ADDIS ABABA UNIVERSITY

COLLEGE OF NATURAL AND COMPUTATIONAL SCIENCES

SCHOOL OF INFORMATION SCIENCE

ASSESSMENT OF THE EFFECTIVNESS OF CARD BANKING SECURITY IN THE ETHIOPIAN FINANCIAL SECTOR

By

DANIEL GEBREHAWARIAT

JUNE, 2017

ADDIS ABABA, ETHIOPIA

ADDIS ABABA UNIVERSITY

COLLEGE OF NATURAL AND COMPUTATIONAL SCIENCES

SCHOOL OF INFORMATION SCIENCE

ASSESSMENT OF THE EFFECTIVNESS OF CARD BANKING SECURITY IN THE ETHIOPIAN FINANCIAL SECTOR

A Thesis Submitted to School of Graduate Studies of Addis Ababa University in Partial Fulfillment of the Requirements for the Degree of Master of Science in Information Science

By: Daniel Gebrehawariat

Advisor: Lemma Lessa (PhD)

June, 2017

Addis Ababa, Ethiopia

ADDIS ABABA UNIVERSITY

COLLEGE OF NATURAL AND COMPUTATIONAL SCIENCES

SCHOOL OF INFORMATION SCIENCE

ASSESSMENT OF THE EFFECTIVNESS OF CARD BANKING SECURITY IN THE ETHIOPIAN FINANCIAL SECTOR

By: Daniel Gebrehawariat

Name and signature of Members of the Examining Board

Lemma Lessa (PhD)	_____	_____
Advisor	Signature	Date
Million Meshesha (PhD)	_____	_____
Examiner	Signature	Date
Tibebe Beshah (PhD)	_____	_____
Examiner	Signature	Date

DECLARATION

This thesis has not previously been accepted in substance for any degree and is not being concurrently submitted in candidature for any degree in any university.

This thesis is the result of my own investigations, except where otherwise stated. Other sources are acknowledged by citations giving explicit references. A list of references is appended.

Signature: _____

Daniel Gebrehawariat

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

Advisor's Signature: _____

Lemma Lessa (PhD)

ACKNOWLEDGMENTS

First and foremost, I would like to thank the almighty God and his Holly Mother for giving me the strength, ability and opportunity to undertake this study. Without his blessings, this achievement would not have been possible.

My sincere gratitude goes to my advisor Dr. Lemma Lessa for his continuous support on my thesis, for his motivation, enthusiasm, encouragement, and insightful comments. His guidance helped me in all the time of the research and writing of this thesis.

I take this opportunity to thank all the financial sector staffs specially the IT departments for being cooperative for this study.

I would also like to extend my gratitude to all my instructors in the school of information science for their support and motivation.

I am also grateful to my good friend Christian Kassa for his valuable comments and feedback on my thesis draft.

My acknowledgement would be incomplete without thanking the source of my strength, support and unconditional love, my family. Thank you all.

DEDICATION

I dedicate this thesis to God Almighty my creator, my strong support, my source of inspiration, wisdom, knowledge and understanding.

Table of Contents

List of Tables

LIST OF FIGURES

LIST OF ACRONYMS

ASV	Approved Security Vendors
ATM	Automatic Teller Machine
CHE	Card Holder Environment
CHD	Card Holder Data
COBIT	Control Objectives for Information and Related Technology
CVV	Card Verification Value
DMZ	Demilitarized Zone
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
INZ	Internal Network Zone
IPS	Intrusion Prevention System
ISSA	Information Systems Security Association
ISACA	Information Systems Audit and Control Association
ISM	Information Security Management
ITIL	Information Technology Infrastructure Library
NTP	Network Time Protocol
PAN	Payment Account Number
PCI-DSS	Payment Card Industry Data Security Standard
PDA	Personal Digital Assistant

POS	Point of Sales Device
PCI DSS	Payment Card Industry Data Security Standard
QSA	Qualified Security Assessors
TLS	Transport Layer Security
VPN	Virtual Private Network

ABSTRACT

Information is the most valuable and fundamental asset in the financial sector as it plays a major role in supporting the business operations and facilitate an organization to achieve a competitive advantage in the market. Information is valuable and critical; it is also vulnerable to a variety of attacks from both inside and outside of the organizations. Currently financial sectors are repetitively attacked by cybercrimes in addition to other internal and external attacks to their electronic payment system which is costing them in billions and affecting their business. To address this concern, it is indisputable to assess information security management practice in the financial sector card banking system using international information security standard as a benchmark and identify gaps and recommend the best security practices to help the financial sector to meet the standard security compliance.

In this regard, two financial sectors were selected using purposive sampling method that issues electronic card and card PIN among the total financial sectors in Ethiopia which includes banks and e-payment processors. Regarding the target population, all the IT staffs in the two selected sectors were included to be part of this study. Thus, quantitative data was collected using PCI-DSS security standard questioners; twenty seven questioners were distributed and twenty five were filled and returned which comprise 93% among the total distributed questioners. Further to the questioners, observation and document viewing was made to strengthen the respondents' information. Accordingly, the data is processed using IBM SPSS Statistics V.20 tool.

The result shows that most of the essential security practices and management activities in the financial sectors doesn't comply the international security standard. In this regard, most of the indispensable security requirement that would address the financial sectors from security risk is below the acceptable level as there is no periodic vulnerability assessment, no access control in some critical areas, password policy and procedures is not implemented on some critical components, no change management procedure and information security policy is not maintained to be carried out in the daily operation. In general, the study shows that information security management and practice is not well maintained to address the current information security risk associated to the financial sector. Furthermore, this study identified the major security factors that prohibit the financial sectors from the PCI-DSS security standard compliance. Thus, the

study provides directions and action items that can support the financial sector to be security standard complaint based on the findings.

CHAPTER ONE

INTRODUCTION

This chapter intends to introduce the background of the research, statement of the problem, research questions and the objectives of the research. Furthermore, the chapter describes the significance of the study and the scope of the research.

1.1 BACKGROUND

In the current competitive business environment, Information is the most valuable and fundamental asset in any organization. Therefore, protecting the security of information is very important and becoming a top priority for many organizations (Heru et al 2011; Teece, 2010). To protect this valuable asset, information, there should be a proper information security practice and management that keep information from a wide range of internal and external threats and preserve its value to the organizations.

Information security is a broad subject that covers technology, operations and people to ensure integrity, confidentiality and availability of data. It also involves in the day to day operation of an organization to ensure the success and progress of the business and to get the customers trust on top of the competitive advantage of the business.

Securing information is required to build bridge of trust between the client of the service and the presenter of the service as Information security is related to the protection of information technology assets against the risks of loss, misuse, disclosure or damage (Rezakhani et al., 2011). Therefore, it is essential to give much consideration for information security as much as the value of the business which is determined in the value of its information.

It is important that confidentiality, integrity and availability are the most inclusive concern of information security. Business continuity planning places a significant emphasis on protecting the availability of information as part of the overall objective of business recovery. In general, the goal of information security management is to protect the confidentiality, integrity, and availability of information and to mitigate the various risks and threats associated to information (Posthumus and von Solms, 2004). In this regard, organizations should be examined to realize their stand on information security practice and management and address risks and threats that affects the business continuity and reputation.

Information security management includes the deployment and management of countermeasures to threats and risks on top of implementing and following information security policy, procedures and standard in the day to day activities of the organization.

As Shi-Ming et al (2006) noted, if organizations follow the guidelines and standards to set up their security policy, they could own a tighter and more complete IT environment. Organization could also safeguard their business value and benefit from IT if there is a well-developed information security management. In addition to this, businesses also need to implement rules and controls around the protection of the valuable information and systems that store and process of information, and this protection is attained through the proper implementation of information security policies, standards, guidelines and procedures.

As a result of emerging and development of internet, electronic commerce has emerged allowing business to more effectively interact with their customers and other corporations inside and outside their industries. One industry that is using this new communication channel to reach its customers is the banking industry (Omariba et al., 2012). However, security vulnerabilities and breaches remain a major concern for financial sectors as they cost billions of dollars in downtime, maintenance and disruptions (Roumani et al., 2016).

Electronic payment service is a new technology that has many capabilities and also many potential problems, Due to its lower transaction costs, twenty-four hours services, increased control over transactions, higher volume of transactions in less time, remote transaction facilities, and much wider array of banking products and services, e-banking has become an integral part of modern banking (Singh Brar et al., 2012).

Currently various standards have been developed in which emphasis is placed in part on other target groups related to the business. The use of security standards in the financial sectors such as banks do not only improves the level of security, their use also makes it easier for to agree on which security safeguards should be implemented to protect the valuable information and on which type of security standard the organization should be compliant. The number one priority for making compliance work is assessment and evaluation. If the organization weaknesses are not known in terms of information security then this makes it nearly impossible to put the best practices into action (Munirul et al., 2011).

According to Munirul et al., (2011), security compliance is one of the major issues in information security management. Hence, many different framework, guidelines, and standards were proposed by researchers, practitioners, consultants, and professional to protect organization information assets (Choobineh et al., 2007). The most widely used international standards are: COBIT, ISO 27001&2 and PCI-DSS (Payment Card Data Security Standard)

Among these widely used standards, PCI-DSS is a very first industry-wide standard which focuses on the credit card industry that aims at achieving a strong protection of sensitive consumer and card data, and preventing major security issues. The standard sets force requirements in many aspects, including secure networks, card data protection, access control, vulnerability management, security assessments and reporting (PCI Council 2010).

PCI-DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data and manage IT security and privacy risk in credit card transactions (Spremic, 2011).

To that end, any bank that runs ATM, POS (Point of sale) machine, issues debit cards, credit card and electronic payment sector that do business with the merchants need to be complaint to PCI-DSS security standard security compliance.

Currently data breaches occur regularly and as financial sector, banks and electronic payment sectors are very frequent target from hackers who often successfully compromise sensitive information. In this regard, being PCI-DSS security standard compliance is indisputable. As PCI-

DSS standard is used to improve the security of electronic and online banking data and to facilitate consistent security measures to mitigate data breaches and fraud, the researcher will use PCI-DSS security standard checklist to assess the current information security management in the Ethiopian financial sector focusing on the card banking security on top of using ISO security standard checklist to assess the general aspect of information security management in the financial sector.

The organizations selected for this study are financial sectors in which one is a bank and the other is an electronic payment processor. As a banking sector, bank ABC provides all the major banking services that a commercial bank is expected to provide with the vision to be the bank of choice for customers, employee and shareholders and the mission to be customer focused financial services through competent, motivated employees and modern technology to maximize the value of its stakeholders. The Bank is among the four banks that issues electronic payment card and PIN security numbers at its premises to provide card banking service to its customers.

The second financial sector where this research is conducted is XYZ S.C. It a consortium owned by six Ethiopian private banks established in 2009 by the visionary banks to save the high investment cost of the modern payment platform and deliver electronic payment services to financial institutions with a shared system. It commenced operation officially on July 5, 2012.

The company has a vision to move the society from cash based economy to a greater use of electronic payment system. It is also dedicated to contribute to the modernization of national payment System in the country by optimizing economies of scale in investing on card payment infrastructure through providing interconnectivity and interoperability among banks through shared network. To that end the sector issues, electronic card and PIN to the member banks at its premises.

Thus, as this research focuses on the information security management in the financial sectors focusing on the card banking services, the two financial organizations are selected and the research is conducted accordingly.

1.2 STATEMENT OF THE PROBLEM

Financial sectors provide different financial services to their customers. With more financial transactions being processed by their central computer systems, the sectors are also concerned about the security of their system, in particular with the unwarranted access to their accounts. Furthermore, individuals are also concerned with the secrecy of their personal information (Omariba et al., 2012). Thus, protecting individuals' financial information is one of the fundamental activities to be undertaken by all financial organizations to enhance the business.

Business partners, suppliers, and vendors are seeing security as the top requirement, particularly when providing mutual network and information access. Financial sectors ability to take advantage of new opportunities often depends on its ability to provide open, accessible, available, and secure network services since having a good reputation for safeguarding information will increase market share and profit (Ula et al., 2011).

According to Kumar et al., (2008), Security weaknesses cause a negative impact on organizations such as financial loss, reputations, and loss of customer confidence. However information is a very crucial asset for organizations, it is relatively immature discipline and needs additional academic study and research. Moreover, there is a growing need for research to verify the management challenge, discover current management deficiencies identify best practice, devise mythologies and specify requirement for the management of information security (Yildirim et al, 2011).

Businesses find themselves in need to adopt standards for various reasons which vary from business requirements to regulators and compliance mandates. Establishment of proper corporate governance, increasing risk awareness and competing with other enterprises are some business drivers to mention. Some firms pursue certifications to meet market expectations and improve their marketing image (Walid and Bassil, 2013).

To provide fast and appropriate response to security incidents and to ensure interoperability between the financial sectors, there is a need for a systematic and predefined information security management. And to that end, it is crucial to assess the current security management of the financial sectors.

Here in Ethiopia, most of the banks have implemented a core banking system that interconnect all branches with the head quarter, and few banks and electronic payment system processors are connected to the international payment system on top connecting to a national switch to transact electronic payment services using ATM and POS (Point of Sale) machine. For all these, technology plays a vital role for carrying out the delivery of financial services whereas the risk followed the implementation of these technologies and the problem associated with it are not well considered.

It is clear that, merchants, especially large merchants, merchant-acquirers, payment networks, and card issuers hold large amount of sensitive data. These entities can also contract any number of functions to third parties, which are often referred to transaction processors, such as international data processors. Loss of this data often leads to significant financial and nonfinancial damage (Liu et al., 2010).

Although with the advent of technologies the financial sectors have been able to reach more customers, it has also enhanced the risk for customers who often feel reluctant and insecure in opting for such services. There is a need for the sectors to evaluate their current operating practices (Raghavan et al., 2014). To address all these issues related to the security of the financial institution such as banks, there should be a standardize information security practice implemented to protect the organization from external and internal security threats and risks.

Since, according to Spremic (2011), adopting industry best practices (e.g. CobiT, ISO 27000, PCI-DSS) and adjusting IT infrastructure with high-level executive objectives makes companies to lower IT risks, which is related to infrastructure and operational risks.

While a usage of payment cards such as credit cards, debit cards, and prepaid cards continues to grow, security breaches related to payment cards have led to billion dollar losses annually. In order to offset this trend, major payment card networks have founded the Payment Card Industry (PCI-DSS), which has designed and released the PCI Data Security Standard (DSS). This standard guides service providers and merchants to implement stronger security infrastructures that reduce the risks of security breaches (Heru et al., 2011).

And this security standard, PCI-DSS, is used to assess the information security status of organizations and provide a mitigation and road map to make the organization secured and

complaint. As a lot of vulnerabilities exist in the defense system of financial sectors and services, it is clear that there is a need to investigate the organization security status and decide on the measures to be undertaken to combat security threat (Florêncio and Herley, 2011).

Currently the financial sectors are expected to be compliant to the security standard such as PCI-DSS in order to be connected to the international payment brands. In addition to that, being security standard complaint will enable the financial sectors to protect their valuable asset from the current internal and external attacks.

On the contrary, most banks and electronic payment processors in Ethiopia often fail complying PCI-DSS in time due to improper security settings, incorrect configurations, low levels of encryption and poor policies and procedures. Assessing those controls using PCI-DSS standard checklist could have prevented costs in business disruption as well as monetary fines and makes the financial sectors competitor in the international market by enabling them to provide international card services such as VISA International, MasterCard, Union Pay and the like.

PCI-DSS security standard reduce the risk of electronic payment including debit card, credit card and internet banking data loss by preventing, detecting, and reacting to potential breaches or hacks that lead to an account data compromise since one of the goal of PCI-DSS is to protect electronic payment system from risk and threats and minimize data breach risk.

Regarding the Ethiopian financial sectors information security practice, few studies had been made previously using ISO security standard. The studies made are focused on the general information security practice and information security culture of the Ethiopian financial sector however, as most of the financial sectors are currently engaged to the electronic banking services such as card banking, an assessment should be made to explore the effectiveness of electronic banking security such as card banking security of the financial sectors to provide recommendation and action items as per the findings.

The advantage of this new technology to the financial sector is unquestionable as it brings value added services and enables any time any place banking using electronic card. Though card banking has these capabilities, there are also potential risks associated with this service such as card fraud and the like and much is not done to assess these potential risks that are disrupting the business and damaging the reputation of the financial sector.

Financial sectors are more exposed to security risk and threat than other sectors, while they adopt new technology to expand the business. Thus, the financial industries need to identify their current security status and updated their status according to the new information security standard (Kassa, 2016).

Electronic banking has many security issues which includes fraud, data loss and lacks information security in general (Arif Shaikh, 2014). To address all these information security issues related to the card banking security, this study is made using PCI-DSS security standard check list to assess the effectiveness of information security practice and management of the card banking security in the financial sector and to identify the factors that prohibits the Ethiopian financial sectors from PCI-DSS security standard compliance.

1.3 RESEARCH QUESTIONS

In this study, the researcher aims to answer the following research questions which are designed to attain the research objectives.

- How is the effectiveness of information security management practice in the Ethiopian financial sector?
- What are the factors prohibiting the effectiveness of information security management towards Payment Card Industry Data Security Standard (PCI-DSS) in the Ethiopian financial sectors?

1.4 RESARCH OBJECTIVE

The general objective of this research is to assess the effectiveness information security management in the financial sector and to provide direction and action items as a recommendation which can support the financial sectors to be security standard compliance.

1.4.1 SPECIFIC OBJECTIVES

- To review related literatures in the area of information security management and comprehend the current state of the subject in relative to financial sectors.

- To assess information security management practice in the Ethiopian financial sector using international security standards such as PCI-DSS standard checklist and information security literatures review on the subject.

- To identify the most important security factors that prohibits the effectiveness of information security management in the Ethiopian financial sector towards international security standard.

  To provide recommendation as action items for management intervention in order to meet security compliance.

1.5 SIGNIFICANCE OF THE STUDY

- ✓ It can help the financial sector to improve their information security management practice according to international security standard.

- ✓ It can make the financial sector to identify their security risk areas and take measures based on the recommendation of this study.

- ✓ It can aware the financial sector to know their current status towards PCI-DSS security standard compliance and improve their competitiveness in the international market to provide international payment services.

- ✓ It can aware the PCI council to comprehend the current level of the financial sectors in Ethiopia towards the PCI-DSS Certification.

- ✓ It can serve as a benchmark for practitioners and researchers who want to conduct more research in information security management area in the financial sector.

1.6 SCOPE AND LIMITATION OF THE STUDY

As the issue of information security is becoming very critical, different studies have been conducted in different time to address issues related to the subject by different scholars. The studies which had been previously conducted mostly focused on the general information security management of organizations such as banks using ISO security standard as a measurement instrument and recommend best practices accordingly.

This study however, assessed the current practice of information security management in the financial sector specifically banks and electronic payment processors using PCI-DSS security standard as a major instrument to measure the current stand of the financial sector in related to information security practice and management and literature review in information security. Unlike the previous researches, this study focuses on the card banking security of the financial sectors.

The study is also intended to identify the security factors that prohibits the financial sectors from the international security standard, PCI-DSS, and provide a recommendation that guide banks and electronic payment processors to be PCI-DSS security standard complaint. As a target group, the study focuses on the IT executives and experts in the head quarter of the bank and electronic payment company as all the IT staffs are existed at the head quarter.

Regarding the limitation of this study, information related to information security is much more confidential and sensitive in the financial industry. Thus, as information at the financial sector is very confidential and sensitive, it needed effort and continuous communication with the financial sectors management to convince as their information wouldn't be disclosed to any third parties for the sake of their reputation however, one of the bank refused to cooperate to this research at the last moment due to the above reason. And in this regard, the researcher was obliged to proceed with one bank that issues electronic card and PIN, and one electronic payment processor. And the other limitation is, due to time and resource constraint, the research focused

on card banking security, however, electronic banking services such as mobile banking and online banking security are also need to be studied. Regarding the target group, only 27 people are participated in this study as the numbers of the financial sectors studied are only two. And in the future studies, it is recommended to make more financial sectors that are issuing electronic cards to be part of such studies to increase the number of participant.

