An examination of the extent of implementation of the information security system and IT audit system in Ghananian Banks

Sylvester Hatsu
Department of Computer Science, Accra Polytechnic Accra, Ghana

Martin B. Ujapka
Ghana Technology University College (GTUC), Takoradi Campus

Enoch D. Mpimwood,
Ghana Technology University College (GTUC), Takoradi, Campus

Abstract
The study examined the impact of information security and information technology (IT) audit in selected banks in Ghana. The study specifically, ascertained the degree of exposure to threats, it examined the extent of implementation of information security and IT audit system in the bank to protect information from threats, determined the impact, the performance and finally identified the challenges of the banks in managing information security system. A structured questionnaire was used as the main research instrument. Four banks were selected for the study, including two local and two foreign banks. A total of 20 employees (5 from each) were sampled from the Headquarters of each bank in Accra. Only managers, IT managers, and Risk managers were sampled. The study found that the sampled level exposure of banks to threats to information systems is low. Local banks were however more exposed to threats than foreign banks. Largely the banks managed threats to information system by implementing strategies, including having an information security policy, information security organization, asset and human resource security system, information access control IT Audit system. The performance of banks in information system was moderate. Information security and IT audit system had correlated positively to the overall performance of the banks. Availability of information security policy has significant positive impact on bank performance. The study encouraged the banks to improve upon their information security and IT audit practices to ensure improvement in the performance of the banks in information security management.

Keywords: Employee, Technology, Audit,Management

1.0 Introduction

1.1 Background of the study

Rapid strides in Information Technology (IT) and its swift adoption by the commercial banks have enabled banks to use IT extensively to offer products and services to customers apart from automating internal processes. Some opportunities arising from the intensive use of IT are multiple delivery channels to customers, development of new products and processes, reduction in service delivery costs and potential for financial inclusion initiatives. Developments in IT have also brought along a whole set of challenges to deal with. Rapid changes in technology, complexities, high costs, security and data privacy issues, new laws and regulations and inadequacy of trained manpower are some challenges faced by banks. Inadequate IT controls could result in cyber frauds and poor implementation of technology could lead to unsound decision making based on inaccurate information/data. There is therefore the need for banks to implement an information security system in order to safeguard information systems. Information security, according to the International Standards Organization (ISO), is the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities" (ISO-27002, 2005). Information security management involves planning for and implementing a structure as well as the processes that provide for the alignment of an information security strategy with business objectives and applicable laws and industry standards (Bowen, Hash, & Wilson, 2006).

The ISO Information technology Security techniques (ISO-27002, 2005) observes that information security is becoming increasingly more important for both public and private sector businesses, especially in the banking sector as the interconnection of networks and the sharing of information resources to increase the complexity of controlling access and preserving the confidentiality, integrity, and availability of data. According to Ross, et al.

(2007), information security is crucial for information systems, and is central to the survival of a company. Banks in Ghana therefore need to have information security measures in order to avoid collapse. IT Audit, on the other hand, is the process of collecting and evaluating evidence to determine whether a computer system has been designed to maintain data integrity, safeguard assets, allow organizational goals to be achieved effectively, and uses resources efficiently. Data integrity relates to the accuracy and completeness of information as well as its validity in accordance with the norms. An effective information system leads the organization to achieve its objectives and an efficient information system uses minimum resources in achieving the required objectives. The IT Auditor must know the characteristics of users of the information system and the decision making environment in the auditee's organization while evaluating the effectiveness of any system.

1.2 Problem Statement

The banking sector in Ghana is one of the most important financial sectors in the country. Investment in security technology; E-business is generated widely in this financial sector. A considerable range of information and transactions is exchanged internally; among employees and externally; among other banks of concern. On the other hand, such information is communicable with customers as well. The banks also exposed to various threats in the form of cyber fraud, hacking etc. according to Schneier (2004), the threats to organizational information and information systems are increasing in occurrence and in complexity and emphasizes the urgency for organizations to learn how to better protect their information and information systems. The Basel Committee on Banking Supervision (1998) expects such risks to be recognized, addressed and managed by banking institutions in a prudent manner. Given the instances of cyber fraud in banks, it is necessary to improve controls and examine the need for proactive fraud risk assessments and management processes in commercial banks. There is therefore the need for the bank to implement and audit information security to guard against risks to information and to enhance the performance of the bank. The impacts of information security and information audit on banks have been investigated by researchers (Mansour & Nayelf, 2013; Buchanan & Gibb, 2008). The studies have found that general controls of information systems auditing in general are usually applied by the bank and that there is a significant relationship between general controls of information systems auditing and information systems performance, and general controls of information systems auditing has a significant impact on information systems performance. However, literature search found virtually no literature on the impact of information security and IT audit in Ghana. The current is an attempt to bridge this knowledge gap.

