COLLEGE OF BUSINESS AND ECONOMICS

DEPARTMENT OF ACCOUNTING AND FINANCE

The Relationship Between Internal Audit And Information Security: An Exploratory Investigation: Incase of Addis Ababa City Administration.

By

Debebe Tesfaye

June, 2018

Addis Ababa, Ethiopia

The Relationship Between Internal Audit And Information Security: An Exploratory Investigation: Incase of Addis Ababa City Administration.

By

Debebe Tesfaye

A Research paper Submitted to the Department of Accounting and Finance College of Business and Economics

Presented in Partial Fulfillment of the Requirements for the Degree of Master of Science in Accounting and Finance

Addis Ababa University

Addis Ababa, Ethiopia

June,2018

Declaration

I, the under signed, declare that this thesis is my original work and has not been presented for a degree in any other University, and that all source of materials used for the thesis have been fully acknowledged.

Declare By:-

Name:_____

Signature:_____

Date:_____

Confirmed by Advisor:

Name:_____

Signature:_____

Date:_____

Internal Examiner

Name:_____

Signature:_____

Date:_____

External Examiner

Name:_____

Signature:_____

Date:_____

Abstract

The internal audit and information security functions should work together synergistically: the information security staff designs, implements, and operates various procedures and technologies to protect the organization's information resources, and internal audit provides periodic feedback concerning effectiveness of those activities along with suggestions for improvement. The purpose of this exploratory mixed methods study is investigate how internal audit and information security are relate to each other to protect the organization's information resources and internal audit practices in Addis Ababa City administration. Anecdotal reports in the professional literature, however, suggest that the two functions do not always have a harmonious relationship. This research is present the first stage of a research program designed to investigate the nature of the relationship between the information security and internal audit functions. It will report the results of a series of semi-structured interviews with both internal auditors and information systems professionals. The researcher analyzed the factors that influence the nature of the relationship between the internal audit and information security functions, describe the potential benefits organizations can derive from that relationship, and present propositions to guide future research.

Acknowledgements

First I would like to thank almighty God, the reason for the success. Secondly my appreciation and thanks goes to my advisor P.Laxmikantham (PhD) for his devotion throughout the paper, invaluable comments and motivated to me to finalize this paper.

My gratification also goes to Selam Abera my previous girl friend now she is my wife and covered the whole tuition fee. I am also indebted to thank the employees and directorates of Addis Ababa city education bureau, Finance and economic development bureau, House development bureau and Road authority bureaus for their genuine response and cooperation in providing the necessary data requested.

Thanks to you all!

Tables of contents page

List of tables' page

List of abbreviations

AICPA: American Institute of Certified Public Accountants

ERP: Enterprise Resource Planning

CICA: Canadian Institute of Chartered Accounts

COBIT: Control Objective for Information and Related Technology

COSO: Committee of Sponsoring Organization

IA: Internal Audit

IAF: Internal Audit Function

IIA: Institution of Internal Audit

IOD: Institute of Directors

ITGI: Information Technology Governance Institute

ISACA: Information System Audit and control Association

IS: Information Security

NIST: National Institute of Standards and Technology

PO: Probationary Officer

PRMIA: Professional Risk Managers' International Association

PWC: Price Water House Coopers

CHAPTER ONE
INTRODUCTION

This thesis reports on a study of the relationship between internal audit and information security an exploratory investigation in case of Addis Ababa city administration with four selected city's bureaus. Therefore this chapter consists an introduction about the chapter, background of the study, background of Addis Ababa city, statements of the problem, research problems, objectives of the study, significance of the study, delimitation of the study and organization of the study.

1.1 Introduction

Information security is necessary not only to protect an organization's resources, but also to ensure the reliability of its financial statements and other managerial reports (AICPA and CICA, 2008). Consequently, (COBIT4 ,ITGI (2007), a normative framework for control and governance of information technology, Stresses that it is a component of management's governance responsibilities to design and implement a cost effective information security program. As a result, IS(information security) researchers have begun to investigate various dimensions of information security governance. One stream of research has focused on measuring the value of investments in information security (Gordon and Loeb 2002; Gordon 2003;Cavusoglu 2004a;Iheagwara 2004;Bodin 2005, 2008; Kumar 2008). A second stream of research has examined government reactions to disclosures of information security initiatives (Gordon 2010) and incidents (Campbell. 2003;Cavusoglu 2004b; Ito 2010). A third stream of research has examined ways to improve end user compliance with an organization's information security policies (D'Arcy2009;Bulgurcu 2010; Johnston and Warkentin 2010; Siponen and Vance 2010; Spears and Barki 2010).

Little attention, however, has been paid to the operational aspects of information security governance(Dhillon2007). Indeed, in their review of prior IS research on information systems security governance, (MishraandDhillon2006, 20) conclude that the "role of human actors and

issues relating to management of people in the organization is not emphasized in popular definitions of information systems security governance." In particular, they note that the view of information systems security governance used in prior research "does not allow incorporating the importance of the audit process of systems and management ofsecurity details at operational level of business process" (Mishra and Dhillon 2006).

In addition, a recent web-survey conducted by the Institute of Internal Auditors (IIA) recommends a partnership approach between internal audit and IT operations to improve returns on IT control activity investments (Phelps andMilne 2008).This lack of attention to the operational dimension of information security governance in general and to the specific relationship between the internal audit and information security functions is surprising, given the emphasis the normative literature places on these issues. For example, COBIT specifically prescribes thatmanagement should "establish and maintain an optimal co-ordination, communication and liaison structure between the IT function and the corporate compliance group". In addition, "the controlenvironment should be based on a culture that…encourages cross-divisional co-operation and teamwork. Furthermore, it is important to "obtain independent assurance (internal or external) about theconformance of IT with the organization's policies, standards, and procedures.

In most organizations, both the information systems and internal audit functions are involved with information security. The IS function has a primary responsibility for designing, implementing, and maintaining a cost-effective information security program. Internal audit provides an independent review and analysis of the organization's information security initiatives. Ideally, the feedback provided by internal audit can be used to improve the overall effectiveness of the organization's information security.

The remainder of this research is organized as follows. Section 2 reviews prior literature and presents a model of how the internal audit and information security functions can work together to help organizations achieve a cost-effective level of information security. Section 3 is describe the structured interview and questionnaire method and provides demographic background about the interviewees and questionnaire the organizations for which they worked. Section is present

the common themes that emerged from the interviews. Section 5 has concluded the paper by developing a model of the factors that affect the relationship between the internal audit and information security.

1.2 Background of the study

Organizations employ a variety of tools and procedures to provide a desired level of information security. Accountants and auditors typically categorize controls as being preventive, detective, or corrective in nature (Ratliff 1996). Firewalls, intrusion prevention systems, physical and logical access controls, device configuration, and encryption are widely used methods used to prevent undesirable events. Intrusion detection systems, vulnerability scans, penetration tests, and logs are examples of controls designed to detect potential problems and security incidents. Incident response teams, business continuity management, and patch management systems are commonly used examples of controls designed to correct problems that have been identified.
Information systems researchers have developed an alternative way to categorize information security-related controls based on the stage during an attempted information security compromise in which the control is most likely to be effective (Ransbotham and Mitra, 2009).

According to (Ransbotham and Mitra2009), the three types of information systems security controls differ in their objectives. Configuration controls directly reduce the likelihood of an information security compromise by blocking targeted reconnaissance efforts. Access controls also directly reduce the likelihood of compromise by blocking unauthorized attempts to access the system. In contrast to the other two categories, monitoring controls do not directly reduce the risk of an information security compromise. Instead, monitoring controls indirectly reduce the risk of an incident by improving the effectiveness of the other two categories of controls. For example, proper documentation reduces the risk of overlooking key systems when altering default configurations, employing patches, deploying firewalls, and implementing other types of security controls. Similarly, log analysis can help identify the causes of incidents; such knowledge can then be used to modify existing controls to reduce the risk that a similar attack will succeed in the future.

Ransbotham and Mitra focus on the role of the information systems security function in implementing all three types of controls. However, as normative frameworks (e.g., COBIT, COSO, etc.) suggest, the organization's internal audit function should periodically assess the effectiveness of internal controls, including those related to information systems security.

1.3. Background of Addis Ababa city

Addis Ababa is the capital and largest city of Ethiopia. It is the seat of the Ethiopian federal government. According to the 2007 population census, the city has a total population of 2,739,551 inhabitants. In 2017 the population of the city closer to 4 Million. As a chartered city (Central Statistical Agency. 2010). Addis Ababa has the status of both a city and a state. It is where the African Union is and its predecessor the OAU was based. It also hosts the headquarters of the United Nations Economic Commission for Africa (ECA) and numerous other continental and international organizations. Addis Ababa is therefore often referred to as "the political capital of Africa" for its historical, diplomatic and political significance for the continent.

The site of Addis Ababa was chosen by Empress Taytu Betul and the city was founded in 1886 by Emperor Menelik II. Menelik, as initially a King of the shewa province, had found Mount Entoto a useful base for military operations in the south of his realm, and in 1879 he visited the reputed ruins of a medieval town and an unfinished rock church that showed proof of the medieval empire's capital in the area before the campaigns of Ahmad ibnIbrihim.

The economic activities in Addis Ababa are diverse. According to official statistics from the federal government, some 119,197 people in the city are engaged in trade and commerce; 113,977 in manufacturing and industry; 80,391 Homemakers of different variety; 71,186 in civil administration; 50,538 in transport and communication; 42,514 in education, health and social services; 32,685 in hotel and catering services; and 16,602 in agriculture. In addition to the residents of rural parts of Addis Ababa, the city dwellers also participate in animal husbandry

and cultivation of gardens. 677 hectares (1,670 acres) of land is irrigated annually, on which 129,880 quintals of vegetables are cultivated (Central Statistical Agency. 2010). It is a relatively clean and safe city, with the most common crimes being pick pocketing, scams and minor burglary. The city has recently been in a construction boom with tall buildings rising in many places. Various luxury services have also become available and the construction of shopping malls has recently increased.

The administration of Addis Ababa city consists of the Mayor, who leads the executive branch, and the City Council, which enacts city regulations. However, as part of the Federal Government, the federal legislature enacts laws that are binding in Addis Ababa. Members of the City Council are directly elected by the residents of the city and the Council, in turn, elects the Mayor among its members.

1.4. Statements of the problem

In the age of globalization the prober use of information and apply internal audit is crucial point. The internal audit and information security functions should work together synergistically in order to improve the efficiency and effectiveness of the organizations. The information security staff designs, implements, and operates various procedures and technologies to protect the organization's information resources, and internal audit provides periodic feedback concerning effectiveness of those activities along with suggestions for improvement. Anecdotal reports in the professional literature, however, suggest that the two functions do not always have harmonious relationship. In Addis Ababa city administration, for example 2013, the Addis Ababa City Audit Bureau reported that has discovered six major discrepancies. Among these are the fact that AAWSA has no documentation showing it has repaid the 625.7 million birr credit it owes the World Bank and other creditors. The researcher intention to conduct research about the relationship between IA and IS that to set a bench mark for another researcher.

The purpose of this study is, therefore, designed to investigate the nature of the relationship between the information security and internal audit functions in Addis Ababa city administration focusing on the following specific objectives:

a)To investigate the relationship between internal audit functions and information security.

b) To show the relationships among different types of information security control.

c) To describe differences in access to top level management that may influence the relationship between internal audit and information security.

d) The reality that to enhance the relationship between internal audit function and information security with technology integration practice.

e) To identify the nature of the relationship between IA and IS and factor affects the nature of the relationship between the two functions.

1.5. Research questions

The purpose of this study is to examine the relationship between internal audit and information security to protect the organizations' information resource as well as to maintain the proper use of internal audit functions. Accordingly, to attain the objectives ought to state above the study to answer the following questions:

1) What are the basic relationships between internal audit functions and information security?
2) Do differences in access to top level management influence the relationship between internal audit function and information security?
3) What variable influence the relationship among different types information security control?
4) What can be done to enhance (increase, improve, develop) the relationships between internal audit and information security with technology integration practice in the organizations?

1.6. Objectives of the study

The followings are the general and specific objectives of the study.

1.6.1 General objective

The main objective of this study is to investigate the relationship between internal audit functions and information security in Addis Ababa city administration.

1.6.2 Specific objectives

Specifically, this study has the following objectives:

1. To identify factor that affects the activities of internal audit with technology integration practices in the organizations.
2. To assess the top level management influence towards the relationship between internal audit and information security in the organizations.
3. To identify the attitudes of information technology (IT) professionals towards internal activities.
4. To forward ideas on how to improve the relationship between internal audit and information security with the use integrates technology in the organizations.

