of Database Management*, 14(2), i - ii.
8. Dhillon, G. (Ed.). (2001). Information security management: Global challenges in the new millennium. Hershey, PA: Idea Group Publishing.
9. Dhillon, G., & Backhouse, J. (1996). Risks in the use of information technology within organizations. *International Journal of Information Management*, 16(1), 65-74.
10. Dillman, D. A. (2000). *Mail and internet surveys* (2nd ed.). Toronto, Ontario, Canada: John Wiley & Sons.
11. Elof, J. and Elof M., (2003) Information Security Management: A New Paradigm. Proceedings of the 2003 annual research conference of the South African institute of computer scientists and information technologists on Enablement through technology.

12. Ernst and Young. 2003 Global Information Security Survey 2003. (Web Document) URL:  
[http://www.securitymanagement.com/library/EY\\_Survey1103.pdf](http://www.securitymanagement.com/library/EY_Survey1103.pdf)
13. Evaluation. ISO/IEC JTC Document. (Web Document) URI.  
<http://www.gammassl.co.uk/ist33/N636.pdf>
14. Fulford, H. and Doherty, N., (2003), The Application of Information Security Policies in Large UK Based Organizations: An Exploratory Investigation, Information Management and Computer Security, Vol. 11, No. 3, pp.106-114.
15. Glorioso, R. M. & Desautels, R. E. (1999). Disaster Recovery or Disaster Tolerance: The choice is yours. Disaster Recovery Journal [online]. [Cited October 21, 2011] Available from Internet URL  
<http://www.drj.com/articles/spr99/glor.htm>
16. Halliday, S., Badenhorst, K. & von Solms, R. (1996). A business approach to effective information technology risk analysis and management. Information Management and Computer Security, 4(1), pp. 19-31
17. Harris, S. (2003) *Certified Information Systems Security Professional (CISSP) All-In-One Exam Guide 2nd ed.* Emeryville, CA: McGraw-Hill / Osborne.
18. Harris, S. (2006) *Risk Management: Key elements when building an information security Program.* Article Retrieved January 7, 2012 from  
[http://searchsecurity.techtarget.com/tip/0,289483,sid14\\_gci1210562,00.html](http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1210562,00.html)
19. Higgins, H. N. (1999). Corporate system security: towards an integrated management approach. Information Management & Computer Security, 7(5), 217-222.
20. Hone, K., Eloff, J., H., P. (2002). Information security policy — what do international information security standards Computers & Security, 21(5), 402-409.
21. Hong, K., Chi, Y., Chao, L., & R., Tang, J. (2007). An empirical study of information policy on information security elevation in Taiwan. Industrial Management & Data Systems,
22. Honour, D. (Ed.) (n.d.) *Defining Business Continuity.* Web Article. Retrieved April 17, 2012 from <http://www.continuitycentral.com/feature0398.htm>

23. IBM Global Services. (2000). Managing information technology in a new age [online]. [Cited October 18, 2000] Available from Internet URL <http://www.ibm.com/services/whitepapers/gsw1178f.html>
24. Information Security Management System.(Web Document) URL: <http://www.bridgepoint.com.au/WhitepapersBPC.html#1>
25. ISO/IEC 17799:2005. 'Code of practice for information security management'. ISO (International Organization for Standardization) and IEC (International Electrotechnical Commission). Accessed 25<sup>th</sup> October 2011 at ANSI using URL: <http://www.ansi.org/>
26. ISO/IEC 27001:2005. 'Information Technology - Security Techniques – Information Security Management Systems - Requirements'. ISO (International Organization for Standardization) and IEC (International Electrotechnical Commission). Accessed 20<sup>th</sup> October 2011 at ANSI using URL: <http://www.ansi.org/>
27. IT Governance Institute (ITGI), (2000), COBIT Framework, COBIT Steering Committee.
28. Kankanhalli, A., Teo, H.H., Tan, B.C.Y., and Wei, K.K. 2003. "An Integrative Study of Information Systems Security Effectiveness," *International Journal of Information Management* (23:2), pp 139-154.
29. Kissel, R. (Ed.) (2006) National Institute of Standards and Technology: *Glossary of Key Information Security Terms*. [E-Version] Retrieved April 15, 2008 from <http://csrc.nist.gov/publications/nistir/NISTIR->
30. Krutz, R. & Vines, R. (2001) *CISSP Prep Guide: Mastering the Ten Domains of Information Security*. New York, N.Y.: Wiley & Sons.
31. Leach, J. (2003) Improving User Security Behaviour. *Computers and Security* Vol. 22, No. 8, 2003. pp. 685-692.
32. Lciwo, J., Kajava, J., & Nesland, L., *Information Security Guide-Lines for End-User Computing*. Agder College, Computer Center, Kristians and, Norwegen, 1994.
33. Lucas, A. (n.d) Thomas Jefferson Wheel Cypher. Online Article Retrieved April, 2012 from [http://www.monticello.org/reports/interests/wheel\\_cipher.html](http://www.monticello.org/reports/interests/wheel_cipher.html)

