Information Security Management Framework for Effective Implementation of Integrated Financial Management Information System (IFMIS): The Case of MoF

By

Yafet Mekonnen

A Thesis submitted to AAU School of Information Science in partial fulfillment of the requirements for the Degree of Master of Science in Information Science and System

Advisor: Wondwossen Mulugeta. (PhD)

Date: August, 2020

Addis Ababa, Ethiopia

ADDIS ABABA UNIVERSITY

COLLEGE OF NATURAL AND COMPUTATIONAL SCIENCES

SCHOOL OF INFORMATION SCIENCE

Information Security Management Framework for Effective Implementation of Integrated Financial Management Information System (IFMIS): The Case of MoF

Yafet Mekonnen

Name and signature of Members of the Examining Board

Name	Title	Signature	Date
Dr. Wondwossen Mulugeta	Advisor	_____	_____
Dr. Dereje Teferi	Examiner	_____	_____
Dr. Michael Melesse	Examiner	_____	_____

Declaration

I declare that this thesis is my original work, has not been presented for degrees in any university and all the sources of materials used for the thesis have been accordingly acknowledged.

Student

Yafet Mekonnen

_____

This thesis has been submitted for examination with my approval as university advisor.

Advisor

Wondwossen Mulugeta (PhD)

_____

Acknowledgement

First and foremost, I would like to thank the almighty God to let me finish my work. I would like to express my deepest gratitude to my advisor, Dr. Wondwossen Mulugeta, for his time and excellent guidance.

My sincere thanks also go to all the directors, IT department staffs and also Staffs of HRM directorate and MOF corporate communication for providing me the business domain knowledge and data resources to conduct this research.

Finally, I would like to thank my family and friends MoF and FPPA Information Technology department staffs for their support in valuable suggestions.

Abstract

The main purpose of the study is to propose Information Security management framework for integrated financial management information system (IFMIS). In this study, MoF was selected using purposive sampling that issues service for different financial sectors around in Addis. The target population constituted 108 employees, the IFMIS and IT staffs located at MoF were included to be part of this study. Data was collected by means of questionnaire; interview and group discussions and analyzed using descriptive statistics. The analyses include frequency distributions, tables, figures and Narrative description. 108 questionnaires were distributed and 84 (78.8%) were returned. In addition to the questionnaires, observation and document review was made to strengthen the respondents' view. Accordingly, the data is processed using IBM SPSS V 20.0 Statistical tool. The framework that is proposed extracted from ISO security standard, NIST cyber security framework, literatures, and supported by findings from survey conducted in the MoF. The components are interwoven and all together support implementation of effective security solutions.

The study shows that the financial information security management framework and practice is not well maintained to address the MoF information security managements with associated to the IFMIS system. In general, the study shows that there is no standard to security, technical challenge management associated with the financial sectors. The study recommends that the management should involve on any aspect of the IFMIS project to improve the efficiency and minimize risks and technical challenges, the Ministry should have standard information security management framework and risk management techniques and policy to minimize and manage the risk and system. One of the best ways to make sure employees will not make costly errors in regard to information security is to institute organization-wide security awareness initiatives that include, but not limited to face-to-face and multi-media based awareness, techniques that can be fairly inexpensive to implement such as posters, do and don't lists and warning banners. These methods can help ensure employees have a solid understanding of the organization security policy, procedure and best practices. With the intention of elaborating on the underlying research that produced it, the proposed ISM framework for IFMIS was presented and discussed in detail – all the components, sub components, as well as the processes followed in preparing the framework. Finally, recommendations are given for the Ministry to act in short and long-term basis to improve the information security management awareness of its employees and in turn improve better information security management practice in the IFMIS.

Key words: IFMIS, MoF, Security, Information Security Policy, Information Systems Security

Table of Contents

List of Figures

List of Tables

List of Acronyms

MOF	Ministry Of Finance
PE	Public Entity
IFMIS	Integrated Financial Management Information System
IBEX	Integrated Budgetary Expenditure system
NBE	National Bank of Ethiopia
NPDC	National Planning and Development Commission
DSRM	Design Science Research Methodology
ISM	Information Security Management
ISP	Information Security Policy
ICT	Information Communication Technology
ISO	International Organization for Standardization
IEC	International Electro Technical Commission
COBIT	Control Objectives for Information and Related Technology
HIPAA	Health Insurance Portability and Accountability Act
DHCP	Dynamic Host Configuration Protocol
XML	Extensible Markup Language
SQL	Structured Query Language
LAN	Local Area Network
WAN	Wide Area Network
WSUS	Windows Server Update Service

Chapter One

1. Introduction

Nowadays, Information Technology (IT) has been widely applied in every aspect of our day to day life in business, government, education etc. With our increasing dependency on information technology, the consequences of computer crime can be extremely serious (Mahncke, McDermid, & Williams, 2009).

According to Al-Alawi, et al (2016), information is considered as lifeblood and a backbone for most institutions, and an invaluable asset in today's IT enabled world. Maintaining information systems security among the employees in the form of information systems security awareness is extremely important to protect the institutions' information systems. Information security awareness is used to refer to a state where users in an organization are aware of and ideally committed to their security mission, often expressed in end-user security guidelines (Siponen, Pahnila, & Mahmood, 2010). Siponen et al., (2010) further stated information security awareness is a serious business as information security techniques or procedures can be misused, misinterpreted or not used by end-users, thereby losing their real usefulness.

Although security awareness related matters range from simple information security guidelines to well-developed information security education programs in nearly all organizations in the age of the information society, their nature is not well understood, resulting for example, in ineffectiveness of security guidelines or programs in practice (Siponen, 2000). The failure of an organization's own employees to adhere to their information security policies constitutes a key threat (Puhakainen&Siponen, 2010); and to ensure that employees follow their organizations' security policies, developers have proposed several policy-compliance measures (Siponen et al., 2010).

Information security is very important in most organizations. An acceptable level of information security can only be introduced and maintained if the correct set of security controls, both procedural and technical, is identified, implemented and maintained. The process of identifying the most effective set of security controls can be a very complicated, resource-intensive process. A number of large British companies have joined forces to

establish a Code of Practice for Information Security Management. This document provides guidelines to any organization to identify and introduce a set of controls that will provide an acceptable level of protection to information resources. The Code of Practice is based on ten categories that should be presented in most organizations, these are: security policy, organizational security, assets classification and control, personnel security, physical and environmental security, computer and network management, system access control, system development and maintenance, business continuity planning, compliance to legal requirements (Solms R. , 2013b).

Some government organizations in Ethiopia are being forced to establish/ rules and procedures for Information Security Management especially in financial organizations. To manage ISM, it provides guidelines to any organization to identify and introduce a set of controls that will provide an acceptable level of protection to information resources. And also by the national information security policy of the federal democratic republic of Ethiopia September 2011 bases on some categories that should be presents in most organizations like international rules, these are: security policy, organizational security, assets classification and control, personnel security, physical and environmental security, computer and network management, system access control, system development and maintenance, business continuity planning, compliance to legal requirements.

1.1. Integrated Financial Management Information System (IFMIS)

Integrated Financial Management Information System is an automated system that is used for public financial management. It interlinks planning, budgeting, expenditure management and control, accounting, audit and reporting.

IFMIS is designed to improve systems for financial data recording, tracking and information management. This is in response to increasing demands for greater transparency and accountability in the management of the public's finances. The IFMIS system ensures higher degree of data quality improves workforce performance for improved business results and links Planning, Policy objectives and Budget Allocations. The system also: enhances reporting capabilities to support budget planning, automates the procurement process: requisition, tendering, contract award and payment, facilitates auto-reconciliation of revenue and payment with automatic file generation, facilitates automated revenue collections for improved cash forecasting, provides accurate and up to date information on the Government's financial position.

IFMIS provides governments with a tool that can support financial control, management, and planning. By managing a core set of financial data and translating this into information for management, these three financial functions are supported. More narrowly defined, an IFMIS is a computer application that integrates key financial functions; accounts, budgets, and promotes efficiency and security of data management and comprehensive financial reporting.

IFMIS are usually considered in terms of core and non-core financial functions while public financial management is a broad field with multiple systems: Core function is accounting and reporting functions, while non-core functions include budgeting, commitment control, cash management and disbursement functions. The common specification of the core functions does not include all of the components needed for effective financial control and, by definition, therefore, will increase risk.

The limited comprehensiveness of the conventional core functions of an IFMIS stems in large part from the private sector origins of IFMIS technology. In short, IFMIS do not' get the basics right' for public sector financial management. This raises the question of how they can constitute 'best practice'.

A 2006 paper by the Kennedy School of Government presented a case study of Ethiopia as an illustration of a successful and to some extent unconventional approach to automating public financial systems. This case study is especially interesting as it challenges the traditional wisdom usually associated with such schemes.

In Ethiopia, the automation process faced major challenges of resource, capacity, infrastructure, changes in government and dependency on foreign aid policies. Therefore, the reform strategy prioritized a pragmatic sequential approach based on the logic to ensure that the “basics” are in place before moving to more complex systems. A strategic choice was made to drive the automation process from the procedural requirements which were defined by the users, through an incremental and iterative approach, with government staff extensively being involved. The reform process first focused on bringing existing system up to date through simplification, elimination of backlogs and sequential procedural change before introducing new systems. Constant consideration was given to limit the burden imposed on scarce staff throughout the whole process. This strategy was justified by low level of skills, evolving fiscal decentralization and the general degradation of the financial system that had taken place over the previous years.

1.2. Statement of the Problems

Information security is concerned with the quality of information and the technical mechanisms and infrastructures used to protect information assets. Information security management focuses on information security governance and ensuring its realization at the operational level. There are many unresolved problems associated with effective information security management in developing countries.

The modern day challenge of organizations especially in developing country is to have in place information technology systems that can effectively serve the needs of the organization, meet the rapid technological changes and be flexible to accommodate enhancements. It is imperative that a proposed new management information system should be adequately planned for and accommodates the needs of its myriad users to forestall the eventuality of system failure. (Ngibuini, 2010).

Extant literature reveals that most information security attacks are based on employees, were employees are the subject and objective for most information security attacks. As Connolly, Lang and Tygar (2017) stated, humans are the weakest link in the information security chain and the root cause of numerous security incidents in organizations.

Woretaw and Lessa (2012) explained information security awareness in the Ethiopian especially in financial sector is unsatisfactory. Though securing the information assets of financial sector now a days is becoming a matter of existence for the business, there are scarce number of similar studies in information security awareness and adherence in Ethiopian financial industries. Although there are standards and other frameworks designed to assess information security awareness and adherence in organizations, existing standard can't fit to all organizational contexts. Rather, contextual factors (organizational, national, environmental, etc.) affect the design of such programs. According to Alnatheer and Nelson (2009) major international Information security management standards are written from a Western perspective, without knowing how applicable security concepts and practices are to other cultures, which has different social, organizational, and security cultures. Organizations should never randomly choose their information security awareness program; instead their program should be based on their specific need (Xiong, 2011). Information security culture is an assumption about what is and what is not acceptable in relation to information security. Information security as a subset of the corporate culture entails that it is influenced too by the

parent organization‘s culture. Researches indicate that insider behavior poses a more serious threat to the security of information than outsider behavior.

As most organizations, MoF has invested huge amounts of government money and time in technical solutions such as firewalls, antivirus, intrusion-prevention system to prevent government budget overspending and etc, However,as (Alageel, 2003; Amare, 2015) stated organizations often pay too little attention to the most important and vulnerable security component, the human part. MoF is one example of such organizations which need to implement technical as well as human aspects when it comes to securing the organization assets. The reason is humans are the weakest link when it comes to security (Alageel, 2003; Amare, 2015; Siponen, 2000). MoF has developed an information security policy which is a good start on going forward to tell staffs what is right and wrong when it comes to securing the organization’s assets. There is a saying “a chain is only as strong as its weakest link” meaning an organization especially a process or a business is only as strong or powerful as its weakest person.

This research, therefore, tries to fill this gap by proposing information security management framework for effective implementation of IFMIS in MoF context which enhance the existing knowledge. The proposed framework can also be used as a guideline by the ministry to conduct information security management for successful and secure IFMIS system for its employees to strengthen, and also manage to government finical, property, procurement and other IFMIS modules.

1.3. Research Question

In the following research questions

1. What are the current management practices in relation to information security influencing factors to in the context of MoF?
2. Which existing security mechanisms best fits for the implementations of IFMIS?
3. To what extent the information security management is effective in MoF?

1.4. Objectives of the Study

1.4.1. General Objective

The general objective of this study is proposing Information Security Management framework for Integrated Financial Management Information System (IFMIS) in MoF.

1.4.2. Specific Objectives

The study is guided by the following specific objectives

- To recognize the requirements of the effective information security management in the Ministry of Finance (MoF).
- To study the dimensions of information security management.
- To evaluate the impact of information security management on the effectiveness of applying IFMIS in Ministry of Finance (MoF).
- To define the priorities that should be addresses by the Government with regard to information security management.
- To understand the correlations between information security management fields and the security of IFMIS.
- To propose information security management framework that could be used to manage and secure IFMIS.

1.5. Significance of the Study

IFMIS/IBEX project will greatly benefit from this research as the study will have a contribution in their program of designing better IT systems.

Generally the importance of this study stems from the following aspects:

- This study considered as the first one in this field that has studied the information security management in Governmental projects in MoF and its impact on the effective implementation of IFMIS.
- To recognize the gap between the real situation and the prospects in the field of information security management.
- Motivate the researchers 'interest to penetrate the fields of information security management and IFMIS and the requirements to apply each one and the relations between them.

1.6. Scope of the Study

This research work is about Information Security Management for Strategic and Effective Implementation of Integrated Financial Management Information System (IFMIS) in MoF. So it covers the accumulate organizations and employee's, related information security management activities in IFMIS/IBEX project with the IT System of the organization. It also

serves as a benchmark for practitioners and researchers who want to conduct more research in information security management framework areas in MoF.

1.7 Organization of the Study

The study is organized into six chapters. The first chapter is the introduction part, which includes background of the study, statement of the problem, research questions, objectives, significance and scope of the study. The second chapter is literature review which covers literature from different sources that support the work of the researcher. In it, it mainly discusses about concepts of ISM, Security management framework. The third chapter is about the research methodology like research design, sampling technique, data collection instruments, procedures etc. The researcher started by describing design science research methodology as the appropriate methodology for creation of artifacts. The fourth chapter is data presentation and analysis which discusses about the analyzed data that were collected through semi structured interviews, focus group discussion, questioners and document analysis. Based on the analysis and findings of the study an information security management framework is proposed in chapter five, evaluation of the proposed ISM framework is also discussed under this chapter. Finally the last chapter covers conclusions and recommendations. At last list of reference materials and appendixes are included at the end of this thesis.

Chapter Two

2. Literature Review

This chapter presents an overview of different published literature that are related to ISM framework considered as important to support this study. The chapter further discusses mainly about Information Security, Information Security framework, Information Security framework management practices in different institutions, IFMIS practices and different types of security frameworks and related works.

2.1. IFMIS Implementation Strategy

MoF uses the IFMIS system as the sole accounting system for all government entities and any accounting done outside the system is considered irregular. The government implementation strategy on IFMIS project on ministries, department, agencies and counties also has an effect on the success or failure of the system. The way in which the move from the previously manual system to the compulsory IFMIS system is rolled out may affect the way it is perceived and accepted by the new users. The number of trainings done prior to the roll out of the system and the availability of infrastructure for using the system are also likely to affect and implementations of the organization.

2.2. Information security

Information is one of a financial institution's most important assets. Protection of information assets is necessary to establish and maintain trust between the financial institution and its customers, maintain compliance with the law, and protect the reputation of the institution (Council, F.F.I.E, 2006). Similarly Tse, et al. (2013) stated IT systems contain a wealth of private financial information. These data are used as a shared secret between sectors and their customers and others. As access to computer stored data has increased, information security has become respectively important. McGlasson (2007) stated that the most important part of a good organization IT security infrastructure is information security management. In order to protect the information assets and prevent fraud activities, the financial industries should design and implement information security strategies. For this kind of scenarios McGlasson (2007) suggested two solutions, the first is establishing information security management framework and the second is organizing information security awareness training program.

Security of the information assets is a requirement for all types of organization, whether to protect the business or to meet legal or regulatory requirement as organizations are totally dependent on their IT systems to capture, store, process and distribute organization information (Jones, 2010). For this, information security is and has always been the discipline to mitigate risks impacting on the confidentiality, integrity and availability of a company's IT resources (Von Solms, 2006).

According to Nieles et al (2017) information Security is the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to ensure confidentiality, integrity, and availability. Information security is the process by which an organization protects and secures its systems, media, and facilities that process and maintain information vital to its operations (Council, F.F.I.E, 2006). It is simply the process of keeping information secure protecting its availability, integrity, and privacy. Similarly Abdyli (2014) stated the most well-known theoretical model which treats information security is the CIA triad or CIA triangle as shown in Figure 1.

Figure 1 CIA triad

Figure 2.1: CIA Triad

Source: Abdyli (2014).

According to Abdyli (2014) information security includes:-

- Confidentiality – is described as the protection of information, application, system and network from unapproved access. It relies to the safeguard of information by illegal admission regardless in what form is stored.
- Integrity – is described as the protection of information, application, system and network from unauthorized change, be intentional or accidental.
- Availability – is the affirmation that information, assets and resources are available only to those authorized.

Effective Information Security incorporates security products, technologies, policies and procedures. Products such as firewalls, intrusion detection systems, and vulnerability scanners alone are not sufficient to provide effective information security.

Most of the research done on corporate that deals with security in Information Systems (IS) were focused mainly on the technical aspect of IT such as firewalls and anti-virus software which rely more on technology than the employees using the systems. Researchers are now starting to realize that the human interaction with the IS of the firm is just as important as the technical, and that information security cannot be achieved solely through these technological tools (Herath& Rao, 2009). Many researchers now believe the biggest threat to information security remains internal Boss et al (2009), Vroom & Von Solms, (2004), and Kankanhalli et al 2003). Swartz (2007) outlined several cases in which employees stole data while still working for their company, yet the majority of employee security breaches occur accidently or unintentionally Keller et al (2005) and (Sumner, 2009). There are currently many theories on the best way to combat these issues. These range from the importance of cultivating an information security policy to significance of employee training and awareness.

According to Gebrehawariat (2017) a successful organization should have the following multiple layers of security in place for the protection of its operations.

- Physical security – to protect the physical items, objects, or areas of an organization from unauthorized, access and misuse.
- Personal security – to protect the individual or group of individuals who are authorized to access the organization and its operations.
- Operations security – to protect the details of a particular operation or series of activities.

- Communications Security – to protect an organization's communications media, technology, and content.
- Network security – to protect networking components, connections, and contents.
- Information security – to protect the confidentiality, integrity and availability of information assets, while they are in storage, processing, or transmission.

Gebrehawariat (2017) added the information security is achieved through the application of policy, education, training and awareness, and technology.

2.3. Information Security Management

Information security management(ISM) is defined as "a systematic approach to encompassing people, process and Information Technology (IT) systems that safeguards critical systems and information protecting them from internal and external threats" (Barlas, Queen, Randowiz, Shillam, & Williams, 2007). ISM is increasingly important within organizations, becoming a strategic imperative as security threats continue to escalate (Okin, 2006). Security and privacy are among the top ten management concerns, according to a 2005 survey of executive IT managers (SIM, 2006). The absence of a well-defined information policy is currently regarded as the most serious problem with security in organizations today (Biegelman& Bartow, 2006). Navigating the multitude of existing security standards, including dedicated standards for information security and frameworks for controlling the implementation on IT, presents a challenge to organizations. The framework is intended to promote a cohesive approach which considers a process view of information within the context of the organizational operational environment (Sipior& Ward, 2008).

2.4. Information Security Framework

Information security framework ensures the overall security of information in an organization by eliminating business risks. Information security does not focus only on technological issue, but also points out other important elements of an organization such as people, process, business strategies etc., which also mandates the need for information security. The comprehensive information security framework should incorporate the following key elements:

- Recommended sound security governance practices (e.g., organization, policies, etc.)
- Recommended sound security controls practices (e.g., people, process, technology)

- A guide to help reconcile the framework to common and different aspects of generally adopted standards (e.g., COBIT, HIPAA, etc.)
- An analysis of risk or implications for each component of the framework
- A guide of acceptable options or alternatives and criteria, to aid in tailoring to an organizations operating environment
- A guide for implementation and monitoring
- Toolset for organizations to test compliance against the framework (HITRUST)

A comprehensive security framework boils down to three familiar basic components: people, technology, and process. When correctly assembled, the people, technology, and process elements of your information security program work together to secure the environment and remain consistent with your firm's business objectives (Kark et al 2007). Diagram 1 shows the concept of people, process and technology.