1.7. Significance of the Study

Since the application of internal audit function and information security are very essential to protect the organization information resource and to control the implementation of rules and procedures in the organization, the strong relationships between internal audit and information security in the organization with the appropriate use of technology integration practice has crucial importance. It is true that maintain the strong relationship between internal audit and information security in the organization will play a key role to

Protect any wastage of resources as well as it is help to implement efficient use of organization resources.

The research is expected to come up with the necessary findings regarding the major problems that the relationship between internal audit and information security in Addis Ababa City administration. This study is, therefore significant for the following reasons:

a) It provides valuable information about the major problems that the relationships between internal audit and information security has in Addis Ababa city administration.
b) It helps all pertinent bodies to design a viable strategy, which in turn can promote internal audit control and information security in Addis Ababa city administration.
c) To the best knowledge of the writer, a thorough study was not carried so far in Addis Ababa city administration that could alleviate prevalent problems of internal audit and information security and hence will help as a spring board for further studies on similar issues in contributing additional information and document base.

This could enable the concerned bodies like Office of Audit General, IT department, Ministry Finance and Economic cooperate. So as to explore possibilities of developing more effective ways of using information security and internal audit control at Addis Ababa city administration.

1.8 Delimitation of the study

To carry out any research work, it should be important to delimit the study to a manageable size. Based on this theoretical base, this study is delimited the investigation of the relationship between internal audit and information security in selected four government bureaus in Addis Ababa city administration.. Hence the researcher is conducted the study in the four available government bureaus found in the administrative city of Addis Ababa.

These bureaus are: Addis Ababa city Finance and Economic development bureau, Addis Ababa city Education bureau, Addis Ababa Road authority and Addis Ababa Urban development bureau.

1.9 Organization of the study

There are five Chapters in this thesis. The first chapter consists of an Introduction about the thesis, Background of the study, Background of Addis Ababa city administration, Statement of the problem, Significance of the Study, Delimitation of the Study and Limitation of the Study. Chapter two is dealt about Reviewed related literature, Chapter three put forward the Research methodology which consists of population, method of sampling and method of data analysis, Chapter four Analyses results obtained. This chapter is organized in such a way that it constitutes presentation regarding the state the relationship between internal audit and information security in Addis Ababa city administration. Finally the Fifth chapter draws out findings, conclusions and forward recommendations for the improvement of the relationship between internal audit information security practices in the government organizations for further strengthening.

Generally this chapter indicates the overall view of the research what it looks like after it is completed. It also gives a clue what method it used, the importance and significance of the research, the research question and statements of the problem, findings and the ultimate beneficiaries of the research.

CHAPTER TWO
REVIEW OF RELATED LITERATURE

In this chapter, studies conducted on the relationship between internal audit and information security internationally as well as locally were surveyed, reviewed and presented. The literature was reviewed based on the nature of the relationship between internal audit and information securit**y,** the influence of internal audit on information security effectiveness, the role of internal auditor's in government organizations, Perceptions of information security professionals and factor affects the relationship between internal audit and information security in the government organization.

2. The nature of the relationship between internal audit and information security

In most organizations, both the information systems and internal audit functions are involved with information security. The IS function has a primary responsibility for designing, implementing, and maintaining a cost-effective information security program. Internal audit provides an independent review and analysis of the organization's information security initiatives. Ideally, the feedback provided by internal audit can be used to improve the overall effectiveness of the organization's information security.

These two functions should work together synergistically to maximize the effectiveness of an organization's information systems security program. Indeed, (Wallace 2011)provide evidence that the level of cooperation between the internal audit and information security functions is positively associated with the organization's level of compliance with the IT-related internal control requirements of the Sarbanes–Oxley Act.

Prior research suggests that there should be positive organizational benefits associated with a good relationship between the internal audit and information security functions. (Wallace 2011) found that a good relationship between the internal audit and information security functions resulted in better compliance with Sarbeansoxley. Further, (Steinbart 2013) found that a good relationship between internal audit and information security improved the information security professional's perceptions of the overall effectiveness of the organization's information security efforts. One explanation for these finding is (Steinbart 2012) report that information security professionals believed that the internal audit feedback helped them improve the design of access controls. (Steinbart 2012) also report that auditors believed the quality of the relationship between the two functions affected audit efficiency: a poor relationship between the two functions led to efforts by information security to hide evidence of the problems from the auditors.

2.1The influence of internal audit on information security effectiveness:

It is important to regularly monitor and assess the effectiveness of information security controls and processes (NIST 2012). However, the value of monitoring and assessment is enhanced when done by someone who was not responsible for designing, implementing, and performing the activities being reviewed (ITGI 2012a). One way to provide independent monitoring and assessment is to have the internal audit function periodically review and evaluate the organization's information security activities. Thus, the internal audit function can potentially contribute to effective governance and management of IT by providing an independent assessment of controls and processes (ITGI 2012a). Until recently, little was known about the effect of internal audit activities on an organization's information security program. (Steinbart2012) conducted in depth interviews at four organizations and found that information security professionals believed that a good relationship with internal audit improved over all information security effectiveness in several ways.

In addition, information security professionals indicated that internal audit feedback was useful in improving the design of role-based access controls (Steinbart2012). Subsequent research involving a survey of information security professionals from multiple industries (Steinbart2013) validated those anecdotal accounts, finding that a good relationship between the information security and internal audit functions improved the information security professionals' perceptions about the overall effectiveness of information security. Steinbart(2013) also found that the extent and frequency of internal audit reviews of various information security processes affected the quality of the relationship between the internal audit and information security functions.

Yet there has been scant research into the role of internal audit in information security. (Ransbotham and Mitra 2009) included "audit controls," by which they meant monitoring and assessment, as one of three elements necessary to reduce the risk of security compromise. In their model, such monitoring played an indirect role in improving information security by providing feedback that could be used to improve the effectiveness of the other technologies and processes comprising an organization's information security program. Although Ransbotham and Mitra did not empirically test that research proposition, subsequent accounting research found that a good relationship between the internal audit and information security functions produces benefits. For example, a good relationship between the two functions results in a higher level of compliance with Sarbanes-Oxley requirements (Wallace 2011) and is inversely related to the number of security incidents and security-related audit findings (Steinbart2013). In addition, (Steinbart2012) report that information security professionals believed that audit feedback helped them to improve the effectiveness of access controls. Thus, there is some evidence that internal audit can contribute to information security effectiveness.

Although the information security and internal audit functions share a high-level, common goal of maximizing the effectiveness of the organization's efforts to protect its information resources, the task of developing and managing proper relationships between the two functions involves a host of complex behavioral issues (Dittenhofer2010). On one hand, the practitioner literature

notes that differences in attitudes and behaviors often make it difficult for the information security group to develop good relationships with other complianceoriented functions, such as records management (Anderson 2012). On the other, auditors must not impair their objectivity and independence (Behn.1997; Carcello 1992; Schroeder 1986; Stoel2012). Therefore, it is important to understand the factors that determine the quality of the relationship between the information security and internal audit functions. (Steinbart2013) found that the frequency and scope of internal audit's review of various information security components had a positive influence on information security professionals' perceptions of the quality of relationship with internal audit.

2.2. The role of internal auditor's in government organizations

The internal auditor's contributions are widely recognized in the literature in promoting good corporate governance and implementing a system of internal controls within the organization. They help to reduce the cost of raising capital if the organization is looking for external financial assistance, and also to enhance the share price if it is seeking equity funds. IAs also carry out assurance activities at specific scheduled times to check the adequacy and effectiveness of internal control procedures in the organization. IAs also report to audit committees at the board level on their findings and opportunities for improvement as required. However, the use of ERP changes the role and function of IAs.

Strategists are involved with the strategic planning and decision-making of the organization. The researchers develop an understanding of the business process reengineering with users including management, and facilitates the consultants' work. ERP experts evaluate the control features of an ERP system and assess current and future risk exposure. They also highlight the importance of soft controls and delegate the accountability of control.

Communicators maintain the relationships among all parties across the organization and facilitate the adoption of audit controls with users, as well as with consultants from outside the company. IT experts update and unify terminology to take advantage of the integrated nature of the ERP system. They share expertise, knowledge, and ideas with IS/IT management. As a

strategist, the IA provides top management with advice that helps management to set the corporate objectives. According to the new Committee on Sponsoring Organizations Enterprise Risk Management, the organization's mission and risk appetite drive its objective-setting process, which defines high-level strategic objectives and the specific objectives required to accomplish them, namely the operating, financial reporting, and compliance objectives (Ramamoorthi and Weidenmier, 2006). Strategic objectives affect the organization's choice of ERP infrastructure and risk level.In addition, (Pierce 2007) proposes five duties of the IA as a strategist in ensuring the success of ERP implementation.

These five duties are:

(1) Secure executive sponsorship and create awareness for program risk management. This helps to enlist the support and resources necessary for successful risk management program.

(2) Take a holistic approach to identifying programs at risk. A broad strategic perspective helps the IA to better understand and prioritizes the program-risk landscape, with its wide-ranging and often disparate risk elements.

(3) Create an active and ongoing program risk management process. Such an ongoing process entails regular audits, the ability to track the trends relating to a program, and faster follow-up on remediation plans. It allows IAs to identify the risks more quickly and to alert the stakeholders.

(4) Build a program audit team with the necessary specialized skills and experience. Having the right people with the right skills to focus on program risk can make the difference between success and failure in risk management.

(5) Include program issues in a consolidated risk analysis. The prioritization of programs, based on their inherent risk, assumes that all challenges facing those programs are risks.

As an ERP expert, the IA is needed to ensure ERP system does not compromise the internal control mechanism. (Arens and Loebbecke 2000) further propose four general guidelines for the separation of duties, which can be applied in an ERP-based organization:

(1) Separation of the custody of assets from accounting. This prevents a person with custody of an asset from disposing of the asset and adjusting the records to conceal the action.

(2) Separation of the authorization of transactions from the custody of related assets. The authorization of a transaction and the handling of the related asset by the same person increase the opportunity for fraud.

(3) Separation of operational responsibility from record-keeping responsibility. If division is responsible for preparing its own records and reports, there may be tendency to bias the results to improve its reported performance.
(4) Separation of information technology duties from duties of key users outside IT. Program modifications should be performed only by authorized IT personnel. Users outside IT should be responsible for authorizing transactions, online data entry, correction of errors in input, and reviews of output from the system.

2.3 Perceptions of information security professionals

The internal audit and information security functions should play complementary roles in an organization's information security program. The information security function should focus on the design and implementation of the security plan, while internal audit should assess and evaluate the functioning of the plan's components (ISACA Journal Volume 2, 2014**)** yet, in practice, the relationship between the two functions is not always positive.

At its worst, the relationship can become so adversarial that it impairs effective governance, as exemplified by one information systems (IS) manager: "…It has been a game of cat and mouse. The auditors are trying to catch IT doing something and IT is trying to prevent audit from finding out."In part, this may reflect the general friction between the accounting and IS functions. But, it also likely reflects the tension that exists among the information security function and other compliance-oriented groups (e.g., records management) within the organization.

What causes friction between the internal audit and information security functions? What actions can management take to improve that relationship? What are the benefits, if any, of having a better relationship between internal audit and information security?

2.4. Factor affects the relationship between internal audit and information security

To create the desired relationship between internal audit and information security, there should be factors identified clearly and based on that the two functions made relationship for the common goal finally obtained. The followings are factors that affect the relationship between internal audit and information security.

2.4.1. Perceived role of internal audit

Internal Audit Function (IAF). At the same time the internal audit profession has realized that it will have to adapt to the changing environment in which it operates as reflected in a statement made by (PWC, 2008b) after a study performed on the perceived status of internal auditing in 2012 concludes:"The rapid growth of the profession and the many changes in the business environment makes it essential for the internal audit profession to adopt new mindsets if it wants to remain a role-player in the future."

As the internal audit function (IAF) is highly important and dynamic field for the business environment, much information should be available on what is expected from the IAF with regard to enterprise risk management. Furthermore, it should be certain whether the board and senior management are aware of what the potential role and function of internal auditing could be to assist in fulfilling their responsibilities. Perceptions are compared with the activities currently performed by the IAF, as well as what the Standards of the Institute of Internal Auditors (IIA) expect from internal auditors.