34. Maynard, S. and Ruighaver, A. (2002) Evaluating IS Security Policy Development. Presented at 3rd Australian Information Warfare and Security Conference 2002
35. McAnally, P., DiMartini, B., Hakun, J., Lindman, G. & Parker, R. (2000). Real-time data availability solutions: Does your business have a need for speed? Disaster Resource
36. Proceedings of the 2003 annual research conference of the South African institute of computer scientists and information technologists on Enablement through technology.
37. Pyati, A., (2005) WSIS: Whose Vision of an Information Society? URL: [http://www.firstmonday.org/issues/issue10\\_5/pyati/index.html](http://www.firstmonday.org/issues/issue10_5/pyati/index.html)
38. Sharon Halliday, Karin Badenhorst & Rossouw Von Solms (1996). "A business approach to effective information technology risk analysis and management". *Management & Computer Security*. Vol 4 No. 1. 19-31
39. Thomson, M. and R. Von Solms (1998) Information Security Awareness: Educating Your Users Effectively. *Information Management and Computer Security*. Vol 6, No. 4, 1998, pp. 167-173.
40. Von Solms, R. (1998a) Information Security Management (1): Why Information Security is so Important. *Information Management and Computer Security*. Vol. 6
41. Von Solms, R. (1998b) Information Security Management (2): Guidelines to the Management of Information Technology Security (GMITS). *Information Management and Computer Security*. Vol. 6, No. 5, (1998) pp. 221-223.
42. Von Solms, R (1999). Information security management: why standards are important. *Information Management and Computer Security*, 7(1), pp. 50-57
43. Von Solms, B. (2000) Information Security – The Third Wave? *Computers and Security*. Vol. 19, No. 7, (2000) pp. 615-620.
44. Von Solms, B. (2001) Corporate Governance and Information Security. *Computers and Security*. Vol. 20, No. 3, (2001) pp. 215-218. 4, (1998) pp. 174-177.
45. Whitman, M., & Mattord., (2004) *Management of Information Security*. Boston, Ma: Thomson.



46. Yhan, G., (2005). ISO 17799: Scope and implementation – Part 1 Security Policy.  
<http://www.infosecwriters.com/texts.php?op=display&id=335>
47. Yourdin, E. (2002) *Byte Wars: The Impact of September 11 on Information Technology*. Upper Saddle River, NJ: Prentice Hall.

# Appendix I

## QUESTIONNAIRE

You are kindly requested to fill the questionnaire your responses will not be used adversely; the purpose is to collect relevant information for on "*Information Security Management in Government Ministries, a case of Ministry of Youth Affairs and Sports*". The purpose of this survey is to enable the researcher to collect relevant data for analysis.

1. What kind of application software do you use?

- |                 |                          |                     |                          |
|-----------------|--------------------------|---------------------|--------------------------|
| Word processing | <input type="checkbox"/> | Accounts            | <input type="checkbox"/> |
| Database        | <input type="checkbox"/> | Desktop publishing  | <input type="checkbox"/> |
| Spreadsheets    | <input type="checkbox"/> | Integrated packages | <input type="checkbox"/> |
| Communication   | <input type="checkbox"/> | None of the above   | <input type="checkbox"/> |