1.3 Objectives of the study

1.3.1 Main objective

The main objective of the study is to assess the impact of information security and information technology audit in the banking sector of Ghana.

1.3.2 Specific Objective

i. To ascertain the degree of exposure to threat on information systems in the banking sector of Ghana
ii. To examine the extent of implementation of the information security system and IT audit system by the banking sector to protect information from threats
iii. To determine the impact of the information security system on the performance of information security systems in the banking industry
iv. To identify the challenges of the banks in managing information security system.

1.4 Research Question/ Hypothesis

1.4.1 Research questions

i. What is the degree of exposure to threat on information systems in the banking sector in Ghana?
ii. What is the level of adequacy of the information security system and IT audit system put in by the banking sector to protect information from threats?
iii. What is the impact of the implementation of the information security system on the performance of information security systems in the banking industry?
iv. What challenges hinder effective implementation of the information security system and IT audit among banks in Ghana.

Literature Review

2.1 Introduction

The chapter reviews literature on the concept of information security and it evolution, undertake an overview of threats and vulnerability to information system, risk assessment, organisational barriers to implementation of information security strategies, critical elements to information security strategies and performance evaluation of information system.

2.2 Concept of information security system

An Information system is viewed as a group of components that interact to produce information" (Kroenke, 2007), also an information system collects, processes, stores, analyzes, and disseminates information for a specific purpose. While Computer-based information system is an information system that uses computer technology to perform some or all of its intended tasks (Turban and others, 2006), information systems exist to help business achieve their goals and objectives, as we know the business themselves do not do anything and it cannot act. It is the people within a business who sell, buy, design, produce, finance, market, account, and manage. So information systems exist to help people who work in a business to achieve the goals and objectives of that business (Kroenke, 2007). The basic components of information system are: hardware, software, database, networks, procedures, and people (Turban and others, 2006).

3.0 Methodology

3.1 Introduction

This chapter describes the methodology used to achieve the research objectives. It encompasses the research design of the study, the population and sampling that is, the target population, sample size; and sampling techniques adopted. It also involves the sources of data, the data collection instrument and the data collection method. The chapter also gives indication of how the data collected is analysed.

3.2 Research Design

A research design provides the basic directions for conducting the project. In particular, a research design should provide relevant information that will most efficiently and effectively address the research questions or hypotheses (Hair et al., 2007). Hair suggested that there are three distinct research designs: exploratory; descriptive; and causal (explanatory).This study is also exploratory, descriptive and explanatory. Franke et al., (2008) stated that "the descriptive method of research is to gather information about the present existing condition." The rationale for adopting the descriptive method was to give a clear picture by describing the level of exposure of the banks to information threats/risk, and also to describe the extent of implementation of the information security system and IT audit in the banking industry.

Explanatory studies also seek to provide vivid explanation for the causes and or effects of one or more variables (Saunders, Lewis, & Thornhill, 2009). The study is also explanatory because it sought to examine the impact of information security and IT Audit on the performance of information systems of banks. The study quantitative data gathered through the use of a structured questionnaire was used to achieve the purpose of the study. Descriptive and inferential statistics were used to analyse the data.

3.3 Population and Sampling

According to Hair et al. (2007) representative samples are generally obtained by following a set of well-defined procedures, which are: defining the target population; selecting a sampling method; and determining a sample size. Therefore, as recommended by Hair et al. (2007), this section briefly explains the study's approach to these three main procedures for selecting the representative sample.

3.3.1 Target Population

According to Huysamen (1990), a population as encompassing "the total collection of all members, cases or elements about which the researcher wishes to draw conclusions. The study's population of interest was all the employees of foreign and local banks in Ghana.