According to corporate governance guidance (COSO, 2004: 83; AS/NZS, 2004: 27; Spencer, 2005: 8-9;Atkinson, 2008: 42-45; IOD, 2009: 73-74), the responsibility for risk management lies with the board and senior management. Many companies implement a board risk committee to assist with this task (PWC, 2006:34-35; PRMIA, 2008; IIA Research Foundation, 2009b: 50). A further tendency is to set up a separate risk department and/or a chief risk officer to assist with

this task (Beasley et al., 2005: 529; De la Rosa, 2007; PRMIA, 2008: 13; Hettinger, 2009: 49). This leaves the IAF independent to provide the board with assurance on the risk management framework and process.

According to Standard 2120 (IIA, 2009a: 28-29) the IAF must evaluate the effectiveness of the risk management process. According to Practice Advisory 2120-1 (IIA, 2009a: 107-110) and a position paper (IIA, 2004), the ideal role for internal auditing is to verify the adequacy and effectiveness of the risk management process(es); that is verify whether management has planned and designed the process in such a manner that it provides reasonable assurance that the company's objectives and goals will be achieved. The activities can be divided into core activities (such as providing assurance on the risk management process, providing assurance that risks are evaluated correctly, evaluating the risk management process, evaluating the reporting of key risks, and reviewing the management of key risks); legitimate activities that may be performed with certain safeguards (refers to consulting activities that the internal auditor may undertake); and activities that are not appropriate to the IAF's role (such as taking responsibility for risk management).

2.4.2. Frequency of audit reviews of information security

It is hard to develop a good relationship unless there is fairly frequent interaction. In the context of the relationship between the internal audit and information security functions, the most likely form of interaction involves audit reviews. However, audit reviews of information security are affected by internal audit's level of technical expertise, making it difficult to distinguish between the frequency of review and expertise factors in the interviews. For example, the previously quoted CISO who stated that he had a positive relationship with internal audit, but that they focused on business processes (e.g., fraud prevention), also indicated that he did not think the internal auditors in his organization possessed much technical expertise (and the auditor interviewed at that same organization agree.

Frequent internal audit review of information security may also serve as a preventive control—if information security personnel are aware that their work is being actively monitored by internal

audit, they are more likely to remain in compliance with corporate information security policies and procedures. Normative frameworks clearly indicate that such review and assessment is a critical component of effective information security. For example, the monitoring, evaluating, and assessing of controls is one of the five top-level categories of enabling processes in the COBIT 5 Framework (ITGI 2012a, 2012b) deemed necessary for effective governance and management of information technology. Similarly, NIST Special Publication 800-53 identifies security assurance, which is defined as "the measure of confidence that the security functionality is implemented correctly, operating as intended, and producing the desired outcome" as one of the key components to effective information security (NIST 2012, pp. 18-19).

What are Ethiopian governmental organization internal audit problems?, what looks like the contribution of the managers to build the strong relationship between internal audit and information security?, the role of internal auditor's on government organization, the role of internal auditor's on information security effectiveness and factors that affects the relationship between internal audit and information security are the main concern of the researcher.

The other concern of the researcher is that try to indicate the solutions about the problems which hinder the relationship between internal audit and information security functions. This is done through participating all concerned party with the necessary resources. Top managements regular and continuous communication with IA and IT professionals about information security issues are vital point to create strong bond between the two functions. The rapid growing of technology in terms of information technology, information security system and modern internal audit practice issues are emphasized.

Hence, this study tries to fill this gap in terms of assessing the needs and challenges of building successful relationship between internal audit and information security Ethiopian government organizations.

CHAPTER THREE
RESEARCH DESIGN AND METHODOLOGY

This chapter presents what research design and method was employed to answer the research questions formulated. Review of the research methods: descriptive, exploratory, qualitative, quantitative and mixed research methods are made and choice of the research methods and the reasons for that is stated. Questions answered in this part are: What research paradigm is used? How samples for the study are selected and why? What data collection techniques are employed? How data is analyzed?

3.1. Main research design components

The researcher preferred the following research design to reach a sound and applicable internal audit control and information security. On other words, to answer the research question properly.

a. ***Literature Review:*** This research starts with a literature review focusing on key concepts from the areas the relationship between internal audit and information security studies.

b. ***Assessing The Current IA and IS Practice and Challenges:*** A mixed research methods (Qualitative and Quantitative methods) was applied to assess the current *IA and IS* practice, success factors, and problems that impede the implementation of IAF(internal audit function) and ISS (information security system) in government organization. The rationale for selecting mixed methods design is to get a better understanding of the problem identified in this research. The mixed methods approach would allow for both text and statistical analyses of data, and would permit

more flexibility when designing questions for survey interviews, i.e. both open- and close-ended questions (Anene& Annette, 2007).

3.1.2 Steps that has been taken during this study

1. Conducting a literature review to capture ISM concepts
2. Assessing the current IA and IS practice and challenges
3. Collected data was analyzed
4. The findings resulting the data analysis (3) will be discussed with respect to the research question
5. These findings (4) were interpreted within the context of the research framework.
6. The thesis concludes with a summary of the findings.

3.2 Research methodology

The research design was impacted by the result of the literature review. The study was conducted using survey questionnaire, and interview as a method of data collection and mixed research method as a research paradigm. The strategy of inquiry for this approach is concurrent procedures. Concurrent procedures strategy is defined as situations "… in which the researcher converges quantitative and qualitative data in order to provide a comprehensive analysis of the research problem" (Anene& Annette, 2007).

Mixed methods research refers to the research or lines of inquiry that integrate one or more qualitative and quantitative techniques for data collection and analysis. Qualitative collection methods, including interviews, focus groups, participant observation, and open-ended survey items have great potential for exploring new topics, assisting theory building, and providing context for quantitative data (Matthias ,2012). Open-ended questions are used in organizational research to explore, explain, or reconfirm existing ideas. Whereas quantitative methods work best in isolating variables and demonstrating correlates associated with variation, qualitative data

collection techniques are particularly effective at gaining insight into the processes and events that led up to the observed variation (Dean , 2008). Combining, or linking, quantitative and qualitative data collection methods within studies can provide numerous benefits. These advantages are described for three broad reasons:

Mixed methods research is defined as a technique that “mixes or combines quantitative and qualitative research techniques, methods, approaches, concepts or language into a single study” (Dean 2008). Mixed methodology today is a natural complement to traditional qualitative and quantitative research. Therefore, to conduct this research the researcher used descriptive survey method. This method was selected for this particular study because it was found an appropriate technique for collecting vast information and opinion from respondents. It is also relevant to gather detail description of existing condition and practices of the relationship between Internal Audit and Information Security in government organization.

3.3 Source of data

The primary data sources used in this study are Head of Bureaus, IT directorate and Internal Audit directorate who has decision power related to IA and IT security. This is because, IA departments and IT departments manage all internal control and the information systems functionalities including its security while the security experts or system administrators make sure that the systems are functioning as per the required policy, procedures, government organization requirement, etc. In addition, secondary sources of data such as relevant best practices in information security policy, internal audit findings standard and procedure documents were reviewed.

3.3.1 Sampling design and sampling techniques

The researcher used the following sampling components: population, sampling method, and sample frame and sample size to prepare sampling design.

3.3.2 Population

The population of the study was eighty (18) Addis Ababa City Government bureaus in Addis Ababa. Among those, four government bureaus were selected. And the researcher collected 4 (four) bureaus data.

3.3.3 Sampling method

This study employed both Non-probability and probability sampling method. The researcher used the lottery sampling technique; as such it is a Non-probability sample method, for interview and questionnaires purpose in all bureaus. Because of the time constraint the sampling method used for the interview was purposive sampling technique and as such, it is a non-probability sampling. Purposive sampling refers to situations where participants are selected based on their specialized insight or special perspective, experience, characteristic, or condition when there is something the researcher wishes to get and understand (Yegidis&Weinbach, 1996). In addition, probability sampling was used to select sample Addis Ababa city government bureaus out of eighty bureaus. To select sample bureaus additional techniques were used. That is, stratified sampling government bureaus and lottery method to select sample bureaus from strata. From the total number of eighty government bureaus in Addis Ababa City Administration four bureaus were selected for the study. The following procedures were generally used in determining the sample:

1. The total number of bureaus, by name, has been taken from Addis Ababa city administration.

2. Then apply stratified probability since they are homogenous.

3. The proportion for selection was determined by computing the ratio of the required sample (n) to the population of the study (N), proportion 4/18 =2/9.

4. The stratified bureaus were multiplied by the obtained proportion to get the number of banks that are included in the sample of the study.

5. Apply lottery method to select sample banks after stratified sampling was done.

6. Purposive sampling technique was applied to bureaus head office, IA directorate and IT security directorate of sampled bureaus.

7. Distribute questioners and conduct interview with bureaus head office, IA directorate and IT security directorate of sampled bureaus.

3.3.4 Sample scope

Sampling scope refers to a list or set of direction that identifies the target population. Thus, the target population of this study is those 4(four) selected bureaus.

3.3.5 Sample size

The sample size of this study is 4 bureaus. This means 22.22% of the total population ((4/18)*100%).

3.4 Instruments of data collection

Generally, two types of instruments, namely: questionnaire, and interview were employed for the data collection. The primary data was collected through questionnaire (structured) and interview (unstructured).

3.4.1 Questionnaire

A questionnaire was designed based on the three categories such as Physical and Environmental, Technical, and Administrative. The questions items are open and closed on practices and status

in internal audit control and information security. The questioners were prepared and distributed to bureaus head office, IA directorate and ICT directorate of sampled bureaus.

The questionnaire developed for IA professional, IT professionals and other employees had 24 questions in four categories. The first section dealt with the relationship between internal audit and information security. Second section dealt with top management influence towards the relationship between internal audit and information security.. And the third section deals with the factors which affects the nature of the relationship between internal audit and information security.

3.4.2 Interview

Informal information about interviewees' experience and knowledge has been collected by the researcher prior to conduct an interview. They possess the experience and perspective in internal audit and information security system that this research wishes to understand. Given the internal audit professional and information security system experience and background of potential interviewees, purposive sampling method seems the most logical choice for data collection in this research (Anene& Annette, 2007).

The main purpose of this interview session is to supplement and increase the validity and reliability of the information obtained through the questionnaire. The following points were addressed. These are: questions about IA and IT security development and implementation practice, what are the problems that impede and the success factors in development and implementation of IA and IT security and how do you identify your bureaus requirements prior to select best practices or controls?, and what kind of IA and IT risk management methodology used?

The appointment was given to interviewees approximately two days before their scheduled interview date. The average time for the interviews was 30 minutes. All interviews were conducted face-to-face, in person, at the interviewees' site of business.

3.5. Procedures

The data-gathering tool used in the study was drafted on the basis of the reviewed literature and the intended data to be collected. The set of questionnaires were distributed to the respondents. The data collection process was administrated by the student researcher. All interviews have been done by the student researcher. Data collections through interview were conducted by speaking to the respondents face to face. Before conducting the interview, the student researcher has tried to create conducive atmosphere and explain the purpose of the interview to them. As a result necessary information was collected, organized and processed separately for interpreting and summarizing purpose to produce the major findings.

3.6. Method of data analysis

After the collecting of raw data, classification and tabulation was done by the researcher to make it ready for the analysis. All collected data was organized and processed separately for each item in a way appropriate to answer the questions in the problem statement. Descriptive statistics was used to analyze the data. In addition to these verbal descriptions was used to present the data.

The research method used to conduct this paper and components of research design with the steps used are clearly explained. The researcher is used the primary sources of data get from through questionnaire and an interview. The population of the study is eighty and the target group is four. Both probability and non probability sampling method was used to collect a data through questionnaire and an interview respectively. The methods of data analysis used was descriptive statistics by using tabulation and verbal explanations.

CHAPTER FOUR
FINDINGS INTERPRETATION AND IMPLICATION

The findings are organized in to four (4)basic categories namely, the relationship between internal audit and information security, top management influence towards the relationship between internal audit and information security, the factors which affects the nature of the relationship between internal audit and information security and fourth the perceived role of internal audit.

Each category has list of the relationship between IA and IS security domains. In this section findings of the study and its interpretations are presented under each question items whereas implications are stated at the end of each relationship categories.

4.1. General information

The aim of the field study is to discover the state of the relationship between internal audit and information securities of government bureaus. Questionnaires and interview questions were used as instrument to carry out the study. The questionnaires were used to collect data about the relationship between internal audit and information security and the student researcher own additional points which are relevant to inspect IA and IS practice in the government organization . The summary of the findings of each question item under each security domains in the surveyed government bureaus is attached at the end as ***appendix*** in which the government bureaus namelessly represented from 1-4. The thesis research findings are classified into two major areas viz.; findings from the interviews and findings from questionnaires. Questionnaire findings provided insight into how the relationship between internal audit and information securities are managed in surveyed government bureaus. Findings from Interview clarified the general issues in the relationship between internal audit and information security in addition to supplement the questionnaires.