Other \_\_\_\_\_

2. Please indicate which of the following do you make use of

- |                       |                          |
|-----------------------|--------------------------|
| Internet              | <input type="checkbox"/> |
| E mail                | <input type="checkbox"/> |
| Intranets             | <input type="checkbox"/> |
| Electronic commerce   | <input type="checkbox"/> |
| None of the above     | <input type="checkbox"/> |
| Other (specify) _____ |                          |

3. The internet is used for the following business issues

- |                                      |                          |
|--------------------------------------|--------------------------|
| Gathering information                | <input type="checkbox"/> |
| Establishing business presence       | <input type="checkbox"/> |
| Routine communication with customers | <input type="checkbox"/> |
| Other services (Indicate)            |                          |

4. Information security is an issue that the government should be concerned with

- |                   |                          |          |                          |
|-------------------|--------------------------|----------|--------------------------|
| Strongly agree    | <input type="checkbox"/> | Agree    | <input type="checkbox"/> |
| Undecided         | <input type="checkbox"/> | Disagree | <input type="checkbox"/> |
| Strongly disagree | <input type="checkbox"/> |          |                          |

Please evaluate the following statements by placing an X in the most appropriate column

		Strongly agree (5)	Agree (4)	Undecided (3)	Disagree (2)	Strongly disagree (1)
<b>Section A: Planning and Organization</b>						
<b>I) Security Policy</b>						
5	Roles and responsibilities for information security in the ministry are well defined e.g. someone is responsible for back-ups, registering users on the system, planning against disaster, liaising with service providers					
6	We have a documented information security policy					
7	Staff are aware of security policy					
8	All staff are given adequate and appropriate information security education and training					
9	Staff are well informed as to what is considered to be acceptable and unacceptable usage of information systems e.g. e-mail and internet conduct					
<b>Section B: Organizational Security</b>						
10	A director (or equivalent) member of staff has a responsibility for information security					
11	Expertise on information security is available and where not, external advice is sought					
12	Third party (outsider) access to our information system requires approval by a senior manager					
<b>Section C: Asset classification and control</b>						
13	We can identify and locate all assets (including software, hardware, staff and services ) used in information handling					
14	We control local and remote access to our information assets adequately					
15	Our staff know what to do with information with regard to its storage, usage, archiving, back-up and destruction					
<b>Section D Personal Security</b>						
16	Staff are aware that security incidents must be reported to management immediately					
17	Staff have been trained to secure their computers at all times when moving from their work stations e.g. locking and logging off their computers when going to tea break or lunch					
18	There is a formal disciplinary process for employees who have violated our security policies and practices					
<b>Section E: Physical and environmental security</b>						
19	Our organization contains high value portable goods or stock					

		Strongly agree (5)	Agree (4)	Undecided (3)	Disagree (2)	Strongly disagree (1)
20	We have appropriate physical and environmental security procedures in place to prevent interference with business premises and information systems					
20	Staff who travel with portable computers are aware of the risk relating to theft and the potential liability through compromised data					
21	Visitors to our organization are always escorted around the building and are never left to wander on their own					
22	Our servers are maintained in air conditioned , fire retardant power conditioned secure facilities					
<b>Section F: Communication and operation management</b>						
23	We are confident , that in the event of equipment failure, theft or a site disaster, our data backup and storage would enable us to retrieve our information with minimal business interruptions					
24	Our systems are updated/upgraded according to a structured plan and not in an ad-hoc fashion					
25	In the event of a security incident, procedure clearly define what to do and who to call for assistance					
26	We are confident that our antivirus systems are up-to date and in the event of a virus outbreak, we could be able to prevent our systems as best as possible					
27	Despite being connected to public networks, we are confident that our systems are adequately protected by our internet service providers (ISP) security and / our own firewalling systems					
28	Appropriate mechanisms are in place to authenticate users logging into our systems					
<b>Section G: Access control</b>						
29	Users may log on/ gain access to our systems without being formally registered by their own user accounts					
30	A password management system is in place which specifies the frequency of password changes as well as minimum password complexity e.g. password must be changed after every two weeks with X characters					
31	Our organization controls access to information via access control policy which specifies which users have access to what data					
32	We ensure that information processing facilities are only used for authorized business purposes					