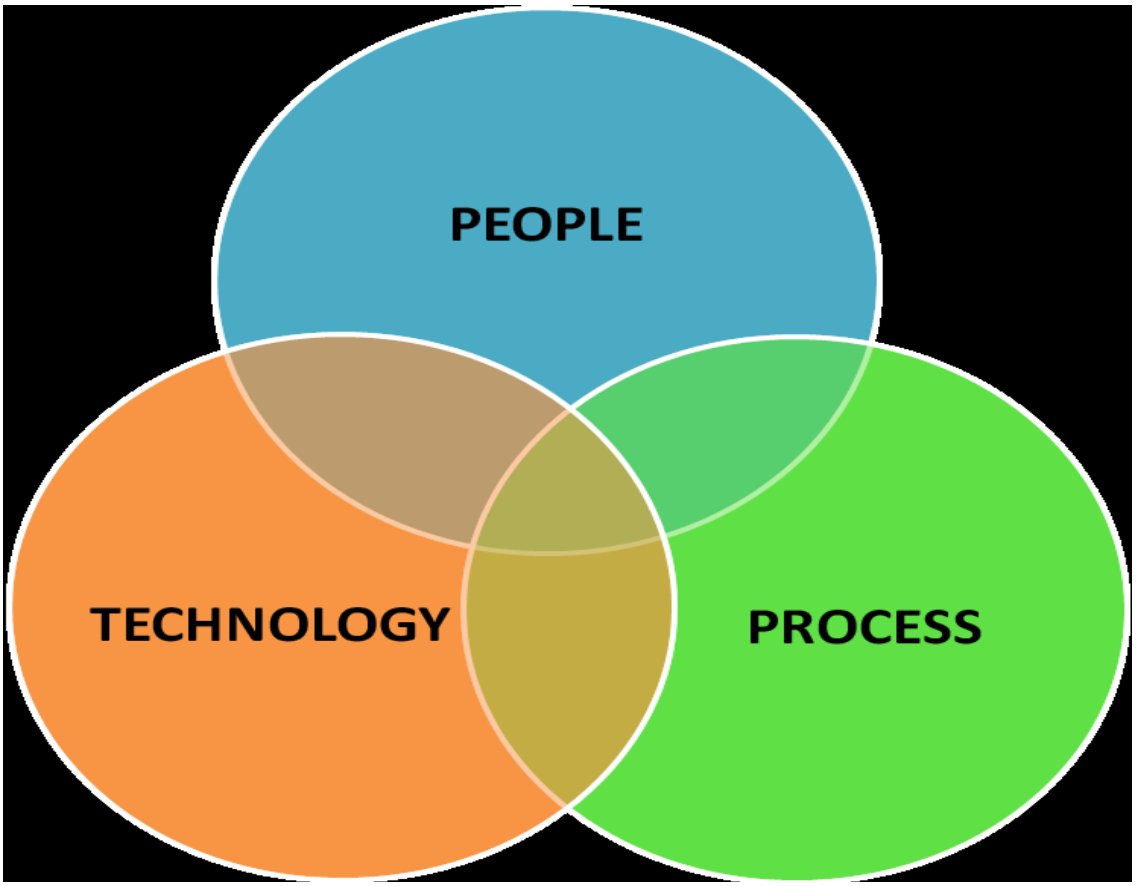

Figure 2.2: Information Security Framework

2.5. Information Security Policy

Management of information requires a working set of procedures, guidelines and best practices that provide guidance and direction with regards to security. An information security policy is defined as an aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information (Nieles, Dempsey, &Pillitteri, 2017). Nieles et al., (2017) further stated in making these decisions, managers face difficult decisions with regard to resource allocation, competing objectives, and organizational strategy, all of which relate to protecting technical and information resources as well as guiding employee behavior. Information security policy is a well-defined and documented set of guidelines that describes how an organization manages, protects its information assets and makes future decisions about its information systems security infrastructure. Security procedures document precisely how to accomplish a specific task.

According to Diver (2007) a security policy should fulfill many purposes. It should:

- Protect people and information
- Set the rules for expected behavior by users, system administrators, management, and security personnel
- Authorize security personnel to monitor, enquiry, and investigate
- Define and authorize the consequences of violation
- Define the company consensus baseline posture on security
- Help minimize risk
- Help track compliance with regulations and legislation

Diver (2007) stated policies must be useable, workable and realistic. In order to achieve this, it is essential to involve and get commitment from major players in policy development and support such as senior management, audit and legal as well as from those people who will have to use the policies as part of the daily work. Another important element to achieve this is to communicate the importance and usefulness of policies to those who have to live by them.

According to Instant Security Policy (2008) a security policy must specifically accomplish three objectives. These are allowing for the confidentiality and privacy of a company's information, provide protection for the integrity of a company's information and provide for the availability of a company's information. This is commonly referred to as the CIA Triad of

confidentiality, integrity, and availability, an approach which is shared by all major security regulations and standards.

2.6. Information Security in Ethiopia

Due to technology transformation in today's Ethiopian, information security has become one of the key points for customer attraction, retention, and profitability (Negussie, 2015). Currently, financial sector in Ethiopia is one of the rapidly growing sectors of the country's economy. Tebkew (2013) in his study stated that in order to get national and international competitive advantages, information must be properly managed from its creation up to disposal. However, from information security aspect, each IFMIS has applied some component of an information security policy such as: acceptable use policy of IT equipment, backup policy, anti-malware… etc. The scholar further stated IFMIS have invested on IT security devices as part of their System project. However, managing these IT security devices may be challenging since they do not have overall or comprehensive Information Security Management (ISM) framework which serve as a guide to develop and implement their own information security policy based on their own requirement in line with National Bank of Ethiopia's (NBE) directives. On the other hand, Tebkew (2013) discussed Ethiopian business competition has motivated the advancement of services enabled by IT which in turn increased the information security risk. These threats to information and information systems can include intentional attacks, environmental disruptions and human/machine errors, and result in great harm to the national and financial security interests of the country since Ethiopian IT capabilities are still in a developing phase and are immature compared with leading western countries which are technically developed.

Negussie (2015) stated information security issue is not only a problem that technology can address alone but also a problem of a management to solve. Legal frameworks in the form of policy and standards are the primary prerequisites to establish efficient and reliable security governance systems in Ethiopian. Negussie (2015) further stated in almost all Ethiopian banks and others government sectors, management does not give that much emphasis to information security, for implementing a good and effective information security governance management commitment and support is highly mandatory. There are challenges to formulating, implementing and compliance of Information Security Policy (ISP) in Ethiopian such as management commitment and support due to lack of awareness, lack of a special

training to information security personnel, complexity of the subject matter, and resistance with employees to comply with ISP and lack ongoing employees' awareness on security issues (Negussie, 2015). Nowadays, NBE and NPC is forcing each financial sector, government projects to recruit dedicated information security personnel so that he/she directly engage in the process of protecting the organization's information assets. However, since information security industry needs such a huge initial infrastructure investment and personnel technical efficiency, MoF face similar challenges when trying to secure their organization.

Woretaw and Lessa (2012) explained the level of information security awareness in Ethiopian financial sector is unsatisfactory. One of the greatest threats to information security could actually come from within a company or organization. According to Amare (2015) most organizations are not even aware of insider threat problem. Inside attacks have been noted to be some of the most dangerous since these people are already quite familiar with the infrastructure. It is not always dissatisfied workers and corporate spies who are a threat. Most of the times, it is the non-malicious, uninformed employee (Brodie &Wanner, 2009). The majority of insiders do not consider the consequences of their actions when undertaking an attack. Educating employees about the consequences of such attacks from the perspective of both the business and the wrongdoer may act as a preventive to such attacks. When employees learn to behave securely through training, these beliefs will influence attitude and ultimately behavior.

2.7. IFMIS Reliability and Efficiency

Miheso (2013) in his study on adoption of integrated financial management information systems by the National government concluded that over 90% have been informed how IFMIS will affect their current work practices and 95% say that IFMIS is stable with little or no down time. 83% are sure that IFMIS processes match with their manual processes and 73% said that all activities in the department are run within the IFMIS system. 23% respondents said that the exchequer budget release of funds on the IFMIS does not coincide with the manual funds release process. 25% did not agree that all payments approvals are only carried out in IFMIS. 45% indicated that purchase orders were not exclusively through IFMIS. 78% are sure that Local Purchase Orders (LPO's) and invoices were manually captured into the IFMIS system.

Peterson (2011) undertook a study on Reforming Public Financial Management in Africa. Reforms succeed when they are aligned with the four drivers of public sector reform: context, ownership, purpose and strategy. Public financial management is a core function of the state and its sovereignty and it is not an appropriate arena for foreign aid intervention, governments must fully own it, which was a key to the success of Ethiopia's reform. The purpose of PFM reform should be building stable and sustainable 'plateaus' of PFM that are appropriate to the local context and they should not be about risky and irrelevant 'summits' of international best practice. Plateaus not summits are needed in Africa. Finally, a strategy of reform has four processes: recognize, improve, change, and sustain. Ethiopia succeeded because it implemented a recognize-improve-sustain strategy to support the government policy of rapid decentralization. All too often, much of PFM reform in Africa is about the change task and climbing financial summits.

Nyabuto (2009) undertook a Survey of the Extent of Implementation of Integrated Financial Management Information System (IFMIS) as a Tool for Sustainable Financial Management in Government. The data was analyzed using preliminary analysis procedures that included percentages and frequencies. It was through such a descriptive survey that the study established that IFMIS implementation was behind schedule.

The results revealed that there was resistance in the Ministries for the use of IFMIS. This implies that for IFMIS to succeed, such resistance must be overcome. Possible reasons for resistance included lack of training and fear of the unknown. Despite the resistance, it was found out that IFMIS had succeeded though still implementation was behind schedule. Consequently the government of Kenya has immensely benefited from the advantages of a computerized accounting system which is more reliable than the former stand-alone legacy systems.

Spriano (2013) carried out a study on the successes and failures of e-Government projects in Developing Countries: a case study of Zambia. The study used an online survey based on a modified version of the Heeks Factor Model that focuses on soft human aspects known to be critical in the implementation of e-government projects. Data was collected from 121 respondents from Zambia between the month of September and October 2012. The results of the study indicted a rating score of 55.1 based on Heeks 100 point scale implying a mighty fail totally or partially. In addition the awareness of the e-government projects was found to be inadequate.

Njonde and Kimanzi (2014) carried out a study on Effect of integrated financial management information system on performance of public sector using the case of Nairobi county government, the study found out that 68% of the respondents agreed that accuracy and speed were some of the benefits realized from using the IFMIS. 34% recorded no benefits realized on use of the system. 84% of the respondents from that study indicated that budgeting has improved by use of IFMIS and that there was timely preparation of the budget.

2.8. The Information Security Management Framework

The ISM framework considers global, national, organizational, and employee standards to guide ISM. This framework is intended to promote a cohesive approach which considers a process view of information within the context of the entire organizational operational environment. The four levels of guiding standards for ISM are presented in Figure 1 and are discussed in the following sections.

The researcher caution corporations, using this guiding framework that the relations among the four levels of information security depicted in Figure 1 are complicated. For example, at the international level, standards may vary by country. Similarly, at the national level, various government agencies may have possibly conflicting standards. Organizational standards may not be in line with those of business partners. Employee practices may be influenced by professional rules of conduct in addition to organizational policy.

2.9. International Organization for Standardization ISO 27001:2013

ISO/IEC (2013) (the International Organization for Standardization) and IEC (the International Electro technical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity.

The objective of the standard is to provide requirements for establishing, implementing, maintaining and continuously improving an information security management system. The design and implementation of an organization's information security management framework is influenced by the organization's needs and objectives, security requirements, the organizational processes used and the size and structure of the organization. The standard stated it is important that the information security management system is part of an integrated

with the organization's processes and overall management structure and that information security is considered in the design of processes, information systems, and controls. It is expected that an information security management system implementation will be scaled in accordance with the needs of the organization. The standard further stated any personnel doing work under the organization's control shall be aware of the information security policy, their contribution to the effectiveness of the information security management system, including the benefits of improved information security performance; and the implications of not conforming with the information security management framework requirements.

Figure 1: The Information Security Management Framework based on Guiding Standards

Figure 2.3: The Information Security Management Framework based on Guiding Standards

2.9.1. Global Standard for Information Security Management

The most widely accepted global standard for ISM across industries and geography is the International Standards Organization / International Electro technical Commission (ISO / IEC) Code of Practice, document number 27002 (Biegelman& Bartow, 2006; Langley, 2006; Rasmussen, 2005). ISO / IEC 27002:2005 provide a commonly accepted security architecture framework of guidelines and general principles for developing organizational security standards and effective security management practices. The standards address people, processes and IT systems to assist in identifying, quantifying and managing threats to information.

ISO / IEC 27002:2005 was originally written by the United Kingdom (U.K.) Government's Department of Trade and Industry (DTI) and published as BS 7799 by the British Standards Institute (BSI) in 1995 (Langley, 2006). BS 7799 was eventually internationalized and adopted by ISO in 2000, as ISO/IEC 17799, "Information technology - Security techniques - Code of practice for information security management," after several revisions. ISO/IEC 17799 was most recently revised in June 2005 and subsequently renumbered to ISO/IEC 27002 in July 2007 to align with the ISO/IEC 27000 series standards. This series is intended to provide further guidance for ISM system requirements, risk management, metrics and measurement, and implementation (Rasmussen, 2005).

Global standards must also consider the increasing activities of international terrorist groups and organized criminal syndicates (Trim, 2007). Terrorists and criminals are forming alliances and using increasingly sophisticated technologies to devise new activities threatening to IT. Thus, governmental transnational intelligence sources should be consulted by organizations to remain apprised of emerging concerns (Trim, 2007). Information security is a concern for all organizations across the world, necessitating the sharing of global intelligence. A balance between security and privacy, that is acceptable to the majority of the community worldwide, must be found (Berinato, 2007).

2.9.2. National Standards for Information Security Management

At the national level, governments create information security standards and regulations. Within the United States (U.S.) for example, there is no single authority to reference for organizational ISM. The lack of a strong enforcement mechanism to protect personal information is one of the primary criticisms of U.S. privacy practices (Fredericks, 2005).

However, several laws are directed toward specific industry sectors. Organizations in the public sector and the regulated industries are required to demonstrate proper ISM procedures and controls associated with storage, backup, encryption, security, and protection of confidential data to avoid penalties for noncompliance (Mohamed, 2007).

Several federal laws are directed toward specific industry sectors to increase corporate responsibility in protecting consumer privacy and accountability for the substance of their financial reports. The current regulatory environment within the United States has made ISM a strategic necessity. For example, the Financial Services Modernization Act of 1999, also known as the Gramm-Leach Bliley Act (GLBA), requires financial institutions to maintain the privacy of electronically stored customer information through security controls for data

integrity and for identifying with who this information is shared (Federal Trade Commission, n. d.). The Health Insurance Portability and Accountability Act (HIPAA) of 1995 is intended to protect electronic health information (Hewitt, 2004). Standards for policies and procedures to limit unauthorized access to medical information were set in the Security Rule, published February 2003 (Gue, 2003). Section 404 of the Public Company Accounting Reform and Investor Protection Act of 2002, or Sarbanes-Oxley, requires publicly held companies to annually evaluate their financial reporting controls and procedures (AICPA, 2004). Although information security is not explicitly addressed, compliance may be incomplete without adequate security controls. Another example of federal legislation is the Family Educational Rights and Privacy Act (FERPA), which protects the privacy of student education records (Family Educational Rights, n.d.). Controls are required to prohibit unauthorized access and to control the sharing of the information.

Similar to the necessity to consider the increasing activities of international terrorist groups and organized criminal syndicates for global standards, national standards must also take into account the actions of such perpetrators. In the U.S. for example, the number of computer intrusions or attacks is rising. The U.S. Department of Homeland Security reported a 152% increase in such activities from fiscal year 2006 to 2007, from a recorded 24,000 reports of attempted breaches on private and federal systems to 37,000 (Montgomery, 2007). Security concerns may be specific to countries, regions, and industries, again calling for the need to share intelligence and security information across these units. However, such information sharing requires a balance between privacy interests and national security.

2.9.3. Organizational Standards for Information Security Management

Organizations must formulate their own practical and effective ISM in support of international standards, government regulations, and business goals (Biegelman& Bartow, 2006). Organizations tend to focus on technical solutions (Rasmussen, 2005). A disproportionate focus on technical security countermeasures, with less consideration for management controls, can contribute to the continuation of security concerns (D'Arcy &Hovav, 2007). However, in developing an organizational information security policy (ISM), information security should be linked to a business necessity. For example, The Vanguard Group, Inc. vigilantly guards the privacy of clients' social security numbers which are critical to the operations of the world's only virtual investment company (McGee, 2006). Customer concerns are an important factor to ISM practice (Ezingeard& Bowen-Schrire, 2007). A

balance between adequate data protection and reasonable, confidential use of information must be made (Fredericks, 2005). This balance extends to the use of out Sipior& Ward sourcing. If, for example, an outsourcer in a distant low wage country is used to maintain stored information, it may be more difficult to control security and privacy.

2.9.4. Information Security Management by Employees

Ultimately, the policies and procedures of the ISM are carried out by employees. Most security failures are related to errors caused by employees ("Security: Protect information first," 2007). For example, strategic level employees may poorly design an information security policy (ISP); Tactical and operation level employees may misinterpret a poorly designed policy or bypass policy requirements. Organizations recognize that their employees must protect information (Fredericks, 2005), as privacy breaches by employees can be an unwitting avenue to noncompliance. The biggest security threat results from malicious or negligent employees or from faulty controls and oversight (Swartz, 2007).

Thus, it is in the interest of the organization to hire employees whose individual privacy concerns, perceptions, and actions are congruent with professional values. As mentioned, outsourcers may not employ the same controls and oversight as those applied by employees of the corporation itself. The concern about the use of outsourcing, mentioned in the discussion of organizational standards, extends to employee practices as well. Recognizing the consequences of the ISM on employees and the organization is critical (Mogul, 2002). Security practices of employees should be placed within the more holistic security management decision-making context (Trim, 2007).

2.10. Related Works

Abdyli, 2014 study on proposing employees information security awareness program for Bank industry in Ethiopia. The research tried to answer three questions, what is the current information security awareness creation practice. What should the topics of an information security awareness program and how should the information security awareness program be organized to deliver the necessary information to Bank employees? A quantitative research approach with case study method is used. Findings showed that the information security awareness level of Bank employees is unsatisfactory.

Nigussie, 2015 assessing the practices of information security and identifying the challenges of information security policy helps the organizations to formulate and implement their information security policies efficiently and effectively. It will also help to inspire researchers on the study area.

Xiong, 2011 study on building information security management framework. This thesis defined three research questions in order to building a successful information security awareness programmed for NLI: What should the curriculum of an information security awareness programmed for NLI be? How should the information security programmed be organized to effectively deliver the necessary information to NLI employees? How should the effectiveness of the information security awareness programmed be measured in NLI?

Tebkew, 2013, Woretaw&Lessa, 2012 and others stated in the table had work on the information security system practices, to assess the current information security culture and identify key problems, to propose and develop information security management framework which will work in different in Ethiopia.

The researcher has comprised those researchers work like objectives, key findings and literature reviews.

Table 2.1: Related Works

Author	Objective	Key Finding
(Abdyli, 2014)	examine the level of technical observation on information security with a special focus on information security policies	Identified financial sector in the Republic of Kosovo is ready to implement the information security policies
(Alageel, 2003)	Research various prominent computer security training programs information assurance training and education	developed an information security management framework for the organization
(Alnatheer& Nelson, 2009)	to identify issues and factors that assist the implementation and the adoption of IS culture and practices within the Saudi environment	proposed a framework for understanding information security management and practices in the Saudi context
(Amare, 2015)	to examine the insider threat of the Ethiopian banking industry	identified insider threat and motivations within the Ethiopian banking industry, recommends best practices to mitigate those insiders malicious activities within the Ethiopian banking sectors
(Connolly, Lang, &Tygar, 2017)	investigate how procedural security countermeasures tend to affect employee security behavior	indicated that procedural security countermeasures tend to increase information security awareness, which, in turn, has a tendency to encourage compliant behavior
(Da Veiga, 2015)	To examine the level of information security culture between employees who had read the information security policy and employees who had not read the policy	provided statistical evidence that reading the information security policy contributes to influencing the information security culture positively

(Durmus, 2014)	to outline the awareness level of internet users and IT security personnel in public institutions	- identified that absence of security measures has caused some vulnerabilities in organization network - propose participants with relative website anda suggestion document
(Kruger, Drevin, & Steyn, 2006)	to describes a suggested ISM framework that may assist management of evaluating ICT security	proposed a framework for evaluating ICT security
(Negussie, 2015)	to asses information security and ISP practices, and to identify the challenges and prospects of information security policy in the Ethiopian banking industry	proposed recommendations in formulating and implementing ISP and ISM framework
(Siponen, 2000)	to construct a conceptual foundation for information systems/organizational security framework	a theoretical framework and selected current methods for increasing security awareness for employees
(Tebkew, 2013)	to propose and develop information security management framework which will work in banking industry in Ethiopia	developed information security management framework for the IFMIS
(Tse, et al., 2013)	to evaluate current information security practices in the financial industry and assess the information security awareness level for the employees in the industry	suggested that IT security management education should be made to different level of staffs such as executives, professional and general staffs

(Woretaw& Lessa, 2012)	to assess the current information security culture and identify key problems	recommended measures that can be implemented by practitioners to enhance the information security culture in the banking sector in Ethiopia
(Xiong, 2011)	building information security management framework	Proposed ISM framework for IFMIS to secure government budgets, use and update polices and other work policies and standards.