1.7 ORGANZATION OF THE THESIS

This research is organized in five chapters. These include:

Chapter 1: it introduces the background of information security practice and management in relation to the financial sectors specifically electronic banking and card banking security. The chapter also includes statement of the problem, research questions, and research objectives, significance of the study and scope of the study

Chapter 2: in this chapter, literature in information security, information system vulnerability, information security threats, common information security attacks, information security risk assessment and management, information security management, information security management roles, information security management process, information security management certification, critical success factors of information security management**,** information security risk in the financial sector, information security management in the financial sector, information security management standards and best practice, information security governance, information security compliance and finally, PCI-DSS (payment card industry data security standard) is reviewed and discussed thoroughly to provide an overview and explore the topic.

Chapter 3: this chapter describes the research design and methodology used. Thus, the chapter includes, research design, source of data, sampling technique, research population , data collection methods, pilot study, validity, reliability, Statistical data analysis and ethical consideration.

Chapter 4: in this chapter, the collected data is analyzed, interpreted, described and discussed based on the significance of the key findings in light of what was already known about the research problem.

Chapter 5: this chapter concludes the research and provides recommendations as per the findings.

CHAPTER TWO

LITRATURE REVIEW

2.1 INFORMATION SECURITY

The rapid development of information technology, personal computers, telecommunication, and the internet, makes people to access information at any place and at any time. Though most of people acquire this information legally, some hackers have been trying to bypass the security loophole and attack the computer systems (Farn, et al., 2004). The attack could come from either the external or the internal organizations. The attack can either be Denial of Service (DoS) or be big damage of the whole framework. Due to this, the concept of information security has become a big issue for the whole world (Farn, et al., 2004). The significance of protecting information from such disclosure gets a big attention in organizations; however the security attack is increasing aggressively from time to time.

It is clear that most of the information in the organization is collected, processed and stored on computers and transmitted across networks to other computers. The rapid growth and widespread use of electronic data processing and electronic business conducted through the Internet, along with numerous occurrences of international terrorism, fueled the need for better methods of protecting the computers and the information they store, process and transmit (Singh, et al., 2004). Thus, as Information becomes the fundamental asset within any organization, the protection of information as a valuable asset, through a process of information security, is of equal importance (Thomson and von Solms, 2005). Since as valuable assets, information plays a vital role in the organizations competitive advantage and such asset, information, need to be protected for the sake of the survival of the organization.

According to Jones (2009), the security of the information assets is a requirement for all types of organization, whether to protect the business or to meet legal or regulatory requirement as organizations are totally dependent on their IT systems to capture, store, process and distribute

company information. For this, Information Security is and has always been the discipline to mitigate risks impacting on the confidentiality, integrity and availability of a company's IT resources (Basie von Solms, 2006).

Information security is given different definitions by different scholars. Essentially, information security is defined as the process of protecting information and information infrastructure (both content and services) from unauthorized access that results in disclosure, modification or destruction of information, and modification or disruption of IT services in order to provide confidentiality, integrity, and availability (Zhi, et al.,2013; NIST 2009).

The security of information is not a new problem that has arisen with the increasing use of computing to process store and transmit information, it is just an old problem in a new environment (Jones, 2009). The security of information systems in organizations has become increasingly important in the modern information intensive environment. In an era of global connectivity and increased use of ICT by organizations, the need to protect information systems from security breaches has become significant (Zhi Xian, 2013) and with the increasing organizational dependence on information systems, information security has become a very critical issue in enterprise (Feng, et al.,2014). Since Information security has evolved from addressing minor and harmless security breaches to managing those with a huge impact on organizations' economic growth, such as the leakage of credit card information of payment companies and cost millions of dollars in penalties to regulatory compliance bodies.

It is therefore very important for companies to notice that their strength in attaining and sustaining competitiveness in the highly volatile, demanding and uncertain markets lies in their ability to securely protect their information assets and IT infrastructure (Dlamini, et al., 2009). Organizations invest much in technology innovation and upgrading the existing infrastructure to support the business and address their customer need. However, if not the technology and the infrastructure is supported securely at an acceptable level, investing much only in technology and infrastructure wouldn't bring the expected result.

According to Singh et al. (2005), a successful organization should have the following multiple layers of security in place for the protection of its operations.

i. Physical Security: To protect the physical items, objects, or areas of an organization from unauthorized, access and misuse.

ii. Personal Security: To protect the individual or group of individuals who are authorized to access the organization and its operations.

iii. Operations Security: To protect the details of a particular operation or series of activities.

iv. Communications Security: To protect an organization's communications media, technology, and content.

v. Network Security: To protect networking components, connections, and contents.

vi. Information Security: To protect information and its critical elements, including the systems and hardware.

In general, given the integral role of information technology in today's enterprises, information security has to be a key component in modern enterprise planning and management (Singh et al. 2005). This entrenchment of security was also driven by the increasing growth of electronic transactions, and fueled partly by the internet as electronic commerce proliferated with the growth of networks. To keep information secure, the organization should make sure the confidentiality, integrity and availability of information at an acceptable level and address the issue towards protecting information security.

The C.I.A. triangle has been considered the industry standard for security and basic component for information security. It was solely based on three characteristics that described the utility of information: confidentiality, integrity, and availability Singh et al. (2005). As it is mentioned in figure 2-1, the integration of confidentiality, integrity and availability is the most vital aspect in protecting information and services from external threats.

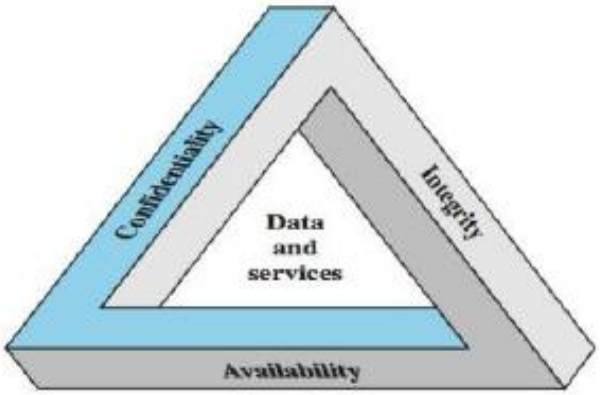

Figure 2-1: Information security components; adapted from Singh et al., (2005)

Confidentiality: Confidentiality is making sure that information is only seen by people who have the right to see it; keeping information secret from unauthorized access is probably the most common aspect of information security. The need for keeping information secret arises from the use of computers in sensitive fields such as government and industry. An organization needs to guard against those malicious actions that endanger the confidentiality of its information.

Integrity: Integrity refers to the trustworthiness of data or resources, and it is usually phrased in terms of preventing improper or unauthorized change. Integrity means ensuring that information remains intact and unaltered. This means watching out for alterations through malicious action, natural disaster, or even a simple innocent mistake. Integrity includes both the correctness and the trustworthiness of the data.

Availability: Information created and stored by an organization needs to be available to authorized users and applications. Information is useless if it is not available. In some cases information needs to be changed constantly, which means that it must be accessible to those authorized to access it. The aspect of availability that is relevant to security is that someone may deliberately arrange to deny access to data or to a service by making it unavailable (Singh et al., 2005). Thus confidentiality, integrity and availability are the basic component of information

security which every organization that gives value to its information has to address by ensuring its existence in designing any secure system.

2.1.1 Information Systems Vulnerability

Currently, Business environments continue to change with increasing dependence on information technology and pervasive use of the Internet. This greater connectivity has increased the vulnerability of information systems to various security threats. Several surveys have indicated that the challenges associated with information security are far from resolved (Rhee, et al., 2012). Information security vulnerability is a big threat to organizations information especially to the sensitive information. If sensitive information is vulnerable and exposed to the external parties it could create destruction by affecting the competitive advantage of the business in the organization in addition to losing customers trust which is also directly related with the organizations existence in the market.

Vulnerability is a weakness which allows an attacker to reduce a system's information assurance and to exploit vulnerability (Lokhande and Meshram, 2013). As Feng et al. (2014), security vulnerability could propagate and escalate through the causal chains of security risk factors via multiple paths, leading to different security risks in information systems. Existing approaches largely focuses on risk probability and severity without considering vulnerability propagation. Given the increased dependence of businesses on computer-based systems and networks, vulnerabilities of systems are growing (Choobineh et al., 2007). Considering the level of Security vulnerability in the organization and mitigating in time will minimize the security risk. It will also minimize the cost that the organization spends in managing risks if the mitigation is done at the earliest or before it creates any damage in the organization information asset.

Security vulnerabilities and breaches remain a major concern for firms as they cost billions of dollars in downtime, maintenance and disruptions. Although researchers in the fields of security and vulnerability prediction have made significant contributions, the number of vulnerabilities continues to increase (Roumania, et al., 2016).

With respect to vulnerability, research finding also suggest that organizations need to stress that they could be subject to information security threats if employees do not take IS security seriously and comply with policies (Vance et al., 2012). Hence, information security training related to security vulnerability should be given to employee to address problems that could occur due to negligence.

2.1.2 Information Security Threats

The problem of information security is considered as an afterthought dates back to the era of checklists. Once a system has been implemented, it was a norm to follow a checklist to address whether any of the security 'holes' remained unplugged. While the information security community has recognized the inadequacy of checklists as a means to address security concerns, the checklist culture has, however, prevailed. Therein resides the problem of information security being considered as an afterthought. The lack of recognition of the importance of accounting for security during system and product development has resulted in little or no budget allocation for security. The result is that, if there is any security, it tends to be "bolted-in" rather than "baked-in (Choobineh et al., 2007). For any product development, system implementation, or upgrade incorporating information security is unquestionable and sufficient budget should be allocated to address security issues at an acceptable level.

As it is stated by Chang and Lin (2007), most information security problems are caused by the negligence of people, rather by attack events. Therefore, it is important to train and manage the problem-prone people. An acceptable level of information security can only be introduced and maintained if the correct set of security controls is identified, implemented and maintained. Identifying a reasonably effective set of security controls can be a very complicated and resource-intensive process, which requires special resources and expertise most companies do not possess. Therefore, well organized and regular information security awareness training in the organization plays a vital role in evading problems that could occur due to negligence.

Another problem is the measures used to secure information on a computer, as opposed to most other areas of security, are largely hidden from the user and have been made to achieve their

function without visible signs of activity and are not visually checkable. With computer systems, the firewall, the IDS and many of the access control devices work without direct interaction with the user as system designers have 'improved' the interface to reduce the level of inconvenience that the legitimate user has overcome in order to carry out their role (Jones, 2009**).** And to address this problem, there has to be unremitting follow up of the functionality of these security tools using monitoring tools. Thus we can be sure as the existing security devise are active enough to protect the asset at the organization premises.

In addition to these, one of the most commonly overlooked and poorly managed security domains is that of appropriate security controls over physical information processing infrastructure. The organization's information security policies should encompass physical and environmental security to ensure that all sensitive assets and processing facilities are secured, and protected by defined security controls linked to business risk (Khan, 2010). Since information security policy gives a direction for the information security within an organization. And if the information security comprises the organization's business objectives and there is the management's willingness supporting the implementation of the policy, it will be much more effortless to operate the organization business in a controlled and secure manner. So that all the security controls will be in effect to protect the organization's information at an acceptable level.

The increasing sophistication of information security threats and the ever-growing body of regulation has made information security a critical function within many sectors of business (Hyeun-Suk, et al., 2009**).** If this critical information of an organization is compromised, the organization can suffer serious consequences, that is, in the form of loss of income, loss of customers' trust and maybe legal action etc. (Khan, et al., 2011).

There are many threats to the integrity, confidentiality, and availability of information maintained by organizational systems (Workman, et al., 2008). And there are many countermeasures to address these security threats. These countermeasures include firewall, antivirus, encryption, and intrusion detection systems (IDS), security patches, and password change control systems. An antivirus product may be combined with a comprehensive management solution, including automatic update and early warning services. An IDS monitors

events occurring in a computer system or network and uses anomaly detection or misuse detection to analyze them for suspect. These security technologies are constantly evolving to respond to the ever-changing nature of the threats and the novel methods adopted by the threat agents (Kumar, et al., 2008).

Currently, Information technology has dramatically increased online business opportunities; however these opportunities have also created serious risks in relation to information security (Soomro, et al., 2016). According to (Ren-Wei, et al., 2003), there are four specific threats, which, if they occur, will weaken trust or completeness of operational functions, products or services or disturb operational sustainability.

Threat	Explanation
Unauthorized changes to, leaking or corruption of information	This threat is made up of intentional or non-intentional release of information and intentional additions, changes or corruptions to information by the staff accessing or not accessing information processes in its normal dispensation of duties.
Changes to, or corruption of information due to carelessness	This threat is made up of loss, addition, change or corruption of information due to carelessness, oversight or unintentional action. The possibility of this threat occurring arises out of human action or non-action, hardware, software or communication failure and natural disasters.
Non-delivery or improper delivery of information	This threat is made up of information being unintentionally deleted or improperly delivered due to paper or digital formats. This includes hardware, software and communication failure and natural disasters.
Denial of service or retrogression	This threat is made up of insufficient usability as a result of unplanned short-term or long-term retrogression occurring in the overall workflow or in part of the workflow.

Table 2-1: Information security threat; adapted from Ren-Wei et al., (2013)

Therefore, with the increasing diversity of threats, in addition to the solution on engineering side, an establishment of complete education training, the verification and validation of Penetration test, the security evaluation of certification and accreditation are all required (Farn, et al., 2004).

2.1.3 Common Information Security Attacks

As noted by Singh et al., (2005), the following are some of the information security attacks. **Attacks Threatening Confidentiality:** Two types of attacks threaten the confidentiality of information which is snooping and traffic analysis. Snooping refers to unauthorized access to or interception of data whereas traffic analysis refers other types of information collected by an intruder by monitoring online traffic.

Attacks Threatening Integrity: The integrity of data can be threatened by several kinds of attacks which include modification, masquerading, replaying and repudiation.

Attacks Threatening Availability: Availability is mostly threatened by Denial of service (DOS) attacks which may slow down or totally interrupt the service of a system. The attacker can use several strategies to achieve this. They might make the system so busy that it collapses, or they might intercept messages sent in one direction and make the sending system believe that one of the parties involved in the communication or message has lost the message and that it should be resent.

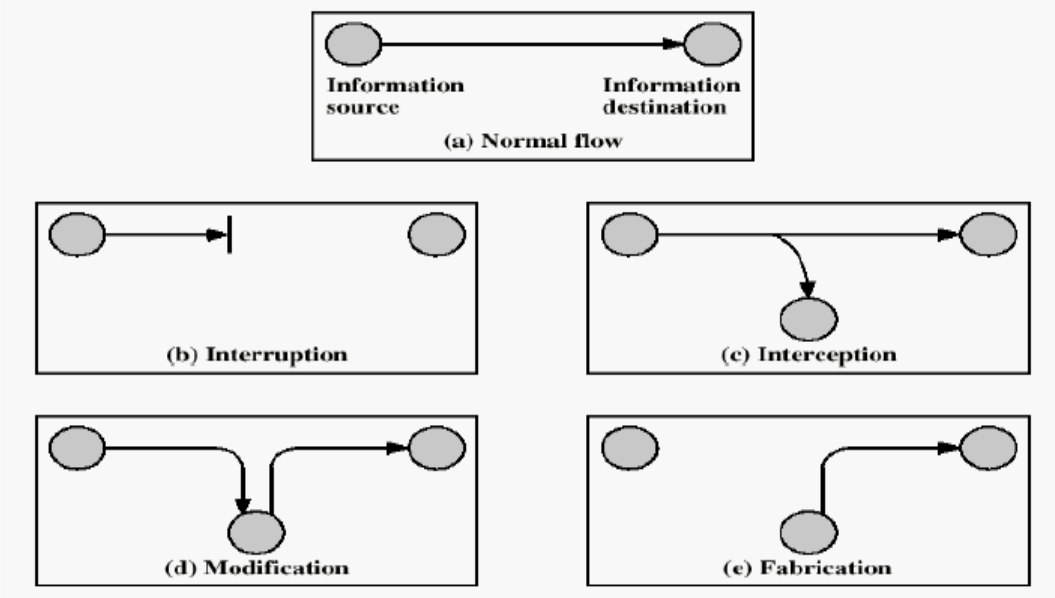

Figure 2-2: Type of information security attacks; adapted from Singh et al., (2005)

Interruption: This is an attack on availability disrupting traffic physically breaking communication line.

Interception: This is an attack on confidentiality Overhearing, eavesdropping over a communication line

Modification: This is an attack on integrity corrupting transmitted data or tampering with it before it reaches its destination

Fabrication: This is an attack on authenticity Faking data as if it were created by a legitimate and authentic party (Singh et al., 2004). These are the common information security attacks that affect the confidentiality, integrity and availability. Organization has to be aware of these attacks and take the appropriate measures to protect the valuable information assets at their premises.

2.1.4 Information Security risk Assessment and management

Exposure to security risks can lead to adverse consequences for organizations, such as leakage of sensitive information and interruption or destruction of critical IT services and inadequate risk assessment, or the absence of one, implies that the organization has not used its resources to best

advantage in addressing security risk exposure. Inadequate risk assessment, or the absence of one, implies that the organization has not used its resources to best advantage in addressing security risk exposure (Zhi et al., 2013).

As Feng et al (2014) stated, after the risk assessment, risk has to be analyzed for management accordingly. Security risk analysis mainly focuses on analyzing vulnerabilities and threats to the information resources and deciding what countermeasures to take for reducing risk to an acceptable level. However, security risk analysis for information systems is a very challenging task due to the complex and dynamic environment

Once the process of risk analysis is complete, risk management should follow which is planning, monitoring and controlling activities based on information produced by risk analysis activity' It involving the identification and implementation of security controls to reduce risks to an acceptable level as indicated by the assessed measure of risk. Risk reduction can be achieved by avoiding risk, transferring risk, reducing the likelihood of threats, reducing the vulnerabilities, reducing the possible impacts, detecting unwanted events early, reacting and recovering depending on the specific business environment and circumstances in which the organization conducts its business (Gerber and von Solms, 2005).

The risk management process provides the compliance between the business objectives or missions and the necessity of the organization asset protection cost effectively. The risk analysis is the process of identification of factors, which have the influence over the information security. The risk assessment focus to the four main outcomes: determine the threats to the organization mission, prioritization of these threats in accordance with the risk levels, define controls and protection measures and the development of action plan for these measures implementation (Pavlov and Karakaneva, 2011).

Figure 2-3: Risk management process; adapted from Humphreys (2008)

If a security incident has been recognized, a security management process requires methods to ensure that known security vulnerabilities are closed and open security issues are resolved. Generally, information security ensures business continuity, minimizes risk, and maximizes return on investments and business opportunities (Munir and Manarvi, 2010**).** To address these, risk assessments play a crucial role by identifying potential threats to the organization and provide a perfect opportunity to implement effective controls to protect critical processes and assets (Khan, 2010). That's the reason most scholars gives much consideration to risk management as one of the tools to protect organization asset while discussing information security.