4.2. Study sample

The following Addis Ababa city government bureaus were included in the study. These are: Addis Ababa City Education Bureau (AACEB), Addis Ababa City Finance and Economic cooperation Bureau (AACFECB), Addis Ababa City Road Authority (AACRA) and Addis Ababa City House Development Bureau (AACHDB) .These government bureaus were selected by lottery method.

4.3. Respondent information

The respondents of the research include IA staffs, ICT staff and other employee from the selected government bureaus who are engaged professional position about internal audit and information security.

4.4. Questionnaire

The questionnaire was given to Addis Ababa City Education Bureau internal audit and IT staffs in one of the sampled bureaus as a means of testing whether the questions were easily understood. After getting recommendations from these groups of people and my adviser, the questionnaires were personally distributed to the bureaus listed in 4.2. And then the student researcher has collected the filled questionnaires. The questionnaires are attached as an *appendix* the end of this document. Cooperation letter which was written by Addis Ababa University and introductory statement about privacy of respondents is a document which is attached to a survey questionnaire in order to raise the motivation of the respondents and to create suitable zone. This is used as a guarantee that the information provided is to be used only for the stated purpose. The survey was carried out in 4 Addis Ababa City government bureaus from May 3 - 12, 2018. The survey was done in person to increase the response rate and also succeed in the study even though it is time taking to get responses from a given government bureaus.

4.5. Response

Questionnaires were collected from all the 4bureaus to which questionnaire were distributed. Therefore, the response rate is 100% calculated using: ***Number of completed questionnaire*** = ***4= 1.0 X 100= 100% Number of questionnaire sent out 4***This shows that the response rate is high and it could be considered valid for proceeding with the analysis of data obtained.

4.6. Findings

In this section, the results from data analysis are presented and addressing the main concept sof the relationship between internal audit and information security which make up the themes .The data analysis result is depicted using charts in percentage which refers to the number of bureaus having or not having the relationship between internal audit and information security situations. As has been indicated in 4.2 (response) above, the result of the analysis is based on the responses obtained from 4 bureaus. For the sake of simplicity findings of the questionnaire was summarized and attached as an ***appendix C*** at the end of this document.

Table 4.1

Summarize the organization selected and results obtained.

Addis Ababa City government bureaus	Number of response obtained	percentage
Addis Ababa City Education Bureau	24	96%
Addis Ababa City Finance and Economic cooperation Bureau	20	80%
Addis Ababa City Road Authority	22	88%
Addis Ababa City House development Bureau	23	92%

Source: Questionnaire data

As observed from the table, the response rates appear to be good representation of all the bureaus where they have closely equal percentage. To the best of the researcher's understanding, more responses were easily given from the newly established bureaus relatively than the older bureaus. To summarize the findings of the survey data, three sets of interviews were held with relevant respondent groups. The target respondents, the selection process and the interview process are described next.

The first interviews were with internal audit directorates and IT security directorates of selected bureaus. The bureaus were purposively selected and included in the interview from the above sample used for the survey data collection based on willingness of internal audit directorates and IT security directorates for interview. These were the following Addis Ababa city Government Bureaus:

o Addis Ababa City Education Bureau)…----------Participant A

o Addis Ababa City Finance and Economic cooperation Bureau ----------Participant B

o Addis Ababa City Road Authority ----------Participant C

o Addis Ababa City House development Bureau ----------Participant D

The second interviews were conducted with the head of the four Addis Ababa city government bureaus. The above interviewees were considered appropriate as the operations of government bureaus and they are mobilizing huge resources (Financial resource, Capital resource and human resource).

4.7. Demographic data of questionnaire respondents.

In the next section, analysis of the data are based on the information collected from the selected four bureaus internal audit professionals, IT professionals and other employee in the organizations in terms of the respondents' gender, age, experience, qualification and related matters will be presented. In terms of gender, respondents have the following background:

Table.4.2

Gender distribution of respondents

Gender	Frequency	percent
Male	49	54.44%
Female	41	45.56%
Total	90	100%

Source: Questionnaire data

This summary indicated that 54.44% of the respondents are males and the remaining 45.56% are females. It can be observed from the data that women participation isgood in professional positions in the government bureaus and gender issues are not a problem because the gap between female and male employee is narrow.

The age distribution of the respondents was as summarized below (Table 4.9):

Table 4.3

Ages of respondents

Age Range	Frequency	Valid percent	Cumulative percent
<30	26	28.88%	28.88%
31-40	42	46.67%	75.55%
41-50	17	18.89%	94.44%
>50	5	5.56%	100%
Total	90	100%	

Source: Questionnaire data

The significant proportion of respondents was in the age range of 31 to 40 years constituting 46.67% of the respondents, followed by those in the age range of up to30 years 28.88%. This tells us the age 30-40 posses 75.55% are productive age and this can contribute for well performance of the bureaus. And also assures that the respondents were with appropriate level of maturity to assume professional positions making them appropriate to answer the survey questions properly. 24.45% of the respondents ranged from 41-50 and above 50 year shows that their number becomes decreases as their increase. In terms of total experience respondents did have the following backgrounds.

Table 4.4

Experience of respondents

Experience	Frequency	Valid percent	Cumulative percent
<10	41	45.56%	45.56%
11-20	33	36.67%	82.23%
>20	16	17.77%	100%
Total	90	100%	

Source: Questionnaire data

It is significantly important that the respondents possessed experience (from 1 to 10 years) experience and 11- 20 years of experience in the professional position which enables them to understand very well the issues raised in the questionnaires in light of their bureaus. However, respondents having above20 year experience in the professional position relatively posses fewer percentage than those who have 1-10 year experience and 11-20.Having more experience in the professional position may affect positively the quality of information gathering through questionnaire and an interview. But it does not mean that respondents those who have less experience affect negatively the quality of information given through the questionnaire and interview. Comparatively it is expected that the employee professional having more experience may give detail and narrative information about their organization and experience they posses than those having less experience. Finally, the reason why the employee professionals in bureaus

predominantly for greater than 20 years are very few is that because of high turnover searching for better salary and other benefits.

Table 4.5

The nature of the relationship between IA and IS

1. There is little friction between IA and IS	Frequency	Percentage	Cumulative
Disagree strongly	9	10%	10%
Disagree slightly	13	14.45%	24.45%
Neither/nor	13	14.45%	38.9
Agree Slightly	46	51.1%	90.01%
Agree strongly	9	10%	100%
Total			
2. The relationship between IA and IS staff is close and personal	Frequency	Percentage	Cumulative
Disagree strongly	11	12.21%	12.21%
Disagree slightly	23	25.56%	37.77%
Neither/nor	14	15.56%	53.33%
Agree Slightly	32	35.56%	88.89%
Agree strongly	11	12.21%	100%
Total	90		
3.There is a good working relationship between IA audit and IS	Frequency	Percentage	Cumulative
Disagree strongly	3	3.33%	3.33%
Disagree slightly	17	18.89%	22.22%
Neither/nor	9	10%	32.22%
Agree Slightly	46	51.11%	83.33%
Agree strongly	15	16.67%	100%
Total	90		
4.IS and IA work together to assure IS are secure and reliable	Frequency	Percentage	Cumulative
Disagree strongly	37	41.11%	41.11%
Disagree slightly	22	24.45%	65.56%
Neither/nor	12	13.33%	78.89
Agree Slightly	10	11.11%	90%
Agree strongly	9	10%	100%
Total	90		

Source: Questionnaire data

The above four questions are about the relationship between internal audit and information security. Significantly 51.1% of the respondents agree slightly that there is little friction between internal audit and information security followed by the respondents 14.45% disagree slightly and agree strongly 10%. The respondents of 35.56% agree slightly that there is close and personal relationship between internal audit and information security followed by the respondents 25.56% disagree slightly. 15.56% of the respondents were said nothing about the question they asked. The rest of the respondents 10% disagree strongly and 10% agree strongly that there is close and personal relationship between internal audit and information security.

Question three and four are about working relationship between internal audit and information security. The respondents of 51.11% are agree slightly followed by 18.89% of the respondents disagree slightly. The respondents who disagree strongly are very fewer than those who strongly agree and these shows there is good working relationship between internal audit and information security. Regarding the working relationship about the security and reliability of information system, significance of the respondents responded disagree strongly 41.11% followed by disagree slightly 24.45%.Those agree slightly and agree strongly are 11.11% and 10% respectively. This indicates even though there is working good working relationship between internal audit and information security; it is not reflected by the issue of information system.

Table 4:6(5, 6, 7,8,9,10,11 and Ques. no 12)

The influence of top management towards the relationship between IA and IS

5.In my organization, top management provides adequate resources for IS	Frequency	%	Cumulative
Disagree strongly	38	42.22%	42.22%
Disagree slightly	13	14.45%	56.67%
Neither/nor	4	4.44%	84.45%
Agree Slightly	8	8.89%	70%
Agree strongly	27	30%	100%
Total	100		

6.In my organization, top management regularly communicates with employees about the importance of information security	Frequency	Percentage %	Cumulative %
Disagree strongly	42	46.67%	46.67%
Disagree slightly	20	22.22%	68.89%
Neither/nor	6	6.67%	75.56%
Agree Slightly	18	20%	95.56%
Agree strongly	4	4.44%	100%
Total	90		
7.In my organization, top management believes that information security is an important issue	Frequency	%	Cumulative %
Disagree strongly	6	6.67%	6.67%
Disagree slightly	17	18.89	25.56%
Neither/nor	3	3.33%	28.89%
Agree Slightly	44	48.89%	77.78%
Agree strongly	20	22.22	100%
Total	90		

8.In my organization, top management is more proactive as opposed to reactive with respect to information security issues	Frequency	%	Cumulative %
Disagree strongly	19	21.11%	21.11
Disagree slightly	20	22.22%	43.33%
Neither/nor	14	15.56%	58.89%
Agree Slightly	28	31.11%	90%
Agree strongly	9	10%	100%
Total	90		

9.Considering the past 3 years, I think top management's commitment to providing adequate resources for information security has	Frequency	%	Cumulative
Disagree strongly	35	38.89%	38.89%
Disagree slightly	17	18.89%	57.78%
Neither/nor	19	21.11%	78.89
Agree Slightly	13	14.44%	93.33%
Agree strongly	6	6.67%	100%

Total	90		
10.Considering the past 3 years, I think top management's communication of the importance of information security issues has increased	Frequency	%	Cumulative %
Disagree strongly	4	4.44%	4.44%
Disagree slightly	22	24.45%	28.89%
Neither/nor	14	15.56%	44.45%
Agree Slightly	42	46.66%	91.11%
Agree strongly	8	8.89%	100%
Total	90		

11.Considering the past 3 years, I think top management's view of the importance of information security has increased	Frequency	%	Cumulative %
Disagree strongly	6	6.67%	6.67%
Disagree slightly	14	15.56%	22.23%
Neither/nor	8	8.89%	31.12%
Agree Slightly	51	56.66%	87.7%8
Agree strongly	11	12.22%	100%
Total	90		

12.Considering the past 3 years, I think top management's anticipation of information security issues has increased	Frequency	%	Cumulative %
Disagree strongly	2	2.22%	2.22%
Disagree slightly	23	25.56%	27.78%
Neither/nor	16	17.78%	45.56%
Agree Slightly	45	50%	95.56%
Agree strongly	4	4.44%	100%
Total	90		

Source: Questionnaire data

Questions 5, 6, 7, 8, 9, 10, 11 and 12 are about the top management influence towards the relationship between internal audit and information security. The question about top management provides adequate resources for information security, 42.22% of the respondents disagree strongly followed by 30% agree strongly. The rest of the respondents 14.45% and 8.89%

disagree slightly and agree slightly respectively. These shows that the top management influences to build the relationship between internal audit and information security by providing adequate resource are very week. 46.67% of the respondents and 22.22% are disagreeing strongly and disagree slightly respectively about the regular communication of top management with employee. Only 20% of the respondents are agreeing slightly about regular communication of top management with employee. This shows that the attention given information security issue is very low.