2.11. Summary

It is a must for MoF to pay more attention to the information security management issues within the financial sector especially IFMIS nowadays. The organization should establish information security governance framework and organize information security management frameworks.

According to NIST (2003), a strong IT security management cannot be put in place without significant attention given to organization IT users on security policy, procedures, and techniques, as well as the various management, operational, and technical controls necessary and available to secure IT resources.

In addition, those in an organization who manage the IT infrastructure need to have the necessary skills to carry out their assigned duties effectively. Failure to give attention to the area of information security management puts an enterprise at great risk because security of organization resources is as much a human issue as it is at ethnology issue.

Existing information security management frameworks are contextual and are not customized for Ethiopia. Contextual factors such as organizational, national and environmental affect the design of such model, frameworks and etc. There is also a local research gap in this area.

Chapter Three

3. Research Methodology

3.1. Methodology

The methodology is the way (or route) the researcher will need in order to achieve a certain result which can be knowledge, insight, design, intervention, or solution (Jocker & Pennink, 2010). Two approaches characterize much of the research in information science: behavioral science and design science. According to Hevner, March, Park, & Ram (2004), the goal of behavioral science is to identify and codify emergent properties and laws governing human and organizational behavior as it affects and is affected by the existing information systems. But the goal of design science is to create innovative artifacts that extend human and social capabilities and aim to achieve desired output. Design science research methodology help to provide a road map for researcher who want to use design as a research for information system research. (Peffers, 2007, p.8) The general objective of this research is proposing knowledge management framework that can promote indigenous knowledge management for agriculture. In order to meet this objective, this research will adopt design science research methodology. Because design science methodology is focused on the creation and evaluation of innovation information technology artifacts. According to (Peffers, 2007, p.3). The design science methodology process includes six steps: Problem identification and motivation, objective of the solution, design and development, demonstration, evaluation and communication.

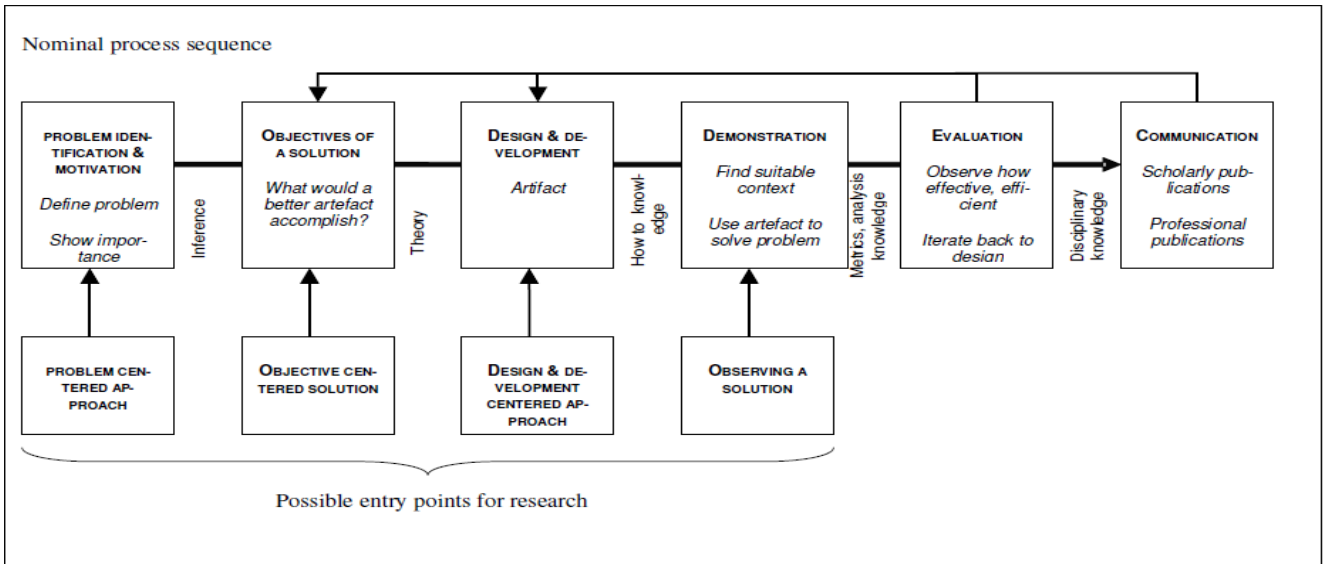

Figure 3.1: Design Science Research Methodology Process Models (Peffers et al., 2006)

3.2. Problem Identification and Motivation

This step is used to define the specific problem and justify the value of a solution. Justifying the value of a solution accomplishes two things: it motivates the researcher and the audience of the research to peruse the solution and to accept the results and it helps to understand the reasoning associated with the researcher's understanding of the problem (Peffers, Tuunanen, et al., 2006).

In this stage, the specific problem in IFMIS security management system is defined and the researcher will come up with a solution by proposing IS management framework that can integrate with other systems. The problem is mentioned previously in the statement of the problem. The lack of any security management mechanizes, IS framework, unfriendly for users and other related security related issues. So there is a need for an IS management framework that can manage and use properly. Literature had shown that one of the major problems in the IFMIS systems. This research, therefore, tries to fill this gap by proposing information security management framework for strategic and effective implementation of IFMIS in MoF context which enhance the existing knowledge. The proposed framework can also be used as a guideline by the ministry to conduct information security management for successful and secure IFMIS system for its employees to strengthen and to government finical, property, procurement and other IFMIS modules.

3.3. Objectives of the Solution

In this part, the research aims to infer the objective of a solution from the problem definition and knowledge of what is possible and feasible. The objective of the solution is to integrate IFMIS working environment and its security by using the proposed ISM framework. The success of the implementation of new ISM security framework depends on the success of communication between IFMIS security agenda and the formal MoF IT policy and other integrated systems.

3.4. Methods, Data Collection Instruments for Problem Identification

3.4.1. Research Approach and Method

Research approach is a plan and procedure for research that range the steps from broad assumptions to detailed methods of data collection, analysis, and interpretation (Creswell, 2013). The two basic approaches to research are quantitative and qualitative, not forgetting a mixture of both. Quantitative approach involves the generation of data in quantitative form

which can be subjected to rigorous quantitative analysis in a formal and rigid fashion (Kothari, 2004). It generates statistics through the use of large-scale survey research, using methods such as questionnaires and structured interviews. Whereas qualitative approach tries to explore attitudes, behavior and experiences through such methods as interviews or focus groups (Dawson, 2002). Qualitative approach also attempts to get an in depth opinion from participants. This research will follow qualitative research method. The researcher also uses a case study also known as a method for in depth study. "A case study method is a careful and complete observation of an individual or a situation or an institution is done; efforts are made to study each and every aspect of the concerning unit in minute details and then from case data generalizations and inferences are drawn" (Kothari, 2004).

3.4.2. Data Type and Source

The source of data includes both primary and secondary type of data. The instrument includes for the primary data, questionnaire and interview are the main ones while for the secondary data, review of different manuals, and journal with regard to the Information Security Management for Strategic and Effective Implementation of Integrated Financial Management Information System (IFMIS) in MoFare studies in more detail. The primary data is collects from employee of the IFMIS/Ibex project and other government institutions that is accountable for MoF.

3.4.3. Primary Data

The researcher uses observation, semi-structured interviews and group discussions.

Semi- structured Interview

Semi structured interviewing help the researcher to know specific information which can be compared and contrasted with information gained in other interviews(Dawson, 2009, p.27). The interview will be conducted with information technology, IFMIS/IBEX project, HR, Finance and others departments.

This is done for IFMIS/ibex project IT experts to understand what kind of ISM framework enabler and barriers are there, others to understand how modern working environments is fundamental for their work and supported by different systems.

Group Discussion

Focus Group may be called discussion group or group interview. A number of people are asked to come together in a group to discuss certain issue (Dawson, 2009, p.29). Focus group discussion will be conducted for IFMIS users to study the current status of acquiring, sharing, preserving and using ISM knowledge's in IT departments. The advantage of using focus group includes the ability to gain understanding about group insight and can receive a wide range of responses during discussion.

3.4.4. Secondary Data

Secondary data is data that already exist, may easily be obtained and has historical value. The data is considered overall to be useful when establishing comparisons and evaluating data. Secondary data is divided into internal and external secondary data. Internal secondary data is data that has already been produced by organizations and private individuals and gathered to constitute a veritable data source. External secondary data are studies that have been published or are in the process of being published within the studied research area and are indispensable to the spread of the specific knowledge and evolution of the research *(Thietart, 2001).* Moreover, secondary data has been developed to help to solve the problem in hand and should therefore be relevant, accurate and available. Looking at secondary data is useful not only to find information but also to better understand and explain the research problem. Examples of information being viewed include books, journal articles, online data sources and web pages (*Ghauri & Grønhaug, 2005).* In this thesis, the secondary data is collected mainly from the internet and MoF library. The researcher has gathered the secondary data from the official website of the MoF and some other related websites. The e-news papers, e-journals and e-books have also been used to collect data.

3.4.5. Research Population and Sample Size

The population of this study is the, employees of MoF, Governmental Institutions that are accountable to MoF. The research has focused on the staff of information technology, computer based and information archiving departments in those institutions because it discusses the Information Security from a managerial perspective. A comprehensive case studies method is used to apply this study on the Governmental Institutions, in which this population consists of (108) employees in a variety of job levels working in departments, such as information technology, IFMIS/IBEX project, HR, Finance and others departments. Additionally 12

technical employees in a variety of job levels working in network, security and system administrators were included.

Target Population

No.	Department/Organization	Gender		Total	Education level					Remark
		Male	Female		L.4	Dip.	Deg.	Mas.	Others	
1	IFMIS Project	19	10	29	0	0	18	10	1	
2	IT Experts (Support)	7	4	18	3	7	8	0	0	
3	Human Resource	5	3	8	0	0	7	1	0	
4	Finance and Property Management	5	11	16	2	5	9	0	0	
5	Network Administrator	5	3	9	0	0	6	3	0	
6	System Administrator	4	3	7	0	0	5	2	0	
7	Security Administrator	9	3	12	0	0	8	4	0	
8	MiNT	3	2	5	0	0	4	1	0	
9	INSA	3	1	4	0	0	1	3	0	
Total Population				108	5	12	66	24	1	

3.4.6. Case Study

In this study, cases itself are in the centrums of the research problem, since the aim of the research is to propose information security management framework for Strategic and Effective Implementation of Integrated Financial Management Information System (IFMIS) in MoF. Therefore, the phenomenon as a whole is an important factor in this research, containing both, the theoretical knowledge of the research and the IFMIS context around it.

3.5. Design and Development

In this stage, the study aims to create artifact solutions like framework, constructs, models, methods. A design research artifact can be any designed object in which a research contribution is embedded in the design. After defining the objective of the solution the proposed framework is developed based on the prior literature that is focused on security management framework.

3.6. Demonstration

Demonstrate the use of the artifact to solve one or more instances of the problem. The researcher uses the developed artifact to solve the existed problems in a better manner to prove that the idea works. Resources required for the demonstration includes effective knowledge of how to use the artifact to solve the problem. The researcher follows mixed quantitative and

qualitative data collection instruments. Both primary and secondary data source is used in this study.

3.7. Research Design

Research design is the conceptual structure within which research is conducted (Kothari, 2004). Accordingly, the researcher of this study design arrangements as follows

3.8. Evaluation

The evaluation framework is an essential stage. In this stage, the study aims to observe and measure how well the framework supports a solution to the problems. This activity can be done by comparing the objective of the solution to the actual observed results from the demonstration. Thus, evaluation is used to prove how the proposed framework is effective and efficient to solve the problem in IFMIS. The proposed IS management framework is evaluated by key experts which are consists of IFMIS staffs and other IFMIS user departments.

The evaluation is conducted in two steps. First, the draft IS management is demonstrated to the key experts and accept the overall comments. Then after modifying the framework based on their comments, the second evaluation is captured by using questionnaires and the questionnaire content is criteria are adopted from (Ahmad, 2010; Prat, Comyn-Wattiau, &Akoka, 2014; Taddele, 2015). The researcher focuses on the four dimensions. Utility and applicability of the framework, consistency with organization, the content of the framework, and usefulness of the framework.

3.9. Communication

Communicate the problem and its importance, the artifact, its utility and novelty, the rigor of its design, and its effectiveness to researchers and other relevant audiences. The contribution of this effort will be disseminated for relevant experts.

3.10. Ethical Concerns

The researcher will use a recommendation letter from the university. During the interview and focus group discussion, the researcher will be cautious in maintaining ethical standards, including confidentiality and respect for the community members specially the elders. To respect the participants' right to privacy and the result will be present anonymously. The data gathering process will be held on the consent or agreement of the respected bodies. A researcher will give promise to provide copy of thesis work to the organization to implement it. Finally the data collected from the MoF will be used for education purpose only.

Chapter Four

4. Data Analysis and Discussion

4.1. Introduction

This chapter presents the findings followed by discussion. The results section report findings of the study based on the methodology applied to gather information. The discussion is to interpret and describe the significance of the findings against to research question.

This analysis employs the information gathered from interview and questionnaires from the key informants. Each table has a consolidated description based on the information that the researcher gathered.

4.2. Response Rate

To propose ISM framework for IMFIS the researcher collected and distributed the research questioners for data collection purpose, depending on sample of the study, a total of 108 questionnaires were distributed to respondents and 86 of them are collected but from the collected questionnaire 4 of them are not fit for analysis as a result of incompleteness the total questionnaire used for analysis is 82. Therefore the response rate stood at 76 percent which show the response rate is acceptable for analysis.

4.3. General Information

4.3.1. Respondents Gender

Table 4.1: Gender of Respondents

		Frequency	Percent
Valid	F	30	36.6%
	M	52	63.4%
	Total	82	100.0%

The table above shows sex composition of respondents that participated in filling questionnaires. As per the result, from the total respondents, 52(63.4%) of them are Male while the remaining 30(36.6) are Female employee of the Minister.

4.3.2. Educational Background of Respondents

Table 4.2 : Educational Background of Respondents

		Frequency	Percent
Valid	Level 4	3	3.66%
	Diploma	5	6.09%
	Degree	52	63.41%
	Masters	14	17.07%
	Others	8	9.76%
	Total	82	100.0%

Table 4.2.Above shows educational background of respondents. From the total respondents, 3(3.66%), 5(6.09%), 52(63.41%) are level 4, Diploma and Degree holders respectively while educational background of the remaining 14(17.07%) and 8(9.76%) are Masters and others respectively.

4.3.3. Job Category of Respondents

Table 4.3: Job Category of Respondent

		Frequency	Percent
Valid	a. Management level	16	19.5%
	b. Senior level	36	43.9%
	c. Officer level	23	28.0%
	d. Junior level	7	8.6%

Table 4.3.Above shows among the respondent's senior level staffs are covering the highest percentage of 43.9%, 28.0% officer level staffs, 19.5% management and 8.6% are junior level.

4.3.4. Work Experience of Respondents

Table 4.4: Work Experience

		Frequency	Percent
Valid	0-5 years	9	10.97%
	5-10 years	23	28.04%
	10-15 years	27	32.92%
	above 15 years	23	28.04%
	Total	82	100.0%

Respondents of the questionnaire served the Minister for different period of time as per the result depicted in the table above. From the total respondents, 9(10.97%) of them are with the ministry for five years and below, 23(28.04%) fall in between six to ten years of service, 27(32.92%) are with the ministry for above eleven years to fifteen years and the remaining 23(28.04%) are in service of the ministry for above fifteen years. It is possible to state that majority of the respondents are with the ministry for a long period of time which means they know the ministry very well from which it is possible to get the required information for the study especially financial sectors.

4.4. Security Incident and Reporting

In the second section respondents' internet usage and time spent on it, their experience of information security incidents and whether they report to responsible party or not if any incident occurred were asked and their response is summarized as shown in Table 1.The internet usage of respondents have a ratio of 96.4% in favor of usage. The rest 3.6% respondents don't use internet that indicates most of the respondents has the experience of using Internet that might further indicates the likeliness of the IFMIS/IBEX/ibex project employee subjected to security incidents. Among those who use internet, 49.8% can be categorized as an 'average spending time' while 23.1% and 17.0 % of them can be categorized as 'little spending time' and 'very little spending time' respectively. The respondents who spend "much" and "very much" time to use internet were 6.7% and 3.5% respectively. The cumulative 58.2 % of respondents were categorized as internet users who spend an average and beyond average time that likely identified them as Employees 'spend average of their time on internet that it makes them possible targets in un trusted network internet. This emphasizes how the information security concerns are more important issues to be realized. Of course,

whatever time spent, there is a security risk since there is internet involvement. Membership for social media such as Face book, Instagram, and WhatsApp is getting more attraction nowadays as seen from the respondents answer with having a highest 79.3% compared to those who doesn't 8.5%. This also indicates respondents may be subjected to any security incidents far more using social media. Therefore, it is important to aware them how to act in using such media. Durmus (2014) also agreed in the importance of awareness for social media users on how to act along with the code of conduct in social media.

Table 4.5: Frequency Analysis of Security Incidents and Reporting

Question	Option	Frequency	Percent
Q6.Do you use internet?	a. Yes	79	96.4
	b. No	3	3.6
Q7.How much time do you spend on the Internet?	a. Very Little	14	17.0
	b. Little	19	23.1
	c. Average	41	49.8
	d. Much	5	6.7
	e. Very Much	3	3.5
Q8.Do you have a membership for any social media platform like Facebook, Twitter, Instagram and so on?	a. Yes	75	91.5
	b. No	7	8.5
Q9.Which personal information that you mostly share in social media? (You can select more than one option)	Picture	65	79.3
	Video	39	47.5
	Name, surname	13	15.9
	Birth date	7	8.5
	Name, surname of family members	5	6.1
	Identification number	3	3.7
	Phone number	0	0
	E-mail address	12	14.6
	Researches/studies	17	20.7
	Emotions	14	17
	Thoughts	9	10.9

	Hobbies	23	28.0
Q10.Have you ever faced with incident about information security?	a. Yes b. No	37 45	45.1 54.9
Q11.Do you think that you will probably face with such incidents in the future?	a. Yes b. No	49 33	59.8 40.2
Q12.You faced with a content or post in a social media or a website that violate your personal rights. Where do you report?	a. My family and/or friend b. The nearest police department c. Relative website admin d. Internet Service Provider e. Cyber Security Office (Information Network Security Agency-INSA) f. Prosecution Office g. I do not know where to report h. I do not report	7 3 9 3 6 1 31 22	8.5 3.6 10.9 3.6 7.3 1.2 37.8 26.8
Q13.When you faced with unwanted content or post (encourage/help suicide and prostitution, harmful drugs, gambling, nudity, sexual harassment and crimes against Ethiopia etc.). Where do you report?	a. My family and/or friend b. The nearest police department c. Relative website admin d. Internet Service Provider e. Information Network Security Agency-INSA f. Prosecution Office g. I do not know where to report h. I do not report	17 11 8 6 3 2 21 14	20.7 13.4 9.8 7.3 3.6 2.4 25.6 17.1

Respondents were asked about which personal information they mostly share in social media. Respondents' respond picture more than 79.3%, video more than 47.5%, hobbies 28% and birth date 8.5% in decreasing order. Most of the time when we join a social network information such as name, surname, picture, emotions, thoughts, hobbies and researches/studies are asked to share. However, sensitive information such as identification number, phone number and sometimes email address should not be given or shared to anyone. We should also reconfigure the privacy settings of social media we use otherwise everything we do will be public or visible to everyone. The respondents' security practice is a little bit above average but needs

progressive awareness because one way or another their social media usage and sharing may conflict with the organization policies and procedures.

Almost one third of the respondents have faced information security incident and 59.8% of the total respondents think that they will probably face with such incidents anytime in the future including those didn't face yet. This indicates that employees may need to have a basic understanding how to use the internet in order to protect them from cyber-attacks such as social engineering and phishing attacks.

According to Durmus (2014) if a person face with a post or a content that violates his/her rights the correct way of behavior is to consult to "relative website admin", "cyber security branch offices" affiliated to police department in the city you live and "prosecution offices". In this context, the respondents who will report to relative website admin, cyber security office and prosecution office are 10.9%, 7.3% and 1.2% respectively. Employees that will report to the nearest police department are 3.6% where 8.5% report to their families and 3.6% report to internet service provider. However, this result is unsatisfactory compared with the respondents who do not know where to report or even do not report any having more than 53%. Respondents know less about the authority in charge of concerning cyber-attacks and violation of personal rights on the internet when they are violated.

The respondents awareness level is somehow similar with the previous question when it comes to facing with unwanted content or post (encourage/help suicide and prostitution, harmful drugs, gambling, nudity, sexual harassment and crimes against Ethiopia etc.).And where they report if any? Here 13.4% report to the nearest police department, 3.6% report to cyber security office and 20.7% report to their families or friends even if it didn't concern them. However, 25.6% do not know where to report and 17.1% totally do not report indicating the awareness level is unsatisfactory. This means more than 45% of the respondents do not take any counter measures for this kind of cybercrimes.