3.3.2 Sample Size

According to Saunders et al. (2009), the size of the sample and the way in which it is selected will definitely have implication for the confidence in data collected and the extent to which it can be generalized. The study included 4 banks, 2 local banks and 2 foreign banks. 5 employees were selected from each of the banks making 10 employees of the each category of banks (local and foreign) giving the overall sample size of 20 respondents. The sampled respondents included general managers, risk managers, and IT managers.

3.3.3 Sampling Technique

Non-probability sampling techniques were adopted. Purposive sampling technique was used to select the employees of the bank. Purposive or judgmental sampling allows the researcher to use his judgment to select cases that will best enable the researcher to answer the research questions in order to achieve the objectives (Saunders et al, 2009). This was used because there are a limited number of people that have expertise in the area of study. The selection of the sample was also convenient because only the target group of respondents who were willing to participate in the study were sampled.

3.4 Data Collection Instruments

According to many scholars, in the use of survey strategy, the main instruments used are self-administered/interviewer administered or structured/unstructured interviews and questionnaire or a combination of both (Saunders et al, 2009). In this study, a structured questionnaire was used as the primary research instrument.

3.4.1 Design of the Questionnaire

The questionnaire was structured in five sections (A-E)

Section A examined the demographic profile of the respondents. The demographic profile of the respondents included items such as: gender, age, level of education, position held in the bank, and job tenure. **Section B** measured the degree of exposure to threat on information systems in the banking sector in Ghana. Items were measured on Five-point Scale: 1=Very low; 2=Low; 3=Moderate; 4=High; 5=Very High. The threats to information included Natural threats, human threats and environmental threats. **Section C** examined the extent of implementation of information security and IT audit by the banking sector to protect information against threats. Items were measured on a Five-Likert Scale 1=strongly disagree; 2=Agree; 3=Neutral; 4=Agree 5=Strongly agree. The items in this section were based on the According to International Standards Organization ISO-27002 Security Technique's principles for initiating, implementing, maintaining, and improving information security in public and private organizations (ISO-27002, 2005). **Section D** evaluated the performance of the information security system of the selected banks. Items were measured on Five-point scale: 1=Very low; 2=Low; 3=Moderate; 4=High; 5=Very High. Items included: increase financial performance, increased operational efficiency, quality of information outputs etc. **Section E** identified the challenges of the banks in managing information security system.. Items were measured on a Five-Likert Scale 1=strongly disagree; 2=Agree; 3=Neutral; 4=Agree 5=Strongly agree. Items in the questionnaire.

3.4.2 Validity and Reliability of Research Instrument

Reliability and validity tests are important to ensure the accuracy and consistency of the variables. According to Hair et al. (2007) for a scale to be reliable the questions must be answered consistently by respondents in a manner that is highly correlated. If they do not, the scale would not be reliable. For the purpose of this research, the reliability of the questionnaire was determined through Chronbach alpha (α). This method allows for the calculation of the coefficient if one variable is removed from the original set, making it possible to identify the subset that has the highest reliability coefficient. If all the results are above 0.7, the scales are judged to be reliable (Sousa et al., 2006). However Hair et al. (2007) stated that lower coefficients may be acceptable depending on the research objectives. For example, Nunnally (1978) suggested that alpha coefficients of 0.50 to 0.60 are deemed acceptable for exploratory research. Reliability and validity were again ensured through the following measures; using my supervisor to evaluate the research instruments for conceptual clarity. This was to improve the content, layout, sequence and instructions on the questionnaires. Content validity was ensured by IT experts.

3.4.3 Data Collection

The survey questionnaires were distributed to the target respondents through face-to-face. Ample time (about 2weeks) was allowed for the respondents to complete the questionnaire. The completed questionnaires were retrieved through personal contact for data processing and analysis.