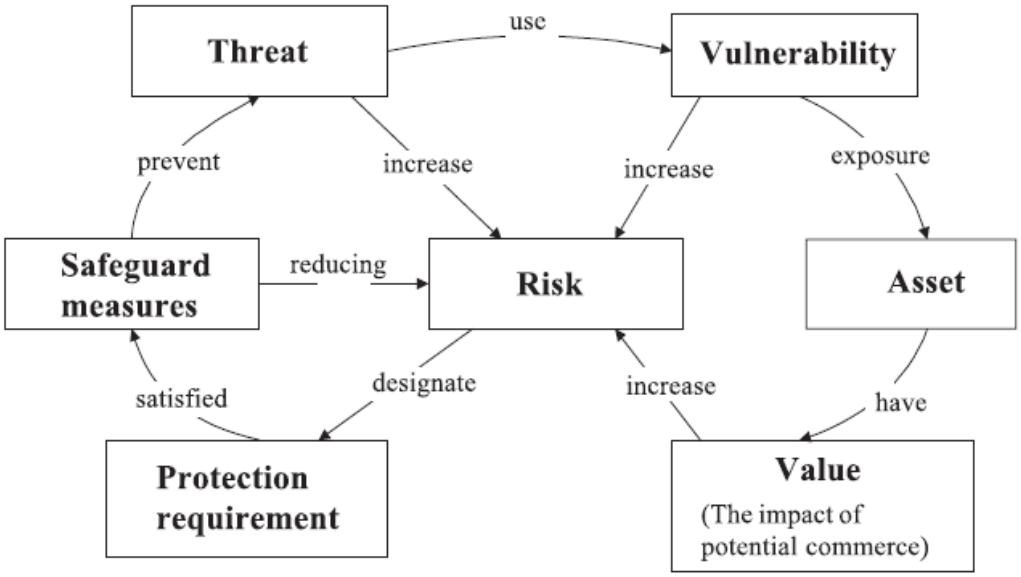

Figure 2-4: vulnerability, threat and risk association; adapted from Farn et al., (2004)

2.2 Information security management

Historically, management of information security has mostly relied on technical control measures; however, research has shown that the majority of information security failures occur because of violations of controls by trusted personnel. This suggests that management of information security can only be adequately assured if the emphasis goes beyond technical controls and incorporates business process and organizational issues (Choobineh et al., 2007). As most studies implies, incorporating information security management with business and organization issue in addition to technical control is unquestionable. Since, nowadays business is leading the technology and for that the organization business objective has to be understood and managed properly from the security aspect.

It is clear that Information Security arena has expanded over recent years growing from a technical initiative and labeled IT Security towards a broader and more business focused concern, for the protection of information in all its forms across the organization. It is no longer simply the aim to protect confidentiality, integrity and availability of information but

Information Security aims to deliver real business benefits now by both protecting and yet facilitating the controlled sharing of information and managing the associated risks across a changing threat environment (Ashenden,2008).

As Park et al (2010) stated, information security management is important to both public and private sector businesses. In any industry, an information security management system is an enabler that supports e-business and is essential for risk management activities. The interconnection of public and private networks and the sharing of information assets increase the difficulty of controlling access to and handling of information. And this increase the exposure and vulnerability of originations information to the external parties which may direct to risks associated with security.

According to Posthumus and von Solms, (2004), the goal of information security management is to protect the confidentiality, integrity, and availability of information and to mitigate the various risks and threats to such information. We thus define ISM as a systematic process of effectively coping with information security threats and risks in an organization, through the application of a suitable range of physical, technical or operational security controls, to protect information assets and achieve business goals. ISM is primarily concerned with strategic, tactical, and operational issues of the planning, analysis, design, implementation, and maintenance of an organization's information security program (Choobineh et al., 2007).

Information security management consists of a series of processes by which formal, informal and technical controls are applied to address security risks (Sveen, et al., 2009). Technical controls include firewalls, intrusion detection systems, and other such devices that regulate access to resources. Informal controls such as training and education influence security culture (Zhi et al., 2013). To manage information security at an acceptable level, both technical and informal controls should be put into effect.

If all these controls are not in effect, risks will not be adequately addressed. On top of the controls, information security management also plays the biggest role in protecting the valuable information since, without management it will be difficult to understand what has been done, why, by whom and for what purpose (Debi, 2008). As Chang and Lin (2007), solid security products or technology alone cannot protect an organization without a good management policy

and implementation. Thus, the key factors in successful information security management are the effective compliance of security policies and proper integration of people, process and technology (Eminagaoglu, et al., 2009). Since Effective information security reduces risks by protecting the organizations against threats and vulnerabilities and the impacts to their resources (Desisa and Beshah, 2014).

In general, implementing and configuring the security tools by itself is not a solution to protect organization information unless it is properly managed. Policies and procedures should also incorporate information security in regard to people, process and technology.

Information security measures reduce the risk of unwanted incidents. Failures of information security are clearly adverse events which cause losses to businesses; information security is thus a risk management discipline that manages the cost of information risk to the business (Blakely et al., 2001). In this view, effectiveness is understood as the ability of a measure to reduce risk to an acceptable level and making sure the existing security control mechanisms are in effect (Peláez, 2010). To address these, organization should implement the necessary security controls and measurers following the information security policy and procedures of the organization and minimize the risk exposure attain to effective information security management.

One of the key success factors in analyzing and measuring the effectiveness of information security is to ensure that the organization has a thorough understanding of the assets which are most valuable to them, and those assets have been allocated an appropriate level of classification based on roles and responsibility, sensitivity and criticality of the asset relative to prioritized risk (Khan, 2010). If all the valuable assets are not included in the scope for security management and the risk assessment wouldn't fully cover the assets, there will not be effective information security management in the organization.

In the case of the effectiveness with reference to ISM, some questions arise. These questions are aimed at securing the recognized risks and therefore also at counter designed to detect threats or minimize damage due to attacks measurements (Boehmer, 2008). These countermeasures include antivirus software, firewalls, intrusion detection or prevention, and encryption (Kumar et al., 2008).

Effective information security also highlight the development, communication, and publication of endorsed information security policies; and ensure a comprehensive understanding of the current-state security, while driving towards a realistic and business based target-state (Khan, 2010). Thus, in addition to the technical measures, policies and procedures that direct the security management should be properly followed and the required security awareness should be created among the employees in the organization.

Effectiveness of information security measures is also understood as the ability of a measure to give a positive return of investment, the ability of a measure to assist the organization to meet legal requirements, the individual and organizational awareness and behavior in a positive direction and the ability of a measure to reduce risk to an acceptable level. These four perspectives are clearly interrelated, although they describe different expectations of the performance of the information security measures. How legal and regulatory requirements are met will for instance depend more on people and procedures than on technical security measures. What is needed is the right combination of measures that reduce the business risks to an acceptable level by ensuring compliance (Hagen, et al., 2008).

2.2 Information Security Management Roles

Information technology has dramatically increased online business opportunities; however these opportunities have also created serious risks in relation to information security. Previously, information security issues were studied in a technological context, but growing security needs have extended researchers' attention to explore the management role in information security management (Soomro, et al., 2016). The management role in managing information security is imperative as they have much influence in approving the budgeting and direct the implementation of policies and procedures that manages information security related to the business objectives.

Management of information security is primarily concerned with strategic, tactical, and operational issues surrounding the planning, analysis, design, implementation, and maintenance of an organization's information security program (Choobineh, et al., 2007).

Some of the most salient issues include asset valuation, auditing, business continuity planning, disaster recovery planning, ethics, organizational communication, policy development, project planning, risk management, security awareness education/training, and various legal issues such as liability and regulatory compliance. Ideally, information security management activities should be driven by organizational objectives so that no resources are expended on security without an explicit documented understanding of how it supports the organizational mission (Choobineh, et al., 2007).

All the controls including logical, technical and administrative, which uses to manage information security in the organization, should be properly integrated to address the security issue related to the business objective of the organization. According to ISO/IEC 27000 (2016), information security is not always taken into account in the design and development of information systems. Further, information security is often thought of as being a technical solution. However, the information security that can be achieved through technical means is limited, and may be ineffective without being supported by appropriate management and procedures within the context of an ISM. Integrating security into a functionally complete information system could be difficult and costly. An ISM involves identifying which controls are in place and requires careful planning and attention to detail. As an example, access controls, which may be logical, physical, administrative or a combination, provide a means to ensure that access to information assets is authorized and restricted based on the business and information security requirements**.**

In consideration of the importance, many outstanding institutes such as published information security guidelines and standards for protecting the confidentiality, integrity and accessibility of information. If firms follow the guidelines and standards to set up their security policy, they could own a tighter and more complete IT environment. That is, firms could safeguard their business value and benefit from IT according to the well-developed information security management (Shi-Ming, et al., 2006).

And the board of directors and the top management have a direct responsibility to ensure that all information resources of the company are secure and such security has to be maintained by the due diligence from all units at all levels throughout the whole organization (Chang and Ho

2006). In general, organization needs to have duly designed and implemented management structures and practices to protect its information asset, which is very important to the organization and can serve as a powerful weapon to survive a highly competitive environment (Chang and Ho 2006).

In order to provide convincing arguments to management to initiate an information security program, Information Security Officers must also identify risks to organizational processes and develop a measurement system capable of determining the effectiveness of controls introduced in accordance with relevant standards business (Peláez, 2010). However the senior management plays the vital role to ensure the availability of resources related to the security management, information security team is also responsible in verifying the functionality of the implemented security tools based on the policy and procedure in a daily basis.

In general, management shall provide evidence of its commitment to the establishment, implementation, operation, monitoring, review, maintenance and improvement of information security management (ISO 27001, 2005).

2.2.1 Information security management Process

According to Humphreys (2008), it is very important for an organization to check how effective its information security management is in practice. In order to enable this to happen, the organization needs to establish a measurement process to measure and assess how effective the controls are at protecting their information assets.

Identifying the location of sensitive data, run a risk assessment exercise to identify vulnerabilities with underlying processes and technologies, and complete a gap analysis are part of the information security process and other security related processes are asset management, information classification and inventory of IT architecture which are necessary to PCI DSS requirements. Human resources security, physical and environmental security, communication and operations management, access control and incident management are additional processes that require adequate information security management process to avoid failure in responding to the security standard requirement (Ataya, 2010).

Recently, many companies are continuously investing in information security management as a means to improve the information security management process so as to protect the enterprise's information assets and strengthen their competitiveness since, considering the social responsibility of enterprises according to class action suits against accidents of personal information leakage, the issue of information security is accepted as a matter of survival for the enterprise (Park, et al., 2010). In the current competitive business environment, it's not only hackers and cyber criminals that hunt for information but organizations that make similar business also do these activates to understand the business strategy and business plan to disrupt the business and get advantage of it.

In general it is very important that an organization is able to check how effective its information security management is in practice. In order to enable this to happen, the organization needs to establish a measurement process to be able to measure and assess how effective the controls are at protecting their information assets (Humphreys, 2008).

The information security management process includes systematically established documentation and continuous procedure management to improve the safety and reliability of the assets of an organization, and for realizing information confidentiality, integrity and availability which are the goals of information security, and includes the continuous enhancement of information security (Rezakhani et al., 2011).

2.3 Information Security Management Certification

As it is explained by Park et al., (2010), there are four major motivations or benefits of enterprises attaining information security management certification. First, when an enterprise receives Information security management certification, there are positive public relations effects of better corporate image, followed by additional customers, resulting in sales increase. It showed that preventing intrusions would have cost saving effects as damage from potential accidents can be prevented. Second, attaining information security reliability affects an increase in transaction stability. While information security management certification directly affects an increase in corporate value, attaining the information security reliability affects transaction stability, thus helping the stability of the information assets of the enterprise. Third, attaining

information security reliability positively affects an increase in trust and fourth, increasing information security awareness positively affects an increase in security awareness. Having the certification provides motivation for all employees and thus affected strengthening employee capability and awareness of information security.

For all these motivations on the organizations business related to profit and customers trust, in addition to protecting organization information security by complying standards, security certifications importance in the current competition is indisputable.

For the certification process, security auditing on the organization information assets in the scope is mandatory. According to Rowlingson and Winsborrow (2006), the achievement of accredited certification requires an audit process to be conducted by external auditors. This audit process reflects the requirements of ISO 27001 and the European standard EA-7/038 which are designed to assess the adequacy of the processes employed by a company to manage its information security posture and to identify evidence of their regular use. In addition, the audit process is required to critically review the security risk assessment and risk management practices and decisions of the company. The certification process itself is of a continuous nature. Following the initial grant of a certificate there are regular surveillance audits on an annual basis, which must produce a satisfactory result in order for the company to maintain its certification status. In addition, every three years a company must undergo a complete reassessment of its information security arrangements in order for certification to be maintained.

2.4 Critical Success Factors of Information Security Management

As it is stated on (ISO 27001, 2005), Information technology code of practice points out six critical success factors of successful information security management. The factors are business alignment, organizational support, organizational awareness, IT competence, security control development, and performance evaluation.

2.4.1 Business Alignment

Information plays a major role in supporting an organization's business operations. During each business operation information comes into contact with technology, people and process elements, which have been said to form a part of each business operation. Every one of these elements has the potential to present a very real risk to an organization's business information assets. Thus, in order to ensure that business information continues to provide useful support to an organization's business operations, several key characteristics of this information need to be preserved (Posthumus and von Solms 2004). Business-aligned security management is based on business objectives, values, or needs, as opposed to being technology asset focused (Spears and Barki, 2010). Organizations business is leading the technology to provide the requested services that the business offers. For this, information security management should be aligned with the business rather than focusing only on the technology.

In the earlier time, organizations invest to a great extent on the IT infrastructure to support the business and were unwilling to expend on investing on information security infrastructure. As a result, different organization's businesses had been affected by security threat

Information security, which once was considered as just overhead costs, is now widely recognized as a strategic investment in business operations. The firm's enterprise risk management strategy should address all significant threats to the organization. An integrated approach is needed. IT security managers need to evaluate whether security investments are meeting organizational goals and objectives. They must take into account the business mission of the information systems. There is a need to set goals and develop performance measures for evaluating security processes and outcomes (Herath, et al., 2010).

As Kayworth and Whitten (2012) stated, it is important to integrate information security into mainstream aspects of the business in designing an effective ISM. One of the primary tasks security managers face is to determine the balance between enabling the business and securing information assets. Overprotection through strict controls may inhibit business responsiveness, while lax controls may create unacceptable risks for information assets. Thus, organizations should consider both and implement the security at least at an acceptable level.

2.4.2 Organizational Support

Organizational support comes from organizational factors which are related to the organization structure and managerial decisions around information security (Werlinger et al., 2009). If there is a defined information security structure in the organization from bottom up to the management level, it would be easier for managing risk and handling security incidence at the earliest.

Executive leaders can demonstrate commitment in a variety of ways, including funding, allocation of human and financial resources, promotion of buy-in, and stressing the importance of security to other groups within the company (Kayworth and Whitten, 2010). Hence management must actively support safety efforts at all these levels.

Management must also consider and allocate sufficient resources to carry out day-to-day activities to accomplish both short-term and long-term information safety goals. An effective safety program needs an appropriate level of resources committed by the organization. The resources required for effective ISM may include sufficient staff, time, money, information, methods used in safety works, facilities, tools, machines, etc (Aksorn and Hadikusumo, 2008). And there should be the management commitment to support all these to be integrated and implemented to support the organization information security.

2.4.3 Organization Awareness

Secure management of information systems is crucially important in information intensive organizations. Although most organizations have long been using security technologies, it is well known that technology tools alone are not sufficient. Thus, the area of end-user security behaviors in organizations has gained an increased attention (Herath and Rao, 2009). Information security awareness is about ensuring that all employees are aware of the policies and regulations concerning securing the organization information and it should be the primary part of the organizations' overall information security management plan.

According to AliMaqousi, et al., (2013), user information security awareness is a major component within industry good practice since security organizations should focus on making users intrinsic to the security process through education, training, and awareness. Due to an

inadequate level of user cooperation and a lack of knowledge, employees may misuse or misinterpret many security techniques and become the greatest threat to the organization's information security (Niekerk and Solms, 2010).

A successful safety program can be achieved if all employees are given periodic education and training in order to improve their knowledge and skills on safety at work (Aksorn and Hadikusumo, 2008). For this, Organization should sponsor security awareness, training, and education programs to increase the overall awareness of information security and to improve compliance-related behaviors (Kayworth and Whitten, 2012).

As Khan (2011), information security awareness is about guaranteeing all employees are aware of the rules and regulations regarding securing the information within organization. Information security awareness should therefore form an integral part of any organizations' overall information security management plan

Most organizations need information systems to survive and prosper and thus need to be serious about protecting their information assets. Many of the processes needed to protect these information assets are, to a large extent, dependent on human cooperated behavior. Employees, whether intentionally or through negligence, often due to a lack of knowledge, are the greatest threat to information security (Niekerk and Solms, 2010). Therefore, in addition to technological security solutions deployed; an organization has to have an information security awareness program for its users (Maqousi, et al., 2013).

2.4.4 IT Competence

IT competence enables a company to plan, organize, execute, and invest on information security effectively (Chang and Ho 2006). To this end, financial sectors awareness of customer's need for new services is increased and makes them to avail the services that satisfy the need using new technology. This makes the use of IT to increase the level of competition.

Businesses succeed or fail on the basis of competitive advantage or the lack of it. The open nature of security protocols, the popularization of security capabilities, and the extent of

commercialization within the security industry all have serious implications for whether businesses can use security technologies to create competitive advantage. If security technologies cannot provide competitive advantage, should they be perceived simply as a necessity? After all, no business wants to be insecure (Stewart, 2005).

2.4.5 Security Controls Development

The National Institute of Standards and Technology classifies information security controls into three categories which are; technical, operational, and management controls (Baker and Wallace, 2007).

(1) Technical controls, which traditionally include products and processes (such as firewalls, antivirus software, intrusion detection, and encryption techniques), focusing mainly on protecting an organization's ICTs and the information flowing across and stored in them;

(2) Operational controls, which include enforcement mechanisms and methods for correcting operational deficiencies (such as physical access controls, backup capabilities, and protection from environmental hazards); and (3) Management controls, which target information security's nontechnical areas, such as usage policies and business continuity planning.

Hence, while developing a security controls in the organization, organizations should consider all the three security aspects and make the information assets protected at the maximum level. By doing this, organization can protect their business from external disclosure and get customers trust. As Chang and Ho (2016), security controls development can be a very complicated and resource-intensive process which requires special resources and expertise. Therefore, proper consideration and follow up is required on the security tool which will be deployed to address the security issues.

2.4.6 Performance Evaluation

If organization implemented information security at an acceptable level to protect the business and information assets, the performance will be increased by getting more customers who will be willing to make business with the organization.

Information security management practice influences organizations upon their performance in various areas such as competition edge, customer satisfaction, corporate image, credibility, trust, and reputation (Herath et al., 2010). According to NIST (2008), the requirement to measure information security performance is driven by regulatory, financial and organizational reasons. Agencies can use performance measures as management tools in their internal improvement as it is the means for tying the implementation, efficiency, and effectiveness of security controls to the organization success and help to demonstrate the value of information security to their organization.

2.5 Information Security Risk in the Financial Sector

Technology enables the banking services to address the customers' problem by meeting the expectations and provides advanced electronic and online banking solutions. However, while the use of technology to support the business increased and gets advanced, the risk related to the business is also increasing and makes the banks exposed to external parties.

According to Abu-Shanab and Matalqa (2015), e-banking revolution changed the business of banking fundamentally by providing many benefits for customers and new business opportunities for banks but it imposes banking risks and many challenges especially in terms of security issues. To address this problem, security aspects should be taken in consideration at all levels of financial organizations, to protect themselves against various types of fraud and attacks. It is comprehensible that the information in the sectors is one of the most sensitive assets than any other organizations. Customers relies their trust on this sector to transact their accounts online and use e-banking services and desire the utmost confidentially of their accounts.

Customers anticipate the financial sectors to make its financial information confidential to build more trust and expand the business. Otherwise, if banks loss customers trust at any level, the business will be affected and its existence in such competitive environment will be in question. To address this issue, the financial sector should focus much more on the confidentiality of its customer by protecting their data using information security management.

As it is known, the banking industry provides a business using new communication media to offer its customers value added service and convenience (Omariba, et al., 2012). The services

include automated teller machines (ATMs), credit cards, debit cards, smart cards, electronic fund transfer (EFT) systems, mobile banking, etc. On the transaction level, e-banking include account access, balance transfer, bill payment, bill presentment, customer service and administration etc.