4.5. E-mail Security

This section covers security areas such as email usage, spam email, phishing links. The findings are shown in Table 4.6

Table 4.6: Frequency Analysis of Email Security

Question	Option	Frequency	Percent
Q14.Do you use e-mail address?	a. Yes b. No	79 3	96.3 3.7
Q15.What is Email Spam?	a. Spam is an anti virus solution b. Spam is a firewall c. Spam is an unwanted and mass e-mails d. Spam is an e-mail attachment	9 6 60 7	10.9 7.3 73.2 8.5
Q16.What do you do when you got an e-mail asking to update your personal info by clicking the link in the e- mail body?	a. I click the link if logo and address of the ministry right b. I do the same if my close friends update their info c. I make a call to system admin to get information about thee-mail d. I do not have any idea	35 27 13 7	42.7 32.9 15.8 8.5
Q17.What do you do when you got an e-mail from your friend but file extension of the attachment and domain	a. It is safe to open up attach as the sender is friend of mine. b. I reply to e-mail to confirm if it is really sent by my friend	8 23	9.8 28.1
name of the address (the section after '@' sign) is weird?	c. I create new post to send to my friend's address in my contact to for confirmation d. I do not have any idea	19 32	23.1 39.0

In terms of email address 96.3% of the respondents use email to communicate where as3.7% do not use it. Among this, 73.2% of the respondents know about spam email which is a satisfactory result.

Participants' response when they got an email to update their personal information by clicking the link in the email body is unsatisfactory with only 15.8% make a call to IFMIS/IBEX project office to get information about thee-mail. The rest 42.7% click the link if the logo and address of the ministry IT departments right, 32.9% do the same if their close friends update their information, and 8.5% do not have any idea what to do with it. This result is unsatisfactory regards phishing attacks awareness.

Almost 28% of the respondents replied I do not have any idea what to do when they got a phishing email and asked to forward to other people. The respondents that forward to all of their contacts results 9.8%and that forward to their closet contacts count 28.1%. Only23.1% of respondents notify the sender not to forward chain e-mails which is a good security behavior. The same is true when respondents receive file extension of the attachments and domain name addresses are confusing where 39.0% replied I do not have any idea what to with it. This finding shows that more than 75% the respondents will probably be vulnerable to phishing attacks by-email.

4.6. Safely Use of Internet and Computer

These section present finding which includes precautions taken in case stolen computers, locking user account and distinguishing a safe website. The results are shown in Table 4.

For the distribution of respondents regarding which precautions they take in case their laptop is stolen, all the choices are correct. However, one thing to consider is that their importance level varies based on priority. The first thing is to note down the serial number and physical address of the laptop a separate safe place to find easily lately (Durmus,2014).This indicates keeping its serial number and physical MAC address is highly important to find a stolen device. Here 36.3% of the respondents' backup sensitive data and 24.4% set password for their user accounts. Even if the answers are right, the respondents who keep its physical MAC address (8.5%) and keep its serial number (17.3%) are unsatisfactory level as compared with the first two. The list continues with 6.5% both encrypt their sensitive data and install GPS software to trace, 5.4% install an alarm software and 3% mark a sign on their laptop. Among all the choices the respondents are interested in backup their sensitive data and set passwords for their user accounts rather than being able to keep its serial number and/or MAC address in the first place. This finding shows although the choices are correct, the level of especially keeping its serial number is very unsatisfactory.

Table 4.7: Frequency Analysis of Safety use of Internet and Computer

Question	Option	Frequency	Percent
Q18.Which precautions do you take in case your laptop is stolen? Choose more than one	a. Keep its physical (MAC) address	7	8.5
	b. Keep its serial number	29	17.3
	c. Backup my sensitive data	61	36.3
	d. Encrypt my sensitive data	11	6.5
	e. Install an alarm software	9	5.4
	f. Set passwords for my user accounts	41	24.4
	g. Mark a sign to unrecognizable place on my laptop	5	3.0
	h. Install a GPS software to trace remotely	11	6.5
Q19.Do you lock your user account with password when you took a little break from work or leave your seat? Choose more than one	a. I only lock in my business laptop	11	6.7
	b. I only lock in my personal computer	32	19.6
	c. I use it in both	75	46.0
	d. I do not lock as I go back to work in short time	31	19.0
	e. I do not lock as my data is not that critical	14	8.6
Q20.How do you distinguish if a website is safe to surf or not? Choose more than one	a. Websites that offer freeware are safe	9	6.1
	b. Online casinos are safe	4	2.7
	c. It is safe if a security logo exists	31	21.1
	d. It is safe if the web browser shows small gold lock pad	8	5.4
	e. It is safe if its address starts with "https://" instead of "http://"	22	15.0
	f. It is safe if it appears to be popular	6	4.1
	g. I am having difficulty in distinguishing	67	45.6

The next part is whether the respondents lock their user account with password when they took a little break from work or leave their seat. Respondents that use password in both business and personal computer count less than 50% which is unsatisfactory level. The rest 19.6% only lock their personal computer and 6.7% only lock their business laptop whereas 19% and 8.6% do not lock as they go back to work in short time and their data is not that critical respectively. Literatures such as Abdyli (2014), Durmus (2014) and Xiong (2011)tell us the correct way of behavior is to use password protection in both personal and business computers even if we will go back in home and business environment or even if data we stored is not much critical. This is just a way of developing a proper security habit before gaining it as behavior.

Employees were also asked how to distinguish if a website is safe to sure for not. There are two answers here, it is safe if the web browser shows small gold lock pad and if its address starts with “https://” instead of “http://”. However, only 5.4% and 15% respectively select those choices. More than 45% of the respondents have difficulty indistinguishing. This is also very unsatisfactory level and need high attention.

4.7. Threats and Preventive Measures

This section presents findings related to file sharing software and threats generated by them, software updates, antivirus usage and backup as follows. The results are illustrated in Table 4.8

Table 4.8: Frequency Analysis of Threats and Preventive Measures

Question	Option	Frequency	Percent
Q21.Have you ever used file sharing software like uTorrent, BitTorrent, eMule and so on?	a. Yes b. No	31 51	37.8 62.2
Q22.Which ones are the threats originated by file sharing software?	a. I may violate copyright of music, video or any other software b. The program I downloaded may include malicious software c. I may allow bad guys with bad intentions to see my personal data	23 47 12	28.1 57.3 14.6

Q23.What do you think about updates of your types of software installed in your computer?	a. I install at once if there is available update	31	37.8
	b. I install few days later after I take care of my other tasks	17	20.7
	c. I get help from my closest friends	15	18.3
	d. I do not have any idea	19	23.2
Q24.What type of antivirus software do you use in your computer?	a. I use free antivirus software	37	45.2
	b. I use cracked antivirus software	7	8.5
	c. I use license paid antivirus software	19	23.1
	d. I do not use antivirus software	5	6.1
	e. I do not have any idea	14	17.1
Q25.How often do you make security scanning in your computer?	a. Never	11	13.4
	b. Rare	23	28.1
	c. Average	32	39.0
	d. Often	9	11
	e. Very often	7	8.5
Q26.How often do you backup your data in your computer?	a. Never	13	15.9
	b. Rare	18	21.9
	c. Average	37	45.1
	d. Often	11	13.4
	e. Very often	3	3.7
Q27.Which one of the statements below is true?	a. Only firewall is sufficient in a computer	5	6.1
	b. Only antivirus software is sufficient in a computer	11	13.4
	c. Both antivirus software and firewall perform same functionalities	21	25.6
	d. Both antivirus software and firewall need to be used updated in a computer	45	54.9

Employees that have ever used file sharing software such as torrent and BitTorrentare20%. Out of which 28.1% respondents knows these file sharing software may violate copyright of music, video or any other software, 57.3% knows the downloaded program may include malicious software and 14.6% knows it may allow bad guys with bad intentions to see their personal data. All answers are correct however, the percentage is very less. This awareness level is not enough and seen as below average.

Regarding updating installed software 37.8% of employees install at once if there is available update. This is number is way below average resulting unsatisfactory level. 20.7% install updates days later after they take care of other things and 18.3% get help from their close friends while 23.2% do not have any idea what to do.

More than 80% respondents use different types of antivirus for their computer system while 17.1% do not have any idea about the types of anti viruses and 6.1% do not use any. Employee's usingafreeantivirussoftwareare45.2%, using cracked antivirus of twareare 8.5% and using licensed software are 23.1%. Employees close to 60% perform security scanning in average or often period while the rest rarely or never perform security scanning. Most types of free antivirus software do not provide full protection.

They commonly come with features to scan hard-drives and external drives while licensed one's are able to provide full protection like anti-spam filtering, identifying unsafe phishing websites, and malware and firewall protection. As for the cracked antivirus software, too few of them are free of Trojans or backdoors (Durmus, 2014). Therefore, using a license paid antivirus is better and also costly compared to the rest. As an organization all we can force all employees to use license paid antivirus by installing on each device. However we cannot force users what to use since each have its pros and cons, but we can teach them the differences.

Employee's take back up of their computer data on average and above level of more than 53% of the total respondent. They were also asked about firewall and antivirus. 54.9% of the employees answered that both antivirus software and firewall need to be used updated in a computer. This is average level and needs to be communicated compared to the rest incorrect choices counting39.6%.

4.8. Password Management and Security

This section describes findings related to setting a password, interval of changing it and sharing to other people as follows in Table 4.9.

Table 4.9: Frequency Analysis of Password Management and Security

Question	Option	Frequency	Percent
Q28.What do you think about changing your passwords?	a. I change my password only if I doubt that somebody stole it	26	31.7
	b. Changing process is boring	5	6.1
	c. I change my password regularly	33	40.2
	d. I change my password only if I have to give it to my friend	18	21.9
Q29.How do you set your password?	a. I use the password preset by the system	7	8.5
	b. I set short password not to forget	21	25.7
	c. I set all of my passwords same not to forget	9	10.9
	d. I set my password including upper, lower letters, numbers and special characters	34	41.5
	e. I set my passwords with 8 characters at least if the system allows	9	10.9
	f. I use password generate or tool	2	2.4
Q30.With whom do you share your computer's authentication password?	a. I share with my trusted friend	28	34.1
	b. I share with my trusted relative	7	8.5
	c. I share with IT division in my corporate	9	10.9
	d. I don't share with anyone	38	46.3

There were three correct answers for the password setting questions namely I set my password including upper, lower letters, numbers and special characters, second I set my passwords with 8 characters at least if the system allows and third I use password generator tool. Respondents that select the mentioned answers count 55%. However, 45% of them selected the wrong answers I use the password preset by the system, I set

short password not to forget and I set all of my passwords same not to forget. These are not good security practices and need focus because password is critical aspect when dealing with authentication and authorization of system. Employees that change their passwords regularly take 40.2% while those who change their password only if they doubt that somebody stole it and those who change their password only if they have to give it to a friend counting 31.7% and 21.9% respectively. This is close to average level regarding changing on regular basis but a lot need to be done to make this critical aspect understood by employees so that all of them should follow these good practices regards password. There is a bad security practice related to password sharing. The number of employees that do not share their password only counts 46.3% which is unsatisfactory result and the rest share their password to their close relative, friend or the IT department. It is a must to create awareness to employees about password management.

4.9. Information Security Terms and Social Engineering

This last section presents findings of information security terms and social engineering as shown in Table 4.10.

Table 4.10: Frequency Analysis of Information Security Terms and Social Engineering

Question	Option	Frequency	Percent
Q31.Who is responsible for Information Security?	a. Information owner	24	29.3
	b. Information user	43	52.4
	c. Information manager	15	18.3
Q32. "A chain is as strong as its weakest link." What does this motto mean to you?	a. It could cause security vulnerability if an IT personnel walkout	7	8.5
	b. An information security awareness level in a place is as much as a person who has least information security knowledge in place	41	50.0
	c. Information security is provided only if you have skilled technical team	19	23.2
	d. A corporate can be exposed to vulnerability if an un trusted	15	18.3

	employee is recruited		
Q33.What does "social engineering" mean?	a. It is a security add-on checking if a website is safe b. It is an art of deception that makes use of getting information that need to be kept secret in normal circumstances by using convincing and influencing abilities c. To be exposed to insulation by an entity you have just met on social media	22 51 9	26.8 62.2 10.6

Employees answer to who is responsible to information security among Information owner, Information user and Information manager choices, 52.4% of them answered information user while the other two choices have very less percentage. Here all choices have more or less equal impacts on information security however the respondent's only focus on one entity. This awareness is unsatisfactory and all the three parties should have been selected with close percentage since they have proportionally high impact on security.

Employees were asked to obtain if a general security statement has a meaning for them, a chain is as strong as its weakest link. Where 50.0% of the employees got the correct answer an Information Security Awareness level(ISA) in a place is as much as a person who has least information security knowledge in place which is average level getting that humans are the weakest links (Alageel, 2003; Connolly et al., 2017 and Kruger et al., 2006). They were also asked about what a social engineering means in security term where 58% of the respondents have average and above level of know-how that it is an art of deception that makes use of getting information that need to be kept secret in normal circumstances.

4.10. Technical Category Result

A total of 12 questionnaires were distributed in person for the technical users and all of them were responded. The technical category questionnaire is categorized into ten sections. The first is related to demographic features and the rest nine sections deals with technical aspects related to information security awareness. The data were analyzed using frequency analysis. The presentations and findings are as follows.

The first section includes findings of gender, age, qualification, job category and work experience and presented in Table 4.11.

Table 4.11: Frequency Analysis of Technical Category Demographic Features

Question	Option	Frequency	Percent
Q1. Gender	Male	10	83.3
	Female	2	16.7
Q2. Age	18-24	2	16.7
	25-34	6	50.0
	35-44	1	8.3
	45-54	2	16.7
	> 55	1	8.3
Q3. Professional qualification	Diploma	0	0
	Degree	9	75.0
	Masters	3	25.0
	PhD	0	0
Q4. Job category	Management	5	41.67
	Senior Level	2	16.67
	Officer Level	1	8.33
	Junior Level	4	33.33
Q5. Work experience	0-1 year	0	0
	1-3years	4	33.33
	3-5years	0	0
	5-10 years	5	41.67
	Above 10 years	3	25

As we can see from Table 8 the technical questionnaire respondents are composed of 83.3% to 16.7% in favor of male participants. Most of the age range [25-34] fall 50% while [18-24]and [45-54] take 16.7% each. More than 75% of the respondents have first degree at least. The job category distribution has 45.5% of management level staffs and the rest contains senior, officer and junior level employees. Respondents who have 5-10 years or above experience are more than 60% and one third of the respondents have 1-3 years of experiences.

4.10.1. Security Standards, Procedures and Training

This section includes findings of nine questions related to security standards, procedures and training and presented using tables.

Table 4.12: Frequency Analysis for Use of Security Technologies

Question	Option	Frequency	Percent
Q6.Which security technologies do you use in your organization? (You can select more than one option)	Antivirus software	10	83.3
	Firewall appliance	8	66.7
	Web Application Firewall	2	16.7
	Database Firewall	3	25.0
	Antispyware software	0	0
	Virtual Private Network	4	33.3
	Vulnerability/Patch Management	12	100.0
	Data encryption on storage units	1	8.3
	Web / URL filtering	4	33.3
	Application Firewall	3	25.0
	Log management software	1	8.3
	End point security / NAC (Network	12	100.0
	Admission Control)	1	8.3
	Data loss prevention / content monitoring	4	33.3
	Server-based ACLs (Access Control Lists)	12	100.0
	Information Forensic Tools	12	100.0
	Public Key Infrastructure (PKI)	2	16.7
	Smart cards and keys	12	100.0
	Wireless security	12	100.0
	Virtualization specific tools	3	25.0
	Static accounts user name and passwords	12	100.0
	Biometric Information Security	1	8.3
	Management System Other	2	16.7

As seen in 4.12 employees have answered antivirus software, firewall appliance, vulnerability/patch management, end point security, information forensic tools, public key infrastructure, wireless security, virtualization and biometrics are mostly used in the organization. However, the organization doesn't have/use

technologies such as web application and database firewall, and data loss prevention or content monitoring. This is a major issue since we cannot say we are secured without confirming that our data and web applications are secured in the first place. This implies the organization's data and web applications are not secured enough and their content is not monitored properly even if the organization has firewalls which work on network layer level. It is further shown that information security management system is not used as well.

Table 4.13: Frequency Analysis of Q7- Q9

Question	Option	Frequency	Percent
Q7.Do you follow a standard for network and information security in your organization? (You can select more than one option)	a. ISO/IEC27001/2	2	20.0
	b. PCI DSS (Payment Card Industry Data Security Standard)	1	10.0
	c. COBIT (Control Objectives for Information Technology)	0	0
	d. NIST (National Institute of Standards and Technology)	1	10.0
	e. Another information security standard	0	0
	f. None	1	10.0
	g. I do not have any idea	5	50.0
Q8. Do you have any procedure in case of being exposed to Cyber-attack?	a. Yes	3	25.0
	b. No	2	16.67
	c. We use another technology/method	2	16.67
	d. I do not have any idea	5	41.67
Q9. Which information security policies do you put into practice in your organization?	a. Network policies	8	66.7
	b. User policies	7	58.3
	c. Laptop policies	4	33.3
	d. Intrusion Detection/Prevention policies	2	16.7
	e. Patch/Updating policies	1	8.3
	f. Another policy	0	0
	g. None of them	0	0
	h. I do not have any idea	3	25.0

As we can see from Table 4.13, 50% of the technical staffs do not have any idea about standard network and security policy and cyber attacks and 10% answered we do not use or follow any standard. This implies there may not be a specified standard for network and information security in the organization and if there is one, it

is not well communicated for all the staffs and not well enforced as we can see from these contradicting responses. On the other hand, 70% respondents do not know or have any procedure in case of being exposed to cyber-attack. This is a frightening finding since nowadays no single organization is safe from cyber-attacks and having no or poor countermeasures will jeopardize the business (Siponen, 2000). Multiple information security polices used in the organization, network polices having the highest percentage 66.7%. However, intrusion detection/prevention polices and patch/updating polices are fearless which are a major gap. The lack of these polices cause such as vulnerabilities in systems and may highly increase attack level (Siponen, Pahnila, & Mahmood, 2010). Abdyli (2014) stated without standards that provide objective criteria for information security choices, Information security experts make choices based on undeserved aspects that might include lack of Knowledge, supposed constraints, inappropriate confidence and personal motivation. Abdyli (2014) further stated it is recommended that internal policies defined by the ministry are to be applicable and in line with these international standards. The support of management of the project is also necessary on the implementation phase of these standards.

"The Ministry need to use a different mechanism like making effective service and ICT infrastructure policy, security policy for doing risk assessment on the service and ICT infrastructure to manage the challenges it is mandatory increase the number of well-trained ICT professionals to fix the problem in the right time in order to doesn't return back the problem regularly." (ICT Department Head)

Table 4.14: Frequency Analysis of Q10-Q14

Question	Option	Frequency	Percent
Q10. Are your employees being trained about Information security management framework?	a. Yes b. Sometimes c. No d. Another	0 3 9 0	0 25.0 75.0 0
Q11. How often do you train your employees about information Security?	a. Once a year b. Once a week c. Few times a year d. Once a month	3 0 9 0	25.0 0 75.0 0

Q12. Do you follow any resources, materials for oncoming technologic news and developments?	a. I follow some resources at home	4	33.33
	b. I subscribe to news bulletins and get-mail regularly	2	16.67
	c. I benefit from the organization web portal	1	8.33
	d. I sometimes follow magazines	4	33.33
	e. Organization training is enough for me	0	0
	f. I do not follow any resource	1	8.33
	g. Another	0	0
Q13.Have you ever experienced any security incident in your organization network? (e.g. threat, attack, malicious software) If any, how many times did you face?	a. 1- 5times	2	16.67
	b. 6-10times	0	0
	c. More than10	0	0
	d. Never experienced	10	83.33
Q14. How long does it take to close the security breaches?	a. Between 0-3months	0	0
	b. Between 3-6months	0	0
	c. Between 6-9months	1	8.3
	d. Between 9-12months	0	0

In Table 4.14 respondents were asked about whether their employees are being trained about information security awareness where 75% of them answered they are not. Out of the 25% who answered they sometimes do train, only 16.7% of them train their employees few times a year. This is very unsatisfactory result. It is one objective of this paper that employees have information security awareness program. For instance, if employees are not aware on information security, it will be difficult for them to protect the corporate at the same time themselves from any kind of security attacks (Connolly, Lang, &Tygar, 2017). This implies employees must be aware of information security within their organization, and information security awareness programs must be established in line with IFMIS/IBEX/IBEX project information security policies and relevant measures (Abdyli,2014).Employees stay informed with IT materials by subscribing to news bulletins and get email regularly taking 58% of the total respondents. While following magazines and following some resources at home take 33.3% each. This indicates more than 80% of the respondents stay

informed about information technology including security aspects which is a good security practice. Employees who experienced a security incident were 10% and the time it took to close the security breach is between 6-9 months. This finding doesn't mean the organization is this much secured or cyber-attacks were not attempted as the numbers were expected to rise since it is a financial institution. There may be different reasons for this outcome for instance, the less incident number may indicate that there were not really any major attacks or may be employees are protecting the organization's reputation or image against outsiders.

"For the futures Minister has on progress to work a policy, strategy and any kind of formal written security policy that governs the IFMIS/ibex and other employees." (*Project* Manager and IT Department head)

4.10.2. Firewall, IPS, Management, Penetration and Traffic Control

This section presents findings of ten questions related to firewall, IPS, management, penetration and traffic control. The table presentation is as follows.