3.5 Data Analysis

In this research, data analysis is done by using both descriptive inferential statistics. Descriptive statistics such as frequency, mean, and standard deviations were used to present the findings of the study. The mean value represents the average response of all respondents, while the standard deviation represents the spread of the responses on the scale. Correlation and regression methods were used to examine the impact of information security and IT audit on the overall performance of information system of the banks. Kendall‘s tau correlation coefficient was used. Kendall‘s tau correlation coefficient is a non-parametric test because the response of variables was measured on a five-point scale. The two most widely used non-parametric correlation analysis tests are the Spearman‘s rank correlation coefficient (Spearman‘s Rho) and Kendall‘s rank correlation coefficient (Kendall‘s tau). Bryman and Cramer (2001) argue that Spearman's rho is more commonly used. On the other hand, tau deals with tied ranks (i.e. Two or more respondents are in the same rank) better than rho. Since there is existence of tied ranks (eg. more than one IT officials, or risk managers) in data of this study, Kendall‘s tau is chosen to be the statistical method for hypothesis testing. Moreover, this method has been commonly used in previous researches (Abdel-Maksoud et al., 2005; and Hutaibat, 2005). In terms of the value of a measure of association, Botsch (2011) provides a guideline specifically for Kendall‘s tau is as follows:

- Less than + or – 0.10: very small/weak
- + or – 0.10 to 0.19 : small/weak
- + or -0.20 to 0.29 : moderate
- + or -0.40 or larger : strong

Also, the multiple regression method was used to examine the impact of information security and IT audit systems on the overall performance of the banks in information security systems. Data analysis was done with the help of the statistical software of Statistical Product and Service Solutions (SPSS Version, 20).

Presentation and Interpretation of Findings

4.1 Introduction

This chapter presents the results of the analysis of the data gathered from the field of study. It starts with the demographic profile of the respondents. Section 4.3 determines the degree of exposure to threats on information systems in the selected bank; Section 4.4 examines the extent of implementation of the information security system and IT audit system by the banking sector to protect information from threats. Section 4.5 determines the impact of the information security system on the performance of information security systems in the banking industry. Section 4.6 identifies the challenges of the banks in managing information security system

4.2 Demographic Profile of Respondents

This section presents the demographic characteristics of the respondents who were Employees of the four selected banks. The profile of the respondents included; gender, age, educational background, position held, and tenure of work.

4.2.1 Gender Distribution of Respondents

Regarding the gender distribution of the 20 respondents (Table 4.1), majority, and 60.0% (n=12) were males while the remaining, 40 % (n=8) represented females. This means that there were more male employees who were willing to respond to the questionnaires than their female counterparts.

Table 4.1: Gender Distribution of Respondents

Category	Number	Percent
Male	12	60.0
Female	8	40.0
Total	20	100.0

Source: Field Survey Data, 2014

4.2.2 Age Distribution of Respondents

With regard to the age distribution of the 20 employees of the banks (Table 4.2), a majority, 45% (n=9) were within the age group of 20-39years. This was followed by those who were between 30-39 years of age. This group constituted 30% (n=6) of the respondents. Also, while 20% (n=4) on the respondents were 40-49years of age, only one of the respondents was 50 years and above. All the respondents were 20 years and above. The implication is that the respondents were matured enough to indicate their decision to participate in the study.

Table 4.2: Age Distribution of Respondents

Category	Number	Percent
20-29 years	9	45.0
30-39years	6	30.0
40 - 49 years	4	20.0
50yrs and above	1	5.0
Total	20	100.0

Source: Field Survey Data, 2014

4.2.3 Educational Qualification

In examining the educational qualification of the employees of the selected banks as shown in Table 4.3, a majority, 70% (n=14) had the First Degree/Professional certificate qualification, 15% (n=3) held a Masters' degree qualification and the remaining 15% (n=3) held a Diploma qualification. Overall, all the respondents had Diploma qualification or higher academic qualification. This has implication of the ability of the respondents to read and understand the issue of E-banking risk management under investigation.

Table 4.3: Educational Qualification

Category	Number	Percent
Diploma	3	15.0
Degree/Professional	14	70.0
Masters/PhD	3	15.0
Total	20	100.0

Source: Field Survey Data, 2014

4.2.4 Position Held in the bank

Out of the 20 respondents, 55% (n=9) indicate they were IT managers, 25% (n=5) were risk managers, and the remaining 20% (n=4) were the general managers. This distribution is presented in Table 4.4 below

Table 4.4: Position Held in the bank

Category	Number	Percent
General Manager	4	20.0
Risk manager	5	25.0
IT manager	11	55.0
Total	20	100.0

Source: Field Survey Data, 2014

4.2.5 Job Tenure

Respondents were also asked to state how long they had been working with the bank and the following responses were found (Table 4.5): 55% (n=11) had between 1-5years of working experience in the banks, 35% (n=7) had 6-10 years working experience, and finally 10% (n=2) had between 11-15years working relationship with their banks. On the average, the respondents were found to have 1-5 years of working experience with their banks. The implication is that respondent had enough time to have witnessed E-banking risk and the practice E-banking in their bank.