From the banking sectors point of view, the use of internet has significantly reduced the physical costs of banking operations, including the costs of information processing and transmission (Abu-Shanab and Matalqa, 2015) however, the security related risks cause financial sectors to lose the gains of internet banking if problems are not properly addressed. One of the risks is identity theft, which can occur by using an unconventional attack like: phishing, pharming, spoofing, key logging, screen logging, Trojans horses, other malicious codes or transaction poisoning (Vrîncianu and Popa, 2010; Singh Brar et al., 2012). Moreover there are many potential problems associated with this industry due to imperfection of the security methods (Omariba et al., 2012) including cybercrime which is prevalent in the financial institutions, with hacking, identity theft and malicious software (Mugari, et al., 2016).

The main benefits that financial sectors provide using e-banking is customer satisfaction in addition to the profit that they gain by providing this service. Since customers can access their accounts whenever, from anywhere, and this creates more relationships between customers and banks while the risk of using e-banking is still in exist. Customer confidence is vital for the financial sector since determined security concerns increase confidence and makes the relationship between the banking sectors and their customers well-built.

According to Raghavan and Parthiban (2014), there are a number of frauds or cybercrimes witnessed in the electronic payment processors and the banking sector, like ATM frauds, Cyber Money Laundering and Credit Card Frauds. In general all the frauds are executed with the ultimate goal of gaining access to users account, steal funds and transfer it to some other bank account. In some cases the cyber criminals uses the banking credentials like PIN, password, certificates, etc. to access accounts and steal meager amount of money; whereas in other cases they may want to steal all the money and transfer the funds into mule accounts.

On top of this, a significant number of breaches in the security of electronic banking (e-Banking) system reported each year, drawing attention to the need to protect and inform customers about the risk of exposure to malicious actions initiated by cyber-criminals. Financial institutions and

consumers recognize the fact that attacks and financial frauds are becoming more complex and are perpetrated by a different class of criminal (Vrîncianu and Popa, 2010). Billions of financial data transactions occur online every day and bank cybercrimes take place every day when bank information is compromised by skilled criminal hackers by manipulating a financial institution's online information system. These causes huge financial loses to the banks and customers (Jassal and Sehgal, 2013).

As Alber and Nabil (2015) noted, the threats and security breaches is highly increase in recent years. Some banks have already faced some security threats represented in Trojan virus, Spam, Spyware/malware, Hacking and stealing information etc. Therefore, the financial industry as a whole should be aware enough to accommodate the issue of information security in its own strategic policies.

2.6 Information security management in the financial sector

Banks' ability to take advantage of new opportunities often depends on its ability to provide open, accessible, available, and secure network connectivity and services. Having a reputation for safeguarding information and the environment within which it resides enhances an organization's ability to preserve and increase market share (Ula, et al., 2011). To attain this, management must allocate sufficient resources to carry out day-to-day activities to accomplish both short-term and long-term information safety goals. An effective information security management program needs an appropriate level of resource commitment including sufficient staff, time, money, information, methods used in safety works, facilities, tools, machines etc (Aksorn and Hadikusumo,2008).

Information security management is an ever changing issue. The need for better services and functionality must constantly be supplemented with stronger security measures to counteract the risks. Moreover, these security measures must be highly swift and must be quickly deployed evolve customers trust. To that end, the financial sector should work very hard towards addressing this issue and the top management should play the biggest role to fulfill these needs.

As Smith and Jamieson (2006) explained, the active support of top management was ranked the most important issue and rated number one in priority survey. While top management is

ultimately accountable and charged with the task of initiating and supporting important projects with adequate funding and resources, they can also support information security as an important enterprise-wide function in many ways, including funding, allocation of human and financial resources, promotion of buy-in, and stressing the importance of security to other groups within the organization (Kayworth and Whitten, 2010).

Jassal and Sehgal (2013) also points out that, the unique aspect about information security in banking industry are that the security posture of a bank does not depend solely on the safeguards and practices implemented by the bank; it is equally dependent on the awareness of the users. This makes the task for protecting information confidentiality and integrity a greater challenge for the financial sectors. Financial institutions have made, and should continue to make, efforts to educate their customers. Thus, management should implement a customer awareness program and periodically evaluate its effectiveness.

2.7 Information Security Management Standards and best practice

Identifying a reasonably effective set of security controls can be a very complicated and resource-intensive process, which requires special resources and expertise most companies do not possess. Therefore, there exists an urgent demand for ISM standards, which offer guidelines to organizations by identifying and introducing a set of controls conducive to an acceptable level of information resource protection (Chang and Ho 2006). Information security has a vital role in supporting the activities of the organization by protecting its assets from external exposure. And to make sure that if the implementation of information security in the organization is at an acceptable level, there should be a standard or benchmark which regulates governance over information security.

Several private and government organizations developed standards bodies whose function is to setup benchmarks, standards and in some cases, legal regulations on information security to ensure that an adequate level of security is preserved, to ensure resources used in the right way, and to ensure the best security practices adopted in an organization. For this, the five big standards are the most widely used standards for information security such as ISO27001 (International Standard Organization), BS 7799 (British Standard), PCI-DSS (Payment Card

Industry Data Security Standard), ITIL (Information Technology Infrastructure Library) and COBIT (Control Objectives for Information and Related Technology) (Susanto et al., 2011).

According to Susanto (2011), each standard playing its own role and position in implementing ISMS, several standards such as ISO 27001 and BS 7799 focusing on information security management system as main domain and their focus on, while PCI-DSS focus on information security relating to business transactions and smart card, then ITIL and COBIT focuses on information security and its relation with the Project management and IT Governance.

Organizations which have published information security standards and gained great acceptance includes International Standardization Organization (ISO), Information Systems Audit and Control Association (ISACA), Information Systems Security Association (ISSA), National Institute of Standards and Technology (NIST), British Standards Institution (BSI), Information Security Forum (ISF), Payment Card Industry Security Standards Council and others.
Several security standards are continuously published and gain acceptance; some of them provide guidelines, others promote best practices, while a few can be used as a basis for certification (Tsohoul, et al., 2010). Therefore, by adopting industry best practices (e.g. CobiT, ISO 27000, PCI-DSS) and adjusting IT infrastructure with high-level executive objectives, companies can lower IT risks, especially security and operational risks (Spremic, 2011).

		ISO 27001	BS 7799	PCIDSS V2.0	ITIL V4.0	COBIT V4.1
1.	*Information Security Policy*	√	√	√	√	√
2.	*Communications and Operations Management*	√	√	√	●	√
3.	*Access Control*	√	√	√	√	√
4.	*Information Systems Acquisition, Development and Maintenance*	√	√	√	●	√
5.	*Organization of Information Security*	√	√	√	√	√
6.	*Asset Management*	√	√	√	√	√
7.	*Information Security Incident Management*	√	●	√	√	√
8.	*Business Continuity Management*	√	√	√	√	√
9.	*Human Resources Security*	√	√	√	●	√
10.	*Physical and Environmental Security*	√	√	√	●	√
11.	*Compliance*	√	√	√	√	√

Table 2-2: The big five standards adapted; from Sustano et al., (2011)

As shown in table 2-2, the big five standards are ISO, PCI-DSS and COBIT, ITIL, and BS.

ISO is a non-governmental organization that forms a bridge between the public and private sectors. On the one hand, many of its member institutes are part of the governmental structure of their countries, or are mandated by their government; also other members have their roots uniquely in the private sector, having been set up by national partnerships of industry associations whereas BS (British standard) Standards is the UK's National Standards Body (NSB) and was the world's first. BS Standards works with manufacturing and service industries,

businesses, governments and consumers to facilitate the production of British, European and international standards.

The other standard, ITIL, is the abbreviation for the guideline IT Infrastructure Library, developed by CCTA, now the OGC (Office of Governance Commerce) in Norwich (England) developed on behalf of the British government. The main focus of the development was on mutual best practices for all British government data centers to ensure comparable services.

COBIT is an IT governance framework and supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks. COBIT enables clear policy development and good practice for IT control throughout organizations. COBIT emphasizes regulatory compliance, helps organizations to increase the value attained from IT.

Among all these standards, PCI-DSS is a worldwide information security standard defined by the Payment Card Industry Security Standards Council. The standard was created to help industry organizations that process the financial sectors electronic card payments to prevent credit card fraud through increased controls of data and its exposure to compromise.

2.8 Information Security Governance

In terms of information security, due diligence should be undertaken to ensure risks are known and managed when it comes to dealing with company assets and their protection. This involves appropriate diligence in identifying and assessing the business and information security risks, as well as implementing an effective system of controls, and that regular monitoring and reviews are undertaken in order to ensure the controls remain effective. In other words there should be an information security governance process in place in particular to protect the organization's information assets (Humphreys, 2008).

The main objective of Information Security Governance is to set up an Information Security Committee which senior management or representatives of board of directors are required. This

can help to align the IS strategy with corporate strategy so that the effective Information Security policies as well as its enforcement can be adopted (Daniel, 2013). Information security governance is the set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring objectives are achieved, ascertaining risks are managed appropriately and verifying that the enterprise's resources are used responsibly (ula et al., 2011). To manage the deployment, controlling and monitoring of the security tools and aligning with the business strategy of the organizations, top management involvement is very compulsory and to that end, information security governance is mandatory in information security management in the organization.

Information security governance is a complex issue requiring the commitment of everyone in an organization to do their bit in order to protect their company's valuable business information assets (Posthumus, and von Solms, 2004). Thus, the collaboration of the top management with the lower line security experts is important in addressing the security issue in time. Furthermore, good IT Governance today demand that risks should be lowered and properly managed, and an essential part of such risks mediation is enforcing compliance. Within Information Security Governance, the role and activity of compliance measurement and enforcement had become a very important component of IT risk management in the company (Basie and Solms, 2005).

In general, as Van solms (2006) stated, information Security Governance is an integral part of Corporate Governance, and it consists of: The management and leadership commitment of the board and top management towards good information security, the proper organizational structures for enforcing good information security, full user awareness and commitment towards good information security and finally the necessary policies, procedures, processes, technologies and compliance enforcement mechanisms all working together to ensure that the confidentiality, integrity and availability (CIA) of the company's electronic assets (data, information, software, hardware, people etc). And there is a need to explore information security governance in order to demonstrate the role of the boards and the management in terms of protecting these vital business information assets (posthumus and solms, 2005).

2.9 Information Security Compliance

Organizations should be compliant with one of the internationally recognized security standard to make their business expand at an international level on top of protecting their information from being exposed to external parties and which will cause security risk.

Currently compliance has become a critical concern for many industries around the globe and accordingly investment to achieve compliance has increased drastically in recent years. While Information Systems are considered a part of the support architecture, anecdotal evidence suggests that organizations struggle with finding the right tools and guidance on approaches for compliance management (Abdullah, et al., 2009). Compliance in information security requires a team effort that reaches from the highest levels of hierarchy usually the CEO or board to the lowest level employees of workforce who are using the end results of the compliant components (Liberti, 2008). The compliance process starts form selecting a standard that fits to the organization business, floating a bid, assessing the gap, mitigating the gap and delivering mitigation report. In addition to quarterly and semi-annual compliance activates. For all these, the collaboration of the top management with lower level employee is fundamental.

Organizations usually go through an audit process in order to be complaint and get certified with a regulation (Kharbili et al., 2008). Security audits had the strongest effect among security resources and capabilities. Compliance with data protection regulations required organizations to do more to find, disclose and fix breach-related problems (Kwon and Johnson 2012). And the security auditors must have the necessary expertise and know-how to lead compliance checking projects on a certain system or a whole organization, with regard to a regulation (Kharbili et al., 2008).

According to Aristeidis and Ioannis (2009), the audit process towards information security requirements includes risk analysis methodologies and assessment of system policies, network applications and of course constant evaluation towards human involvement. In addition, security practices compatibility is a non-stop effort of monitoring, reviewing and modifying security controls in order to optimize information security infrastructure, management and effectiveness

of existing security policies and procedures. As a result, the certification approval will certify that the management and performance of selected security practices is professionally followed and maintained throughout the entire business operations.

There are two aspects of information security compliance from the PCI-DSS (Payment Card Industry Data Security Standard) perspective, an audit and quarterly scanning (Rowlingson and Winsborrow, 2006). In this regard, an independent security assessor is required to use the PCI audit template to show that each element of the twelve major requirements of PCI-DSS has been assessed. The assessment will be undertaken through a combination of interviews and document reviews such as the data retention policy, key management processes and procedures, risk assessment and incident response plan. Configuration checks may also be made, and evidence of procedures being followed will be sought. In reviewing a company's arrangements the assessor is required to examine contractual arrangements with third party companies that provide outsourced services. A current network diagram will also be required to show the existence of connections, including wireless connections, to cardholder data, and to show where firewalls have been placed for protection (Rowlingson and Winsborrow, 2006).

The security compliance process should also be able to review technical, psychical and administrative security practices and explicitly define how security policies and procedures are to be implemented and integrated with the current security and business activities and also how well business departments' work together to ensure that information security practices are harmonized and consistent (Elephant, 2008).

The first major step of a PCI-DSS compliance effort is to accurately determine the scope of the environment. The scoping process includes identifying all system components that are located within or connected to the cardholder data environment. The cardholder data environment is comprised of people, processes, and technology that handle cardholder data or sensitive authentication data. System components include network devices (both wired and wireless), servers and applications. Virtualization components, such as virtual machines, virtual switches/routers, virtual appliances, virtual applications/desktops, and hypervisors, are also considered system components within PCI-DSS. Scoping must occur at least annually and prior

to the annual assessment. Merchants and other entities must identify all locations and flows of cardholder data to ensure all applicable system components are included in scope for PCI-DSS (PCI-DSS Reference Guide, 2010).

As Tutton (2010) stated, knowing the location of the data is the first step in this process. An organization must know where their sensitive data is in order to protect it. Identifying the location of the data, when at rest and in motion, is critical to all other remediation efforts. Completing this properly and thoroughly will enable to complete proper segmentation, data encryption and other key security controls. Without completing this process effectively, it is most likely going to waste time, money and resources. It is important to know that this process is never officially complete. Data discovery is ongoing, with new applications and systems being deployed, and changes always occurring in the environment. Once the scope of security compliance program is identified, the next step in a compliance approval procedure is the selection of the appropriate security method to ensure that the security standards are fully implemented in the context of the security compliance program of the organization (Jose, 2005).

After the organization gets compliant, it is also expected to keep the compliance status. To this end, organizations have to periodically provide an assurance that they adjusted to meet new requirements induced by emerging threats as well as by changes to their operating environment. With the right choice of management practices, organization, and tools, enterprises can defensibly demonstrate their adherence to a broad spectrum of corporate standards and regulations, including PCI compliance. By increasing the maturity level of information security management, organizations achieve continuous compliance (Ataya, 2010). Failure to comply with the standards and to implement appropriate security controls may result in fines and/or other penalties. The problems faced by non-compliant firms will vary from damages that could at best be a loss of revenue to the worst cases where they would cease trading. Those damages include financial penalties, revocation of card scheme membership, negative publicity, loss of consumer and supplier confidence, reduction in sales revenue (Ataya, 2010).

However, by adopting information security compliance and remain complaint, business institutions are expected to successfully manage the growing number of ongoing security risks (Aristeidis and Ioannis, 2009).

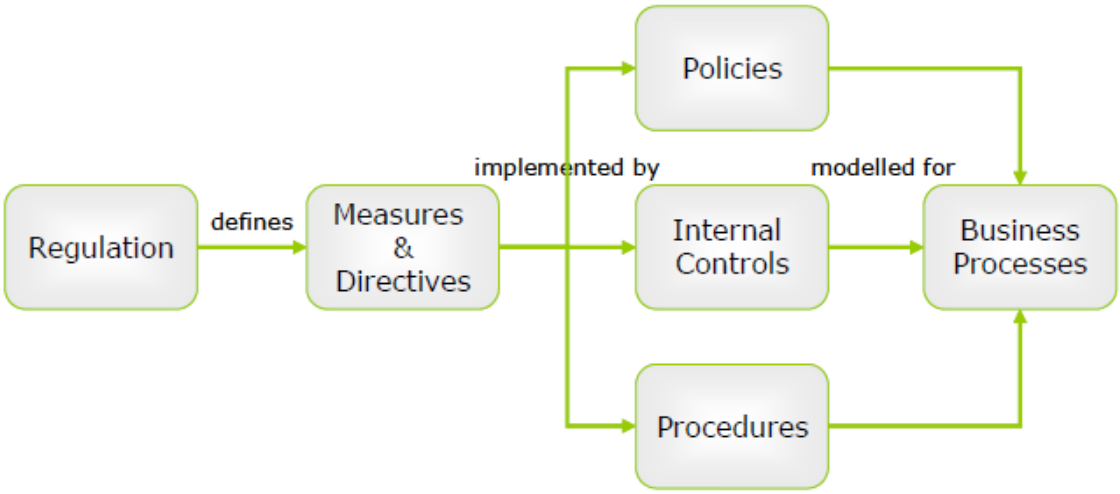

Figure 2-5: Compliance process for business; adapted from Kharbili et al., (2008)

Compliance in information security also requires a team effort that reaches from the highest levels of hierarchy (usually the CEO or Board) to the lowest level (employees) of workforce who is using the end results of the compliant components. The decision to adjust to a security framework depends heavily on the organizational management and transparency of operations. In order to reduce compliance costs while strengthening security, organizations should automate much of the security activity while keeping continuous human monitoring (Liberti, 2008).

2.10 Payment Card Industry Data Security Standard (PCI-DSS)

Usage of payment cards such as credit cards, debit cards, and prepaid cards, continues to grow. Security breaches related to payment cards have led to billion dollar losses annually (Jing Liu, 2010) and to offset these, the PCI-DSS which is the very first industry-wide standard that aims at

achieving a strong protection of sensitive consumer and cardholder data, and prevents major security issues is founded by the collaborative effort of the major payment card networks and issuers including The standard sets forceful requirements in many aspects, including secure networks, cardholder data protection, access control, vulnerability management, security assessments, and reporting (Liu et al., 2010). Unlike the other major security standard like ISO, PCI-DSS more focuses on protecting cardholder information of financial organizations including card service issuer and acquirer.

If financial institutions get complaint with PCI-DSS, they can provide the major international card payment services locally. According to Ataya (2010), one of the major advantage of the this standard is, Issuers and Acquirers of Payment cards are no longer required to follow up to four separate programs (Visa, MasterCard, American Express and Discover) that were applied differently in each region or country of operation for each credit card if the merchant or service provider has passed the PCI-DSS and standard requirements.

A hierarchy of risk-based policies, standards and operating procedures, as imposed by PCI-DSS requirement, lay down key information security directives and mandates for the entire organization to promote a risk aware culture (Ataya, 2010). To that end, PCI-DSS has twelve major requirements divided into six categories as shown in figure 2-2. Each requirement has sub-requirements and some have sub-sub-requirements (Morse and Raval, 2008).

Goals	PCI DSS Requirements
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

Table 2-3: PCI-DSS twelve requirements; adapted from PCI-DSS Reference Guide (2010)

Among these twelve requirement, the mandated security measures range from installing and maintaining firewalls, and the proper use of anti-virus software, to establish incident response plans, vulnerability assessments, along with effective patching and intrusion detection (Rowlingson and Winsborrow, 2006).