Table 4.15: Frequency Analysis of Q15-Q19

Question	Option	Frequency	Percent
Q15. Do you use SSL encryption?	Yes	8	66.7
	No	1	8.3
	I do not have any idea	3	25.0
Q16. Do you use Virtual Private Network (VPN) on your network?	Yes	8	66.7
	No	1	8.3
	I do not have any idea	3	25.0
Q17. Do you perform daily logging on your wired network?	Yes	7	70.0
	No	1	10.0
	I do not have any idea	2	20.0
Q18. Do you use xflow protocols on your network? (e.g. Netflow, netstream, sflow)	Yes	3	25.0
	No	2	16.7
	I do not have any idea	7	58.3

Q19. Do you use authentication protocol in your network structure? (You can select more than one option)	TACACS/TACACS+	3	25.0
	We do not use	1	8.3
	RADIUS	1	8.3
	Smart Card	0	0
	Biometric	0	0
	We use another authentication protocol	0	0
	I do not have any idea	7	58.3

As illustrated in Table 4.15, 66.7% of respondents' uses SSL encryption and VPN connection each to use it for web servers that need encrypted sessions and to communicate with branch network connection through Ethio-Telecom respectively. Employees were asked if they perform daily logging and 70% of the respondents answered they do perform. And only 25% of the respondents use xflow protocols on the network, protocols which can enable administer gather information about traffic flow by sorting particular categories like application or IP address. Employees that uses TACACS/TACACS+ and RADIUS authentication protocols in the network infrastructure are more than 30% while 58.3% do not have any idea what they are using. These are authentication protocols to access network devices where TACACS is vendor specific and RADIUS is vendor independent. These findings shows employees awareness to SSL and VPN are average level where as the use of xflow protocols and authentication protocols are unsatisfactory. This needs to be improved in terms of implementation and communicate or get people to be aware of what they are using for what purpose if it is already implemented.

Table 4.16: Frequency Analysis of Q20-Q23

Question	**Option**	**Frequency**	**Percent**
Q20. Do you make penetration test for web environment?	Yes	2	16.67
	No	7	58.33
	I don't know what is it.	3	25.0
Q21. Do you make necessary filtering for web software?	Yes	7	58.33
	No	0	0
	I don't know what is it.	5	41.67

Q22. Is your network infrastructure wired or wireless?	Only Wired Both Wired and wireless	1 11	8.33 91.67
Q23. Do you have IPS or IDS appliance on your wired network?	We do not use any of them We have IPS appliance but IDS We use both appliances I don't know what is it.	1 1 2 7	8.33 8.33 16.67 58.33

Employees that answered they do not perform penetration test count 58.33% and who do not know whether it has been done or not count 25% of the respondents as seen on Table 4.16. This is not an example of good security practice since the organization cannot identify its vulnerabilities and mitigate the risks before attackers exploit them. Although 58.33% of the respondents do filter web software to protect the traffic, the result is not good enough. The result should also have included the rest of the group to get a better result. The next question was whether the organization has wired or wireless infrastructure or both and 91.67% of the employees answered it has both infrastructures. The usage of IPS and/or IDS by respondents isles and is very unsatisfactory. These important systems if applied properly enable an organization to protect and detect intrusions before they cause disaster to the organization.

4.10.3. Wireless Network Security

This section presents findings of five question related to wireless network security as shown in Table 4. 17

Table 4.17 : Frequency Analysis of Q24-Q28

Question	Option	Frequency	Percent
Q24. Do you have wireless IPS or IDS appliance on your wireless network?	We do not use any of them We have IPS appliance but IDS We have IDS appliance but IPS We use both appliances I haven't any idea	3 0 0 0 9	25.0 0 0 0 75.0
Q25. Are your wired and wireless IPS appliances Integrated each other?	Yes No	8 4	66.67 33.33

Q26. Do you use guest portal on your wireless network?	Yes No We use another technology/ method I haven't any idea	2 6 0 4	16.67 50.0 0 33.33
Q27. Do you perform daily logging on your wireless network?	Yes No We use another technology/method I haven't any idea	2 7 0 3	16.67 58.33 0 25.0
Q28. Do you use WEP on your wireless network security?	Yes No We use another technology/method I haven't any idea	2 4 0 6	16.67 33.33 50.0

The first two questions asked whether the respondents have wireless IPS/IDS and if they do have, are they integrated with the wired network. The respondents replied as they do not use any of them and there is no integration as a result. More than 75% respondents said eitherthe organization doesn't have a guest portal service that isolate guest VLANs from production environment and ease user management or do not have any knowledge about the service.The same is true when it comes to daily logging on wireless network out of which 75% of the respondents answered there is no such thing and they do not recall. On the other hand, 33.33% of the respondents answered Wired Equivalent Privacy (WEP) security is not implemented on the wireless at all. This is a good measure since WEP is the oldest and the weakest of the available encryption protocols. Since WEP was highly vulnerable it was replaced by Wi-Fi Protected Access (WPA) and WPA2 which intended to address many of the problems that overwhelmed WEP. Hence, if we have a wireless network and it is not secured by a means of for example, IPS/IDS there will be definitely an issue. Wireless networks are very vulnerable compared to wired networks and multiple security measures should be taken to protect them such as using WPA/WPA2 protocol, using guest portal etc.

4.10.4. OSI Application Layer Security

This section includes two questions related to voice application and encryption as described in Table 4.18.

Table 4.18: Frequency Analysis of Q30 and Q31

Question	Option	Frequency	Percent
Q29. Do you use voice applications?	Yes	1	8.33
	No	11	91.67
Q30. Are they encrypted?	Yes	3	25.0
	No	0	0
	I haven't any idea	9	75.0

The two questions were concerned whether respondents use voice applications in the organization and are they encrypted if any. However, more than 91.67% replied they do not use any, as a result there is no need to discuss about encryption. If there were any voice application, the data should be encrypted. *"On progress to build a call center for any users of the IFMIS/IBEX system."* (Project manager)

4.10.5. OSI Transport Layer Security

This section describes the respondents perception regards port based packet filtering as presented in Table 4.19.

Table 4.19: Frequency Analysis of Q31

Question	Option	Frequency	Percent
Q31. Do you find port- based filtering enough?	Yes	3	25.0
	No	3	25.0
	I haven't any idea	6	50.0

Port filtering is allowing or blocking network packets into or out of a device or the network based on their port number. More than a quarter of respondents do not apply port filtering and half of the total respondents do not have the knowledge of port based filtering when it comes to accessing different types of servers/services within the organization. This is unsatisfactory result and all respondents should be aware of such things. For instance, insiders may violate this vulnerability unintentionally or even intentionally.

4.10.6. OSI Network Layer Security

This section presents findings of respondents related to network layer security as shown in Table 4.20.

Table 4.20: Frequency Analysis of Q32 and Q33

Question	Option	Frequency	Percent
Q32. Which security feature is configured on your Layer 3 Switches or routers?	ACL (Access Control List)	6	50.0
	We do not use these	6	50.0
Q33. Is authentication configured on your routers?	Yes (MD5)	9	75.0
	No	3	25.0

According to respondents who attempted Q33,50% answered only Access Control List (ACL) is used among the given alternatives. In simple words ACLs are used to filter IP addresses from source to destination based on requirements, that is permit or deny access. However, this feature is not the only one and other security features should be configured on network devices to increase the security posture. Regards whether authentication configured on routers,75% of respondents said Message Digest 5 (MD5) encryption algorithm is configured between routers to authenticate routing packets.*"WSA: Cisco web security appliance used to implement some access polices for the ministry and project office"* (Technical Experts)

4.10.7. OSI Data Link Layer Security

This section describes thirteen question results related to data link layer security such as switch. The results are shown in Table 4.21 and Table 4.22

Table 4.21: Frequency Analysis of Q34-Q39

Question	Option	Frequency	Percent
Q34. Are unused ports disabled?	Yes	4	33.33
	No	3	25.0
	I do not have any idea	5	41.67
Q35. Is port security enabled on your network?	Yes	3	25.0
	No	2	16.67
	I do not have any idea	7	58.33
Q36. Do you use only one VLAN on your network?	Yes	2	16.67
	No	5	41.67
	I do not have any idea	5	41.67

Q37. Do you use Private VLAN (PVLAN) on your network?	Yes	4	33.33
	No	2	16.67
	I do not have any idea	6	50.0
Q38. Do you use 802.1x protocol on your network?	Only in wired network	2	16.67
	In both of them	3	25.0
	I do not have any idea	7	58.33
Q39. Do you use protected port?	Yes	5	41.67
	No	2	16.67
	I do not have any idea	5	41.67

From the above table we learn that unused ports are not disabled enough (33.33%) and similarly port security is not enabled enough (25.0%) in the organization. If properly configured these features assist the organization to protect it from unauthorized malicious user from accessing the network. The respondents' response they have multiple VLANs (41.67%) and also use PVLAN (33.33%).Even if the percentage is not enough, these features enable the respondents to have a well-managed, secured and segmented network not forgetting decreasing the load of network traffic. Most of the respondents do not have any idea whether they are using 802.1x authentication protocols and 41.67% of the respondents answered they use protected ports which Disables employees in the institution communicating with each other while they can access to internet via router. Overall, disabling unused ports, using port security and having multiple VLANs are not showing satisfactory results and should be improved to secure the organization.*"WSA: Cisco web security appliance used to implement some access polices for the ministry and project office"* (Technical Experts)

Table 4.22: Frequency Analysis of Q40-Q46

Question	**Option**	**Frequency**	**Percent**
Q40. Is DHCP Snooping enabled on your network?	Yes	5	41.67
	I do not have any idea	7	58.33
Q41. Is ARP Inspection enabled on your network?	Yes	3	25.0
	I do not have any idea	9	75.0
Q42. Is IP Source Guard enabled on your network?	Yes	3	25.0
	I do not have any idea	9	75.0
Q43. Is Root Guard enabled on your network?	Yes	2	16.67
	I do not have any idea	10	83.33
Q44. Is Loop Guard enabled on your network?	Yes	2	16.67
	I do not have any idea	10	83.33

Q45. Do you use Storm Control feature on your network?	Yes I do not have any idea	2 10	16.67 83.33
Q46. Is MAC Security configured on your network?	Yes No I do not have any idea	3 1 8	25.0 8.33 66.67

As shown in Table 4.22, DHCP snooping and ARP inspection are enabled in the network. Enabling IP DHCP snooping verifies MAC-IP address mappings and stores valid mappings in a database. Both features need to prevent ARP poisoning, attempts to contaminate a network with improper gateway mappings. All the five IP source guard, root guard, loop guard, storm control and MAC security are somehow enabled however, the respondents who do not know about the above concepts is much bigger than expected and should be aware in order to understand their benefits and implement them in the organization. If IP source guard is not enabled switches can be exposed to IP spoofing attacks because they do not filter IP addresses on un trusted layer2 ports depending on DHCPs no opening binding table. Root Guard is used to identify and assign the root bridge for frames so that other switches cannot make change accidentally or intentionally by a malicious user. Setting a false bridge can make switches converge incorrectly and misdirect the traffic to unintended way. Loop guard feature provides extra loop-free topology in some circumstances on highly switched network environments. Storm control feature on switched environments drops the traffic that exceeds certain preconfigured threshold value. As shown from the responses the organization can be exposed to denial of service attacks due to configuration switches which cause loops or due to unnecessary services sending abnormally excessive messages. Few of the respondent response they are using MAC security feature. MAC security feature filters MAC address to provide access to a network so that unauthorized malicious user who has a physical access to ports cannot access the network.

"The Ministry requires well organized risk mitigating technique. Doing risk assessment for the organization is the first step, since the network and security category consists of both wired and wireless network security on top of the technologies applied to protect the premises from unauthorized access and periodic vulnerability assessment and penetration test." (Technical Experts)

4.10.8. OSI Physical Layer Security

This section describes the findings of seven question related to physical layer security as shown in Table 4.23.

Table 4.23: Frequency Analysis for Q47-Q56

Question	Option	Frequency	Percent
Q47. Do you perform user id authentication in all of the gates of your Organization?	Yes No I do not have any idea	6 4 2	50.0 33.33 16.67
Q48. Do you have any user authentication mechanism at the entrance of system rooms?	Yes We use another technology/method I do not have any idea	9 2 1	75.0 16.67 8.33
Q49. Do you use shredder to destroy document assets of your organization?	Yes No I do not have any idea	0 7 5	0 58.33 51.67
Q50. Do you have fire sensors in system rooms?	Yes No We use another technology/method I do not have any idea	10 0 0 2 0	83.33 0 0 16.67 0
Q51. Do you have cooling sensors in system rooms?	Yes No We use another technology/method I do not have any idea	11 0 0 0 1	91.7 0 0 0 8.33
Q52. Do you have power redundancy in system Rooms?	Yes I do not have any idea	10 2	83.33 16.67
Q53. Do you have cameras in system rooms?	Yes No We use another technology/method	11 0 0 0	91.67 0 0 0

	I do not have any idea	1	8.33
Q54. Are the cabinets locked in system rooms?	Yes I do not have any idea	10 2	83.33 16.67
Q55. Do you label the cables plugged in to network devices?	Yes I do not have any idea	11 1	91.67 8.33
Q56. Do you have disaster recovery center?	Yes No We use another technology/method I do not have any idea	0 9 2 1 0	0 75.0 16.67 8.33 0

Half of the respondents respond that the organization uses user id authentication in all the gates while the other half answered either they do not have any knowledge about it or it is not performed at all. However, 75% of the respondents answered there is such mechanism at the entrance of system rooms. More than 50% of the respondents' response they do not use shredder to get rid of sensitive documents. Both fire and cooling sensors are implemented in the organization to notify the employees if any abnormalities occur in system room. Redundant power sources such as generators and uninterruptable power supplies (UPS) are alsoconfiguredtorunthesystemroom24/7.Camerasarealsodeployedtorecordandmonitor any action in the system room. The organization datacenter cabinets are locked to protect network equipment. Respondents also answered that labeling of cables that are plugged to networking devices has been done. These measures help to protect the organization's network equipment and to easily trace the cables if needed. More than 75% of respondents answered there is no disaster recovery site which is a major input for business continuity. This may cause a business down time the organization cannot afford. Organizations just cannot rely on a single datacenter without having properly tested disaster recovery site which is physically far from the existing data center.

" The security unit believes Aligning the ISMS program elements to the ISO 27001 or other security control domains allows OSSC to clearly communicate security obligations and risk mitigation strategies to control and performers, and Now the Information Security management policy Program uses the different security domains like WSP and other Cisco security as an organizing concept for developing the information security

standards, baselines, and policies. The policy review process includes stakeholders (INSA, MinT, NBE). The inclusion of stakeholders from these member organizations in this process has prompted more effective adoption of the Information Security Policy." (Security expert)

4.10.9. End Point Security

This last section describes the findings of three questions related to end point security as described using Table 4.24.

Table 4.24: Frequency Analysis of Q57-Q59

Question	Option	Frequency	Percent
Q57. Do you use a technique that prevents passwords from holding in RAM?	Yes	4	33.33
	No	5	41.67
	I do not have any idea	3	25.0
Q58. Do you use BIOS password in end point stations?	Yes	3	25.0
	No	6	50.0
	I do not have any idea	3	25.0
Q59. Do you get WHOIS service?	Yes	3	25.0
	No	2	16.67
	I do not have any idea	7	58.33

More than 41.67% of respondents do not use a technique to prevent password from holding in RAM. Similarly, more than 50% of respondents do not use BIOS password in endpoint stations. These measures increase endpoint password management however the organization is not benefited since it didn't applied them. The last question was if respondents use WHOIS service. WHOIS is a system that asks the question, who is responsible for a domain name or an IP address? A service used to identify and checks the legitimacy of websites. And more than58.33% of respondents replied either they have no knowledge about it or they do not use the service at all.

"Protect Against Password Hacking - System administrators shall harden their systems to deter password cracking by using reasonable methods to mitigate "brute force" password attacks. For example, some systems will lock an account for a few minutes after several failed login attempts, or detect where the attack is coming from and block further attempts from that location, or at minimum alert an alert in real-time that an attack is underway so that manual action can be taken." (Support Team Leader)

4.10.10.Functionality

This last section describes the findings of three questions related to Functionality of IFMIS/IBEX as described using Table 4.25

Table 4.25: Functionality of IFMIS/IBEX

Question	Option	Frequency	Percent
Q1. Access is available to all appropriate users at any time (24 hours), from anywhere	Yes No I do not have any idea	4 5 3	33.33 41.67 25.0
Q2. Access is available to all appropriate users at any time, from anywhere, with any suitable personal device and browsers?	Yes No I do not have any idea	2 6 4	16.67 50.0 33.33
Q3. Relevant security is built into access rights with a single logon	Yes No I do not have any idea	3 2 7	25.0 16.67 58.33

More than 41.67% of respondents do not access the system at anytime and anywhere. Similarly, more than 50% of respondents access any devices and browsers. Functionality is concerned with the way the IFMIS/IBEX works and meets the demands of the users. It covers access and use and focuses on the integrated digital devices that are available to users. Access covers who, where and when users can access IFMIS/IBEX.

4.10.11.Analysis of Technical Challenge on IFMIS

For the open-ended questions asked on technical challenge of IFMIS the respondent respond in the following way.

Table 4.26: Technical Challenge on IFMIS Open-ended Questions

	ITEM	Yes	No	Total
	Do you have any formal technological training on IFMIS specially Oracle?	73	9	82
	Percent (%)	89.1	10.9	100.0
	Do you have any formal training on Cyber security?	2	80	82
	Percent (%)	2.43	97.6	100
	Does the Ministry have cyber security strategy and Police?	13	69	82
	Percent (%)	15.9	84.1	100.0

The findings showed that regarding the technical challenge on IFMIS, in the case of there is a formal technological training on IFMIS specially oracle database (89.1%) said "yes" and (10.9%) said "no" these indicates that there is a good amount of oracle database training has been given for the technical personnel this leads to decrees the technical challenge caused related with the database but still needs more trained personnel on this area because on the issue the Ministry has sufficient database administrator professional In the case of security direct related with technical challenges have formal training the respondents (2.43%) respond "yes" and (97.6%) respond "no" these indicate that security related technical challenges were not easily fixing. In the case of does the ministry has cyber security strategy and polices to minimize the technical challenges the respondents (15.9%) respond "yes" and (84.1%) respond "no" these indicate that the Ministry faced to much more challenges because it has no efficient policy.

"We can see the IFMIS systems by itself have a capacity to integrate and perform various tasks if we are using the whole exiting module."(Experts)

Table 4.27: Strategies and Implementations on IFMIS

	Items	MEASUREMENT					Total
		Strongly agree	Agree	Neutral	Disagree	Strongly disagree	
1	IFMIS is more efficient than IBEX.	20	22	14	3	1	60
	Percent (%)	33.3	36.7	23.3	5.0	1.7	100.0
2	Does Using IFMIS improve the financial activity in the Country?	18	27	14	1	0	60
	Percent (%)	30.0	45.0	23.3	1.7	0.0	100.0
3	IFMIS enhances progressive improvement in information Available to decision makers.	18	27	11	4	0	60
	Percent (%)	30.0	45.0	18.3	6.7	0	100.0
4	IFMIS increases community access to the county's fiscal information	17	21	14	8	0	60
	Percent (%)	28.3	35.0	23.3	13.3	0	100.0
5	IFMIS can increase fiscal prudence in the county.	13	33	6	8	0	60
	Percent (%)	21.7	55.0	10.0	13.3	0	100.0
6	The county has achieved great success in implementation of its development projects due to efficient financial management.	2	19	27	12	0	60
	Percent (%)	3.3	31.7	45.0	20.0	0	100.0
7	IFMIS has given a complete audit trail to facilitate in audits.	9	24	19	5	3	60
	Percent (%)	15.0	40.0	31.7	8.3	5.0	100.0

8	IFMIS led to reduction of wastage of government resources.	14	33	11	2	0	60
	Percent (%)	23.3	55.0	18.3	3.3	0	100.0
9	IFMIS shortened the period for Preparation of financial statements.	16	27	14	3	0	60
	Percent (%)	26.7	45.0	23.3	5.0	0	100.0
10	IFMIS led to efficient allocation of resources.	12	31	14	3	0	60
	Percent (%)	20.0	51.7	23.3	5.0	0	100.0

This question asked only for 60 employs in the finance, HR, property and other departments in MoF, the findings showed that on the item does the implementation of IFMIS/IBEX improve public finance management? The respondents respond (91.6%) said "yes" this indicate that almost all agree on it. on the item to what extent does your work efficient using IFMIS/IBEX? The respondents respond (66.66%) said great extent and (16.66%) very great extent these indicate that using IFMIS/IBEX efficient tasks has been done. When we compare with IFMIS/IBEX with the previous technology financial system which is IBEX with respect to its efficiency (33.3%) were strongly agree and (36.7%) were agreed. IFMIS/IBEX is more efficient than IBEX but (23.3%) were respond neutral those respondents are not technical and sometimes even if technical they are not that much satisfied on the new technology, whatever in the majority case of the respondents are agree on IFMIS/IBEX is more efficient than IBEX. In the case of IFMIS/IBEX improves the availability of the information for decision makers (30.0%) strongly agree and (45%) agree these indicates that IFMIS/IBEX helps for the decision makers to decide what is going on the cash flow activity and manage it. For the community access the financial information IFMIS/IBEX increases the access rate (28.3%) were strongly agree and (35.0%) were agree these indicate that for the community IFMIS/IBEX provide financial information easily. On the case of IFMIS/IBEX increases financial prudence (21.7%) were strongly agree and (55.0%) were agree these indicate that almost majority agree on IFMIS/IBEX maintain the confidentiality of the financial system. In the case of achieving great success on the IFMIS/IBEX (3.3%) were strongly agree and (31.7%) agree these indicate that less than half of the respondents agree on this issue therefore we are not achieved great success on IFMIS/IBEX. In the case of IFMIS/IBEX reducing wastage of government

resource (23.3%) strongly agree and (55.0%) agree these indicate that IFMIS reduce the wastage of resource on an organization and other pilot organizations.