Table 4.5: Job Tenure

Category	Number	%
1-5yrs	11	55.0
6-10yrs	7	35.0
11-15yrs	2	10.0
Total	20	100.0

Source: Field Survey Data, 2014

4.3 Degree of exposure to threat on information systems

The first specific objective of the study was to ascertain the degree of exposure to threat on information systems in the banking sector of Ghana. This objective was achieved by measuring the level of exposure using a Five-Point Scale and the output shown in Table 4.8 below. Mean and standard deviations were used to present the findings.

Table 4.6: Degree of Exposure of E-banking risk among selected banks

	Respondents						
	1	2	3	4	5	Mean	Stdev
Human threats (e,g hacking)	35.0	30.0	35.0	0	0	2.00	0.85
Environmental threats (e.g., power failure, fire outbreak)	35.0	35.0	30.0	0	0	1.95	0.82
Natural threats (floods, earthquakes, tornadoes, landslides, avalanches, electrical storms)	35.0	45.0	20.0	0	0	1.85	0.74
Overall level of exposure to information threat						1.95	0.74

Source: Field Survey Data, 2014
Scale: 1= very Low; 2=Low; 3=Average; 4=High; 5=Very high

The findings revealed that the degree of exposure to information threats in the selected bank was low to very low (Mean: 1.00-2.99). Low (Mean; 2.00-2.99) rating was found for human threat (hacking). However, the very low exposure rating was given to threats to information systems such as environmental threats (e.g., power failure, fire, outbreak) (Mean=1. 95, Stdev=0. 82), and natural threats (floods, earthquakes, tornadoes, landslides, avalanches, electrical storms) (Mean=1.85, Stdev=0.74). Overall, the degree of exposure to information threats by the sample bank was very low (Mean=1.95, Stdev=0.74). This implication had some threat to their information system by the level of exposure of the threats is very low.

Table 4.7 below compares the level of exposure to information systems by banks (local and foreign) in Ghana. Independent t-test was conducted to compare the difference of the level of exposure of the banks to information system threats.

Table 4.7: Comparison of the exposure information system threats banks

	Bank	N	Mean	Stdev	t-stat	Sig. (2-tailed)
Human threats	Local Bank	15	2.26	0.59	3.254	.003*
	Foreign bank	15	1.53	0.63		
Environmental threats	Local Bank	15	2.06	0.70	2.443	.021*
	Foreign bank	15	1.46	0.63		
Natural threats	Local Bank	15	2.00	0.92	1.160	.256
	Foreign bank	15	1.66	0.61		
Overall threats	Local Bank	15	2.46	0.83	3.207	.003*
	Foreign bank	15	1.60	0.63		

Source: Field Survey Data, 2014
***statistically significant at 5% significant level**

The output shows that, overall local banks are more exposed to information system threats that foreign banks (t=3.2.07, P<0.05). Of the types of information system threats, local banks had a significant higher exposure to human threats (t=3.254, P<0.05), and environmental threats (t=2.443, t<0.05) than the foreign banks.

4.4 Extent of implementation of information security system and IT audit system

The second objective of the study is to examine the extent of implementation of the information security system and IT audit system by the banking sector to protect information from threats. The information security and IT audit practices included in the study were in the areas of; Information security policy, organizing information security, asset and human resource security, information access control and IT Audit. The opinions of the respondents were measured using a five-point Likert scale. Therefore, Mean and standard deviations were used to present the results. Mean: 1.00-2.99-disagree, Mean: 3.00-3.99-Neutral, and Mean: 4.00-5.00-agree. The outcome of the finding is summarized in Table 4.8 below.