The question asked whether top management believes information security is an important issue, 48.89%of the respondents agree slightly followed by 22.22% agree strongly. Only 18.89% disagree slightly and 6.67% disagree strongly. These figures are indicating that the top management believes that information security is an important issue. About pro activeness of the top management towards information security issues, 31.11% of the respondents agree slightly followed by 22.22% and 21.11% disagree slightly and disagree strongly respectively.Only10% agree strongly that the top managements are proactive about information issues.

By comparing the last three years the commitment of top management to provide adequate resources for information security , 38.89% of the respondents are disagree strongly followed by 21.11% respondents said nothing. 18.89% of the respondents disagree slightly about the providing of adequate resources for information security. The rest of the respondents 14.14% and 6.67% are agreeing slightly and agree strongly respectively.

The question asked by considering the last three years managements communication of the importance of information security , 46.66% of the respondents agree slightly followed by 24.45% disagree slightly. The rest of the respondents 8.89% are agree strongly and 4.44% disagree strongly.

For the question raised about the top management's view of the importance of information security increment, 56.66% of the respondents agree slightly followed by15.56% agree strongly. Only 6.67% and 15.56% of the respondents are disagreeing strongly and disagree slightly

respectively. Significantly 50% of the respondents are agree slightly about top management's anticipation of information security issues increment followed by disagree slightly 25.56%. Relatively insignificant number of the respondents 4.44% agree strongly and 2.22% are disagreeing strongly that top management's anticipation of information security issues increment. These shows that there are improvements the last there years in terms of importance of information security, management's view of information security and anticipation of information.

Table 4:7

The characteristics of the nature of the relationship between IA and IS

13.Would you agree that the number of internal audit findings specifically related to information security this year versus three years ago?	Frequency	%	Cumulative
Disagree strongly	38	42.22%	42.22%
Disagree slightly	13	14.44%	56.66%
Neither/nor	18	20%	76.67%
Agree Slightly	12	13.33%	90%
Agree strongly	9	10%	100%
Total	90		

14. In your organization the nature of the relationship between internal audit and information security is characterized by good relationship.	Frequency	%	Cumulative %
Disagree strongly	27	30%	30%
Disagree slightly	23	25.56%	55.56%
Neither/nor	14	15.56%	71.12%
Agree Slightly	15	16.67%	87.79%
Agree strongly	11	12.23%	100%
Total			
15.In your organization the nature of the relationship between internal audit and information security improved the overall effectiveness of the organization's information security efforts.	Frequency	%	Cumulative %
Disagree strongly	25	27.78%	27.78%
Disagree slightly	34	37.78%	65.56%
Neither/nor	4	4.44%	70%

Agree Slightly	17	18.89%	88.89
Agree strongly	10	11.11%	100%
Total			

16. Do you agree that internal audit influence contribute on information security effectiveness in your organization?	Frequency	%	Cumulative %
Disagree strongly	6	6.67%	6.67%
Disagree slightly	14	15.56%	22.23%
Neither/nor	6	6.67%	28.9%
Agree Slightly	38	42.22%	71.22%
Agree strongly	26	28.88%	100%
Total			
17.Do you agree that in your organization information security professionals Perceivedthe internal audit and information security functions should play complementary roles in an organization's information security program	Frequency	%	Cumulative %
Disagree strongly	4	4.44%	4.44%
Disagree slightly	24	26.67%	31.11
Neither/nor	8	8.89%	40%
Agree Slightly	30	33.33%	73.33%
Agree strongly	24	26.67%	100%
Total			

18.Do you agree that the frequency of audit reviews of information security affects the relationship between internal audit and information security positively	Frequency	%	Cumulative %
Disagree strongly	36	40%	40%
Disagree slightly	3	3.33%	43.3
Neither/nor	44	48.89	92.19
Agree Slightly	5	5.56	97.75
Agree strongly	2	2.22%	100
Total			

Source: Questionnaire data

Questions 13, 14, 15, 16, 17, and 18 are about the characteristics of the nature of the relationship between internal audits an information security. The question asked about the number of internal audit findings whether specifically related to information security current year versus three years ago, 42.22% the respondents disagree strongly and 14.44% of them disagree slightly. The 20% the respondents did not know about the internal audit findings whether it related to information security. The fewer percentage of the respondent's 13.33% and 10% are agree slightly and strongly agree respectively. For the question asked about the characteristics of the relationship between internal audit and information security, 30% of the respondents disagree strongly followed by 25.56% disagree slightly.15.56% of the respondents did not know about the characteristics of the relationship. The rest of the respondents 16.67% are agree slightly and 12.23% agree strongly that there is good relationship between internal audit and information security.

Another question raised for the respondents is about the nature of the relationship between internal audit and information security whether it improved the overall effectiveness of the organization's information security efforts. The majority of the respondents 37.78% disagree slightly followed by 27.78% disagree strongly. A few number of the respondents 18.89% agree slightly and 11.11% are agree strongly about the relationship between internal audit and information security improved the overall effeteness of the organization.

The above three questions indicates that the internal audit findings in the organizations are not directly related to information security, the relationship between internal audit and information security is not good and the relationship between internal audit and information security did not improved the overall effectiveness of the organization information security.

Another question asked about that internal audit influence contribute on information security effectiveness in organization and 42.22% of the respondents agree slightly followed by 28.88% agree strongly. The fewer percentage of the respondents 15.56% disagree slightly and 6.67% disagree strongly and 6.67% did not know nothing about. And 33.33% of the respondents are slightly agree that information security professionals perceived the internal audit and information

security functions should play complementary roles in an organization's information security program followed by 26.67% agree strongly. The rest of the respondents 4.44% disagree strongly and 26.67% are disagree slightly .The final question raised to the respondents whether they agree that the frequency of audit reviews of information security affects the relationship between internal audit and information security positively, the majority of them 48.89 did not know about audit reviews of information security affects the relationship between internal audit and information security. But 40% of the respondents are strongly agreed that the frequency of audit reviews of information security affects the relationship between internal audit and information security positively.

From the questionnaires response it is possible to generalize internal audit influence contribute on information security effectiveness, perception of information security professionals about internal audit functions should play complementary roles in the an organization's information security program and review of information security affects the relationship between internal audit and information security positively.

Table 4.8

The perceived role of internal audit

16. During the past there year how IS incidents (breaches, denials of service, etc.) did you have?	Frequency	Percentage(%)	Cumulative %
a. Due to smooth flow of information in the organization	38	42.22%	42.22%
b. Because of the existence of strong relationship between internal audit and IT professional(information security professionals)	30	33.33%	75.55%
c. Due to the effort of internal audit	16	17.78%	93.33%
d. Due to the positives influence of top management towards the relationship between internal audit and information security.	6	6.67%	100%
Total	90		

20. Compared to 3 years ago, the number of information security incidents has	Frequency	%	Cumulative %
a. Significantly increased	38	42.22%	42.22%
b. Significantly decreased	30	33.33%	75.55%
c. Remain unchanged	16	17.78%	93.33%
d. No information security problems have happened	6	6.67%	100%
Total			
21. Consider the total number of audit findings listed in formal internal audit reports during the most recent fiscal year, what is the percentage of internal audit findings related to information security?	Frequency	%	Cumulative %
a. Below 25%	70	77.78%	77.78%
b. 25%-- 50%	6	6.67%	84.45%
c. 51%-75	10	11.11%	95.56%
d. 76%-100%	4	4.44%	100%
Total			
22. What is the role of IA's in your organizations?	Frequency	%	Cumulative%
a. Control and follow practicality of government rules, directives and regulations	46	51.11%	51.11%
b. Maintain strong internal audit control	27	30	81.11%
C. In my organization the role of IA's is not apply as per the rule and regulation	0	0	
d. I do not know well what is the role of IA's in my organization	10	11.11%	92.22%
e. I do not know at all what is the role of internal auditor's in my organization	7	7.78%	100%
Total	90		
23. What are the characteristics of perceived role of	Frequency	%	Cumulative %

internal audit in your organization?			
a. Internal audit function is related mainly with regard to enterprise risk management	53	58.89%	58.89%
b. The internal audit believes that responsibility for risk management lies with the board and senior management.	14	15.56%	74.45%
c. Internal auditor's believe that there influence on information security (IT) professionals contribute on the effectiveness of information security	13	14.44%	88.89%
d. Internal auditor's believe that internal audit function and information security (IT) are equally important in the organization information system.	10	11.11%	100%
Total			

24. Which factor affects the relationship between internal audit and information security in your organization?	Frequency	%	Cumulative %
a. Perceived role of internal audit	49	54.45%	54.45%
b.Frequency of audit reviews of IS	13	14.44%	68.89
c. Top level management influence towards the relationship between internal audit and information security	17	18.89%	87.78
d. Perceptions of information security professionals	11	12.22%	100%
Total			

Source: Questionnaire data

Questions from 19-24 are about the perceived role internal audit. 42.22% of the respondents responded that during the past there year information security incidents have gone through due

to smooth flow of information in the organization 33.33% of the respondent said that information security incidents have gone through the existence of strong relationship between internal audit and IT professional and 16% 0f the respondents said that information security incidents gone through due to the effort of internal audit .Very few number of them (6.67%) responded that information security incidents have obtained through the positive influence of top management towards the relationship between internal audit and information security. Related question were asked which is about the number of information security incidents are increased during three years ago and 42.22% of the respondents said significantly increased followed by 33.33% significantly decreased. A few number of the respondents agreed that the number of information security incidents during three years ago are remain unchanged.

The question Consider the total number of audit findings listed in formal internal audit reports during the most recent fiscal year, what is the percentage of internal audit findings related to information security, the majority of the respondent (77.78%) said that below 25%, 11.11% of them said that internal audit findings related to information security, 4.46.67% insignificant number of the respondent 4.44% and 6.67% said that internal audit findings related to information security are 76%-100% and 51%-75% respectively. The responses tell us the majority of audit findings listed in the in the formal audit reports are not related to information security.

The respondents were also asked about the role of internal auditor's in their organization. Most of the respondents (51.11%) said that the role of internal auditor's in the government organization is Control and follow practicality of government rules, directives and regulations. 30% and11.11%of respondents said that the role of internal auditors are maintain strong internal audit control and do not well about the role of internal auditor's in my organization.

The data collected through questionnaire about the characteristics of perceived role of internal audit in their organization shows that 58.89% of the respondents responded that internal audit function is related mainly with regard to enterprise risk management followed by 15.56% of respondents who agreed internal audit function is related mainly with regard to enterprise risk management. 14.44% and 11.11% of the respondents said that the internal audit believes that

responsibility for risk management lies with the board and senior management and internal auditor's believe that internal audit function and information security (IT) are equally important in the organization information system respectively.

The last question is about factor affects the relationship between internal audit and information security in the organization. The majority of the respondents (54.45%) responded that the perceived role of internal audit affects the relationship between internal audit and information security followed by 18.89% who respond top level management influence is a factor affected the relationship between internal audit and information security in the organization. The rest of the respondents' 14.44% and 12.22%responded that frequency of audit reviews of information security and perceptions of information security professionals are factor affects the relationship between internal audit and information security in their organization respectively.

The above findings shows that the formal internal audit findings were not directly related to information security problems and the role of internal auditors are related mainly with organization risk management. Mainly the perceived role of internal audit affects the relationship between internal audit and information security.

4.8. Demographic data of interview respondents

In the next section, analysis of the data are based on the interview from IA directorate, IT directorate and head of bureaus in terms of the respondents' gender, age, experience, qualification and related matters will be presented. In terms of gender, respondents have the following background:

Table 4:9

Gender distribution of respondents

Gender	Frequency	percent
Male	9	75%
Female	3	25%
Total	12	100%

Source: Interview data

This summary indicated that 75% of the respondents are males and the remaining 25% are females. It can be observed from the data that women representation is low in managerial positions in the government bureaus.

The age distribution of the respondents was as summarized below (Table 4.16.):

Table 4:10

Ages of the respondents

Age Range	Frequency	Valid percent	Cumulative percent
<30	2	16.67%	16.67%
31-40	5	41.66%	58.33.%
41-50	3	25%	83.33%
>50	2	16.67%	100%
Total	12	100%	

Source: Interview data

The significant proportion of respondents was in the age range of 31 to 40 years constituting 41.66% of the respondents, followed by those in the age range of 41 to 50 years25%. From the age 41-50 and above 50 together consists 41.67% that assures that the respondents were with

appropriate level of maturity to assume managerial positions making them appropriate to answer the survey questions properly.