"Regarding the technical challenges on IFMIS a lot of technical challenges but it difficult to find, fix and manage technical challenges at this time, this is due to absence of efficient training and experienced persons."(Senior Experts)

4.11. Components of the Proposed Framework

Components of the framework that are discussed below are extracted from ISO security standard, NIST cyber security framework, literatures, and supported by findings from survey conducted MoF. The components are interwoven and all together support implementation of effective security solutions.

The researchers add some of Components like ISM culture, ISM Ethics, Public Entity ICT and Public Entity. These components are additional and measure for IFMIS sustainability and secure the system

4.12. The Proposed Framework

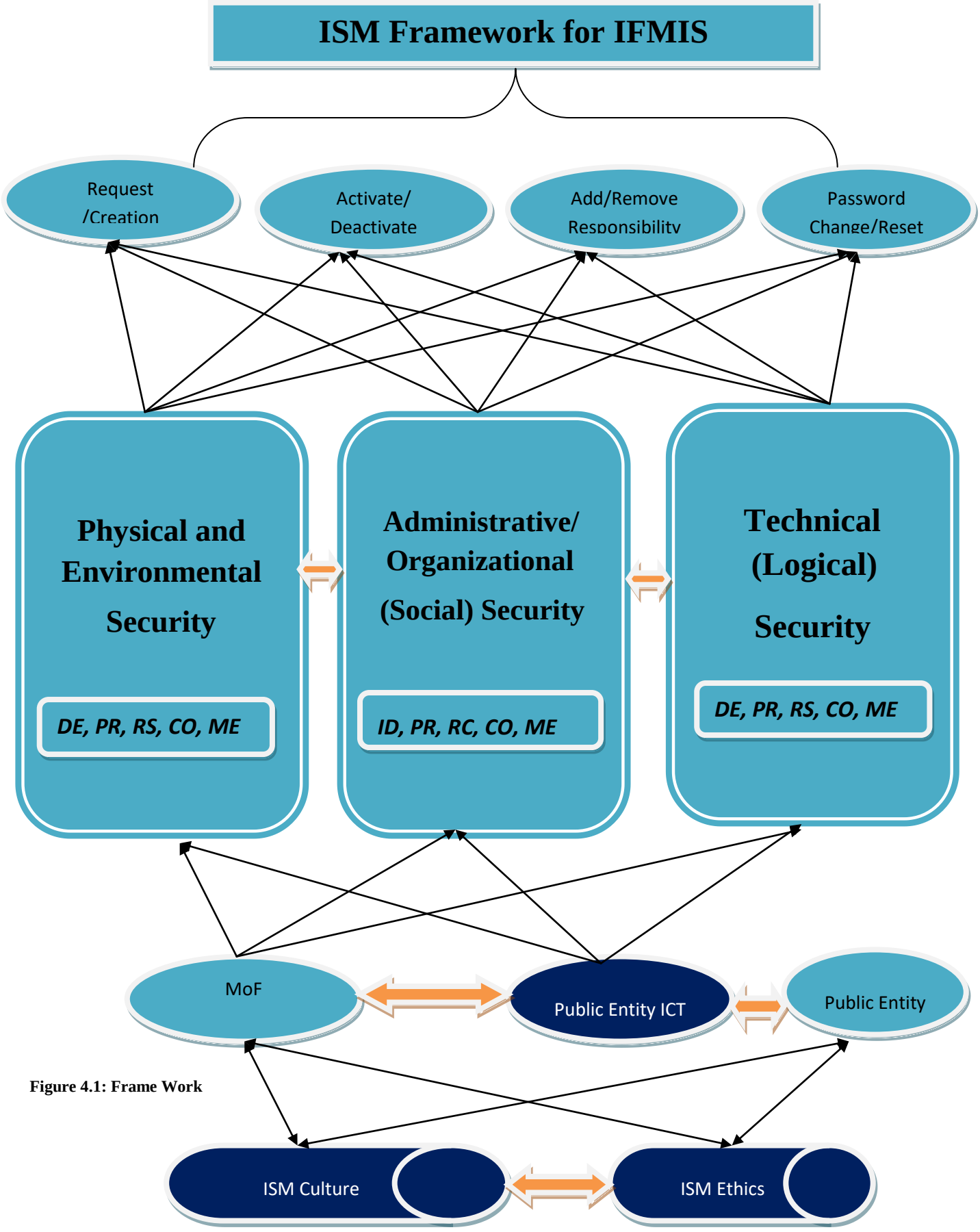

Figure 4.1: Frame Work

4.12.1. Physical and Environmental Security

A. **Secure Areas** – the objective is to monitor and prevent unauthorized physical access, damage, interference to the organization‘s premises and information

B. **Equipment Security** – the objective is to prevent loss, damage, theft or compromise of information processing assets and interruption to the organization‘s online services

Physical and environmental security measures are the means and devices to control physical access to sensitive information and to protect the availability of information and information processing facilities from unauthorized access.

Interview results illustrate that although the organizations included in the research are generally at satisfactory position concerning some of the security elements under this category, still they need to make improvement on some control elements which they are seen weak such as - authorization and checking of ICT equipment entering and leaving the office; ICT equipment disposal and reuse; water leakage management and fire suppression systems; security controls to protect information processing facilities from natural and human caused disasters; and so on. ISO recommends that all items of equipment containing storage media should be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal. Failing to have proper physical security poses organizations to theft, flooding,

4.12.2. Administrative and Organizational Security

Administrative and organizational security defines the human factors of security and involves all levels of personnel within an organization. Implementing technical information security solutions alone is not enough since the effectiveness of information security controls depends on the competency and dependability of the people who are implementing and using it. According to (Martins and Eloff, 2002), the user‘s interaction at a point in any time with computer assets in some way for some reason represents the weakest link in information security. The technical and non-technical issues of information security should be balanced to ensure that the technical issues do not overshadow the non-technical issues (Kritzinger, 2006).

This being the fact, survey findings showed that the public sector organizations are weak in establishing the required administrative controls. Implementing technical information security solutions is not enough since the effectiveness of the technical security controls depend on the competency and dependability of the people who use and implement them. Although the organizations have problems with the technical aspects of security but they are weaker in the administrative (non-technical) aspects of security which deals with the

human element. These include elements security such as human resources security, information security aspects of risk management, change management (including right supervision of outsourced IS projects), and soon. The following are some of the security domains under administrative and organizational security:

A. **Risk Assessment and Treatment** – involves coordinated activities to identifying, analyzing (systematic approach of estimating the magnitude of risks) and prioritizing, and treatment (risk acceptance, mitigation, avoidance, transfer).

Information security risk assessment should be part of the overall risk management strategy. But, the research discloses that the organizations are poor in their risk management strategy in general and in the management of IT related risks in particular. The researcher wonders why the organizations do not have risk management in place with this risk full and continuously changing nature of the world. It is also worth noting that no organization surveyed has risk management department. There is no doubt that the absence of risk management in an organization directly affects its information security risk assessment mechanism (or at least the effort will be incomplete)

B. **Security Policy** – is an instrument that provides management direction and support for information security in accordance with business requirements and relevant laws and regulations. This policy document should be effectively implemented, communicated to all employees and other stakeholders, and periodically reviewed. It dictates employee behavior and states what is expected of them, which in time become part of the information security culture (Martins et al, 2002). A security policy document is made up of group of policies related to different functions and missing one from the group can be considered a threat which may compromise the overall security of the e-service. These policies should also been forced.

The following are some of the security policies that are technical (either automatically created during installation as default or can be customized to suit a need) or non-technical:

- **Virus and spyware protection policy -** detects, removes, and repairs the side effects of virus and security risks by using signatures
- **Firewall policy –** blocks unauthorized users from accessing computers and networks that connect to the Internet; eliminates the unwanted sources of network traffic
- **Intrusion prevention policy –** automatically detects and blocks network attacks and attacks on browsers as well as protects applications from vulnerabilities
- **Password policy** – is configured in the system to force users to comply with the

set rules. Password policy can also be set of rules designed and often part of an organization‘s official regulations and may be taught of as part of security awareness training and defines the standards for creating, protecting, and changing passwords

- **Wireless network security policy** – defines the requirements for the secure implementation of wireless networking technology within the company.
- **Access control policy –** can take many forms. Perimeter barrier devices are often first considered when securing a network. Firewalls in the form of packet filters, proxies, and stateful inspection devices are all helpful agents in permitting or denying specific traffic through the network. Access control also exist on end systems in the form of a privilege level for access to resources, network, functions, applications, configuration files, or data
- **Acceptable use policy –** defines the acceptable behavior of the user towards a system such as a network or webpage
- **Email usage policy –** outlines what is and is not permitted when employees use the organization’s email
- **Software security policy –** orders what software to be installed or not in the organization’s systems
- **IT asset disposal policy –** defines the roles and responsibilities of staff in ensuring the secure disposal of the company‘s IT equipments
- **Network policy –** restricts access towards the network resources of the company and clearly puts who will access it.(Example: a network access policy document maystatethat‒acomputerwithoutantivirusshouldnotconnecttothenetwork‖) which could be taken as administrative, whereas this policy direction may be implemented technically by installing a network access control software to check if a computer has installed antivirus or not when it tries to connect to a network.
- **Remote access policy –** defines how remote users can use the system by telling the standards for connecting to the corporate from any external host or network
- **Special access policy –** intended to control and monitor the special privileges people are given in a system who include managers, team leaders, system administrators, etc.
- **Risk assessment policy –**sets out the principles that the organization uses to

identify, assess, and manage information risk in order to support the achievement of its planned objectives

- **Data center policy –** is intended to ensure the safety and security of individuals and equipment at a data center. These include physical access management, system monitoring, environmental control systems, personnel requiring access (data center employees, authorized staff of the organization, authorized vendors, and visitors) should be clearly explained

C. **Organization of Information Security** – involves managing information security within the organization. An ISM framework should be established to guide the implementation and control of information security. The management should assign security roles and co- ordinate and review the implementation of security across the different parts of the organization. Information security must also extend to external parties as customers, suppliers, contractors, and so on.

Interview results showed that the public sector organizations do not have information security framework; low top management's commitment to security; insufficient budget allocation for security; lack of dedicated structure for security as well as dedicated security personnel, and other weaknesses.

D. **Access Control** – access to information, information processing facilities, and business processes should be controlled on the basis of business and security requirements. These are both physical and logical. Access control is physical in the sense that it includes safeguarding and monitoring unauthorized physical access using human as well as technology solutions (such as biometrics). It is logical in the sense that it includes controlling unauthorized access to information and facilities by defining the right authentication and authorization mechanisms. Therefore, access control could be included in the three security categories – physical, technical, as well as administrative (such as password use policy) security categories.

E. **Information Security Incident Management** – has an objective of ensuring consistent and effective approach applied to management of security incidents and information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken. Organizations should prepare, identify, react, manage, and learn

F. **Compliance** - to avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements; to ensure compliance of systems with

organizational security policies and standards; to maximize the effectiveness of and to minimize interference to/from the information systems audit process.

Information security audit, an assessment mechanism to monitor whether the organization and stakeholders are really complying with the set security requirements, is not a practice in the government organizations. But, since it is not a practice performed in the public sector organizations, they are not getting the benefits from it.

4.13. Technical Security

Technical controls are security controls that are built into and executed by the computer systems. They use technology as a basis for controlling the access and usage of sensitive data throughout a physical and structure and over a network. These can provide automated protection from unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data. They are the means with which administrative policy directions are technologically implemented.

4.13.1. Information Security Cultural Aspects

Information security culture is an assumption about what is and what is not acceptable in relation to information security. Information security as a subset of the corporate culture entails that it is influenced too by the parent organization‘s culture. Researches indicate that insider behavior poses a more serious threat to the security of information than outsider behavior.

According to (Glaser, 2009) security frameworks such ISO/IEC 27001 and ISO/IEC 27002, NIST 800-14, and others too do not encompass and have neglected the role of culture and ethics in information security completely. Hence, this research has incorporated cultural and ethical concepts so that organizations will incorporate these basic security issues in their ISM practices.

Interviews and questionnaire results revealed that information security culture is not well developed in MoF. Indicators are - the management is not considering employees as the organization’s security assets; every employee is not participating in the security awareness programs; sharing of passwords (to some extent); using a common password; leaving their computers open while leaving their desk; downloading items from unsecure sites; using same password for long period of time; less concern for security by the top management; opening YouTube, Face book, and other social medias that which clogs the network bandwidth; and so on. Information security basically is the responsibility of the top management. Hence, the management should play a vital role so as to create the right information security behavior in the organization and make it

part of the corporate culture. The management should also continuously monitor if this culture is on the right way.

4.13.2. Information Security Ethical Aspects

Each public sector organization needs to establish code of conduct that provides direction as to what is acceptable or otherwise. These set the standards of information security behavior expected of all employees in the organization. Good practices are not added to an organization through regulation, incentives and monitoring. They must rather form part of the culture, which is established throughout the organization. Therefore, employees need to incorporate ethical conduct or behavior relating to information security as part of their everyday life in the organization. (Aşuroğlu and Gemci, 2016). Organizations in Ethiopia including the government ones do use different unlicensed software which otherwise will be taken as illegal activity in some other countries. Because ethics is concerned with people and the people are the ones that interact with the information systems, building ethical security behaviors could potentially reduce both accidental and deliberate acts. Hence, the organizations must develop the required code of conduct inherent to the employee's day to day practices.

4.13.3. External Influencing Factors

The ISMS programs of the public sector organizations are significantly influenced by a variety of internal and external factors. The internal or organizational factors that affect the effective implementation of the security programs top management commitment, information security culture, availability of information security policy, risk assessment strategy, technological limitations, and lack of knowledgeable security personnel among others are discussed in the data analysis part of the thesis. Financial security literatures have also identified a broad range of factors that are external or environmental to the organizations but can influence the organization's practices either positively or negatively. These relate to national ICT infrastructure, surrounding environment culture, information security awareness of the society, legal considerations, political requirements, the country's economic strength (financial barrier), inter-organizational cooperation, and inter-governmental cooperation, to mention some.

A. National ICT Infrastructure

Modern and secure telecommunication/ICT infrastructure fosters the development of infrastructure and services, including confidence building and security in the use of

telecommunications/ICTs while bridging the digital standardization gap, conformance and interoperability (ITU). ICT infrastructure is recognized to be one of the main challenges for ISM Framework. Internetworking is required to enable appropriate sharing of information and open up new channels for communication and delivery of new services. For a transition to electronic government, architecture, that is, a guiding set of principles, models and standards, is needed. Many developing countries suffer from the digital divide, and they are not able to deploy the appropriate ICT infrastructure for e-government deployment which is also the case to Ethiopia. The development of basic infrastructure to capture the advantages of new technologies and communications tools is essential for implementing e-ISM Framework security. Different access methods, such as remote access by cellular phones, satellite receivers, kiosks, etc., are being taken in to consideration by governments in order that all members of society can be served. This mechanism is taken as a way to fill the gap in the digital divide. However, security aspects must be thought of along with such endeavors. The security programs of the public sector organizations will not get successful unless the national ICT infrastructure over which the IFMIS service is traversed to/from the public finance is secured.

People should be made aware of not only the usage and adoption of the services but also the associated security problems and the necessary security consciousness. Presumably, the higher the level of human development in security, the less the threats initiated from the public. One of the means through which governments need to guarantee secure financial transactions between organizations and individuals is the design and development of a public key infrastructure. However, the government of Ethiopia has not yet started implementing PKI including digital signature. Therefore, the public organizations are lacking (beyond their mandate) the necessary security framework that could have played its own role in helping their security programs. Putting the right-secured ICT infrastructure in place is not a task to be left for tomorrow for the reason that cybercrime has also reached at the level of national security concern than thinking to secure the individual public sector institutions ‘online service.

B. Societal Culture

Culture refers to the totality of learned behaviors in the context of a social system. It exists only within the contexts of human societies blue print for behavior (Slonim, 1991). Culture influences how people behave and think. An organization is influenced by the communities it is surrounded. Moreover, as a result of globalization, many corporations have become multicultural and

outsourcing takes place on a global scale. Therefore, a clear understanding of cultural characteristics and its impact on information security is crucial. Organizations need to assess their surrounding environment‘s cultural aspects and to analyze their impact on their information security. This enhances understanding of the human factor in information security. These observations reveal valuable insights that are necessary for managing security risks. This approach will also be useful since most huge IT projects in the government institutions are outsourced to foreigners. Therefore, proper IT project management requires having the knowledge of the different cultural aspects of the contracting parties. In general, the organizations should clearly identify what threats and opportunities could their surrounding culture bring to their organization‘s information security practices.

C. Insufficient Funding

It is clearly known from the survey responses that the budget allocated for security is influencing the public sector institutions in acquiring the right security devices, personnel, and awareness and training. Therefore, this insufficient funding ultimately remains to be the leading barrier to battling cyber threats.

4.14. The Six Core Functions of the Framework

These core functions must be performed concurrently and continuously in order to address the security risks posed on IFMIS. These functions act as the backbone of the framework core that all other elements are organized around (NIST, 2018) and functions represent the primary pillars for a successful and holistic security program. They aid organizations in easily expressing their management of security risk at a high level and enabling risk management decisions.

ISO 27001 do not properly identify which function (out of these six) that a specific security element is performing. So, this research has opted to integrate these six core functions from NIST‘s cyber security framework and integrate them to the proposed framework.

Brief description of the six core functions and the expected outcome categories follows:

Identify (ID)

The identify function develops an organizational understanding to manage security risk to systems, people, assets, data, and capabilities. Activities include knowledge of the business context, the resources supporting IFMIS functions, and the related security risks. This enables

the organization to focus and prioritize its efforts. Expected outcome categories within this function include:

- Identifying information assets within the organization to establish the basis of an asset management program
- Identifying cyber security policies established within the organization to define the security program as well as identifying legal and regulatory requirements regarding the information security capabilities of the organization
- Identifying asset vulnerabilities, threats to organizational resources, and risk response activities as a basis for the organizations risk assessment
- Identifying a risk management strategy for the organization including establishing risk tolerances

The identify function develops an organizational understanding to manage security risk to systems, people, assets, data, and capabilities. Activities include knowledge of the business context, the resources supporting IFMIS functions, and the related security risks. This enables the organization to focus and prioritize its efforts.

Protect (PR)

The Protect function outlines appropriate safeguards to ensure delivery of secured ISM framework services and supports the ability to limit or contain the impact of a potential security event. Expected outcome categories within this function include:

- Empowering staff within the organization through awareness and training including role based and privileged user training
- Establishing data security protection consistent with the organization‘s risk strategy to protect the confidentiality, integrity, and availability of information
- Implementing information protection processes and procedures to maintain and manage the protections of information systems and assets
- Protecting organizational resources through maintenance

Managing protective technology to ensure the security and resilience of systems and assists are consistent with organizational policies, procedures, and agreements

In order to perform this function, one of the security devices they must use is IPS (Intrusion Prevention systems). But the survey result showed that there are organizations that are not putting this vital security control in place; means, they are not that effective to safeguard their data and information processing systems, as well as the customers data they collect. There are also organizations which not put in place the right protection mechanisms such as security practices are not properly doing this core function.

Detect (DE)

The detect function develops and implements appropriate activities to identify the occurrence of security events. Expected outcome categories within this function include:

- Ensuring anomalies and events are detected, and their potential impact is understood
- Implementing security continuous monitoring capabilities to monitor security events and verify the effectiveness of protective measures including network and physical activities.

Respond (RS)

The respond function develops and implements appropriate activities to take action regarding a detected security incident. Expected outcome categories within this function include:

- Ensuring response planning process are executed during and after an incident
- Analysis is conducted to ensure effective response and support recovery activities including forensic analysis, and determining the impact of incidents
- Mitigation activities are performed to prevent expansion of an event and to resolve the incident

MoF have poor and even do not have security incident management and reporting as well as business continuity and disaster recovery programs; meaning that they are not in accordance with what NIST recommends to have.