<b>Section H: system development and maintenance</b>						
33	Our systems tend to be bought in , either as off the shelf products or customized systems outsourced from developers					
34	We are aware that systems need to provide audit trails so that usage of the system and data input /changes may be audited					
<b>Section I: business continuity management</b>						
35	We have business continuity plans which specifies who must take what action and what has to be done to ensure that the ministry can continue functioning in the event of a disaster such as fire/ floods					
36	There is a nominated person in the ministry who is responsible for managing business continuity processes					
37	Our security measures have been reviewed within the last year.					
<b>Section J</b>						
38	Prior to this survey, I was aware that there are established international information security standards available for organizations to adopt	<input type="checkbox"/> Yes <input type="checkbox"/> No				
39	If the answer for the 38 above is Yes, which among the following?					
	COBIT					
	SABS ISO/IEC 17799 part 1					
	SABS ISO/IEC 17799 part 2					
	NIST SP 800 series					
	RFC 2196 Site security handbook					
	Other (please specify					
40	In the last 12-18 months, has the ministry experienced any of the following security breaches?					
		Yes	No			
	Inadvertent breach ( e.g. user accidentally deletes file or changes computer configurations)					
	Deliberate attack (e.g. hacker, disgruntled staff gains access , deleting or stealing data)					
	Asset theft					
	Equipment failure					
	Back up failure					
	Data theft					
	Site disaster					
	Copyright infringement (e.g. staff copying pirated software)					
	Compliance (e.g. passing of information to unauthorized people)					

## Appendix II Interview Guide

<b>Value management</b>	<b>Comments</b>
Is there a process in place to determine which IT projects are commissioned based upon a solid business case analysis ?	
Does the process distinguish between mandatory, sustaining and discretionary investment in IT?	
Are the costs, timeliness and functionality of all IT?	
Are there equitable and enforceable Service Level Agreements in place?	
Is there responsibility and accountability for achieving the benefits and controlling costs clearly assigned?	
Is the business case review and evaluation process, fair, transparent, repeatable and comparable using a standardized practice that includes financial worth, the risk of not delivering a capacity and the risk of not realizing the expected benefits?	
<b>Business IT alignment</b>	
Is there a strategic planning process in place that is designed to ensure with organizational goals and objectives?	
Is the process bi-directional, including input from both major stakeholders and IT perspectives?	
Does this process occur at executive level?	
Does the process allow for sufficient mediation between organization an IT imperatives and produce mutually agreed priorities?	
<b>Assessment of Current capability and performance</b>	
Are there processes in place to assess the capability and performance of IT services and solutions?	
Is the assessment process used to assess the baseline data against which the future requirements can be compared?	
Is performance defined in such a way as to determine IT contribution to organizational objectives, functionality, stability, complexity and weakness?	
<b>Strategic plan</b>	
Is there a process in place to develop an IT strategic plan that defines how IT goals will contribute to the enterprise's strategic objectives and related costs and nrisks	
Does the plan define how support IT enabled programs, IT services and IT assets?	
Does the plan define	

How IT will meet its objectives? The measurements to be used?	
Does the plan cover budget , funding sources, sourcing strategies, acquisition strategy , legal and regulatory requirements?	
At what level in the organization are changes to the IT strategic plan authorized?	
What is the time covered by the IT strategic plan?	
Is the plan sufficiently detailed to allow for the definition of tactical IT plans?	
<b>Tactical plans</b>	
Is there a process in place to develop a portfolio of tactical IT plans that are derived from the IT strategic plan?	
Do the plan address all IT enabled programs, IT services and IT assets?	
Do the plans describe the required IT initiatives and resource requirements?	
Do the plans describe how the use of the resources and achievement of benefits will be monitored and managed?	
<b>Portfolio management</b>	
Is there a process in place in which the portfolio of IT enabled programs and services are managed?	
Who participates in the process?	
Does the process identify, define, evaluate, prioritize and manage IT programs based on the requirements to achieve specific organizational goals and objectives?	
Does the process clarify desired organizational outcomes and ensure that program objectives support those outcomes?	
Does the process Assign clear accountability Define projects associated with appropriate programs Allocate resources and funding Delegate authority Commission required projects	
Does the process address organization processes and workflow and attempt to use value added capabilities by leveraging the use of applications and technologies through business process reengineering?	
Does the process serve to determine both the internal and external resource requirement	