In terms of total experience and experience in the current position, respondents did have the following backgrounds:

Table 4.11

Experience of respondents

Year in the current positions * year of experience					
		0-10	11-20	>20	Total
Year in the current position	1	2	1	0	3
	2	1	2	1	3
	3	1	1	2	3
	4	0	0	1	3
Total		4	4	4	12

Source: Interview data

It is evident that the respondents possessed ample experience (from 1 to 20 years) overall experience and above 20 years of experience in the current position which enables them to understand very well the issues raised in the questionnaires in light of their organizations.

However, respondents having only one year experience in their current position outnumbered those having more than one year experience in existing position. This is followed by those having two years and three years' experience in their current positions.

Generally, the top management is in the current positions predominantly for less than three years because their number declines as the number of years of experience in the current position increases indicating high turnover in top management areas. This is further evidenced towards the bottom of the table where only four respondents are in their current positions for equal to 10 years.

4.9. Top Management Attributes

One major factor that determines the relationship between internal audit and information security is top management attributes related to IT such as IT experience, IT expertise, IT operations knowhow know how (ITGI, 2008; Jewer, 2009; Jewer and McKay, 2012). Each of the above top management attributes is assessed using descriptive summary and correlation analysis next.

Top management IT experience is summarized and presented in the following table.

Table 4: 12

Top management IT experience

	Frequency	Percent	Cumulative percent
Very law	2	16.67%	16.67%
Low	3	25%	41.67%
Medium	3	25%	66.67%
High	2	16.67%	83.34%
Very high	2	16.67%	100%
Do not know			
Total	12		

Source: Interview data

The IT experience of top management is 'medium' and above medium ('high and 'very high') as evidenced by 58.34 % of the respondents. And below medium 'low and very low' consists the remaining 41.67% of the respondents stated that the IT experience of the top management is 'low' and. This existence of IT experience makes to build the relationship between internal audit and information security. Hence top management having medium and above medium IT experience can influence the IT staff positively by creating communication based on IT knowledge to improve information security system of the organization. But 41.67% of the top management IT experience is very low which is difficult to maintain good relationship.

Table 4.13

Level agreement IA control positively influences effectiveness of IS

	Frequency	Percent	Cumulative percent
Disagree strongly	2	16.67%	16.67%
Disagree slightly	3	25%	41.67%
Agree strongly	5	41.67%	83.34%
Agree slightly	2	16.67%	100%
Total	12		

Source: Interview data

The top management level agreement of IA control positive influence is 'agree strongly' and below 'agree strongly'(disagree strongly and disagree slightly) as evidenced 83.34% of the respondents .Those agree strongly and agree slightly together consists 58.34% of the respondents. And below disagree slightly disagree strongly consists the remaining 41.67% of the respondents stated that the top level management agree that IA control positively influence the relationship between internal audit and information security. This implies that the majority of top management agree on internal audit control influence effectiveness of information security. Those respondents do not agree the internal audit control influence on the effectiveness of information security is not few. Therefore knowing the importance of internal audit function and its control on information security is expected from the top management.

4.10. The relationship between IA department and IT department.

To build strong information security system in the overall organization, internal audit department and IT department should have good relationship. Hence it is expected more from the top management to facilitate and positively influence to have good relationship.

The following table summarizes and presented top management influence on the relationship between IA and IT department.

Table 4.14

Top management influence on the relationship between IA and IT department

	Frequency	Percent	Cumulative percent
Very poor	3	25%	25%
Poor	3	25%	50%
Medium	4	33.33%	83.33%
Good	2	16.67%	100%
Very good	12		

Source: Interview data

The top management influence on the relationship between internal audit and information security is 'medium' and below medium ('poor and 'very poor') as evidenced by 83.33 % of the respondents. Only 16.67% of the respondents stated that the top managements influence on the relationship between IA and IT department is 'good'. This is shows lack of top managements influence to build good relationship between IT and IA departments. Luck of top managements influence to build good relationship between IT and IA departments is difficult maintain information security system in the government organization.

4.11. The existence of IT departments

There should be IT and IA departments in the organization to maintain good internal audit control and information security system. The following table summarizes and presents the existence of IT and IA department.

Table 4.15
The existence of IT departments

	Frequency	Percent	Cumulative percent
Yes	12	100%	100%
No			

Source: Interview data

The whole respondents stated that there are IT and IA departments in their organization. This shows significantly that the presence of IA and IT departments in the organization help the top managers to build strong internal control and information security system.

4.12. The level of internal audit control in the organization

The overall organization control system is based on the weakness and strength of internal audit day today activities. That means if the internal audit control is strong, the overall organization control system will be strong and vice versa.

The following table summarizes and presents the level of internal audit control in the organization.

Table 4.16

The level of internal audit control in the organization

	Frequency	Percent	Cumulative percent
Very law	1	8.33%	8.33%
Low	3	25%	33.33%
Medium	5	41.67%	75%
High	2	16.67%	91.67%
Very high	1	8.33%	100%
Do not know	-		
Total	12		

Source: Interview data

The level of internal audit control in the organization is 'medium' and below medium ('low and very low') evidenced by 75 % of the respondents. Only 16.67% and 8.33% of the respondents stated that the internal audit control in the organization is high and very high. The result shows that the level of internal control in the organization is not strong as it should be. The existence weak internal audit control in the organization is exposed for wastage of resources and violation of rules and regulations. Therefore establish strong internal audit control in the government organization is not an option, rather it is necessity.

4.13 The level of controlling information security the organization.

Like other tangible and intangible resources, information is the most valuable resource in the current era. As there are rules and regulations to control and administer organization resources, given to special consideration to control and manage information resource is essential point.

The following table summarizes and presents the level of controlling information security l in the organization.

Table 4.17

The level of controlling information security in the organization.

	Frequency	Percent	Cumulative percent
Very law	4	33.33%	33.33%
Low	5	41.67%	75%
Medium	1	8.33%	83.33%
High	1	8.33%	91.67%
Very high	1	8.33%	100%
Do not know	-		
Total	12		

Source: Interview data

About 75% of the respondents stated that the level of controlling information security the in organization is low and very low. Only 16.66%of the respondents said that there is high and very high level of controlling information security in the organization. This indicates that the level of controlling information security in the organization is very weak. In addition to this during the interview the respondents commented that the top management gives attention more about the operation of IT system than information security system controlling.

4.14. Difference in access to top level management

It is expected much from the top management to coordinate the departments in the organization and create conducive work environment. This might be by providing adequate resources, staffing the department by the right skillful and professional employee and made regular communication with employee of the departments. The following table summarizes and presents the top level management difference in access.

Table 4.18

Difference in access to top level management.

	Frequency	Percent	Cumulative percent
Yes	2	16.67%	16.67%
No	10	83.33%	100%
Total			

Source: Interview data

About 83.33 % of the respondents said that no difference in access to top level management influence the relationship between IA function information securities. Only 16.66% of the respondents stated that there is difference in access to top level management influence the relationship between IA function information securities. This indicates that the extent of top level management difference in access to influence the relationship between internal audit function and information security in the organization is very weak. In addition to this during the interview the respondents suggested that the top management consider IA and IT departments like other departments in the organization.

4.15. Interview findings of IA, IT directorate and top management (head office)

The researcher made an interview with four bureaus eight directorate and the head office about top management's attitude towards security, charge of security and IT frame works they are used. The directorates as well as the head offices responded different issues.

" *The top management is concerned about security issues and their attitude is growing from time to time and no charge of security differently but there is charge of information technology system, the bureau top management have good and positive attitude about ICT security issue and they are always worry about information system* 'said the four bureaus directorate.

Another question the researcher asked is regulation, IT and IA demographics and budget allocated for ICT. The demographics of internal auditors and ICT professionals are vary across the bureaus .

'Seven ICT professionals are dedicated and two are non-dedicated, no IT staff assigned to security and no ICT professional in the staff with security certification and the budget allocated shows 25.93%increasement' said education bureau directorate . For the same question Addis Ababa city economic development bureau directorate said that '*the number of IT staff dedicated are twenty three and no IT staff assigned to security and twenty percent of IT professional certified with security. The ICT budget shows 15% increment.*

In Addis Ababa city Road authority and House development bureau stated that, '*Eight ICT professionals(the whole) are dedicated no IT staff assigned to security and no ICT professional in the staff with security certification and the budget allocated in the current year is shows 18.37% increment. But no budget allocated separately for IT security in Addis Ababa city rural road Authority'. And eleven ICT professionals (the whole) are dedicated no IT staff assigned to security and no ICT professional in the staff with security certification and the budget allocated in the current year is shows 15.78% increment. But no budget allocated separately for IT security in Addis Ababa house development bureau.*

The above findings shows that there the same attitude about information security but assigned to IT professionals to security is null in the four bureaus. The number of dedication of IT professionals to IT system is better.

The last questions the researcher asked the directorate is about working relationship of IT and IA, IT and IT security, internal audit IT technical knowledge and the directorate responded as follows.

‘ *there is no strong relationship between internal audit and information communication system regarding to information security issue , the relationship between the two department is just like the relationship as the structure of the organization horizontal. The internal auditors level IT knowledge have is personal which help only office duties and not as such good knowledge with security issues, the internal auditors IT knowledge is only basic’* This clearly shows that there is no strong relationship between internal audit and information security regarding with security issues in all organizations. And the internal auditor’s level of IT technical knowledge is not detail as required to contribute their professional roles in the information security area.

From interview findings the researcher concluded that the top management influence positively to build strong relationship between internal audit and information security in terms of providing the whole necessary resources for information security is weak. Even though there is an improvement about the attitudes of top managements towards information security, they concerned more about the operating of the IT system. There is no the same and similar attitudes towards information security across the four bureaus. The relationship between internal audit and information security departments are just the relationship based on the structure of the organization in the whole four bureaus. The attention given to application of information security issues throughout the four bureaus is low. But availability of IT infrastructure is so good except the absence of performing information security issues. The absence of IT professional certified with information security and not included in the organization structure is the main problem for the application of information security issues.

On the side of IA, luck of the necessary IT technical knowledge to review information securities of IT staff is another main problem. This also hinder the relationship between IA and IT departments. Hence the IT technical knowledge is essential for internal auditors in addition to accounting profession.

CHAPTER FIVE
CONCLUSION AND RECOMMANDATION

The purpose of this chapter is to pinpoint the major findings of the study and indicate recommendations that can help in improvement of the relationship between internal audit and information security government organizations. Thus the chapter is organized as section 5.1 Conclusions which presents major findings of the study, and section 5.2 which presents recommendations based on the findings.

5.1. Conclusions

Prior research suggests that there should be positive organizational benefits associated with a good relationship between the internal audit and information security functions. (Wallace2011) found that a good relationship between the internal audit and information security functions resulted in better compliance with Sarbeansoxley. Further, (steinbart 2013) found that a good relationship between internal audit and information security improved the information security professional's perceptions of the overall effectiveness of the organization's information security efforts. One explanation for these finding is (Steinbart 2012) report that information security professionals believed that the internal audit feedback helped them improve the design of access controls. (Steinbart 2012) also report that auditors believed the quality of the relationship between the two functions affected audit efficiency: a poor relationship between the two functions led to efforts by information security to hide evidence of the problems from the auditors.

The researcher found evidence that the nature of the relationship between the internal audit and information systems security functions are not based on information security issues rather it is based on the relationship as the structure of the organization. Even the work relationship is .a

little bit differences across the four Bureaus studied. At education bureau and road authority and house development the two functions appear to have a strong, positive relationship that provides specific benefits to both parties. In contrast, finance and economic development bureau the two functions do not appear to have a close relationship and interviewees did not mention any specific benefits from interacting with the other party.

Monitoring is an integral component of effective internal control (COSO, 2004). Thus, it stands to reason that regular monitoring of information security controls can improve the overall effectiveness of an organization's information security program (Ransbotham and Mitra 2009). Although monitoring of information security controls can be, and usually is, done by the information security function, additional benefits may accrue when supplemented with review by internal audit (Wallace 2011). The results of this study, however, suggest that the benefits of such independent feedback depend on internal auditors' level of IT knowledge, their attitudes toward cooperation with information security personal top management support and attitude for collaboration between internal audit and information security, and organizational characteristics such as regulatory compliance requirements and formal communication.

5.2. Recommendations

It is difficult to conclude that maintaining the relationship between internal audit and information security is the only way to solve and improve the overall information security problems in the organizations. The relationship between the two functions is not always guarantee to build good information security system. This implies the inherent limitations of internal control; that internal control is designed, the rapid growing of technology especially IT technology and monitored by human beings. However it is possible to improve the relationship between internal audit and information security effectiveness through continuous follow up and support, by providing trained IT security professionals, create strong relationship between IA and IT with good communication in the organization. From the result of this study it is possible to conclude the relationship between internal audit and information security in the government organizations are economical, efficient and effective. Both the respondents to questionnaire and an interview

suggest that the existence of IT department in the organizations cannot achieve the implementation information security issues due to the absence of certified information security professionals and not included in the organization structure . However, Based on the finding the following are specific areas that need due emphasis to improve the relationship between internal audit and information security in the government organizations.