Recover (RC)

The recover function identifies appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a security incident. The Recover Function supports timely recovery to normal operations to reduce the impact from a security

incident. Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cyber security incident. Expected outcome categories within this function include:

- Ensuring the organization implements recovery planning processes and procedures to restore systems and/or assets affected by security incidents
- Implementing improvements based on lessons learned and reviews of existing strategies

Communicate (CO)

Communication is an important tool to share and transmitting happenings, lessons, for internal and external recipients. The communicate functions is suggested by the researcher to be added as the 6th component of the NIST‘s core functions than included in the Respond function as NIST puts. This function is important to be performed by because they are found weak to keep proper documentation on security incidents and other security activities. Therefore the researcher recommends using the template for documenting, reporting, and communicating security incidents to self, to other parties within the organization, and external parties. Expected outcome categories within this function include:

- The organization implements improvements by incorporating lessons learned from current and previous detection/response activities

Monitoring and Evaluation (ME)

Monitoring is the systematic process of collecting, analyzing and using information to track a program‘s progress toward reaching its objectives and to guide management decisions. Evaluation is the systematic assessment of an activity, project, program, strategy, policy, topic, theme, sector, operational area or institution‘s performance; it focuses on expected and achieved accomplishments, examining the results chain (inputs, activities, outputs, outcomes and impacts), processes, contextual factors and causality, in order to understand achievements or the lack of achievements. Hence, including this function as a core function enables the public sector organizations to determine the relevance, effectiveness, efficiency and sustainability of security programs and their contribution in achieving their stated objectives.

4.15. Interaction of Framework's Components

The framework components are interwoven and all together support effective and coherent implementation of security solutions.

Whatever technical and administrative controls are present, unless and otherwise supported with the right physical security controls, they will not be effective. Focusing on one component while neglecting the other will not suffice. Access control policies will be of no good unless implemented with proper technical and physical control components. Putting firm security perimeters, state of the art security cameras, security guards, and so on will not create maximum security position without having proper technical controls such as VPN, digital signature, encryption, and others. Proper technical security configuration and implementation requires skilled personnel which are developed through effective awareness and training programs which in turn is influenced by allocation of sufficient budget. Technical solutions implemented with outdated security devices create security flaws. Acquiring state of the art security devices demand sufficient budget allocation which needs the top management‘s concern. Moreover, putting effective physical and technical security elements require skilled and dedicated personnel. Even skillful personnel, having no proper code of conduct, could take advantage of knowledge of the internal systems to make unethical activities. Information secure employee with the right information security behavior is alert at every move of interaction with information and systems in a way that contributes to the organization‘s security arrangements to be fruitful.

4.16. Security Design

Developing security strategies that can protect all parts of a complicated network while having a limited effect on ease of use and performance is one of the most important and difficult tasks related to network design. Unless there is a security mechanism in place, the whole network resource, company information, important document of the MoF can be stolen or modified by intruders. To protect the information asset of MOF, The researcher recommends the following security mechanisms and technologies to be in placed in this LAN/WAN infrastructure.

4.16.1. Perimeter Security

The perimeter is the first line of defense from outside, the internet or un-trusted network. It is where the internal network ends and the Internet begins. The perimeter consists of firewall and/or router with a set of controlled servers located at DMZ (demilitarized zone). A DMZ typically consists of Web Servers, Mail Agents or any other publically accessible servers. The

network perimeter is, in short, the gateway to the outside world and, conversely, the outside world's gateway to the inside network.

4.16.1.1. Key Threats in Internet Edge

The Internet edge is a public-facing network infrastructure and is particularly exposed to large array of external threats. Some of the expected threats are as follows: Spyware, malware, and adware Network intrusion, takeover, and unauthorized network access, E-mail spam and viruses, Web-based phishing, viruses, and spyware, Application-layer attacks (XML attacks, cross scripting, and so on), Identity theft, fraud, and data leakage.

4.16.2. Web Application Firewall

The Web Application Firewall (WAF) provides firewall services for web-based applications. It secures and protects web applications from common attacks, such as identity theft, data theft, application disruption, fraud , cross-site scripting (XSS) attacks, SQL and command injection, privilege escalation, cross-site request forgeries (CSRF), buffer overflows, cookie tampering, denial-of-service (DoS) attacks and etc The Web Application Firewall's integrated Extensible Markup Language (XML) firewall capabilities extend protection for traditional HTML-based Web applications to modern XML-enabled Web services applications. The WAF solution will have the following features: Web Security, Application Attacks Prevented, HTTPS/SSL Inspection, Web Services Security, Web Fraud Prevention , Content Modification , Platform Security , Network Security , Advanced Protection , Data Leak Prevention, Policy/Signature Updates MoF use BIG IP Web Application Firewall in order to protect web applications which reside in the server farm.

4.16.3. Server Farm Security

Critical applications and data for the MoF will be placed in the server farm, refining the server farm is an act of constant planning. Security is often seen as an add-on service. In reality, security should be considered as part of the core infrastructure requirements. Because a key responsibility of security for the server farm is to maintain the availability of services, the ways in which security affects traffic flows, scalability, and failures must be carefully considered. MoF focus on three areas of server farm security: *isolation; policy enforcement;* and *visibility*.

4.16.4. Cyber Security Management

Cyber security operations protect MoF's assets in accordance with compliance requirements, while ensuring confidentiality, integrity and availability of data and IT services on MoF's network. We will provide cyber operation solutions to cover broad range of services in an effort to deliver a full spectrum cyber operations solution focusing on threat management, and monitoring and incident response. The researcher proposed the following solutions to provide the intended cyber security operations:

4.16.5. Security Information and Event Management

One of the challenges for security operations is identifying significant events from a large number of heterogeneous security devices and systems, correlating those event feeds, and reducing the overall event volume to a level manageable by the analytical staff. In order to automate event collection and correlation, SOCs integrate a Security Information and Event Management (SIEM) as a core solution.

The SIEM solution will have the following features: Log collection from disparate security devices/solutions (applications) and servers Log normalization, filtering and aggregation, Correlation analysis, Real-time alerts (e.g., audio, visual, email, SMS, etc.), Threat management, Risk management, Monitoring, Ticket system based Incident Management, Reports, Retention of data, Web console, and others.

4.16.6. Vulnerability Management System

Vulnerability is a security practice designed to proactively prevent the exploitation of IT vulnerabilities that exist within MoF. The expected result is to reduce the time and money spent dealing with vulnerabilities and exploitation of those vulnerabilities. The VMS solution would have scan the environments to discover MoF physical and virtual assets, Inventory and group assets into a variety of logical organizational categories, Prioritize threats based on potential risk and others.

4.16.7. Network Devices Hardening

Securing devices in a network is one of the most important tasks in network security. This security focuses on routers, switches, firewalls, and other network devices. In this part number of important security tasks, including accessing methods and controls, hardening configuration, identifying unwanted services, managing devices, and monitoring and auditing services will be

covered. Devices such as routers, switches, firewalls, and other network devices are an integral part of the network, and securing these devices is an essential part of the overall network security policy. MoF must have a device security policy that dictates the rules to protect device access and access control. The device security policy can also outline the minimal security configuration for all devices in the network to serve. A device security policy should define rules that spell out who, where, and how these devices will be accessed, in terms of both administrative roles and network services. The device security policy must blend into the overall framework of the high-level requirements of the network security policy.

4.16.8. Windows Server Update Service (WSUS)

Windows server update service helps MOF IT administrators to deploy the latest Microsoft product updates to computers within MOF network infrastructure. By using WSUS, MOF network administrators can fully manage the distribution of updates that are released through Microsoft update to computers in MOF network. The core advantages where WSUS adds value to MOF is that it provides a centralized update management system. By making the update process centrally we can overcome security vulnerabilities and maintain stability within MOF working environment. The figure below shows the placement and traffic flow for MOF AV and WSUS systems.

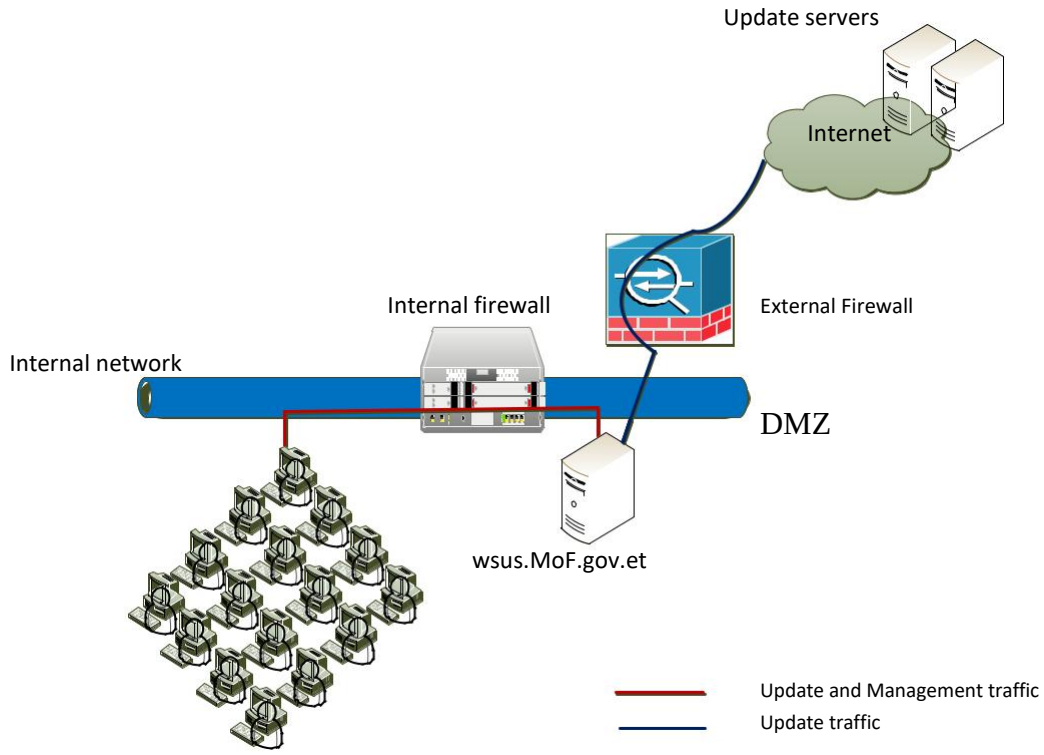

Figure 4.2: MOF WSUS System Design4.16.9 Identity Service Engine (ISE)

Cisco Identity Services Engine (ISE) is a next-generation identity and access control policy platform that enables enterprises to enforce compliance, enhance infrastructure security, and streamline their service operations. The unique architecture of Cisco ISE allows enterprises to gather real-time contextual information from networks, users, and devices. The administrator can then use that information to make proactive governance decisions by tying identity to various network elements including access switches, wireless LAN controllers (WLCs), virtual private network (VPN) gateways, and data center switches. Cisco ISE is a key component of the Cisco Security Group Access Solution.

Chapter Five

5. Evaluation of the Framework

Evaluation is a crucial component of the research process. Through evaluation, the extent to which the artifact supports the solution to the identified problem situation can be measured. The utility, quality, and efficacy of a design artifact must be rigorously evaluated via well executed evaluation methods. IT artifacts can be evaluated in terms of functionality, comprehensiveness, consistency, accuracy, performance, reliability, usability, fit with the organization, and other relevant quality attributes (Hevner, March, & Park, 2004). Aier and Fischer, (2012) (as quoted in (Sonnenberg & Brocke, 2012) suggest criteria to evaluate artifacts that are independent of an artifact type and particularly apply for evaluating design theories. These criteria are utility, internal consistency, external consistency, broad purpose and scope, simplicity, fruitfulness of further research. Another set of evaluation criteria is proposed by (Rosemann & Vessey, 2008) aiming particularly at ensuring the relevance of a DSR artifact, i.e. if an artifact is applicable in practice. These are -importance, suitability, and accessibility of an artifact. Because design is inherently an iterative and incremental activity, the evaluation phase provides essential feedback to the construction phase. Artifact – evaluation methods combination analyses study performed by (Peffers K. ,Rothenberger, Tuunanen, &Vaezi) show that one of the methods that a framework could be evaluated is by conducting expert evaluation.
Therefore, to demonstrate its comprehensiveness, usefulness, level of detail in its context, the proposed framework was evaluated by 5ITsecurity experts from Ministry of innovation and technology (MinT). These experts have long years of professional experience in systems administration and information security. They also did take different courses on security and two of them have certification in security – CIISP. This expert interview method is used by (Kortjan and Von Solms, 2014) for evaluating their cyber security framework and education framework.

With the intention of elaborating on the underlying research that produced it, the proposed ISM framework for IFMIS was presented and discussed in detail – all the components, sub components, as well as the processes followed in preparing the framework. The evaluation is capture by using questionnaires and Interviews. For Questioners that use five levels of rating scale, where 1 stand for strongly disagree and 5 stands for strongly agree. The evaluation criteria are attached as annex III. The interview part is created a clear understanding of the context. Subsequently, the actual interview was conducted. The questions, prepared in a semi-structured form, are as follows:

- Do you agree on the components and sub-components of the proposed framework? If your answer is yes explain components regarding with IFMIS Security perspective.
- Is the framework comprehensive enough?
- Do you think the framework would be relevant in contributing to the ISM practices of the IFMIS? By which mechanisms.
- Any other comments and suggestions?

The results of the evaluation are as follows:

- In terms of the components and sub-components of the framework, the experts approved that the framework has included all the components and sub-components that a security program of an organization uses to protect its IFMIS services. However, one of the experts put his concern – *users of the framework must be referring to the components and sub components put in text form to better understand the overall framework than only referring to the framework's picture. More detailness could be seen on subsequent researches focusing on the sub components such as security awareness and training framework and so on. But the broad nature of the research makes the framework picture to be lacking detailness*.
- In terms of the comprehensiveness of the framework, the experts confirmed that the proposed framework was indeed comprehensive. The components and the sub-components are as inclusive as possible to have the ISO 27002 security elements (detailed on the table). It gives clear picture of what ISO security is and what is expected from each of its elements. The experts further approved that the effort made to link elements from ISO, NIST and literature (cultural and ethical aspects - what the experts believed ISO is lacking) gave the framework more of a comprehensive nature. In general, it covers the basic elements a security framework should include.
- As to the framework's relevancy and contribution to the security practices of the public sector organizations, the experts put their firm believe that this framework will be of a great help to the public sector institutions to their security programs where they have no one to refer to.
- Regarding whether they have any other comments and suggestions, one of the experts said –*information security culture and code of conduct(ethics) should be related to each other with double-headed arrows because an organization having proper information secure culture will be promoting in creating ethical employee and vice*

versa. Hence, the framework is adjusted accordingly. Two of the experts recommended including evaluation and monitoring being included as the 7th core function saying –*monitoring and evaluation enables the organizations to regularly review and check their security practices are achieving their stated objectives".* The third expert, however, opposes this idea –*because this function is performed in the compliance part of ISO*‖. Hence, the framework is adjusted to have this element as the7thcorefunction.Oneofthe evaluators said –*wouldn't it be better to explicitly define and show each technical security control elements in the framework (ex. discussing/showing how Intrusion Prevention Systems used in the framework).* But at the end, the entire group as well as the researcher came to agree that such an idea is found to be too specific as opposed to the broad nature of the framework.

The results of the evaluation showed that the framework is being accepted and valid to help the IFMIS User organizations all user institutions to stand better in their security programs and consequently safeguard their online services and the customer data. However, the proposed framework need to be evaluated through practical application and more research conducted so that it can be modified and enhanced overtime.

With the notion to bring efficient and effective practices, Federal Government of Ethiopia (FGE) is undertaking reforms on its Budgeting scheme and Practices, Accounting, Asset Management, etc and is implementing Oracle E-Business Suite (IFMIS) solution, to shape the reforms. To strengthen the reforms, automating the User Management process has become a must. And, therefore, Ministry of Finance implements and introduces a local custom module called User Management (UM) to best fit its requirements and the business processes.

An ISM framework is used across all the Public Bodies of Federal Government, Regions, Zones and Woredas in the country and has five major functionalities. This centralized ISM framework will help MoF to manage and control all the users of IFMIS from all Public Bodies with improved security and consistency.

The content of the questionnaire is derived from the evaluation criteria recommended by (Ahmad, 2010; Prat et al., 2014; Taddele, 2015). The evaluation has four elements; utility and applicability, consistency with organization, the content of framework and, the usefulness of the framework.

Responses to The lower rating will be expected to be 7(1 lower mark x 7 experts = 7), the highest rating is expected to be 35 (5 x 7 expert= 35), and an average rating is expected to be 17.5. On the whole, these results are supportive, and acceptable by experts who evaluate it. All result is above average, which is shown below in figures.

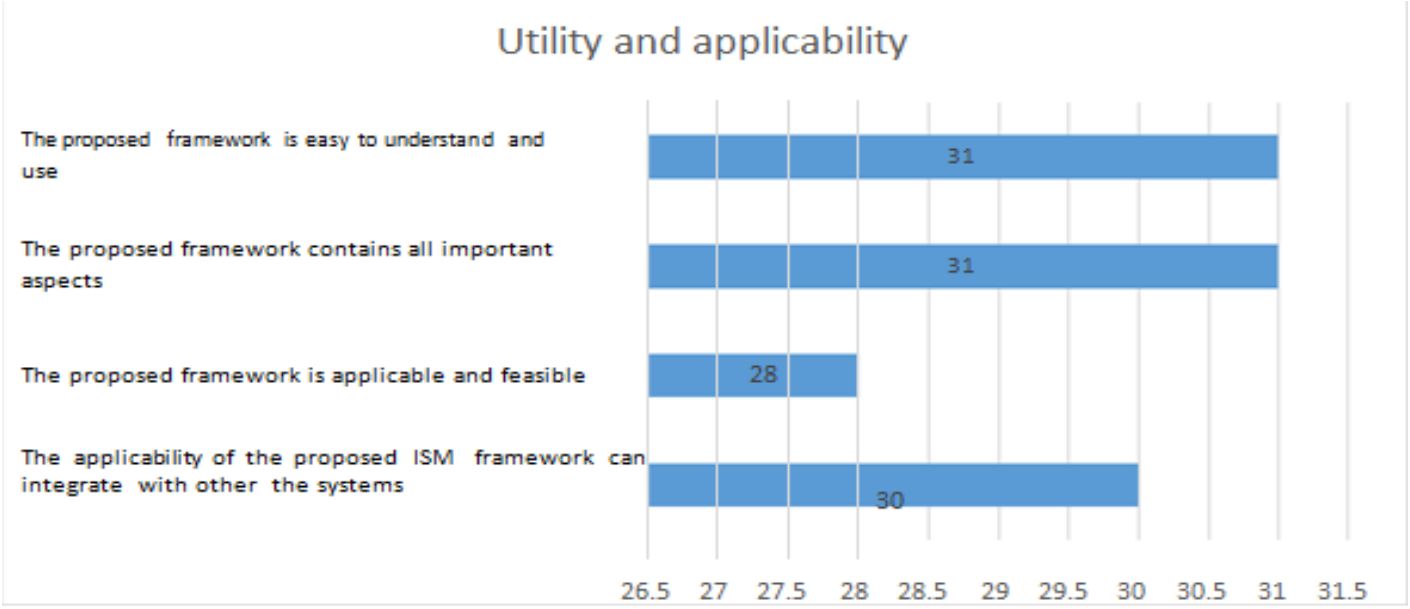

Figure 5.1: Evaluation Result for Framework Utility and Applicability

The above figures (figure 7) show the evaluation framework utility and applicability was easy to understand and use, applicable and feasible and it integrates with other systems. Consistency with people criteria checks the frameworks utility, understandability, ease of use, ethicality against the user/ administrators working at MoF.

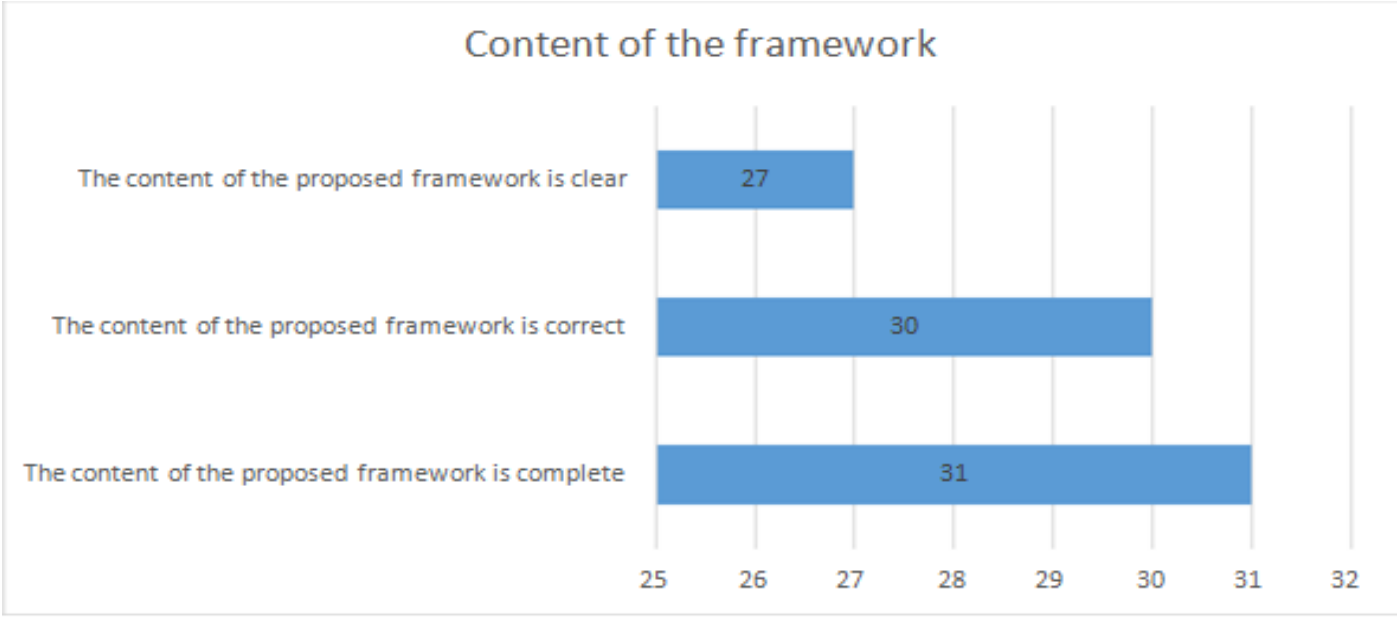

Figure 5.2: Evaluation Result for the Content of the Framework

The above figures (figure 5.2) shows the evaluation framework contents are clear, correct and complete for users/ administrators and others at MOF and PE's.