As Rowlingson and Winsborrow (2008) stated, the PCI requirements apply to all system components, defined as any network component, server or application included in, or connected to the cardholder data environment. Network components include firewalls, switches, routers, wireless access points, and other security appliances. Servers include those for database, Web, email and authentication. Applications include all off-the shelf and custom applications including intranet and Web applications

Despite this, one of the primary issues is that the original scope of PCI-DSS and what it covers within the organization is being misunderstood, and thus the projects that are implementing PCI-DSS are not fulfilling the requirements they were originally designed to meet. QSAs (Qualified

Security Assessors) who are assisting and acting as advisors for organizations seeking PCI-DSS compliance are finding that there are serious errors being made during the initial phases of the very projects that are meant to get the organizations fully compliant. This tends to lead to a lot of confusion and frustration. In some cases, organizations have to completely restart the project from scratch, wasting a significant amount of time, money and resources in the process (Rees, 2010).

To address this problem, before any work can be undertaken, an organization needs to step back and look objectively at how card data flows, rests and is maintained in its organizational environment. Tracking this flow allows the organization to create a set of card data communication diagrams that shows how card data enters the environment and how it moves and is dealt with through the organization during its lifecycle. This needs to encompass both the technological and organizational requirements of the standard (Rees, 2010).

On top of identifying all assets in the premises scope for auditing, it is also compulsory to understand the data flow to manage sensitive information like card data. The flow of sensitive information has to be separated to that of non-sensitive to make information security management easier.

Policies and procedures are also important to ensure that every security practices are being adhered and operational. Additionally the policy should be reviewed for their effectiveness and to see if they are up-to-date as they relate to technology developments and operational procedures. Very often the actual policies and procedures need to be revised to take into account changes within the environment (Tutton, 2010).

Otherwise if there are failure to adhere this, PCI can lead to fines from the credit card companies and withdrawal or limitation of credit card services which could severely hit the bottom line. Perhaps the biggest risk to organizations is the reputational risk impact. In the past if an organization were seen to be guilty of a breach of security this would have negative consequences, but if it now became known that the company did not conform to standards agreed with the credit card providers this could exacerbate the reputational damage. Customers might reasonably feel that the loss could have been prevented. Organizations with a valuable and

widely recognized brand who conduct a large amount of electronic business are at particular risk from such a situation (Rowlingson and Winsborrow, 2006).

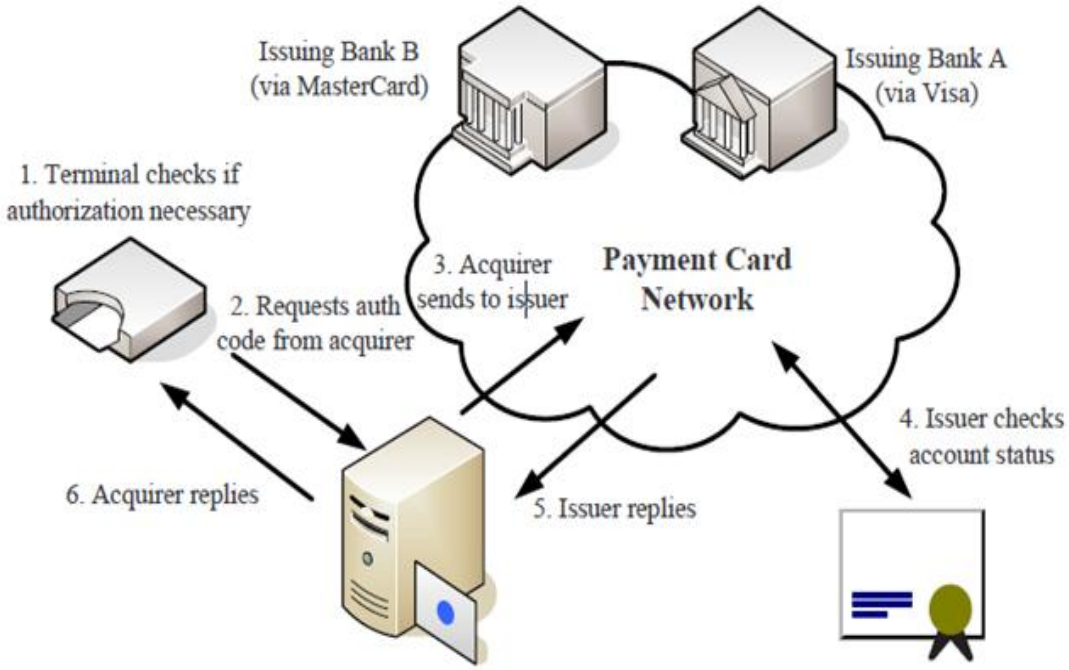

Figure 2-6: Card Data Flow; adapted from Liu (2010)

As shown in figure 2-5, card data passes different authentication and authorization processes before transaction takes place. And for all these processes, standardized security control should be implemented in order to protect card holder data from being exposed to threats.

According to Spremic (2011), the PCI-DSS (Payment Card Industry Data Security Standard) is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data and manage IT security and privacy risk in credit card transactions.

Regarding information security management related to financial sectors, few researches are conducted locally using ISO checklist as a measurement to assess the general information

security practice of the banks whereas, this research focus on the card banking security using PCI-DSS standard checklist.

Author (year)	Objectives	Methods/approach	Key finding
Walid Al-Ahmad and Bassil Mohammad(2014)	Addressing Information Security Risks by Adopting Standards	Case study	Propose Model for Framework Selection
Raghavan and Parthiban(2014)	Assess cybercrime in the banking sector and impact of cybercrimes on bank finances.	Pattern matching technique used	Identified the major cybercrimes in the banking sector
Abu-Shanab and Salam Matalqa (2015)	Explore security issues related to e-banking	An expert opinion method was used to rank different model and techniques	Proposed the superior model and the least effective model
Kelemie Tebkew(2013)	To propose and develop ISM Framework which will work in banking industry in Ethiopia.	Case study	Developed information security management framework for the bank
Susanto(2011)	To set of benchmarks or standards to ensure the best security practices	Introduce various information security standards	The study provides a picture of the position and specialization of each standard usability levels.
Lokhande and Meshram (2013)	Identifying E-Commerce Vulnerabilities, Attacks and Countermeasures	Surveying technique	Identified the security enhancement techniques.
Munir and Manarvi (2010)	Assessing Security risk for banking sector-A Case study of Pakistani Banks	Quantitative risk assessment(questionnaire)	Risk assessment is recommended to all assets in the organization.
Mario Spremic(2011)	Propose IT Risk Management model of IT Governance and IS Audit	Qualitative and Quantitative method	IT risks becomes less and less a technical problem, and more and more the problem of the whole organization i.e. a 'business problem'

Ula etal.,(2011)	Proposes the initial framework for governing the information security in banking system	Survey	A comprehensive information security governance framework is highly needed for banking information system.
Zhi Xian et al.,(2013)	Identifying the factors that influence key decision makers in small to medium enterprises to address information security risks.	Case study	Identify the key factors that influence security expenditure.
Munir and Manarvi (2010)	Identify information security control loophole	Quantitative method	A missing link to information security management
	Propose a security risk analysis model (SRAM)	Case study	SRAM is able to improve the accuracy and efficiency of security risk management for information systems.
Desisa and Beshah(2014)	To develop and evaluate internet banking security framework and its major five security models.	Survey	Recommend holistic multi-layered security
Arif Shaikh(2014)	To examine bankers perceptions of the risk associated to electronic banking and	questionnaire	Risk associated with electronic banking are identified

2.11 Summary

As it is presented by most of the scholars, information security is not a new problem however; it is an old problem in a new environment. Due to the need of global connectivity and business need, organizations dependency to information technology is increasing from day to day.

The growth of information technology and internet makes people to access information at any place and at any time. And this makes organizations to highly depend on their IT systems to collect, process, store, distribute and transmit information across the networks. Along with this, the risk associated with information security is increased including disclosure, modification, destruction and disruption of information which affects the confidentiality, integrity and availability of information in the organization. As it is stated in most of the literatures, there are many threats to the integrity, confidentiality, and availability of information in the organization and there are also various countermeasures to address the security threats. However, implementing the security measures without a proper management brings insignificant contribution towards protecting information. In this regard, information security management plays a vital role in addressing these problems.

Effective information security also emphasizes the development, communication, and publication of information security policies and procedures to ensure the inclusive understanding of the current-state security and follow up the implementation in a day to day basis. To manage information security appropriately and address the security issue at an acceptable level, organizations are expected to be compliance to an international security standard that evaluate the security status and recommend the right tools and measures to be taken on top of managing the security of the existing infrastructure.

Since there are number of frauds and cybercrimes in the electronic payment processors and the banking sector including ATM frauds, Cyber Money laundering, debit card frauds and Credit Card Frauds. All these frauds are executed to gain access to users account, funds and transfer it to some other bank account. The cyber criminals also use the banking credentials like fraud cards, PIN, password and certificates to access accounts and steal money from the account owners and causes huge financial loses to the financial sectors and customers.

As the issue related to information security is persisting, different researchers have conducted researches on the subject for the past years. Among these researches, most of them uses ISO (International Standardization Organization) standard as a security standard bench mark to assess the information security practice of the organizations.

Currently there are various internationally recognized information security standards around the world which includes the most utilizable standards like ISO27001, BS 7799, PCI-DSS, ITIL and COBIT. Among these standards, PCI-DSS focus on information security related to financial institution like banks and electronic payment service providers as it mainly focus on protecting card data transactions, online transaction, smart card and related electronic banking services which brings new business opportunities while it imposes high security risk to the financial sector.

A research was also conducted in Ethiopia to assess information security management in the banking sectors using ISO (International Standard Organization) as a bench mark and a security framework was proposed to address the information security issues. In addition to that, similar researches were also made locally focusing on internet banking and information security audit (Desisa and Beshah, 2014; Kassa, 2016). However, this research focuses mainly on the card banking security and in this regard, it uses PCI-DSS (Payment Card Industry Data Security) security standard as a measurement tool to assess the effectiveness of information security of the financial sectors.

Since most of Ethiopian banks and electronic payment sectors are interconnected to their branches and to the national payment switch to transact electronic card payment services using ATM and POS (Point of Sale) machine. As hacking and cybercrimes are increasing on the financial sectors globally, it is compulsory to assess the effectiveness of card banking security and recommend the best security practices for the Ethiopian financial sectors so that they would get compliant to the international security standards.

Applying this security standard protect an organization from internal and external threat by securing network components, protecting sensitive data, maintaining vulnerability management, implementing access control, regularly monitoring the network and maintaining information security policy.

In the next chapter, the research design and methodology used to get the data from the financial sectors is presented.

CHAPTER THREE

RESARCH DESIGN AND METHODOLOGY

This chapter aims to describe the research design and methodology used to achieve the research goals of this study. Thus, the chapter discussed the research design and techniques used to answer the research questions. Accordingly; research designs, research data, scope of the study and research population are discussed on top of the study instrument questioners, document analysis and observation. The chapter also presents pilot study, validity, reliability, ethical concern and research limitation.

3.1 Research design

A research design is a plan used as a guide in collecting and analyzing research data for the study to be conducted. It describes the methods used to collect and analyze the data that helps to answer the research question. For this research, among the different research designs, case study research design is used to explicate the research and answer the research questions.

The researcher used descriptive approaches to describe and evaluate the extent in which financial sectors are applying Information Security Management and identify the factors prohibiting the financial sectors from Information Security standard compliance. In this regard, quantitative research design was used to investigate, gather and present information about the existing status of the subject which is information security management in this sector. Questioners, which will answer the research question of the study was distributed to the target group in the selected financial sectors and the response was collected, analyzed, discussed and the recommendation to the information security standard compliance was given accordingly.

3.2 Case Study Research Method

In this study, case study research method is used to clarify and describe information security management related to the financial sectors. Information security management problems and solution are likely to reside in this sector and the plan of this research is to identify the significant factors by discovering ideas and insights which are relevant to the research. In this regard, assessment was conducted using questioner in addition to observation and document viewing by through articles review, journals and scientific publication to comprehend the present level of information security management in the financial sectors and the risk associated in the sectors in related to the research quotations.

3.3 Source of Data and Data Collection Methods

Regarding the research data of the study, as a primary data, questioners were used to collect information from the target group of the financial sectors. The questioner is adapted from the PCI-DSS security standard which is an internationally used security standards. After adapting the questioners from these international security standards, the researcher distributed the questioners to the selected financial sectors IT department's staffs including IT executives who will make decision on the IT managerial activities and IT experts including security experts, database experts, network experts and application developers who will make sure the system availability and functionality in addition to preparing policies, procedures and follow up the implementation of the day to day activities of the financial sectors.

Document analysis and observation was also used to get more information from the financial sectors on the matter to strengthen the reliability of the primary data and the result is incorporated with the quantitative data result.

3.4 Study Population and Sampling Technique

3.4.1 Sampling Technique

The researcher used purposive sampling technique and selected two private banks and one electronic payment sector to conduct this research to address the financial sectors that are issuing electronic payment card at their premises. Since, among the seventeen commercial banks in Ethiopia, only four banks print electronic payment card and PIN (Personal Identification) number at their premises to transact money using payment terminals such as ATM and POS machine. And from the four banks that have electronic card issuing service for the electronic payment services, two banks were selected using purposive sampling technique.

The researcher used purposive sampling technique as it provides the deliberate choice based on the qualities of the participant possesses to address the objective of the research. In this regard, the researcher can decide the sample based on what to be studied as per the study objective (Etikan et al., 2015). Since, purposive sampling techniques involve selecting certain cases based on a specific purpose rather than random selection (Teddlie and Yu, 2009)

In addition to the four banks with card banking services, there are two electronic card payment service providers sectors that are established under the Ethiopian national bank license to provide the electronic payment service which serves as a switch among the banks and print the electronic payment card (debit card) and PIN.

The researcher also selected one electronic payment processor among the two using purposive sampling. Hence, 50% of the banks that issues electronic card and PIN, and 50% of the electronic payment processors are selected for this study using purposive sampling method.

Regarding the target population, all the IT executives and IT staffs in the IT department were selected. As the number of IT staffs in the IT department is not as such numerous, the researcher included all the staffs to participate to this research.

3.4.2 Questioners

As a quantitative data collection method, questioners which were adapted from PCI-DSS standards were used. The questioner is categorized in to three major categories which are respondent information, organization information, and the security related questions to measure the current status of information security management in the sampled financial sectors.

The assessment security questioners consists of forty eight questions that covers security scoping, media and facility security, network security, application security, Card data security and encryption, logging and monitoring, policy and procedure and finally implementation of anti-malware and antivirus.

3.4.3 Document Analysis

Regarding document analysis, the financial sectors security policy and procedures which is to be carried out in the day to day activities to protect the organizational information from external and internal threat was reviewed to make sure that it is prepared according to international standard covering all the assets at the organizations premises. The document analysis was also made for the purpose of cross checking the validity of the response given on the questioners.

3.4.4 Observation

Observation was made at the target financial sectors using check list to check the reliability of some part of the questioners in relative with the questioners. The observation includes:

i. The financial sectors detailed network diagram(s) , whether it covers all boundaries in scope including segmentation, boundaries between trusted and un-trusted networks, wireless (if available) and wired networks , types of devices, device interfaces, protocols and security controls.

ii. Shredding or cross-cut process of sensitive card holder, personal identification (PIN) number and related sensitive hard copies and make sure this sensitive information such as cardholder data and personal identification (PIN) number cannot be reconstructed.

iii. If there is a current and maintained diagram which shows cardholder data flows across the systems and networks.

iv. If there is a public access between the Internet and any system component in the cardholder data environment and if DMZ (demilitarized zone) is properly implemented to protect the inside network.

3.5 Pilot study

Although all questioners are adapted from the international standard, PCI-DSS, it is essential to make a pilot study to avoid misunderstanding in the questions and to make sure that no ambiguity and error on the questions so that the researcher would get accurate data from the target population.

To that end, the relevant improvement was made on some of the content and the layout of the questions by the advisor. After the necessary correction was made consulting the advisor, the questioners were distributed to one of the oldest private bank in Ethiopia named Awash International Bank (AIB) for pilot test. And based on the feedback of the pilot test, additional correction and minor modification was made on the questioners.

3.6 Validity

To make sure the validity of the research tool, the questioners were adapted from international information security standards and best practices of PCI-DSS (Payment Card Industry Data Security Service) and ISO (International Standardization Organization).

After the questioners are adapted, modifications and adjustments were made on the formatting after discussing with the advisor. Moreover, pilot test was made by distributing the questioners to one bank and some modification was made based on their feedback.

3.7 Reliability

In order to strengthen the reliability of data collected by using questioners, the researcher used documents by reviewing information security and related policies and procedures further to observing some critical areas such as card and PIN printing rooms, network diagram and card data flow.

3.8 Statistical Data Analysis

Raw data was collected using structured close ended questioners, document analysis and observation from the sampled financial sectors. And the data was edited, coded and utilized using IBM SPSS V.20 tool since, SPSS provides better results as it reduce errors and make the data analysis task easier by eliminating hours of tedious data management and presentation. The data analysis includes frequencies and percentages using tables as a method of presentation.

3.9 Ethical Consideration

The researcher considered all the ethical concerns and follow in all the steps in the research process. Hence, the researcher considered the following during the research process:

- Reference letter, which support to do the study was used to both financial sectors written from the university.

- The questionnaire doesn't have any indication of the person identity. There is no question that asks its personal identification information such as name and department.

- Confidentiality was maintained in all the process and procedures of the study for questioner, document analysis and observation.

CHAPTER FOUR

FINDING AND DISCUSTION

4.1 Overview

This chapter presents the finding of the study and discussed the result accordingly. Hence, the findings are categorized in to eight sections. This includes: security scoping, media and facilities security, network and security, application security, card data security and encryption, logging and monitoring, policy and procedure and anti-malware.

To address this, first, the questionnaires distribution procedure had been completed and the data was collected and verified to discover if there are incomplete and inconsistent responses from the target respondent. Following to the verification of the questioners, the collected data was analyzed using SPSS to explore the results for further discussion and recommendation based on the findings. In this regard, the questioner which has five response options from very high to very low is processed using SPSS tool and changed in to three categories. Hence, very high and high is converted to secure, medium is converted to partially secure and finally low and very low is converted in to not secure.

Regarding the source of the data, the entire respondent of the questioners belonged to the IT department and they had adequate knowledge on the matter one or the other way. The data analysis tool used to analyze the findings of this study was SPSS V.20 (Statistical Package for the Social Science) tool which is a computer program used for statistical analysis with many features to manipulate and analyze quantitative data. On top of the questioners, observation technique was also used as an instrument to strengthen the information gathered from the target population of the selected financial sectors. Regarding the result presentation, frequency and percentage is used in the table form since a frequency table is one of the most basic tools for displaying descriptive statistics which make it much easier to view and understand the result of the data presentation.

4.2 Demographic Properties of Respondent

The demographic data incorporates respondent information and organizational information of the financial sectors. The respondent information covered information such as educational level, employee specialty, work experience whereas, the organizational information verifies if the financial sectors have information security management certifications, and if they don't have one, the question asked for their future plan towards having one of these information security standard compliance certifications.

Respondent Educational Level and work experience	**Frequency**	**Percent**
BSc. Degree	22	88.0
MSc Degree	3	12.0
Total	**25**	**100.0**
<= 5 years' experience	11	44.0
>=6 years' experience	14	56.0
Total	**25**	**100.0**

Table 4-1: Respondent educational level and work experience

All the respondents are working in different division under the IT department and among them, 56% have more than six years of experience in the IT field. And regarding the educational level of the respondent, all of them have academic degree in which, 88% have first degree and the rest 12% has second degree. Thus, though almost all the respondent doesn't have security related information security certifications, they have adequate knowledge with information security management to understand the subject matter and respond to the questioners provided.

In the organizational information, the major question raised is, the availability of information security standard compliance certificate in the organization and if they doesn't have one, their future plan to hold these compliance certification. Thus, one of the financial sectors already has entry level (Level 1) PCI-DSS compliance certificate while the other sector has a plan to work on and holding the PCI-DSS security compliance certificate.