1. The employee of government organization such as internal auditors has to develop themselves with fast growing's of IT knowledge and consider information is one of an important resources of their organization.

2. To build strong relationship between internal audit and information security isa responsibility of top management, directorate, employees and other stakeholders. Hence there should be a clear line of responsibility and structure of monitoring and support the departments.

3. Including certified information security professionals in IT staff is the responsibility of city's human resource and public administration bureau.

4. The top management of the organization should regular communication with internal audit and information communication technology department about information security system of the organization.

5. There should be a frameworks, rules, regulations and directives how information communication technology governed in government organization.

6. Providing the whole necessary resources for the IT staff in order to maintain strong information security system in the government organizations is the responsibility of top management and other concerned government body.

7. Good information flow and line of communication should be existed throughout the employee of the organization to create strong relationship between the department and

top management. Thus information security issues should be communicated to all stakeholders, and other concerned party.

8. The existence of strong relationship between internal audit and information security should be evaluated against clearly established criteria's and should be monitored continuously. This is the responsibility of management and directorates of internal audit and information technology.

9. Finally the relationship between internal audits and information security system in the government organizations is also responsibility of the government authorities to take corrective restructuring of IT staff. The Federal Information Network Security Agency (INSA) should also support the government IT staff together with Office of Audit General (OFAG) to build strong relationship between internal audit and information security system.

REFFERENCES

AICPA and CICA. Trust Services Principles and Criteria. American Institute of Certified Public Accountants and Canadian Institute of Chartered Accountants. 2008.

Anene, L. N., & Annette, L. S. (2007). An Architectural and Process Model Approach to Information Security Management. Lawrence Technological University.

Anderson, K.A. 2012. A Case for a Partnership Between Information Security and Records Information Management. *ISACA Journal* 12 (2): 40-44.

Arens, A. A., Elder, R. J., and Beasley, M. S. (2007). Auditing and Assurance Services (12th ed.). Upper Saddle River, NJ: Prentice Hall.

Arens, A.A. and Loebbecke, J.K. (2000), Auditing: An Integrated Approach, 8th ed., Prentice-Hall,Upper Saddle River, NJ.

Atkinson, P. and Hammersley, M. (1994) Ethnography and participant observation. Handbook of qualitative research. (pp. 248-261)

Atkinson W (2008). Board-level risk committees. Risk Manage. 55(6): 42 - 45.

Beasley MS, Clune R, Hermanson DR (2005). Enterprise risk management: an empirical analysis of factors associated with the extent of implementation

Behn, B., Carcello, J., Hermanson, D.R., and Hermanson, R.H. 1997. The determinants of audit client satisfaction among clients of big 6 firms. *Accounting Horizons* 11(1): 7-24.

Bodin, L. D., Gordon, L. A., and Loeb, M. P.Evaluating information security investments using the analytical hierarchy process. Communications of the ACM 2005;48:79-83.

Bodin, L. D., Gordon, L. A., and Loeb, M. P. Information security and risk management. Communications of the ACM 2008;51: 64-68.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. Information security policy compliance: empirical study of rationality-based beliefs and information security awareness.Quarterly 2010; 34:523-548.

Campbell, K., Gordon, L. A., Loeb, M. P., and Zhou, L. The economic cost of publicly announced information security breaches: empirical evidence from the stock market. Journal of Computer Security 2003;11: 431-448.

Carcello, J., Hermanson, R., and McGrath, N. 1992. Audit quality attributes: the perceptions of audit partners, preparers, and financial statement users. *Auditing: A Journal of Practice and Theory* 11 (1): 1-31.

Cavusoglu, H., Mishra, B., and Raghunathan, S. A model for evaluating IT security investments. Communications of the ACM 2004a;47: 87-92.

Cavusoglu, H., Mishra, B., and Raghunathan, S. The effect of internet security breachannouncements on market value: capital market reactions for breached firms and internet security developers. International Journal of Electronic Commerce 2004b; 9:69-104.

CFO Europe Research Services. Are CFOs from mars and CIOs from Venus? Overcoming the perception gap to enhance the finance-IT relationship. CFO Publishing Corporation, London, 2008.

Chapin, D. A., and Akridge, S. How can security be measured?" Information Systems Control Journal 2005;2.

COSO. Enterprise Risk Management – Integrated Framework: Executive Summary.2004.
COBIT 4.1: Control objectives for information and related technology. IT Governance Institute: Rolling Meadows, IL., 2007.

D'Arcy, J., Hovav, A., and Galletta, D. User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. Information Systems Research 2009;20: 79-98.

Dean, C. V., Achilles, A. A., & Hubert, S. F. (2008). Integrating Qualitative and Quantitative Methods for Organizational Diagnosis. Possible Priming Effects? Auburn University, Alabama. Journal of Mixed Methods Research, Volume 2 number1, Sage Publications

De la Rosa S (2007). Taking a closer look at the role of chief risk officer. IA Advisor, March. Institute of Internal Auditors (South Africa).Johannesburg.

Dittenhofer,M.A.,Ramamoorti, S.Ziegenfuss, D.E., and Evans, R.L. Behavioral dimensions ofinternal auditing: a practical guide to professional relationships in internal auditing. The Institute of Internal Auditors Research Foundation, 2010.

Dhillon, G., Tejay, G., and Hong, W. Identifying governance dimensions to evaluate information systems security in organizations. Proceedings of the 40th Hawaii International Conference on Systems Sciences, 2007.

Ethiopian Central Statistical Agency. 2010. Population and Housing Census 2007 Report, National. at: http://catalog.ihsn.org/index.php/catalog/3583/download/50086. [Accessed 13 December 2016].

Gordon, L. A., and Loeb, M. P. The economics of security investment. ACM Transactions on Information and System Security 2002;5: 438-457.

Gordon, L. A., Loeb, M. P., and Lucyshyn, W. Information security expenditures and real options: a wait and see approach. Computer Security Journal 2003;XIX: 1-7.30

Gordon, L. A., Loeb, M. P., and Sohail, T. Market value of voluntary disclosures concerninginformation security. MIS Quarterly 2010;34: 567-594.

Hawkey, K., Muldner, K., and Beznosov, K. Searching for the right fit: balancing IT security

Hettinger T (2009). Today's CRO: the role, the fit, the purpose. RiskManage. 56(3): 49 - 52.

Iheagwara, C. The effect of intrusion detection management methods on the return on investment. Computers & Security 2004;23: 213-228

Institute of Internal Auditors (IIA), The (2004). IIA position statement: role of internal auditing in enterprise-wide risk management issues.

Institute of Internal Auditors (IIA) (2009a). International professional practices framework.IIA. Altamonte Springs. Florida

Institute of Internal Auditors (IIA) (2009b). A global perspective on risk.Tone at the Top, Issue 43, May. IIA. Altamonte Springs. Florida.

Institute of Directors (IOD) (2009). King report on governance for South Africa. King Committee on Governance. IOD (South Africa). Johannesburg.

ISACA (2014). Control Objectives for Information and related Technology (COBIT).

(COBIT). ITGI. 2012a. *COBIT 5: Enabling Processes.* (IT Governance Institute: Rolling Meadows, IL)

(COBIT). ITGI. 2012b. *COBIT 5 for Information Security*. (IT Governance Institute: Rolling Meadows, IL).

ITGI. *COBIT 4.1:* Control objectives for information and related technology. IT Governance Institute: Rolling Meadows, IL., 2007.

Ito, K., Kagaya, T., and Kim, H. Information security governance to enhance corporate value.NRI Secure Technologies 2010.

Hettinger T (2009). Today's CRO: the role, the fit, the purpose. Risk Manage. 56(3): 49 - 52.

Johnston, A. C., and Warkentin, M. Fear appeals and information security behaviors: an empirical study. MIS Quarterly 2010;34: 549-566.

Kumar, R. L., Park, S., and Subramanian, C. Understanding the value of countermeasure portfolios in information security. Journal of Management Information Systems 2008;25: 241-279.

Matthias, M., Deborah, B., & Birgit, M. (2012) Mixed Methods: Combining Expert Interviews, Cross-Impact Analysis and Scenario Development .University of Canberra, Australia. Electronic Journal of Business Research Methods Volume 10

Miles, M., & Huber man, M. Qualitative data analysis: an expanded source book (2nd edition). Thousand Oaks, CA: Sage Publications, 1994

Mishra, S., and Dhillon, G. Information systems security governance research: a behavioral perspective in 1st Annual symposium on information assurance, Academic Track of 9th Annual NYS Cyber Security Conference, New York, USA , 18-26, 2006.

National Institute of Standards and Technology (NIST). 2012. *Special Publication 800-53, Revision 4: Information Security – Security and Privacy Controls for Federal Information Systems and Organizations*

Phelps, D. and Milne, K. Leveraging IT controls to improve IT operating performance. The Institute of Internal Auditors Research Foundation, 2008

Pierce, T. (2007), "Taming program risk: five critical success factors", Internal Auditing, Vol. 22No. 5, pp. 3-8.

PricewaterhouseCoopers (PWC) (2006). Enterprise risk management benchmarking survey.

PricewaterhouseCoopers (PWC) (2008b). Internal audit 2012: a study examining the future of internal auditing and the potential decline of a Controls-centric approach

Professional Risk Managers' International Association (PRMIA) (2008). Enterprise risk management: a status check on global best practices.

Ramamoorthi, S. and Weidenmier, M.L. (2006), "ERM under construction: is IT next for ERM?",The Internal Auditor, Vol. 63 No. 2, pp. 45-50.

Ratliff, R.L., W.A. Wallace, G.E. Sumners, W.G. McFarland, and J.K. Loebbecke. Internal auditing: principles and techniques, 2nd edition. Altamonte Springs: Institute of Internal Auditors, 1996.

Ransbotham, S., &Mitra, S. Choice and chance: a conceptual model of paths to information security compromise. Information Systems Research 2009; 20: 121-139

sarbanes-oxleycompliance:an exploratory study. Journal of Information Systems 2011; 25: 185-212

Schaffhauser, D. The business of a data breach. Retrieved September 3, 2010, from Campus Technology:

Siponen, M. and Vance, A. Neutralization: new insights into the problem of employee n information systems security policy violations. MIS Quarterly 2010;34: 487-502.

Schroeder, M., Solomon, I., and Vickrey, D. 1986. Audit quality: the perceptions of audit-committee chairpersons and audit partners. *Auditing: A Journal of Practice and Theory* 5 (2): 86-94.

Spears, J. L., and Barki, H. User participation in information systems security risk management.MIS Quarterly 2010;34: 503-522.

Spencer Pickett KH (2005). Auditing the risk management process. Wiley & Sons. Hoboken. New Jersey.

Steinbart, P.J., Raschke, R., Gal, G., and Dilla, W. 2012. The relationship between internal audit and information security: An exploratory investigation. *International Journal of Accounting Information Systems* (13): 228-243.

Steinbart, P.J., Raschke, R., Gal, G., and Dilla, W. 2013. Information Security Professionals' Perceptions about the Relationship between the Information Security and Internal Audit Functions. *Journal of Information Systems* 27 (2).

Stoel, D., Havelka, D., and Merhout, J.W. 2012. An analysis of attributes that impact information technology audit quality: A study of IT and financial audit practitioners. *International Journal of Accounting Information Systems* 13: 60-79.

Wallace, L., Lin, H., and Cefaratti, M. A. Information security and sarbanes-oxleycompliance:an exploratory study. Journal of Information Systems 2011; 25: 185-212.

Yegidis, B. L., & Weinbach, R. W. (1996). Research Methods for Social Workers, 2nd Edition, Allyn and Bacon, Boston, Massachusetts

BIBLIOGRAPHY

Bodin LD, Gordon LA, Loeb MP. Evaluating information security investments using the analytical hierarchy process. Commun ACM2005;48:79–83.

Bulgurcu B, Cavusoglu H, Benbasat I. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS Q 2010;34:523–48. evidence from the stock market. J ComputSecur 2003;11:431–48.

Cavusoglu H, Mishra B, Raghunathan S. A model for evaluating IT security investments. Commun ACM 2004a;47:87–92.