Table 4.8: Information security system and IT audit

	N	Mean	Stdev	Chronbach alpha
Information security policy	20	4.18	0.62	0.882
Organizing Information Security	20	4.21	0.64	0.878
Asset and Human Resource security	20	4.25	0.53	0.873
Information Access control	20	4.35	0.72	0.794
IT Audit	20	4.24	0.59	0.883
Information security and IT audit	20	4.25	0.62	

Scale; 1= Strongly Disagree, 2= Disagree, 3=Neutral, 4=Agree, 5=strongly agree

Information security policy

Table 4.8 presents the results of information security policy put in place by the selected banks to protect information from threats. The information security policy as implemented by the selected banks was (Mean=4.18, Stdev=0.62). This means that the respondents agreed (Mean: 4.00-5.00) that as part of the implementation of information security systems in the selected banks there was information security policy. That is, the respondent agreed that there was a clear definition of the vision and mission of information systems, there was a clear methodology for strategic planning for information systems linked to the overall strategy of the bank, the strategic plan identified key priorities for information systems, and resources that systems need, the information systems unit was involved in building and implement the overall strategy of the bank, the bank has information security team well trained and have good knowledge on their field, and that the bank policy consider information security system as important issue.

4.5 Organizing Information Security

The extent to which the bank organizes information security as part of the implementation of information security and IT audit system was found to be (Mean=4.2, Stdev=0.64). This means that the respondent also agreed that the bank organized information security as part of the implementation plan to information security and IT audit system to protect information against threats. That is, the respondent agreed that the banks ensured that information security goals are identified, meet the organizational requirements, and are integrated in relevant processes, the banks review the effectiveness of the implementation of the information security policy, the banks provide clear direction and visible management support for security initiatives, the banks provide the resources needed for information security, the banks initiate plans and programs to maintain information security awareness, and that the bank ensure that the implementation of information security controls is coordinated across the organization.

4.6 Asset and Human Resource security

The respondents also agreed that the bank implemented information security and IT audit system to include asset and human resource security system (Mean=4.25, Stdev=0.53). This implies that the respondents agreed that the banks undertake an asset inventory to include all information necessary in order to recover from a disaster (including type of asset, format, location, backup information, license information, and a business value), the banks undertake security screening and background checks of all its employees, and that there is information security awareness, education, and training with all essential components of human resource.

4.6.1 Information Access control

As part of the strategy to protect information system from threats, the respondent agreed that the bank implemented information security and IT audit system to include an information access control (Mean=4. 35, Stdev=0. 72). This means that the respondents agreed that the banks have information access control policy, the banks have information user access management, the banks have information network access control, the banks have operating system access control system, there is software application access control system, and that the banks have information access restriction system.

4.6.2 IT Audit System

Regarding the implementation of IT audit system in the banks, the respondents also agreed that the banks have implemented IT Audit in their outfit (Mean=4.24, Stdev=0.59). This implies that the bank undertake periodic security auditing to ensure validation of the controls of the system development life cycle, validation of access controls to installations, terminals and libraries, automation of internal auditing activities, internal training, and collaboration with external auditors.

4.7 Information security and IT audit system

Overall, it can be concluded that, largely, information security and IT audit systems are implemented in the selected banks (Mean=4. 25, Stdev=0. 62). Figure 4.3 shows the pictorial representation of the extent of implementation of information security and IT audit system in the selected banks

5.1 Summary

The purpose of the study was to examine the impact of information security and information technology (IT) audit in selected banks in Ghana. The study specifically, ascertained the degree of exposure to threat on information systems in the banking sector of Ghana, examined the extent of implementation of information security and IT audit system in the bank to protect information from threats, determined the impact of the information security system on the performance of information security systems, and finally identified the challenges of the banks in managing information security system.

The study used a quantitative approach to achieve its purpose. A structured questionnaire was used as the main research instrument. Items in the questionnaire were measured on a five-point ranking scale. Four banks were selected for the study, including two local and two foreign banks. A Total of 20 employees were sampled from Headquarters of each bank in Accra. Only managers, IT managers, and Risk managers were sampled. Descriptive statistics and inferential statistics were used to present the data. Regarding the level of exposure of the banks to threats of information system, the study found that the level of exposure of the selected bank to threats of all kinds to information such as human threat, environmental threats, and natural threats was low to very low. Overall, local banks are more exposed to information system threats than foreign banks (t=3.2.07, $P<0.05$).