4.3 Security Scoping

The security scoping questions provided to the financial sectors comprises of how their inventory device are updated, and whether it included all the necessary information regarding the devises information such as model of devise, location of device, serial number asset identification tag and classification of item type . In addition to this, it verified if there is a detailed network diagram covering all boundaries in scope including network segmentation, if there are boundaries between trusted and un-trusted networks, wireless and wired networks, type of devices, device interfaces, protocols and security controls in the scope.

Thus, the summarized result of the collected information regarding the security scope is as below in table 4-2

	Frequency	**Percent**
Less Secure	8	32.0
Partially Secure	6	24.0
Fully Secure	11	44.0
Total	**25**	**100.0**

Table 4-2: Security Scoping

As the summarized result shows, 32% of the security scoping is not secured, 24% of the security scoping is partially secured whereas the rest 44% is secured in the organisations.

The result shows that hardware and software asset inventory has been maintained in the organisations but the existing inventory is not updated to include all the essential assets which should be under the security scope. Furthermore, the existing inventory didn't have detailed description and function of use.

Regarding the network diagram, there is a detailed network diagrams which covers boundaries in scope including network segmentation and boundaries between trusted and un-trusted networks. However, the Network diagram was not updated with cardholder data components of the organizations since the following was not well illustrated within the diagram:

- The Card Data Environment (CDE) and non-Card Data Environment (Non CDE) data flow is not well mentioned in the network diagram.
- DMZ (Demilitarized Zone) is configured in the premises however; there are components which aren't included in the DMZ zone.
- ATM and POS (Point of Sale) transaction connectivity (Type of connection, systems involved within operation) is not clearly defined to include the end to end connectivity for storing, processing and transmission of transaction data.

4.4 Media and Facilities Security

The media and facility security part of the questioners includes how the removable media that contains sensitive information is properly labeled to protect the information from an authorized access, how the medias are destroyed using procedures supported by legal reasons such as retention period based on business justification, how onsite personnel are identified from visitor and the entry control security as a whole using different technologies such as CCTV and Access control.

The summarized result of media and facility security is as below in the table 4-3:

	Frequency	**Percent**
Less Secure	9	24.0
Partially Secure	10	40.0
Fully Secure	6	36.0
Total	**25**	**100.0**

Table 4-3: Media and Facility Security

The survey result shows that 36% of media and facility is less secured, 40% is partially secured and 24 % is fully secured.

According to the findings, there is no access control policy documented to implement and manage access control. The authentication mechanism to secure the components under the premises is not well built as there is only manual entry control management which is not properly maintained. In addition to this, in some system components, there are no privileges assigned to employee based on the job descriptions, role and need to know basis.

Although all access assigned to persons should be based on the need to know basis and their roles, privilege user management procedure is not in place and, there is no user authorization forms available either.

Regarding sensitive data deletion, there is a secure deletion procedure followed to remove the Card Holder Data (CHD) from the printing machine and workstations however, the retention period is not described and followed properly based on the business justification and retention period set by the national bank.

Access to datacenter is restricted and monitored using CCTV camera and card based access control but physical and logical access to operation areas located in the office work environment is not restricted using access control mechanisms. On top of this, visitor log is not maintained in the form of specific register with escorting details of visitors. Though there is a badge at the

reception to identify the visitors from onsite personnel, it is not often used while visitors are shown up at the premises.

In general, there is no documented procedure existed in the organisation to include the below requirements.

- Maintaining a list of media devices periodically.
- Periodic inspection of media devices to look for tampering or substitution.
- Training personnel to be aware of suspicious thing and to report tampering or substitution of devices.

4.5 Network and Security

The network and security category consists of both wired and wireless network security on top of the technologies applied to protect the premises from unauthorized access and periodic vulnerability assessment and penetration test.

The summarized result found from the financial sector is as below in table 4-4:

	Frequency	**Percent**
Less Secure	2	8.0
Partially Secure	11	44.0
Fully Secure	12	48.0
Total	**25**	**100.0**

Table 4-4: Network and Security

As the result shows, 8% of Network and Security in the organisations are less secured, 44% is partially secured and 48% is fully secured.

Internet connection is separated from the internal network through firewall and router and there is no direct connection between internet and internal network of the organisations. Furthermore,

production and test environment is segmented to protect production environment from any security risk using VLAN technology however, the firewall and router configuration standard has not been documented to include roles, responsibilities and access privileges to the network components. Further to this, services and ports are not restricted for inbound (incoming) and outbound (outgoing) traffic in the card data environment.

Personal firewall is enabled on the windows firewall to prevent personal computer which would be connected to the network however, it is observed that in some computers it can be disabled by users as users has administrative privilege.

There is no successive quarterly wireless scanning and analysis activity that identifies unauthorized access point at the premises. In addition to that, there is no all-inclusive vulnerability assessment and penetration test conducted regularly to verify the security of the whole perimeter and the security system to monitors and responds to networks intrusions, vulnerabilities and irregularities behaviors are not monitored on a 24/7 basis hence, it will not be easier to take immediate action if any internal or external incident occurs.

4.6 Application Security

The application security questioners evaluate the software development process, security patches management, application log monitoring and application change detection mechanisms. The summarized result of the collected data of the application security is as below in the table 4-5.

	Frequency	**Percent**
Less Secure	6	24.0
Partially Secure	9	36.0
Fully Secure	10	40.0
Total	**25**	**100.0**

Table 4-5: Application Security

As per the summarized result, 24% of the application security is less secured, 36% is partially secured and 40% is fully secured.

In the application security, not all system components were installed with the latest patches on time to fix the application from recent virus definitions. There is no application vulnerability assessment and application penetration test conducted periodically or at the time of significant change, and application firewall is not deployed on perimeter location.

Furthermore, the file integrity and log monitoring tool is not fully integrated with all the application systems to alert unauthorised access and modification. It is examined that cardholder data components including Windows servers, Linux servers, Oracle Database, Application, Cisco firewall, Router and Switch are configured to enable audit track and send all logs to centralized system which are file integrity monitoring and log monitoring to monitor the system components. However, not all the component in the scope is integrated and configured to send logs to the log monitoring system. Moreover, logs are not analyzed periodically to examine the security status of the system components.

Data deletion, retention and disposal policy and procedure have not been well documented in the organisations. Hence, data retention requirement such as secure deletion of cardholder data was not addressed descriptively in the security policy and there are few system components where full PAN (Primary Account Number) was displayed. Further to this, there is no card data encryption policy and procedure documented for protection of card data however; the data encryption practice is existed in the premises.

4.7 Card Data Security and Encryption

The card data security and encryption questioners include both card holder data security and the encryption technology used to protect the sensitive data from being exposed to an authorized access.

Hence, this category includes the security of the card data environment and the security of the connection between card data environment and other networks. Further to this, card data such as PAN (Primary Account Number), CVV (Card Verification Value), PIN (Personal Identification

Number) transmission and deletion process, use of cryptography and encryption technologies and the security awareness program to the card data security is assessed. Accordingly, the summarized result of the card data security and encryption is as below in table 4-6.

	Frequency	**Percent**
Less Secure	6	24.0
Partially Secure	13	52.0
Fully Secure	6	24.0
Total	**25**	**100.0**

Table 4-6: Card Data Security and Encryption

As the result of the summarized card data security and encryption security of the organizations shows, 24% of the application is less secure, 52% is partially secured and 24% is fully secured.

In the financial sectors, sensitive data are stored and transmitted with encryption and no PAN number is transmitted through email or other insecure communication channel and the first and the last four digits of the PAN number is encrypted among the sixteen digits to hide and protect the PAN number not to be disclosed to unauthorized access.

Data deletion, retention and disposal policy and procedure have not been well documented in the organisations. Hence, data retention requirement such as secure deletion of cardholder data was not addressed descriptively in the security policy and there are some system components where full PAN (Primary Account Number) was displayed. Further to this, there is no card data encryption policy and procedure documented for protection of card data however; the data encryption practice is existed in the premises.

While data is transmitted over the public network, security protocols such as IPSEC (IP Security) and SSH (Security Shell) is used to secure the end to end connectivity nevertheless, it is not fully implemented with all the connections and some of the application components don’t use cryptography technologies such as SSH (Secure Socket Shell).

Access to sensitive areas are not strictly limited to individuals that there job requires to visit this area and there is no formal and periodic security awareness training though, there is security briefing up on the hiring on new staffs.

Regarding the network diagram that identifies the connections between cardholder data environment and other networks, all the cardholder components are included in the network diagram however, the network diagram doesn't show the cardholder data flows across systems and networks.

4.8 Logging and Monitoring

The logging and monitoring category consist of time synchronization technology (NTP), password management, access management, user management process and account management.

The summarized result of the logging and monitoring response is as below in Table 4-7

	Frequency	**Percent**
Less Secure	10	40.0
Partially Secure	10	40.0
Fully Secure	5	20.0
Total	**25**	**100.0**

Table 4-7: Logging and Monitoring

As per the result shown, 40% of the logging and monitoring is less secure, 40% is partially secured and the rest 20% is fully secured.

There is implemented time synchronization technology in the system components such as servers and network devices however; all the components in the scope are not configured to be integrated with the central time server. There is also no documented procedure to address NTP (Network Time Protocol) configuration in any of the policies and procedures.

Regarding the Account policy, the following are observed:

- There are users who have not logged in for more than 60 days and are not disabled and removed from the system.

- Account lockout has not been configured on some of the components (Servers and Network) based on requirement.

- It is verified that there are system components not configured with minimum password length.

- Some system components are not configured with password complexity enabled (alpha-numeric characters).

- There are system components which are not configured with password history

- In some of the components, Password is not interactive to enforce quality password.

In addition to these, there is no formal user registration process to revoke user access regularly while required up on the termination of employee from the organisation. Vendor supplied default accounts are removed before connecting to the production environment as all the default password makes unauthorized personnel to intrude to the system easily.

4.9 Policy and Procedure

The Policy and Procedure category consists of information security policy and procedure, user management policy and procedure, change management procedures, information security risk assessment process, backup and recovery policy and procedure and incident response policy and procedure.

The summarized result of the information collected from the target financial sectors is as below:

	Frequency	**Percent**
Less Secure	5	20.0
Partially Secure	11	44.0
Fully Secure	9	36.0
Total	**25**	**100.0**

Table 4-8: Policy and Procedures

As the table shows 20% of the organization policy and procedure is less secure, 44% is partially secured and 36% is fully secured.

Information security policies and procedures are in place but it is not carried out in a day to day activities. The organizations aren't providing security training and don't provide refresher training every year as it is documented in the information security policy. Information classification policy is not defined within the organization to maintain proper control of all assets identified with the correct classification.

As a part of the recruitment and training policy, all employees sign on commitment form, which mentioned that they understood the policy and procedures. Non-Disclosure agreements with all employees are maintained.

Changes are not being routed through change management. Access rules are being modified based on specific request from different department but structured formal change management was not followed for systems, firewall and router configuration changes.

4.10 Anti-Malware

Regarding the Antimalware of the financial sectors, the questioners include IPS (Intrusion Prevention System) and IDS (Intrusion Detection System) deployment, IPS/IDS Management and Antivirus deployment and management.

Accordingly, the summarized result found from the financial sectors is as below in the table 4-9.

	Frequency	**Percent**
Less Secure	5	20.0
Partially Secure	8	32.0
Fully Secure	12	48.0
Total	**25**	**100.0**

Table 4-9: Anti-Malware

As the summarized result shows, 20% of the antimalware is less secured, 32% is partially secured and the rest 48% is fully implemented and secured.

Antivirus has been installed on most of the components including servers and client machines but it may not protect all the machines from all type of malicious software since the antivirus is not updated in some components with new virus definitions and new updates.

The Antivirus has not been enabled and configured to generate logs to store log files since it is not configured to be integrated with the log monitoring server. Moreover, there was no antimalware procedure or virus prevention procedure documented to make the action easier while such kind of attack happens in the premises.

In the next section, discussion is made based on the finding of the study.

4.11Discussion

As financial sectors possessed with secured and confidential information, all the vital assets in the premises should be registered and included in the scope for monitoring, otherwise, it can be exposed to unauthorized access easily and create damage to the company's business. As Liu et al., (2010), loss of these assets often leads to significant financial and nonfinancial damage to entities that store, process, or transmit cardholder data and technical and operational system components included in or connected to cardholder data.

Most media in the financial sector contains sensitive information related to the cardholder data such as PAN (Primary Account Number), CVV (Card Verification Value) and PIN (Personal Identification Number). If this sensitive information is compromised by any means, it would create mush damage on the financial sectors business.

According to Bradley and Dent (2010), organizations have struggled to adequately protect their most sensitive information assets, leading in many cases to breaches of security and the loss or disclosure of sensitive data. Many widely publicized incidents of high-profile data losses occurred across the globe in recent years in which of the 90% confirmed breaches that investigated, 285 million records were compromised and that 80% of these records involved payment card data. The report confirmed that fraudulent use of this payment card data occurred in 83% of these cases. Thus, financial organizations should work hard in securing their premises from an unauthorized access and protect their sensitive information and business as well.

Periodic vulnerability scanning, which is every quarter is mandatory for the financial organizations to identify gaps and mitigate on time before the occurrence of any damage. As Lokhande and Meshram (2013), vulnerability is a weakness which allows an attacker to reduce a system's information assurance by intersecting the system flaw, access to the flaw, and exploit the flaw. To exploit vulnerability, attackers only need one applicable tool or technique that can connect to a system weakness. Thus, vulnerability assessment minimizes the risk of being exposed to threats as mitigation would be done as per the vulnerability assessment report.

According PCI-DSS Reference Guide (2010), security vulnerabilities in applications systems may allow criminals to access PAN and other cardholder data. Many of these vulnerabilities are eliminated by installing security patches, which perform a quick repair job for a specific piece of programming code. All critical systems must have the most recently released software patches to prevent exploitation. Entities should apply patches to less-critical systems as soon as possible, based on a risk-based vulnerability management program. Secure coding practices for developing applications, change control procedures and other secure software development practices protects the application system if it is properly followed.

Sensitive information should be encrypted while it is transmitted internally or externally for business need. Encrypted data is intrinsically protected because it is unreadable. This is the

major reason that it is required in so many compliance guidelines and industry standards (Lokhande and Meshram, 2013). And the use of IPSEC (IP Security) encryption ensures secure private communication over the IP networks by facilitating direct IP connectivity between sensitive hosts through untrusted networks (Singh et al., 2014). Since, as Desisa and Beshah (2014), layered security control in the communication channel is recommended for the financial sector while using the public network like the Internet.

In this regard, cryptography technology should also be used to protect sensitive information in the financial sectors. According to Singh et al., (2014), cryptography is used in information security to protect information from unauthorized or accidental disclosure while the information is in transit or in storage. Information security uses cryptography technology to transform usable information into a form that is unusable by anyone other than an authorized user.

One of the major security protections for organization is password security. Since one of the most common types of attack is occurred by week password management practice in the organizations. To address this, organization should have a password management policy that is adhered by all the staffs and there should be password enforcement on every system components.

Hackers can guess passwords locally or remotely using either a manual or automated approach as there are many tools available which can automate the process of typing password after password. Password cracking methods also capture password hash and convert it to its plaintext original. For password cracking, an attacker uses tools like extractors for hash guessing, rainbow tables for looking up plaintext passwords, and password sniffers to extract authentication information. Password crackers sniff authentication traffic between a client and server and extract password hashes or enough authentication information to begin the cracking process (Lokhande and Meshram 2013).

In addition to password management policy, organizations should follow change management policy which is to be followed with every change.
According to Liu et al., (2010), change and release management policies ensure adequate testing and roll back policies. It defines the authorization and escalation processes, incident

classification, and exception management with centralized log management, reviews, and continuous monitoring with appropriate audits.

The information security policy should also include the basic requirements such as assigning risk ranking to vulnerabilities including high, medium and critical risk status in addition to that; there should be clearly stated incident management procedure to be followed. As Susanto et al., (2011) stated, information Security incident management involves identification of resources which are needed for incident handling. Good incident management will help with the prevention and awareness of incidents.

As PCI-DSS Reference Guide, (2010), many vulnerabilities and malicious viruses enter the network via users' e-mail and other online activities unless anti-virus software is used on all systems to protect systems from current and evolving malicious software threats.

Malware, including viruses, worms, and trojans can give access to unauthorized and malicious people. Malware can even enter a computer system via legitimate means such as e-mails and portable computing devices (e.g., laptop computers, PDAs, and smart phones) and storage devices (such as flash drives). Since antivirus software is capable of removing or quarantining known malware, and it is able to generate audit logs actively (Susanto et al., 2011).

Periodic wireless scan is also mandatory for organizations to identify insecure connections availability in the premises and take action accordingly. As Lokhande and Meshram (2013), many people may think about logging in to a random and unprotected wireless network just to get some work done. That's all it takes for someone with ill intent to capture a user's login credentials and work his way onto the wireless network.

In general, the security implementation and security controls of the financial sectors fall in the medium category. Different technologies are implemented to be used to protect the organizations from information security risk however; there is no regular control and management of the security tools. Periodic risk assessment is not maintained in the organizations to assess and identify risks based on its level (critical, high, medium) and take action accordingly before it affect the system and the business.

There are security policies and procedures prepared and documented to manage and control the organizations information security from unauthorized internal and external access but the policies and the procedures are not maintained to be executed in the day to day activities of the organizations. In general, information security management and practices in the Ethiopian financial sectors are not well addressed and maintained in regard to the current security threat and risks associated with the financial sectors.

In this study, in addition to assessing the effectiveness of information security management in the Ethiopian financial sectors focusing on the card banking security, the factors prohibiting the effectiveness of information security management towards Payment Card Industry Data Security Standard (PCI-DSS) are identified. The factors are as below:

- Security scoping in the organizations
- Organizations media and facilities security control mechanism
- Network and Security practice, control and management
- Application Security management
- Card Data Security and Encryption
- Logging and Monitoring management
- Policy and Procedure implementation and practice
- Anti-Malware management

As information security is very fundamental for organizations, particularly for the financial sectors such as banks and electronic payment sectors, information security practice should be maintained at the maximum level. However, in this study, most of the security controls, practices and managements are below the acceptable level. In this regard, financial sectors who are involving in card banking service should work towards PCI-DSS (Payment Card Industry Data Security Standard) security standard compliance to protect their valuable and critical assets from information security threats and risks.

Based on the findings of this study, the research answered the two research questions raised. In this regard, the effectiveness of information security management and practice focusing on the card banking security were assessed using the PCI-DSS security standard checklist, and most of

the information security management and practice are below the acceptable level. On top of this, the factors that are prohibiting the financial sectors from security standard compliance are identified.

Regarding the weakness of this study is, it mainly focus on card banking security which is one part of electronic banking service due to time and resource constraint. However, electronic banking in general including internet banking, mobile banking, card banking are critical services which should be studied. Thus, further researches should be conducted in these areas to address the information security threats and risks in the electronic banking services.