Chapin DA, Akridge S. How can security be measured? InfSyst Control J 2005;2.

COSO. Enterprise risk management — integrated framework: executive summary; 2004. Proceedings of the 40th Hawaii International Conference on Systems Sciences; 2007.

Dittenhofer MA, Ramamoorti S, Ziegenfuss DE, Evans RL. Behavioral dimensions of internal auditing: a practical guide to professional relationships in internal auditing. The Institute of Internal Auditors Research Foundation; 2010.Actual spending versus budget?

COBIT PO7 discusses importance of managing IT talent

COSO-ERM Internal Environment: states need for “commitmentto competence”How would you characterize the working relationshipbetween the IT security staff and internal audit? BetweenIT security staff and the rest of IT?

COSO-ERM Information and Communication: states that effective communication flows down, across, and up the entity

COBIT PO4.15 stresses need to foster between security and compliance, among other functions

COBIT ME2 Maturity model states that higher levels are characterized by increased IT participation in internal control assessments

IIA Sections 2050 and 2110.A2 discuss importance of evaluating IT governance

COSO-ERM Information and Communication: states that effective communication flows down, across, and up the entity

APPENDICES

APPENDIX I: QUESTIONNARIE

Addis Ababa University

Accounting and Finance Master Program

Survey Instrument to be completed by top management

This questionnaire has been designed to gather data for the fulfillment of the thesis requirement for Master of Science in Accounting and Finance. Thank you for participating in this survey on 'the relationship between internal audit and information security in Addis Ababa city administration '.

All of the data will be summarized and no one will be identified from these summarized results. Participation in this study is voluntary. You may decline any questions that you do not wish to answer. There are no known or anticipated risks from participating in this study. Because of the potentially sensitive nature of the study, every effort has been made to protect your anonymity. The data collected from the survey will be maintained on the researcher's computer and the returned questionnaires will be properly kept. All soft copy files will be password protected to ensure security and confidentiality of the data. The data will never be shared with others without your prior consent.

I. General Profile

1. Please state your organization's name----------
---

2. Please confirm—what is your responsibility as a member of top management? ----------
---

3. Gender: a. Male ____ b. Female _____

4. Age:
a. Up to 30 years

b. 31-40 years

c. 41-50 years

d. Above 50 years

5. Qualification and area of specialization (All applicable ----------
---
---

6. Years of experience:

a. Up 10 years

b. 10 to 20 years

c. Above 20 years

7. Number of years in the current position (Approximately)

a. below 5 years

b. 5- 10 years

c. 11- 15 years

d. Above 15 years

10. Approximately how long has the top manager t been in this position?
a. Less than 2 years ago

b. 2-5 years ago

c. 6-10 years ago

d. More than 10 years ago

e. Not applicable

	Very low	Low	Inter mediate	High	Very high	Do not know
1.How would you describe the overall IT experience of the top management of your company?						
2. At what level would you describe the level of internal audit control in your organization?						
3. How would you describe the level of controlling information security in your organization?						
	Disagree strongly	Disagree slightly	Neither/nor	Agree slightly	Agree strongly	
4. To what level would you agree or disagree that internal audit control positively influence the effectiveness of information security?						
\	Very poor	Poor	medium	Good	Very good	
5. How would you describe the relationship between internal audit department and information technology in your organization?						

	YES	No	Do not know	
6. Is there internal audit department in your organization?				
7. Is there IT department in your organization?				
8. Do differences in access to top level management influence the relationship between internal audit function and information security				

APPENDIX I: II

The Interview Guide for IA Directorate
Addis Ababa University
Accounting and Finance Master Program

Interview guide for IA Directorate at Addis Ababa City Administration Education Bureau, Finance and economy development Bureau, Addis Ababa Road Authority and Addis Ababa Urban and House development bureau IT core process owners. Interview is held with IT core process owners who are equivalent of head of selected city's government organizations. The interview took on average from one hour to 1:30 hours. Prior appointment was taken with the interviewee at their convenience.

The questions (designed in mixed language both English and Amharic) include the following but raising issues related to them as the discussion went on:

I. General Profile

1. Please state your organization's name----------
---

2. Please confirm—what is your responsibility as a member of top management? ----------
---

3. Gender : a. Male ____ b. Female _____

4. Age:
a. Up to 30 years

b. 31-40 years

c. 41-50 years

d. Above 50 years

5. Qualification and area of specialization (All applicable ----------
---
---

6. Years of experience:
a. Up 10 years

b. 10 to 20 years

c. Above 20 years

II. Interview question for top management

1. What is top management's attitude toward security? How has it changed over the Past several years?

---

2 . Who is in charge of security?

a. Title?

b. To whom reports?

c. %time spent on security?

3. Which security/IT frameworks(s), if any, are used Adopted in Ethiopia?

---

4. Which regulations are most important to you adopted in Ethiopia?

---

5. IT demographics:

a. Number of IT staff (dedicated versus non-dedicated)

---

b. Number of IT staff assigned to security? Trend?

---

c. Percentage of staff with security certifications?

---

d. IT budget (as % of revenues)? Change/trend?

---

e. IT security budget (as % of IT budget)? Change/trend? Actual spending versus budget?

---

6. How would you characterize the working relationship between the IT security staff and internal audit? Between IT security staff and the rest of IT?

7.What is internal audit's level of IT knowledge? (perhaps use a maturity model: 0–5) — asked this of the information security professional

---

---

8. Audit demographics:

---

a. Size of internal audit

---

b. Percentage certified? Which certifications?

---

c. Internal audit budget (as % of obtained results)? Change/trend?

---

d. % of audit budget devoted to IT/IS audit? Change/trend?

APPENDIX I: III

The Interview Guide for IT Directorate

Addis Ababa University

Accounting and Finance Master Program

Interview guide for IT Directorate at Addis Ababa City Administration Education Bureau, Finance and economy development Bureau, Addis Ababa Road Authority and Addis Ababa Urban and House development bureau IT core process owners. Interview is held with IT core process owners who are equivalent of head of selected city's government organizations. The interview took on average from one hour to 1:30 hours. Prior appointment was taken with the interviewee at their convenience.

The questions (designed in mixed language both English and Amharic) include the following but raising issues related to them as the discussion went on:

I. General Profile

1. Please state your organization's name----------
---

2. Please confirm—what is your responsibility as a member of top management? ----------
---

3. Gender : a. Male ____ b. Female _____

4. Age:
a. Up to 30 years

b. 31-40 years

c. 41-50 years

d. Above 50 years

5. Qualification and area of specialization (All applicable ----------
---
---

6. Years of experience:
a. Up 10 years

b. 10 to 20 years

c. Above 20 years

II. Interview question for top management

2. What is top management's attitude toward security? How has it changed over the Past several years?

---

2 . Who is in charge of security?

a. Title?

b. To whom reports?

c. %time spent on security?

3. Which security/IT frameworks(s), if any, are used Adopted in Ethiopia?

---

4. Which regulations are most important to you adopted in Ethiopia?

---

5. IT demographics:

a. Number of IT staff (dedicated versus non-dedicated)

---

b. Number of IT staff assigned to security? Trend?

---

c. Percentage of staff with security certifications?

---

d. IT budget (as % of revenues)? Change/trend?

---

e. IT security budget (as % of IT budget)? Change/trend? Actual spending versus budget?

---

6. How would you characterize the working relationship between the IT security staff and internal audit? Between IT security staff and the rest of IT?

7.What is internal audit's level of IT knowledge? (perhaps use a maturity model: 0–5) — asked this of the information security professional

---

---

8. Audit demographics:

---

a. Size of internal audit

---

b. Percentage certified? Which certifications?

---

c. Internal audit budget (as % of obtained results)? Change/trend?

---

d. % of audit budget devoted to IT/IS audit? Change/trend?

APPENDIXES: IV

The Questioner Guide for IA, IT professionals and Other employee of the organization Addis Ababa University Accounting and Finance Master Program

The questioner guide for internal audit , IT professionals and other employee of Addis Ababa City Administration Education Bureau, Finance and economy development Bureau, Addis Ababa Road Authority and Addis Ababa Urban and House development bureau internal audit and IT professionals . Question is held with internal audit, IT professionals and other employee who is worked city's government organizations. The question took on average from three hour to four hours. The questions (designed in mixed language both English and Amharic) include the following but raising issues related to them as the discussion went on:

I. General Profile

1. Please state your organization's name----------

2. Please confirm—what is your responsibility as a member of the organization? ----------

3. Gender: a. Male ____ b. Female _____

4. Age:
a. Up to 30 years

b. 31-40 years

c. 41-50 years

d. Above 50 years

5. Qualification and area of specialization (All applicable ----------

6. Years of experience:
a. Up 10 years

b. 10 to 20 years

c. Above 20 years

II. Questions for internal audit, IT security and for other employee

Section B.

1. Please indicate the extent to which you agree or disagree with each of the following statements. If you neither Agree nor disagree, select the uncertain option.

The nature of the relationship between internal audit and information security	Disagree strongly	Disagree slightly	Neither/nor	Agree Slightly	Agree strongly
1. There is little friction between internal audit and information security					
2. The relationship between internal audit and information security staff is close and personal					
3. There is a good working relationship between internal audit and information security					
4. .Members of information security and internal audit work together to assure information systems are secure and reliable					
Total					

2. The influence of top management towards the relationship between internal audit and information security

The influence of top management towards the relationship between internal audit and information security.	Disagree strongly	Disagree slightly	Neither/ nor	Agree Slightly	Agree strongly
5. In my organization, top management provides adequate resources for information security					
6. In my organization, top management regularly communicates with employees about the importance of information security					
7. In my organization, top management believes that information security is an important issue					
8. In my organization, top management is more proactive as opposed to reactive with respect to information security issues					
9. Considering the past 3 years, I think top management's commitment to providing adequate resources for information security has					
10. Considering the past 3 years, I think top management's communication of the importance of information security issues has increased					
11. Considering the past 3 years, I think top management's view of the importance of information security has increased					

12.Considering the past 3 years, I think top management's anticipation of information security issues has increased					

3. The characteristics of the nature of the relationship between internal audit and information security.

The characteristics of the nature of the relationship between internal audit and information security.	Disagree strongly	Disagree slightly	Neither/nor	Agree Slightly	Agree strongly
13. Would you agree that the number of internal audit findings specifically related to information security this year versus three years ago?					
14. In your organization the nature of the relationship between internal audit and information security is characterized by good relationship between internal audit and information security improved the information security professional's perceptions of the overall					

effectiveness of the organization's information security efforts					
15. Do you agree that internal audit influence contribute on information security effectiveness in your organization?					
16. Do you agree that in your organization information security professionals perceived the internal audit and information security functions should play complementary roles in an organization's information security program?					
17.Do you agree that the frequency of audit reviews of information security affects the relationship between internal audit and information security positively					

Section c.

4.The perceived role of internal auditor and IT professionals

Please choose only one alternative from the following choices.

18. During the past there year how information security incidents (breaches, denials of service, etc.) did you have? (7 ordinal responses, from zero to more than 25)

e. Due to smooth flow of information in the organization
f. Because of the existence of strong relationship between internal audit and IT professional(information security professionals)
g. Due to the effort of internal audit
h. Due to the positives influence of top management towards the relationship between internal audit and information security.

19. Compared to 3 years ago, the number of information security incidents has

a. Significantly increased

b. Significantly decreased

c. Remain unchanged

d. No information security problems have happened

20. Consider the total number of audit findings listed in formal internal audit reports during the most recent fiscal year, what is the percentage of internal audit findings related to information security?

a. Below 25%

b. 25%-- 50%

c. 51%-75%

d. 76%-100%

21. What is the role of internal auditor's in your organizations?

a. Control and follow practicality of government rules, directives and regulations

b. Maintain strong internal audit control

c. In my organization the role of internal auditor's is not apply as per the rule and regulation

d. I do not know well what is the role of internal auditor's in my organization

e. I do not know at all what is the role of internal auditor's in my organization

22. What are the characteristics of perceived role of internal audit in your organization?

a. Internal audit function is related mainly with regard to enterprise risk management

b. The internal audit believes that responsibility for risk management lies with the board and senior management.

c. Internal auditor's believe that there influence on information security (IT) professionals contribute on the effectiveness of information security

d. Internal auditor's believe that internal audit function and information security (IT) are equally important in the organization information system.

23. Which factor affects the relationship between internal audit and information security in your organization?

a. Perceived role of internal audit

b. Frequency of audit reviews of information security

c. Top level management influence towards the relationship between internal audit and information security

d. Perceptions of information security professionals