Chapter Six

6. Conclusion and Recommendation

6.1. Introduction

This chapter presents the conclusion and recommendation of the study. The conclusions are derived from the research findings. Its focus on showing how the result relates to the original research question and objective set out in the thesis. The chapter also provides recommendations which are emerged from this study.

6.2. Conclusion

This paper tried to overcome issues that human are the weakest link in information security and are a major threat for organizations information security by proposing Ism frameworks. Information security management framework is one way of overcoming this critical issue. The proposed ISM framework will assist the MoF in terms of creating information security awareness and good practices to its employees to strengthen its security by mitigating vulnerabilities for computer attacks and use the system friendly. The researcher asked three questions; The researcher used a quantitative research approach using a case study method and questionnaire as a data collection technique to meet the desired objectives such as review existing information security ISM frameworks, review the current practice of information security management in the MoF, use also interview and propose a new ISM framework that will guide information security management formwork for IFMIS in MoF.

The key findings are categorized into two categories general and technical. In the general category first section “security incident” the respondents have unsatisfactory knowledge of safe internet usage and incident response. In “email security” employees knowledge to phishing attack links is poor. In “safely use of internet and computer” personal computers security precautions are not practiced good enough, password management is also poor and most of employees are unable how to distinguish whether a IFMIS system is safe to surf or not. In “threats and preventive measures” respondent security practices are below average. For instance updating software, antivirus usage, security scanning and backup are not performed regularly in

a timely manner. In “password management and security” respondents’ password setting, changing and protection practices are unsatisfactory. In “information security terms and social engineering” section respondents’ knowledge to information security responsibility and social engineering needs improvement.

In technical category “security standards, procedures and training” section the organization doesn’t use information security standards, doesn’t have well-organized procedures in case of cyber-attacks and employees are not being trained of information security. In “firewall, IPS, penetration and traffic control” the organization is not performing internal and external penetration testing. The implementation and usage of IPS/IDS and web filtering is unsatisfactory. In “wireless network security” the organization wireless network implementation and security management are not good. In the rest six sections multiple security features are not implemented enough to strengthen the organization security posture such as port-based filtering, enabling port security, disabling unused ports etc. Ignoring these important issues may cause vulnerabilities to multiple cyber-attacks such as denial of service attacks and a business down time which is unacceptable to a financial institution. Overall the employees’ information security awareness is not satisfactory and needs to be dealt with such kind of programs to protect its assets or even its business.

From the respondent the researcher can see the IFMIS systems by itself have a capacity to integrate and perform various tasks if we are using the whole exiting module. On the assessment of technical challenges on IFMIS most of the respondents answered “No” especially on the training provided by the Ministry to minimize the challenges faced on the technical challenging issue. As we knew the one and first technical challenges was security issue but most of the staffs were not taking any cyber security training. Some of the respondent mention about it and some of the technical challenges like for customizing some reports, speed of the system and migration, server performance problem. The commitment of the steering committee of IFMIS and the responsible bodies their fellowship and control are 0(0.0%) and 5(8.3%) are strongly agree and agree respectively which is very small in number but majority of the respondent disagree 10(16.7%) and strongly disagree 22(36.7%) this showed to us the commitment between them are very poor these things brings bad effect on the project.

With the knowledge transfer of IFMIS on the implementation phase the respondent responds 0(0%) strongly agree and 15(25.0%) agree on it but the majority of the respondent responds 28(46.2%) are neutral this showed to us there is small amount in numbers and majority are neutral because there are staff who are not satisfied and not aware on it clearly.

The IFMIS systems implementation is done with vendors with this issue 8(13.3%) strongly agree and 31(51.7%) agree on it but very less respondents are 2(3.3) % disagree and 1(1.7%) strongly disagree. These responses showed to us the project is done by vendors out sourced this thing has its own good and bad effect, which is good for the Ministry getting a chance to use this large and new technology but which is not good to manage the system with vendors out sourced especially according to its security and cost.

Finally, on the conclusion of the technical challenges of IFMIS, most of the respondent agrees that there exist a lot of technical challenges in on IFMIS security even if there were they try to manage the Ministry need to use a different mechanism like making effective service and ICT infrastructure policy for doing risk assessment on the service and ICT infrastructure to manage the challenges it is mandatory increase the number of well-trained ICT professionals to fix the problem in the right time in order to doesn't return back the problem regularly.

The study concludes that lack of the top management awareness and involvement creates a lot of technical challenges in security management system and risks in the Ministry as well as in the life time of IFMIS.

6.3. Recommendations

The findings may assist the organization to really consider the concerns and act responsibly. The proposed ISM framework can be used as-is or as a guideline with minor modification based on the organization decision makers interest. The program needs to be implemented and be practical so that to get solutions related to employees awareness to information security.
The following recommendations are forwarded to the Ministry: -

- The management should be highly committed in order to grasp the effectiveness of IFMIS.

- The management should support the technical staff by providing training especially on security.
- Logically secure hosts and internetworking devices with user accounts and access rights for directories and files.
- The management needs to periodically upgrade IFMIS.
- The Ministry should have effective disaster recovery for the system and highly proficient person in ICT.
- To redesign and implement secure, reliable, available and affordable data enter network infrastructure, which enables the ministry with the ultimate goal of providing secure, effective and efficient infrastructure.
- The Ministry should have effective ICT policy for IFMIS like antivirus, password and integration mechanisms to other systems.
- The proposed IS management framework should be tested further.

6.4. Future Works

This research paper proposed information security management framework for IFMIS in MoF, using frequency analysis technique. The future scholars will be doing the assessment by considering how much the complexity of IFMIS project in order to be effective and enable for the researcher brings key solution. In addition, researchers can wider the scope to incorporate all Government institutions to have a generic information security management framework Considering new technologies and infrastructures.

References

Alageel, S. M. (2003). *Development of an Information Security Awareness Training Programfor The Royal Saudi Naval Forces (RSNF).* Thesis work, Naval Postgraduate School,Monterey, California.

Al-Alawi, A. I., Al-Kandari, S. M., & Abdel-Razek, R. H. (2016). Evaluation of Information Systems Security Awareness in Higher Education: An Empirical Study of Kuwait University. *Journal of Innovation and Business Best Practice, 2016*, 1-23. doi:10.5171/2016.329374

Alnatheer, M., & Nelson, K. (2009).A Proposed Framework for Understanding Information Security Culture and Practices in the Saudi Context.*Proceedings of the 7th AustralianInformation Security Management Conference*, *7*, pp. 6-17. Perth, Western Australia.

Amare, B. (2015). *Assessment of Insider Threat in Ethiopian Banking Industry.*Thesis work, Addis Ababa University, Addis Ababa.

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, R. W. (2009). If Someoneis Watching, I'll Do What I'm Asked: Mandatoriness, Control, and InformationSecurity. *European Journal of Information Systems, 18*, 151–164. doi:10.1057/ejis.2009.8

Brodie, C., &Wanner, R. (2009). *The Importance of Security Awareness Training.*SANS Institute Reading Room Site.

Chang, A. J.-T.,&Yeh, Q.-J. (2006). On security Preparations Against Possible IS Threats Across Industries. *Information Management and Computer Security, 14*(4), 343-360.

Chen, C. C., Shaw, R. S., & Yang, S. C. (2006).Mitigating Information Security Risks by Increasing User Security Awareness: A Case Study of an Information Security Awareness System.*Information Technology, Learning, and Performance Journal*,*24*(1), 1-14.

Connolly, A. Y., Lang, M., &Tygar, D. J. (2017). The Impact of Procedural Security Countermeasures on Employee Security Behaviour: A Qualitative Study. *International Conference on Information Systems Development (ISD2017 Cyprus), 26*, pp. 1-12. Cyprus.

Dawson, C. (2002). *Practical Research Methods.* Oxford, United Kingdom: How To Books Ltd.

Diver, S. (2007).*Information Security Policy–A Development Guide for Large and SmallCompanies.*SANS Institute.

Durmus, A. (2014). *The Observation of Information Security Awareness in Turkey.*Thesis work, Cankaya University, Ankara.

Enat Bank. (2017). *Enat Bank Annual Report.* Addis Ababa: Central Printing Press.

Gebrehawariat,D. (2017). *Assessment of The Effectiveness of Information SecurityManagement in The Ethiopian Financial Sector: Card Banking Security in Focus.* Thesis work, Addis Ababa University, Addis Ababa.

Gundu, T., &Flowerday, S. (2013). Ignorance to Awareness Towards an Information Security Awareness Process. *SAIEE Africa Research Journal, 104*(2), 69-79.

Haeussinger, F. (2015).*Studies on Employees' Information Security Awareness.*Dissertation, Georg - August - University, Göttingen.

Luthy, D., &Forcht, K. (2006). Laws and regulations affecting information management and frameworks for assessing compliance. *Information Management & Computer Security* 14(2)

Tebkew, K. (2013). *Information Security Management Framework For Banking Industry In Ethiopia.* Thesis work, Addis Ababa University, Addis Ababa.

Von Solms, B. (2006). Information Security – the fourth wave.*Computers and Security, 25*(3), 165-168.

Woretaw, A., &Lessa, L. (2012). Information Security Culture in The Banking Sector in Ethiopia. *5th ICT 2012 Ethiopia Conference*, (p. 22 pages). Addis Ababa.

Sumner, M.(2009). Information Security Threats: A Comparative Analysis of Impact, Probability, and Preparedness. *Information Systems Management, 26*(1), 2-12.

Xiong, P. (2011). *Building a Successful Information Security Awareness Programme for NLI.* Thesis work, Gjøvik University College, Gjøvik.

Keller, S., Powell, A., Horstmann, B., Predmore, C., & Crawford, M. (2005). Information Security Threats and Practices in Small Business. *Information Systems Management, 22*(2), 7-19.

Negussie, A. (2015). *Practices, Challenges And Prospects Of Information Security Policy In Ethiopian Banking Industry.*Thesis work, Addis Ababa University, Addis Ababa.

Kankanhalli, A., Teo, H., Tan, B., & Wei, K. (2003). An Integrative Study of Information

Systems Security Effectiveness. *International Journal of Information Management, 23*(2), 139-154.

Kruger, H., Drevin, L., & Steyn, T. (2006).A Framework for Evaluating ICT Security Awareness. *ISSA*, (pp. 1-11). Potchefstroom.

Mahncke, R. J., McDermid, D. C., & Williams, P. A. (2009). Measuring Information Security Governance Within General Medical Practice. *Proceedings of the 7th Australian Information Security Management Conference*, *7*, pp. 63-71. Perth, Western Australia.

NIST.(2003). *Building an Information Technology Security Awareness and Training Program.* Gaithersburg: U.S. Government Printing Office.

Conner, B.,Noonan, T., &Holleyman, R. (2003). *Information Security Governance: Toward a Framework for Action* [White paper] from http://www.bsa.org/country/Research%20and%20Statistics/Whitepapers.acompany

Appendix

General Category Questionnaire

Questionnaire on Information Security Management Framework for Effective Implementation of Integrated Financial Management Information System (IFMIS): The Case of MoF

Dear Respondent,

I am Yafet Mekonnen, a postgraduate student. Currently, I am attending Master of Science and system (Information Science) at Addis Ababa University, Ethiopia.

As part of my accomplishment for the program, my research lies on Information Security Management Framework for Effective Implementation of Integrated Financial Management Information System (IFMIS): The Case of MoF. Therefore, this is to kindly ask you to participate in the survey that needs data from your esteemed organization to assess the issues in relation to Information Security.

This survey is anonymous. No one, including the researcher, will associate your responses with your identity. Your participation is voluntary. You may choose not to take the survey, to stop responding at any time, or to skip any question that you do not want to answer. Your response is extremely important and valuable for the success of the research to achieve the objective of the study by indicating possible gaps, if any, and possible solutions that need to be taken by concerned parties.

Therefore, I appreciate if you spend few minutes from your valuable time according to the instruction for each part.

If you require any assistance or clarification, please don't hesitate to contact me through either of the following methods. Tel: 0910 43 13 50 or Email: yymmk12@gmail.com

Thank you for your kind contributions in advance.

Please choose the appropriate answer and circle the letter of your choice.

Appendix I

Questions for Interview

1. How many employees does IFMIS have in MoF?
2. What are the major applications does MoF uses? (List few of them?)
3. How does the MoF provide security to the applications?
4. What is the access policy for A. management people? B. Technician C. People
5. How does the company identify the risks? What are the ways in which you calculate the risk?
6. Does MoF have any framework for risk analysis and assessment?
7. Which security model Does MoF has?
8. When you encounter an information theft or any other disaster…what procedure you need to follow and who is the person in charge?
9. How does MoF provide security to your network?
10. How do the corporate executives / managers make sure of coordination of policies? What operations do they do?
11. Does MoF provide training to the IFMIS project head/ CIO/ manager? How long? How often? Do they provide training to any other executives?
12. If MoF provides training, what is the policy for training and how often do they provide training relating to training?
13. How the CIO / security manager does conduct security awareness? Training / memos / workshops / intranet / etc.?
14. How do the senior manager / manager ensure coordination of policy?
15. Does MoF have any reporting policy? Reporting to whom? How often? What kind of reporting?
16. What different types of policy does MoF have that ensures security?
17. Does a manager perform any periodic assessment of assets and risks associated with assets? What results have been obtained in previous assessments?
18. Does the MoF have information use and categorization plan? How does it work?
19. Does the MoF have policy for violations, misuse of assets and internal control assets?
20. How does the MoF determine what level of security is appropriate?
21. As a Divisional director what are your roles and responsibilities?
22. How does the MoF spread security awareness among the employees?

23. Does the MoF conduct any kind of surveys to check security awareness among the employees?

24. What are the major applications used by your organization?

25. Does the company have a framework for risk analysis?

26. What are the metrics with which you evaluate the impact of the risks?

27. Does the MoFhave a framework for information security?

28. For Question 27, your answer is yes, how does the current information security framework help your organization?

29. For Question 27, your answer is no, is there any mechanizes to insure information security management framework for IFMIS?

30. How IFMIS employee's access to information is controlled?

31. How secure communication between employee's be ensured?

32. How information security is managed?

33. How an information system is developed in order to be secure?

34. What are the ways in which you achieve confidentiality, availability and integrity of data?

35. How does the MoF implement / enforce policies and procedures?

36. What are the policies and procedures that the MoF follows in order to secure information?

37. How does the MoF provide access to the users?

38. What are the laws and regulations that affect proposing the information security management framework for IFMIS?

39. Does the MoF follow any standard acts such as SOX, HIPPA or a framework such as COBIT, ISO, COSOetc?

Appendix II

Questions for Questioners

Please choose the appropriate answer

Part 1 – Demographic Features	
1. Your gender?	a. Male b. Female
2.Your age?	a. 18 -24 b. 25 -34 c. 35 -44 d. 45 -54 e. > 55
3 What is your professional qualification?	a. Diploma/LevelIV b. BA/BSc c. MBA/MA/MSc d. PhD
4. Which of the following job categories indicate your current position?	a. Management level b. Senior level c. Officer level d. Junior level
1. Your work experience?	a. 0-1 year b. 1-3years c. 3-5years d. 5-10 years e. Above 10years

Part 2– Security Standards, Procedures and etc	
6. Which security technologies do you use in your organization? (You can select more than one option)	a. Antivirus software b. Firewall appliance c. Web Application Firewall d. Database Firewall e. Data Leakage Prevention f. Anti spyware software g. Virtual Private Network h. Vulnerability/Patch Management i. Data encryption on storage units j. Web / URL filtering k. Application Firewall l. Log management software m. End point security / NAC (Network Admission Control) n. Data loss prevention / content monitoring o. Server-based ACLs (Access ControlLists) p. Information Forensic Tools q. Public Key Infrastructure(PKI) r. Smart cards and keys s. Wireless security t. Virtualization specific tools u. Static accounts user name and passwords v. Biometric w. Information Security Management System x. Other

7.Do you follow a standard for network and information security management in your organization? (You can select more than one option)	a. ISO/IEC27001/2 b. COBIT (Control Objectives for Information Technology) c. NIST (National Institute of Standards and Technology) d. Another information security standard e. None f. I do not have any idea
8. Do you have any procedure in case your systems are being exposed to cyber- attack?	a. Yes b. No c. We use another technology/method d. I do not have any idea
9. Which information security policies do you put into practice in your organization?	a. Network policies b. User policies c. Laptop policies d. Intrusion Detection/Prevention policies e. Patch/Updating policies f. Another rpolicy g. None of them h. I do not have any idea
10. Are your employees being trained about information security management?	a. Yes b. Sometimes c. No d. Another
11. How often do you train your employees about information security?	a. Once a year b. Once a week c. Few times a year d. Once a month

12. Do you follow any resources, materials for oncoming technologic news and developments?	a. I follow some resources at home b. I subscribe to news bulletins and get e-mail regularly c. I benefit from the organization web portal d. I sometimes follow magazines e. Organization training is enough for me f. I do not follow any resource g. Another
13.Have you ever experienced any security incident in your organization network? (e.g. threat, attack, malicious software) If any, how many times did you face?	a. 1- 5 times b. 6-10times c. More than10 d. Never experienced
14. How long does it take to close the security breaches?	a. Between 0- 3months b. Between 3-6months c. Between 6-9months d. Between 9-12months
15. Do you use SSL encryption?	a. Yes b. No c. We use another technology/method d. I do not have any idea
16. Do you use Virtual Private Network (VPN) on your network?	a. Yes b. No c. We use another technology/method d. I do not have any idea

17. Do you perform daily logging on your wired network?	a. Yes b. No c. We use another technology/method d. I do not have any idea
18. Do you use xflow protocols on your network? (e.g. Netflow, netstream, sflow)	a. Yes b. No c. We use another technology/method d. I do not have any idea
19.Do you use authentication protocol in your network structure? (You can select more than one option)	a. TACACS/TACACS+ b. We do not use c. RADIUS d. Smart Card e. Biometric f. We use another authentication protocol g. I do not have any idea
20. Do you make penetration test for web environment?	a. Yes b. No c. We use another technology/method d. I do not have any idea
21. Do you make necessary filtering for web software?	a. Yes b. No c. We use another technology/method d. I do not have any idea
22. Do you apply CoPP (Control	a. Yes

Plane Policy)/CPU on your network appliances?	b. No c. We use another technology/method d. I do not have any idea
23. Is your network infrastructure wired or both wired and wireless?	a. Only wired b. Both wired and wireless
24. Do you have IPS or IDS appliance on your wired network?	a. We do not use any of them b. We have IPS appliance but IDS c. We have IDS appliance but IPS d. We use both appliances e. I do not have any idea
25. Which security feature is configured on your Layer 3 Switches or routers?	a. uRPF (Unicast Reverse Path Forwarding) b. ICM Predirection c. ACL (Access Control List) d. Fragmentation attack prevention e. Teardrop prevention f. We do not use these g. Another technology

Appendix III

Safe Use and Security

This section is concerned with how safe and secure the IFMIS environment is for users.

		Yes	NO	Somehow
26	The system aims to provide a high level of safety for its users			
27	All known abuses are easily reported			
28	All known abuses lead to the culprit being found			
30	The system aims to provide security for personal data			

Functionality

Functionality is concerned with the way the IFMIS works and meets the demands of the users. It covers access and use and focuses on the integrated digital devices that are available to users. Access covers who, where and when users can access IFMIS.

		Yes	NO	Somehow
31	Access is available to all appropriate users at any time (24 hours), from anywhere			
32	Access is available to all appropriate users at any time, from anywhere, with any suitable personal device			
33	Relevant security is built into access rights with a single logon			

Appendix IV

ISM Evaluation Criteria

Put a number (1-5) for your evaluation in the corresponding box of evaluation criteria according to the following: (1) strongly disagree, (2) disagree, (3) neutral, (4) agree, and (5) strongly agree

criteria	1	2	3	4	5
Utility and applicability					
The proposed framework is easy to understand and use					
The proposed framework contains all important aspects					
The proposed framework is applicable and feasible					
The applicability of the proposed ISM framework can integrate with other systems					
Consistency with organization					
The implementation of the proposed framework fits with the organization (MoF)					
The proposed framework is harnessing with recent technology					
Content of the framework					
The content of the proposed framework is clear					
The content of the proposed framework is correct					
The content of the proposed framework is complete					
Framework usefulness					
Helps organizations to decide ISM tools and activities					
Provide guidance for Security applications					
Helps to understand the concept of ISM Framework					
Additional suggestion					