Concerning the information security and IT audit system implemented by the banks to protect information from threats, the study found that the systems included information security policy, information security organization, asset and human resource security, information access control, and IT audit systems. Largely all these systems were implemented by the selected banks. With regard to the challenges of the banks in managing threats to information system, the study found that; high cost of investing information security controls, and the unpredictable nature of information security threats were identified as the main challenges.

5.2 Conclusions

Based on the findings of the study, it can be concluded that:

- Regarding the level of exposure of banks in Ghana to information system threats, it can be concluded the level of exposure of banks to threats to information systems is low. Local banks are however more exposed to threats than foreign banks.
- The performance of the bank's information security and IT audit is moderate. Information security and IT audit system have a positive relationship to the overall performance of information systems in the banks. Availability of information security policy has a significant positive effect on the overall performance of an information system.
- The selected bank has some challenges in managing threats to information system, including high cost of investing in information security controls, and the unpredictable nature of information security threats.

References

Allen, J. (2002). Guide to System and Network Security Practices

Bowen, P., Hash, J.,& Wilson, M.(2006). Information Security Handbook

BIS (2003). Risk Management Principles for Electronic Banking,

Canal, V.A. (2005, Sept). On Information Security Paradigms

Caralli, R. (2004). The Critical Success Factor Method: Establishing a Foundation for Enterprise Security Management

Caralli, R., Stevens, C., Wallen, D., White, W., Wilson,W., & Young, L. (2007). Improving theSecurity and Sustainability Processes

FFIEC (2005). Authentication in an Internet Banking Environment,

Hair, J. F., Anderson, R. E., Tatham, R. L. & Black, W. C. (2007). Multivariate Data Analysis (5th Ed.). Prentice-Hall International, Inc.

Harris, S. (2003). Certified Information Systems Security Professional (CISSP) All-In- One Exam Guide 2nd ed.
Harris, S. (2006). Risk Management: Key elements when building an information security Program.
Huysamen, G.K., (1990). Methodology for the Social and Behavioural Sciences. Southern Book Publishers.
Internet Banking and Technology Risk Management Guidelines, Monetary Authority of Singapore, MAS, 2008
ISF (2007). Standard of Good Practice for information security
Jenkins, G. (1999). Information Systems: Policies and Procedures Manual
Kissel, R. (Ed.) (2006). National Institute of Standards and Technology: Glossary of Key Information Security Terms
Krutz, R. & Vines, R. (2001). CISSP Prep Guide: Mastering the Ten Domains of Information Security
Leedy, P. & Ormrod, J (2005). Practical Research: Planning and Design (8th ed.).
Likert, R. (1932). A Technique for Measurement of Attitudes, Archives of Psychology, pp.140.
Management of security risk in information and information technology, APRA, 2010 FFIEC (2006) IT Handbook InfoBase
Nahra, K. & Rein, W. (2007, February). Experience Highlights Need For Data Security Vigilance
Nunnally, C.J., (1978). Psychometric Theory.McGraw-Hill, New York, NY.
Pettey, C. (2005). Gartner Highlights the Evolving Role of CISO in the New Security Order
Robson, C. (2002). Real World Research (2nd Ed.). Malden, MA: Blackwell Publishing.
Saunders, M., Lewis, P., &Thornhill, A. (2009). Research Methods for Business Students (5rd ed.). Prentice Hall Pearson Education.
Sevilla, C. (2002) Information Design Desk Reference Sundaram, A. (2008, May) Security Metrics: Hype, reality, and value demonstration
Sousa, S.D., Aspinwall, E.M. & Rodrigues, A.G. (2006). Performance measures in English small and medium enterprises: survey results. Benchmarking: An International Journal, 13, (1/2), 120-134.
Warren, M., & Hutchinson, W (2000). Information Warfare: Fact or Fiction In S. Qing & J.H.P. Eloff (Eds.) Information Security for Global Information Infrastructures (pp. 411 - 420)
Whitman, M., & Mattord., (2004). Management of Information Security
Wilson. M, & Hash, J. (2003). Building an Information Technology Security Awareness and Training Program
Yourdin, E. (2002). Byte Wars: The Impact of September 11 on Information Technology