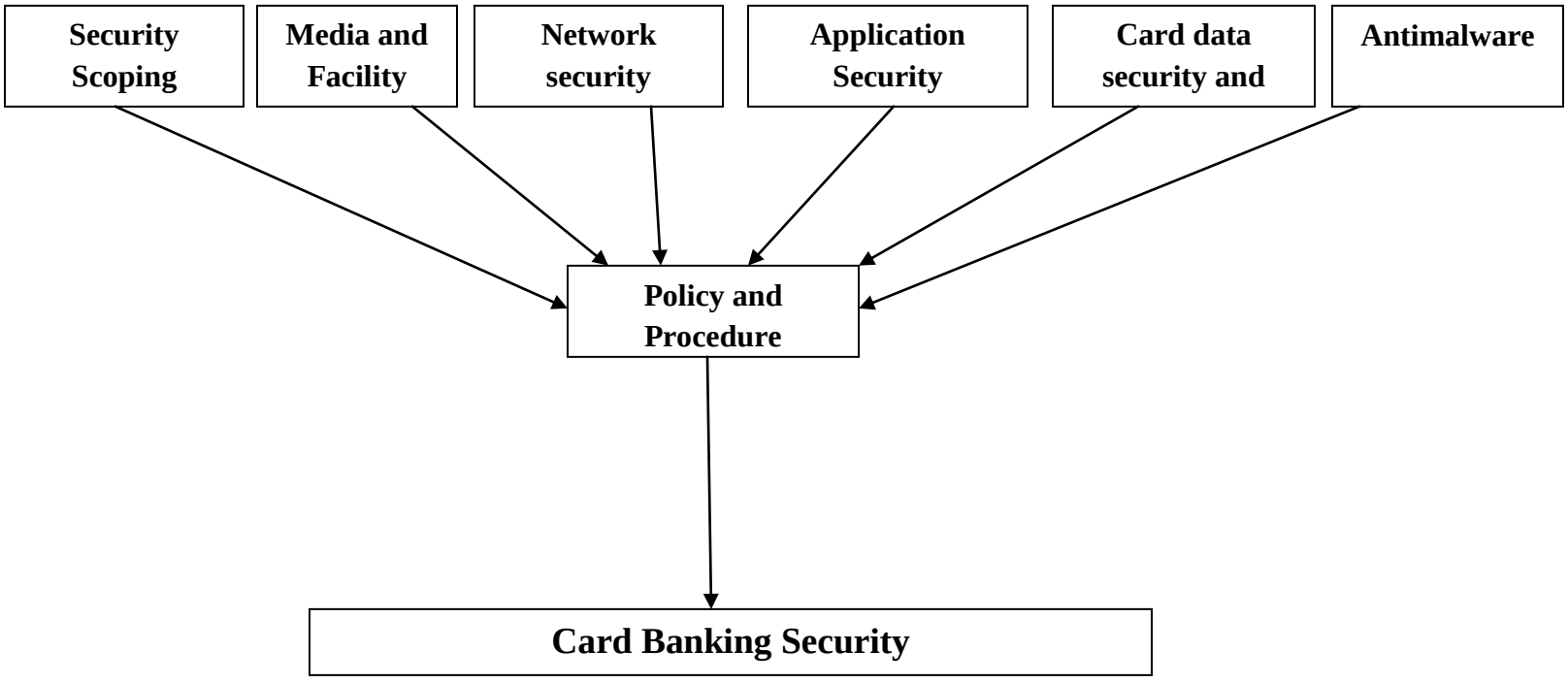

Figure 2-7: Conceptual Framework

4.6 Summary

In this chapter, based on the information collected from the sampled financial sectors using questioners, observation and document analysis, the gap towards effective information security management are identified and discussed. Hence, the result found from the financial sectors IT staffs was analyzed using SPSS v.20 tool and presented in table using frequency and percentage. And in the next chapter, recommendation is given based on the result.

CHAPTER FIVE

CONCLUSION AND RECOMMENDATION

5.1 Overview

The final chapter presents the conclusion of the study and present the recommendation based on the findings of the research. Furthermore, the chapter briefly discusses the research contribution and proposes possible ideas for future studies.

5.2 Conclusion

This research assessed the current information security management practice in the financial sectors focusing on the card banking security and identified the factors that prohibits the financial sectors from international standard security compliance particularly PCI-DSS (Payment Card Data Security Standard).

In addition to that, the factors that prohibit the financial sectors from PCI-DSS security standard compliance are identified from the result of the collected data of the target financial sectors. As most of the categories of the questioners are adapted from PCI-DSS standard and the response collected regarding the security stands fall in the medium grouping, it can be said that nearly all the listed security categories are factors that prohibit financial sectors from security standard compliance which includes security scoping, media and facility security, network security, application security, card data security, data encryption, logging and monitoring and policy and procedures.

Most of the information security practices and management are not well implemented in the financial sectors. The organizations mostly focus in expanding their infrastructure and adapting technologies that support the business need while much attention and priority is not given to the information security in regard to the current security risk and threats. Even for the already

existed security technologies and processes, there is no regular follow up and management using proper policies and procedures.

Since, information security management is a fundamental aspect as threats to the availability, integrity, and confidentiality of the organization's information is great and ever increasing. As financial sectors possess information that is critical and sensitive, the existence of effective information security practice and management is indisputable.

In general, an effective information security management assures a broad understanding of security practice and security management by establishing policies and procedures to be followed in the day to day activities and operations of the financial sectors.

In the current cyber related crimes, it is compulsory for the financial sectors implementing the maximum information security management practice and be complaint with international security standard such as PCI-DSS by addressing the gap associated to the listed categories and maintain information security at an acceptable level at their premises. To address these, recommendation is given as per the finding of the research.

5.3 Recommendation

Organizations should conduct security risk assessment for all devices in scope. And all the important assets that stores, process and transmits sensitive data should be incorporated in the scope to manage, control and monitor the assets during all the operations and to assess and manage risks before it takes place.

As Zhi Xian Ng et al., (2013) stated, the absence of one vital asset from the security scoping implies that the organization has not used its resources to best advantage in addressing security risk exposure. If certain assets were not considered in the risk assessment, then they may be unprotected which lead the organization to adverse consequences such as leakage of sensitive information and interruption or destruction of critical IT services.

In addition to including all the vital assets in the scope, devices inventory need to be updated with detail description and function to identify and classify assets easily and protect from loss and unauthorised access.

Device security operation procedure needs to be documented to include requirement as maintaining a list of devices, periodic inspection of devices to look for tampering or substitution and training personnel to be aware of suspicious behavior and to report tampering or substitution of device.

Following the scope and boundaries, the risk management activities should take place. According to the ISO/IEC 27005:2008 and NIST 800-30:2002, these include defining scope, risk assessment, risk treatment, risk acceptance, risk communication and risk monitoring and review. Within the plan of scope definition, risk assessment, risk treatment plan development and risk acceptance takes place (Tsohou et al, 2010).

Further to this, all media in the organization containing sensitive information should be destroyed using secure data deletion procedure when it is no longer needed for business. As Liu et al., (2010), the media inventory should be stored securely and while those media are useless for legal or business reasons, they must be destroyed permanently.

Regarding the physical security, there should be entry controls to limit and monitor physical access to systems using video cameras and access control mechanisms that monitors individual physical access to sensitive areas such as data center, card printing room and PIN printing room.

According to Susanto et al., (2011), physical and environmental security are used to protect systems, buildings, and related supporting infrastructure against threats associated with their physical environment, buildings and rooms to protect the environment and to avoid damage or unauthorized access to information and systems.

In the cardholder data environment, only authorized personnel are allowed to access to the environment, it is required to limit every possible physical access to cardholder data or system devices. To limit and monitor the physical accesses, appropriate control such as camera and access control should be deployed at facility entry and sensitive areas (Liu et al., 2010).

All network device configuration need to be changed using a defined change management. This change management should include testing and approval of new access rule and connection before it is implemented on the production system.

Organizations should develop change management forms which include detailed business justification for the requested change such as which ports and protocols are required and for what purpose and a roll back procedure should also be maintained. According to Pinder (2006), risk initiated by unexpected events and changes will be mitigated by adequate change management processes.

As a security measure, it is recommended to take back up of the files and place logical access to access this files securely. On top of this, firewall and router configuration backup should be secured and should also be synchronized after every change. As Liu et al., (2010), backup media and files should be kept in a safe and off-line facility.

Regarding the security of network connectivity, only specific services should be allowed on Firewall for inbound and outbound traffic and all cardholder data system and server should be configured outside DMZ segment and there should not be direct connection between internet and CDE (Card Data Environment) which is a secure environment. Personal firewall software should also be installed on employees owned laptops, which will be connected to scoped environment and should be configured in such as fashion that prohibits the users to disable or modify firewall configurations.

When a computer is connected to the network, it becomes vulnerable to attack. A personal firewall helps to protect the computer by limiting the types of traffic initiated by and directed to the computer. The intruder can also scan the hard drive to detect any stored passwords (Omariba et al., 2012).

Organization must have a formal process to approve and test external connections and changes to firewall configurations. The standard demands a justified documentation of unapproved or risky protocols, a description of network managing groups, roles and their responsibilities, and lists of services and ports needed to operate the business. It also requires a review of the firewalls and router settings on a quarterly basis. Every connection from an un-trusted area must be blocked by the firewall (Liu et al., 2010).

System components in the organization should be configured with secured services such as SSH, RDP-SSL, IPSEC VPN and strong encryption technology such as VPN and RDP-SSL. In general, to protect sensitive cardholder data during transmission, strong cryptographic and

security protocols like Internet Protocol Security (IPSEC) and SSL/TLS must be used (Susanto et al., 2011).

According to Liu et al., (2010), organizations are required to implement a firewall for each interconnection between the DMZ and the INZ and between the DMZ and external networks. DMZ, unlike internal network, isolates sensitive shared information and private data from external networks. To deny accesses between cardholder databases and external networks, the firewall must filter out direct traffics between the internal and external networks.

Firewalls should also be used to ensure incoming and outgoing data to be sent to the proper location, over the proper port, using an authorized protocol. Organizations only configure their firewalls to monitor traffic coming into the network. But to prevent malware sending data back to its controller, egress traffic must also be monitored properly (Lokhande and Meshram, 2013).

Time synchronization technology (NTP) should be implemented in all the system components such as Servers and Network devices in the organizations. As to Liu et al., (2010)**,** clocks and times are critical in system component and it should be synchronized among all the system components.

Regarding wireless network, incident management procedure should be documented to include rogue wireless scan activity on quarterly basis. The organisation should also ensure that wireless security policy and procedure should be defined to identify unauthorized wireless networks.

The wireless scan should be performed at least quarterly and wireless rogue access point scan should be performed for all locations and the rogue access point detection should be termed as security incident. To address this, security incident management procedure needs to be followed at the time of unauthorized wireless access point.

According to Lokhande and Meshram (2013), it is not considered logging onto a random and unprotected wireless network to get some work done. That's all it takes for someone with ill intent to capture a user's login credentials and work his way onto the wireless network.

Patch management procedure should be documented to include installation of critical vendor patch within one month and all applicable patches should be installed within vendor defined

timeframe. As Susanto et al., (2011) stated, security patches fix the majority of bugs by installing the latest official security patches no later than one month after the release. Moreover, all of the patches must be tested before deployment.

In the software development process, development and test environments should be separated and there should be a separation of duties between personnel assigned to the development or test environments and those assigned to the production environment. Furthermore, production data should not be used for testing and test data and accounts should be removed before a production system becomes active.

Generally, there should be a separate environments and duties for development, testing, and production in the organization (Susanto et al., 2011) and the databases and applications must have a production environment that is physically and logically separated from the test and development environment (Liu et al., 2010).

Card data encryption policy and procedures should be documented to include Full PAN to only be displayed to specific roles and users with business need. And no PAN data should be stored without encryption in addition to this, SSL/TLS or other cryptography method should be used for cardholder data transmission since insecure channel should not be used for cardholder data transmission.

According (Susanto et al., 2011), organization should render the Primary Account Number (PAN) into an unreadable form when stored via using pads, index tokens, truncation, and should use strong hash functions or a strong cryptography with an appropriate key-management procedure.

Cardholder data should be encrypted while sending it over end user messaging technologies. And no clear text PAN data should be shared over email or any end user messaging technology. In addition to this, all unnecessary default ids, user account need to be disabled or removed. This includes all system components (Firewall, Router, switch, application, and database).

The process needs to be implemented to conduct system configuration and hardening review of all servers, database and network devices during the deployment and all default vendor ids should be replaced with unique ids. Since vendor default passwords and settings are easily

accessible and used by hacker communities to compromise the systems. To overcome such situations, the standards recommend changing the default settings (Susanto et al., 2011).

There should also be a logical access control for account and password features that includes account lockout policy, account lockout duration, session timeout policy, password length, password complexity, Password history and Password expiry configured for all the assets in the scope.

As Liu et al., (2010), passwords should be changed every 90 days, and the minimum length should be seven characters, where alphabetic and numeric characters are both required and the user whose repeated access attempts are over six times should be locked out from accessing the system.

The organisations should develop network and security configuration standard defined to enforce use of IP and Port specific rules on the Firewall and Router with business justification and further public facing server and application need to be placed within DMZ in which, only specific services should be allowed on edge Firewall.

According to Liu et al., (2010), all the public facing web applications need to be protected by installing a firewall layer in front of them or by reviewing them for vulnerabilities with the help of security specialists.

It is important that an organization should have a comprehensive incident handling management process in place which includes, identification, detection and reporting incidents, Analysis and evaluation of incident, responding to the incident, recovery and cleanup of the incident and learning from the incident (Humphreys, 2008).

Incident response plan should be implemented in the organisation by including roles and responsibilities of the person that handles the incidence, incidence management communication strategies, incident response and handling procedures and business recovery and continuity procedures after handling the incidence.

Thus, Antivirus system software should be installed on each platform and it should be configured on all platforms and automatic update must be configured. All system components should be

configured and integrated with the master antivirus server to get periodic full scan. Latest antivirus software update should be installed on all system components and log generation should be configured for further analysis in case any suspicious activity is observed.

IPS (Intrusion Prevention System) should be deployed in the organization to protect the sensitive areas from unauthorized intrusion. As Lokhande and Meshram, (2013), the main functions of IPS and IDS are to identify malicious activity, log information about malicious activity, attempt to block and stop activity, and report activity.

In general, the network must be designed and configured to deliver high performance and reliability to meet the needs of the operations to provide a high degree of access controls and range of privilege restrictions.

System hardware, operating and application software, the networks and communication systems must all be adequately configured and safeguarded against both physical attack and logical attack and unauthorized network intrusion. There should be strong policies regarding use of Intrusion detection systems (IDS) in the premises and firewall and virus scanning tools should be used to protect against unauthorized persons and viruses from entering to the system. To make all communication secure, data should be encrypted to ensure the confidentiality of all data sent. (Jassal and Sehgal, 2013)

All accesses to network resources should be tracked and monitored using log files or audit trails, critical activities can be tracked and analyzed in a further step if something goes wrong. Without the log files and audit trails, it would be difficult to determine the cause of any problem (Liu et al., 2010). To address the effectiveness of information security management in the organizations, all the information security practices has to be exercised at an acceptable level in a daily basis.

And there should be policies, procedures and guidelines to follow up the implementations of the deployed security controls and security activities in order to have easy information security management and effective information security monitoring and controlling in the organizations**.**

In general, scoping should be defined to include all vital assets and periodic update of the inventory list should be done to make sure that all the critical components are incorporated to the scope. While these critical assets are disposed, or data are deleted, proper procedure should be

followed to avoid the exposure of the critical data to an authorized access. Internal and external connection should be secured using VALN and IPSec respectively to separate production environment from other unprotected environment such as internet. Critical application should be secured using encryption and other cryptography technology and patch should be updated regularly. In general, to make sure the implementation of information security in the financial sector, policy and procedures should be carried out in the day to day activities and penetration test should be done periodically both on the application and network level to make sure that gaps and vulnerabilities are mitigated in time.

5.4 Research Contribution

This study represents the basis of the Ethiopian financial sectors such as banks and electronic payment companies that issues and processes electronic payment card at their premises. Hence, financial sectors can use this study to assess their information security management and practice and evaluate their stands towards international information security management standard compliance such as PCI-DSS.

5.5 Future Studies

- Studying other electronic banking services such as mobile banking and online banking.
- Studying the improvement that information security standard compliance brings to the financial sectors.
- Studying information security management in relative with organizational performance.
- Study employees' information security management awareness, practice and adherence to policies and procedures.

References

1. Afshin Rezakhani , AbdolMajid Hajebi and Nasibe Mohammadi (2011). Standardization of all Information Security Management Systems, International Journal of Computer Applications, Ayatollah Boroujerdi University Boroujerd, Iran. Volume 18– No.8, pp. 4-8.

2. Aggeliki Tsohou , Spyros Kokolakis, Costas Lambrinoudakis and Stefanos Gritzalis (2010). A security standards' framework to facilitate best practices' awareness and conformity, pp. 367-376.

3. Ahmed Barakat, Khaled Hussainey, (2013).Bank governance, regulation, supervision, and risk reporting: Evidence from operational risk disclosures in European banks International Review of Financial Analysis, pp.254–273.

4. Al-Ahmad, Mohammad (2013). Addressing Information Security Risks by Adopting Standards Faculty of Arts and Science, Gulf University for Science & Technology, Kuwait Ernst & Young, Amman, Jordan, international journal of information security science Vol. 2, pp.28-43.

5. Ana-Maria Ghirana, Vasile Paul Bresfelean (2012). Compliance Requirements for Dealing with Risks and Governance. Bolyai University, Dept. of Business Information Systems Cluj-Napoca, Romania, pp.752 – 756.

6. Andrew Jones (2009). How do you make information security user friendly? Information security technical report, pp.213 – 216

7. Andrew Ren-Wei Fung, Kwo-Jean Farn, Abe C. Lin (2003). A study on the certification of the information security management systems, Computer Standards & Interfaces, pp.447–461.

8. Aniruddha Singh, Abhishek Vaish, Pankaj Kumar Keserwani,(2014). Information Security: Components and Techniques, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, pp.1072-1077

9. Anthony Vance a, Mikko Siponen b, Seppo Pahnila (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory, Information & Management, pp. 190–198.

10. A.R. Raghavan1 and Latha Parthiban (2014). The effect of cybercrime on a Bank's finances, international journal of current research and academy Volume-2, pp.173-178.

11. Aychiluhim Desisa and Tibebe Beshah (2014), Internet Banking Security Framework: The case of Ethiopian Banking Industry, HiLCoE, Computer Science College, School of Information Science, Addis Ababa University, Addis Ababa, Ethiopia pp.8-13.

12. Basie von Solms, Rossouw von Solms, (2004). The 10 deadly sins of information security management, Computers & Security, pp.371-376.

13. Basie von Solms (2005). Information Security governance: COBIT or ISO 17799 or both? Computers & Security Academy for Information Technology, University of Johannesburg, Johannesburg, South Africa, pp.99-104.

14. Basie von Solms (2006). Information Security – The Fourth Wave, computers and security, University of Johannesburg, Johannesburg, South Africa pp.165-168.

15. Charles Teddlie and Fen Yu (2007). Mixed Methods Sampling: A Typology with Examples, Journal of Mixed Methods Research, p.p77-100.

16. Chatzipoulidis Aristeidis, Mavridis Ioannis, (2009). Evolving challenge in information security compliance, pp.1-8.

17. Cheol-Soon Park, Sang-Soo Jang, Yong-Tae Park (2010). A Study of Effect of Information Security Management System[ISMS] Certification on Organization Performance, IJCSNS International Journal of Computer Science and Network Security, VOL.10, pp.10-21.

18. Debi Ashenden, (2008). Information Security management: A human challenge? information Security technical report, pp.195-201.

19. Ebru Yeniman Yildirima, Gizem Akalpa, Serpil Aytacb, Nuran Bayram (2011). Factors influencing information security management in small- and medium-sized enterprises: A case study from Turkey, International Journal of Information Management, pp.360-365.

20. Edward Humphreys (2008). Information security management standards: Compliance, governance and risk management information security technical report, pp.247-255.

21. Emad Abu-Shanab, Salam Matalqa (2015). Security and Fraud Issues of E-banking, International Journal of Computer Networks and Applications Volume 2, pp.179-187.

22. Georges Ataya, (2010). PCI DSS audit and compliance, IT Management Education at Solvay Brussels School of Economics and Management, Belgium, security technical report 15, pp.138-144.

23. Gunnar Peterson (2010). From auditor-centric to architecture-centric: SDLC for PCI DSS, information security technical report, pp.150-153.

24. Heru Susanto, Mohammad Nabil Almunawar and Yong Chee Tuan (2011). Information Security Management System Standards: A Comparative Study of the Big Five, International Journal of Electrical & Computer Sciences Vol: 11, pp.21-27.

25. Hyeun-Suk Rheea, Cheongtag Kimb, Young U. Ryuc (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior Computers & Security, pp.816-826.

26. Ilker Etikan, Sulaiman Musa, Rukayya Alkassim (2015). Comparison of Convenience Sampling and Purposive Sampling, American Journal of Theoretical and Applied Statistics, Department of Biostatistics, Near East University, Nicosia-TRNC, Cyprus, p.p1-4.

27. Ishmael Mugari, Shingirai Gona, Martin Maunga, Rufaro Chiyambiro (2016). Cybercrime - The Emerging Threat to the Financial Services Sector in Zimbabwe, Mediterranean Journal of Social Sciences MCSER Publishing, Rome-Italy, pp.135-143.

28. ISO/IEC FDIS 27001, (2005). Information technology Security techniques Information security management systems Requirements, pp.1-34.

29. James Rees (2010). The challenges of PCI DSS compliance, Computer Fraud & Security journal, pp.14-16.

30. J.F. Van Niekerk, R. Von Solms (2010). Information security culture: A management perspective, computer and security journal, pp.476-486.

31. Jing Liu, Yang Xiao, Hui Chen, Suat Ozdemir, Srinivas Dodle and Vikas Singh (2010). A Survey of Payment Card Industry Data Security Standard, pp.287-303.

32. Joobin Choobineh, Gurpreet Dhillon, Michael R. Grimaila, Jackie Rees (2007). Management of Information Security: Challenges and Research Directions, Communications of the Association for Information Systems Volume 20, pp.958-971.

33. J. Stuart Broderick (2006). ISMS, security standards and security regulations information security technical report, Strategic Consulting and Symantec Corporation, Central Parkway North, San Antonio, United States, pp.26-31.

34. Juhee Kwon and M. Eric Johnson (2012). Security resources, capabilities and cultural values: Links to security performance and compliances: Center for Digital Strategies, Tuck School of Business, Dartmouth College, pp.1-34.

35. Karin Höne2 and, J.H.P. Eloff (2002). What do international information security standards say? Department of Computer Science Rand Afrikaans University Elsevier Science Ltd, pp.202-409.

36. Kenneth J. Knappa, R. Franklin Morris, Jr.b, Thomas E. Marshallc, Terry Anthony Byrdc, (2009). Information security policy: An organizational-level process model computers & security, pp.493-508.

37. Kerry-Lynn Thomson, Rossouw von Solms, (2005). Information security obedience: a definition, Computers & Security, Department of Information Technology, Port Elizabeth Technikon, Private, South Africa, pp.69-75.

38. Marinela Vrîncianu and Liana Anica Popa (2010). Consideration regarding the security and protection of e-banking services consumers interest, Academy of Economic Studies, Bucharest, Romania, pp.388-403.

39. Martin Bradley and Alexander Dent (2010). Payment Card Industry Data Security Standard (PCI DSS) –What it is and its impact on retail merchants, Royal Holloway Series, pp.16-19.

40. Mariana Gerber, Rossouw von Solms, (2005). Management of risk in the information age, Computers & Security, pp.16-30.

41. Mario Spremic (2011). Standards and Frameworks for Information System Security Auditing and Assurance, Proceedings of the World Congress on Engineering Vol I London, U.K.pp.978-988.

42. Marwane El Kharbili1, Sebastian Stein1, Ivan Markovic, Elke Pulvermüller (2008). Towards a Framework for Semantic Business Process Compliance Management, IDS Scheer AG, ARIS Research Altenkesseler Saarbrücken, Germany, pp.1-15.

43. Mete Emina_gao_glu, Erdem Uc, Sxaban Eren (2009). The positive outcomes of information security awareness training in companies A case study, information security technical report, pp.223-229.

44. Michael Workman a, William H. Bommer b, Detmar Straub (2008). Security lapses and the omission of information security measures: A threat control model and empirical test, Computers in Human Behavior, pp.2799-2816.

45. Mikko Siponen , Robert Willison (2009). Information security management standards: Problems and solutions, Information & Management, University of Oulu, Finland and Copenhagen Business School Denmark, pp.267-270

46. Mohammed Arif Shaikh (2014), Ethiopian Banker's Perception of Electronic Banking in Ethiopia – A Case of Adama City, International Journal of Scientific and Research Publications, Volume 4, pp.1-7.

47. M.T. Dlamini, J.H.P. Eloff, M.M. Eloff,(2009). Information security: The moving target, computers & security, pp.189-198.

48. Munirul Ula, Zuraini bt Ismail and Zailani Mohamed Sidek (2011). A Framework for the Governance of Information Security in Banking System, Journal of Information Assurance & Cyber security, pp.1-12.

49. Nan Feng , Harry Jiannan Wang, Minqiang Li (2014). A security risk analysis model for information systems: Causal relationships of risk factors and vulnerability propagation analysis, Information Sciences, pp.57-73.

50. Nicolas Racz, Edgar Weippl, Andreas Seufert (2010). A process model for integrated IT governance, risk, and compliance management Vienna, Institute for Software Technology, pp.1-15.

51. Phil Pinder (2006). Preparing Information Security for legal and regulatory compliance information security technical report, pp.32-38.

52. Norris Syed Abdullah, Marta Indulska ,Sadiq Shazia (2009). A study of compliance management in information systems research, Association for Information Systems, European Conference on Information Systems, pp.1-11.

53. Raees Khan (2010). Practical Approaches to Organizational Information Security Management, SANS Institute Info Security, pp.1-15.

54. Rajpreet Kaur Jassal, Ravinder Kumar Sehgal (2013). Online Banking Security Flaws: A Study, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, pp.1016-1021.

55. Ram L. Kumar, Sungjune park, and Chandraseker Subramaniam(2008). Understanding the Value of Countermeasure Portfolios in Information Systems Security, Journal of Management Information Systems, Vol. 25, pp.241-279.

56. Robert Rowlingson, Richard Winsborrow (2006). A comparison of the Payment Card Industry data security standard with ISO17799 computer security and fraud journal, pp.16-19.

57. Rossouw von Solmsa, S.H. (Basie) von Solms (2006). Information Security Governance: A model based on the Direct Control Cycle, computers and security Nelson Mandela Metropolitan University, South Africa, University of Johannesburg, South Africa, pp.408-412.

58. PCI DSS Quick Reference Guide 2010. Understanding the Payment Card Industry Data Security Standard version 2.0, PCI Security Standard Council, pp.1-34.

59. Quey-Jen Yeh, Arthur Jung-Ting Chang (2007). Threats and countermeasures for information system security: A cross-industry study, Information & Management, pp.480-491.

60. P. S. Lokhande, B. B. Meshram, (2013). E-Commerce Applications: Vulnerabilities, Attacks and Countermeasures, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, pp.499-509.

61. Qingxiong Ma Allen, C. Johnston, J. Michael Pearson, (2008). Information security management objectives and practices: a parsimonious framework, Information Management & Computer Security, Vol. 16, pp.251-270

62. Shaun Posthumus, Rossouw von Solms (2004). A framework for the governance of information security Computers & Security, Port Elizabeth Technikon, Department of Information and Technology, South Africa, pp. 638-646.

63. Shemeles G.medhin Kassa(2016), Ethiopian Banking Industries Readiness for Information Systems Audit, Ethiopian Bankers Association, Addis Ababa, Ethiopia pp. 1-27.

64. Shi-Ming Huang Chia-ling Lee Ai-Chin Kao, (2006). Balancing performance measures for information security management, Industrial Management & Data Systems, Vol. 106, pp. 242-255.

65. S.H. (Basie) von Solms (2005). Information Security Governance Compliance management vs operational management, Computers & Security, Academy for Information Technology, University of Johannesburg, Auckland Park, Johannesburg, South Africa, pp. 443-447.

66. Shuchih Ernest Chang, Chin-Shien Lin, (2007). Exploring organizational culture for information security management, Institute of Electronic Commerce, National Chung Hsing University, pp.1-34.

67. Shuchih Ernest, Chang Chienta, Bruce Ho, (2006). Organizational factors to the effectiveness of implementing information security management, Industrial Management & Data Systems, Vol. 106, pp.345-361.

68. Steve A. Purser (2004). Improving the ROI of the security management process, Computers & Security, pp 542-546.

69. Tejinder Pal Singh Brar, Dr. Dhiraj Sharma, Dr. Sawtantar Singh Khurmi (2012). Vulnerabilities in e-banking: A study of various security aspects in e-banking, International Journal of Computing & Business Research.

70. Tejaswini Herath , Hemantha Herath & Wayne G. Bremser (2010). Balanced Scorecard Implementation of Security Strategies: A Framework for IT Security Performance Management Information Systems Management, pp.72-81.

71. Thanet Aksorn, B.H.W. Hadikusumo, (2008). Critical success factors influencing safety program performance in Thai construction projects, Safety Science, pp.709-727

72. Tim Kayworth, Dwayne Whitten, (2012). Effective Information Security Requires a Balance of Social and Technology Factors Research Paper No. 2012-52, Mays Business School Texas A&M University, pp.163-175.

73. Usman Munir, Irfan Manarvi, (2010). Information Security Risk Assessment for Banking Sector-A Case study of Pakistani Banks, Global Journal of Computer Science and Technology, Vol. 10, pp.44-55.

74. Yaman Roumania, Joseph K. Nwankpab, Yazan F. Roumani (2016). Examining the relationship between firm's financial records and security vulnerabilities International Journal of Information Management, pp.987-994.

75. Zachary B. Omariba, Zachary B. Omariba, Dr. G. Wanyembi (2012). Security and privacy of electronic banking, International Journal of Computer Science Issues, Vol. 9, pp. 432-446.

76. Zahoor Ahmed Soomro, Mahmood Shah, Javed Ahmed Lancashire, (2016). Information security management needs more holistic approach: A literature review, international journal of information management, pp.215-225.

77. Zhi Xian Ng, Atif Ahmad, Sean B. Maynard (2013). Information Security Management: Factors that Influence Security Investments in SMES, Australian Information Security Management Conference, Edith Cowan University, pp.60-73.

APPENDIX A: Questionnaire

Questionnaire on Assessment of the effectiveness of Information Security Management in the Financial Sector: Card Banking Security in Focus

Dear Respondent,

I am Daniel G.hawariat, a postgraduate student. Currently, I am attending Master of Science in Information Science at Addis Ababa University, Ethiopia.

As part of my accomplishment for the program, my research lies on assessing the effectiveness of Information Security Management in the financial sector focusing on card banking security and identifying factors prohibiting the effectiveness of information security management towards Payment Card Industry Data Security Standard (PCI-DSS).

Therefore, this is to kindly ask you to participate in the survey that needs data from your esteemed bank to assess the issues in relation to Information Security Management.

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

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

If you require any assistance or clarification, please don't hesitate to contact me through either of the following methods. Mobile **251-911-11-95-17** or Email: **danihawari@gmail.com**

Thank you for your willingness to participate in this study.

Please fill the blanks and put" ✓ " sign to the box

I. Respondent Information

1. Job Area/Specialty:

☐ Network ☐ Security ☐ Application ☐ Database ☐ IT Management ☐ Other Specify

2. Qualification: ☐ Bachelor Degree ☐ Master's Degree ☐ PhD

3. Work experience:

☐ Less than 5 years ☐ 6-10 years ☐ 11-15 years ☐ More than 15 years

4. Do you have any security related certifications

☐ Yes ☐ No

If Yes, Please specify_____

II. Organizational Information

5. Name of the Organization:

☐ XYZ S.C ☐ Bank ABC

6. Is your organization certified to any International Information Security Management standard:

☐Yes ☐ No

If yes, please choose:

☐ ISO2701 ☐ PCI-DSS ☐ COBIT ☐ ITIL ☐ Other Specify_____

7. Is there any plan towards one of these certifications?

☐Yes ☐ No

If yes, please choose: PCI-DSS

III. Current State of Information Security Management

NO.	Security scoping	Your perception on the degree that the statement holds for your organization				
		Very high	High	Medium	Low	Very Low
1	There is up-to-date Inventory of devices which includes model of device, location of device, device serial number or other method of unique identification as part of Asset Identification, Classification (Asset Management).					
2.	There are Data flow, Architecture diagrams that explains end to end connectivity, of storing, processing and transmission of ATM transaction, POS Transaction, reconciliation, settlement, debit card issuance and fraud management in the scope.					
3	There is a detailed network diagram(s) that covers all boundaries in scope including network segmentation, boundaries between trusted and un-trusted networks, wireless (if available) and wired networks , types of devices, device interfaces, protocols and security controls.					
NO.	**Media and Facilities Security**	**Your perception on the degree that the statement holds for your organization**				

		Very high	High	Medium	Low	Very Low
4	Removable medias containing sensitive information is properly labeled and protected against unauthorized access at all times.					
5	All medias containing sensitive information are destroyed using secure procedure when it is no longer needed for business or legal reasons according to the Retention policy					
6	There is a procedure to easily distinguish between onsite personnel and visitors (for example, assigning badges)					
7	There are entry controls to limit and monitor physical access to systems using video cameras and/or access control mechanisms that monitors individual physical access to sensitive areas.					
NO.	**Network and Security**	**Your perception on the degree that the statement holds for your organization**				
		Very high	High	Medium	Low	Very Low
8	There is a semi-annual firewall and router rule set review carried out by the team with the necessary credential and knowledge.					

9	There is anti-spoofing and state full inspection or equivalent settings enabled on external firewall and/or router.					
10	There is a comprehensive Vulnerability Assessment and penetration test conducted regularly to verify the security of the whole company's perimeter.					
11	Higher environments (i.e. production) are logically separated/segmented from lower environments (such as test/development).					
12	Deployed security system monitors and responds to any networks intrusions, vulnerabilities, hacking or any irregularities behaviors on 24/7 basis.					
13	There is justification for use of all services, protocols, and ports allowed, including documentation for security features implemented for those protocols considered to be insecure. Examples of insecure services, protocols, or ports including FTP (File Transfer Protocol), Telnet, POP3 (Post Office Protocol), IMAP (Internet Message Protocol), and SNMP (Simple Network Management Protocol) v1 and v2.					
14	Personal firewall software runs appropriately and configured not to be disabled by the user on any employee-owned devices (e.g. laptops) that connects to access the internal network and the internet when outside					

	the network.					
15	Internal and external network vulnerability scans run at least quarterly and after any significant change in the network (new system component installations, changes in network topology, firewall rule modifications, product upgrades.					
16	There is a quarterly wireless scanning and analysis activity that identifies authorized/unauthorized nature of the access point.					
17	There is a quarterly wireless analyzer reports along with details of authorized/unauthorized nature of the access point.					
NO.	**Application Security**	**Your perception on the degree that the statement holds for your organization**				
		Very high	High	Medium	Low	Very Low
18	There is secure software development process document in accordance with industry best practices.					
19	All system components and software are protected from known vulnerabilities by installing applicable vendor supplied security patches and critical security patches within one month of release.					

20	There is a log monitoring tool deployed to review security events for all system components and to identify anomalies or suspicious activity in a daily basis.					
21	There is a change detection mechanism deployed (including file integrity monitoring tools) to alert unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons.					
NO.	**Card Data Security and Encryption**	**Your perception on the degree that the statement holds for your organization**				
		Very high	High	Medium	Low	Very Low
22	The current network diagram identifies all connections between cardholder data environment and other networks, including any wireless networks and show cardholder data flows across systems and networks.					
23	There is a retention period and process for secure data deletion based on the retention period which includes PAN (Primary Account Number), Track, CVV (Card Verification Value) and PIN (Personal Identification Number) in all locations within cardholder data environment (CDE) and outside the CDE.					
24	There is no unprotected PAN (Primary Account Number) transmission by end-user messaging technologies (e-mail,					

	instant messaging, chat, etc.					
25	There is a use of strong cryptography and security protocols such as TLS (Transport Layer Security), IPSEC (IP Security), SSH (Secure Socket Shell), etc to safeguard sensitive cardholder data during transmission over open, public networks.					
26	PAN (Primary Account Number), is masked (the first six and last four digits are the maximum number of digits to be displayed) when displayed on the database, application servers and on hard copy.					
27	There are encryptions for all non-console administrative access and web-based management using strong cryptography technologies such as SSH (Secure Socket Shell), VPN (Virtual Private Network), or TLS (Transport Layer Security).					
28	All sensitive information is encrypted properly whenever it is stored or transmitted over all networks (either internally or externally).					
29	There is a formal security awareness program to make all personnel aware of the importance of card data security upon hire at least annually that they have read and understood the security policy and procedures.					

30	Access to system components and cardholder data is limited only to those individuals whose job requires such access.					
NO.	**Logging and Monitoring**	**Your perception on the degree that the statement holds for your organization**				
		Very high	High	Medium	Low	Very Low
31	Time synchronization technology (NTP) is in use to synchronize all critical system clocks and times and ensure that critical systems have the correct and consistent time received from industry-accepted time sources.					
32	Password management systems are interactive and do enforce a quality password.					
33	There is a formal user registration process assigning and revoking access and access rights to systems and services, and accesses rights are regularly reviewed, and removed upon termination of employment.					
34	Vendor-supplied defaults accounts removed before connecting to the network including Operating Systems, network devises, application, security devises, point-of-sale (POS) terminals etc.					

35	There is a procedure to process and monitor inactive users for 90 days for all platforms in scope and user deletion during termination.					
36	There is a logical access control for account and password features including: account lockout policy, account lockout duration, session timeout policy, password length, password complexity, Password history and Password expiry configured for all the assets.					
NO.	**Policy and Procedure**	**Your perception on the degree that the statement holds for your organization**				
		Very high	High	Medium	Low	Very Low
37	The organization developed and communicated, as appropriate, to all employees a written information technology security policy that complies with international standards such as ISO/IEC 17799.(Policy and Procedure)					
38	Information security policy review take place in response to any changes affecting the basis of the original risk assessment e.g. significant security incidents, new vulnerabilities or changes to the organizational infrastructure.					
39	There is a user access creation, user access deletion, user access modification form/procedure for the platform in					

	the scope.					
40	There is a structured change management process for firewalls, routers, servers, application, etc. while there is a new configuration or upgrade in place.					
41	Information security risk assessments are performed and documented at planned intervals and/or when significant changes occur.					
42	There is an organization chart (or equivalent documentation) which clearly outlines the information security roles and responsibility for all personnel. (Including Structure , Reporting line , Roles and Responsibilities for Information Security)					
43	There are appropriate policies and procedures related to software licensing, development, selection, specification, acquisition, testing, introduction, migration & disposal in place.					
44	There is a backup and recovery policy and procedure documented, tested, and updated regularly for all application level data.					
45	There is an established incident response policy and escalation procedure to respond immediately to a system breach.					

NO.	**Anti-Malware**	**Your perception on the degree that the statement holds for your organization**				
		Very high	High	Medium	Low	Very Low
46	There is prevention and detection system IPS (Intrusion Prevention) or IDS (Intrusion Detection System) deployed with up-to-date signature and version to detect and/or prevent intrusion.					
47	Anti-virus programs are deployed and are capable of detecting, removing and protecting against all known types of malicious software and viruses.					
48	All anti-virus mechanisms are kept current, actively running, perform periodic scans, generate audit logs and cannot be disabled or altered by the users.					

Thank You for your time

APPENDIX B: Observation Checklist

1. Observe to make sure that policy and procedures are prepared as per the international standard, documented and in use in a day to day basis.

2. Observe the detailed network diagram(s) , Whether it covers all boundaries in scope including network segmentation, boundaries between trusted and un-trusted networks, wireless (if available) and wired networks , types of devices, device interfaces, protocols and security controls.

3. Observe shredding or cross-cut process of sensitive information and make sure as cardholder data and other sensitive information cannot be reconstructed.

4. Observe as the current and maintained diagram shows all cardholder data flows across systems and networks.

5. Observe if public access between the Internet and any system component in the cardholder data environment is prohibited and DMZ (demilitarized zone) is properly implemented.