An Investigation on the Current Information System Security Maturity Level of the Banking Industry in Ethiopia

Eskatnaf Bayu
HiLCoE, Computer Science Programme, Ethiopia
fantakse@gmail.com

Tibebe Beshah
HiLCoE, Ethiopia
School of Information Science, Addis Ababa University, Ethiopia
tibebe.beshah@gmail.com

Abstract

The banking sector is one of the pioneers in Ethiopia in adopting new technologies to deliver quality service to customers. However, this would not have been without considering information security management to better handle the risk, system failure, and any other attacks that could interrupt the information system operation. Currently, information security risk is increasing with the advancement of technology. Therefore, companies in the financial industry need to check their information security capability periodically.

The objective of this paper is to assess the existing information security maturity level in the banking industry in Ethiopia. The widely used framework in financial organizations in The Netherlands, De Nederlandsche Bank (DNB) assessment framework, is employed to help information security maturity assessment.

The result of the study indicated that the maturity level of information security management in the Ethiopian banking industry is below the expected standard and there is weak information security control and management. The study also identified that there is no information security framework or standard used by banks, and there is no regulatory framework enforced from the banking regulatory body as well.

Therefore, we suggest adapting an information security framework closing the gap by assessing information security maturity level periodically. In addition, banks should give security awareness training to their employees and should develop information security policy and procedures.

Keywords: Information Security; Information Security Management; Information Security Maturity Level

1. Introduction

Information security refers to the processes or controls that are in place by organizations or owners to protect the information assets from unauthorized access, modification, disruption, disclosure, and deletion. Protecting information assets in an organization is now becoming the highest priority.

The banking sector is one of the influential industries in the Ethiopian economy. In the banking business with the increase of technology and advancement of services, the level of information security risk has increased correspondingly [1]. The attack in an organization's information assets will result in the organization to lose money, to face a loss of customer confidence and negative business reputation [2]. To overcome this issue, banks should have effective system security in place. This is achieved by attaining a high level of maturity by implementing good information security management and doing continues assessment on the information security management gaps. Studying and evaluating the maturity level of system security would help an organization to have an enhanced system security management.

A few years back, banks were not operating their service centrally where their branches were operating independently. These days due to the advancement of technology, high availability of the banking services has become inevitable. To meet this purpose the National Bank of Ethiopia (NBE) has set a

requirement to all banks to implement Core banking systems by the end of June 2011 and integrate electronic interbank money transactions with the EthSwitch or the National Payment Switch (NPS) [5]. Accordingly, almost all banks acquired a Core Banking system and they already integrated their payment solutions with NPS. At this stage, they are using advanced technology to provide better e-banking services. When we are thinking of the advancement of technologies, the information security controls also need to be advanced; otherwise banks may encounter a huge amount of monetary and non-monetary loss. In the banking business, the information security risk has increased in proportion to the advancement of technology [1].

In Ethiopia, almost all banks are delivering their banking services using different products or Electronic Channels such as ATM, Mobile banking, Online banking, SMS banking and other channels anywhere and anytime. These channels have their own associated security risk. As a result, the banks' strategy should be readjusted so that it meets the new challenges with risk balance.

All banks have implemented their own information security controls to protect against cyber attack. However, they are managing the IT security as per their requirement and there is also a gap in managing the implemented security controls. A research by Balcha Reba [4] identified that cyber security and standards do not present in Ethiopia at the time of the study. Therefore, the author suggested professional training on information security management to be given and indicated that information security issue cannot be addressed alone with technology and attention should be given to information security management as well. So far there is no study on information security maturity level assessment in the banking industry in Ethiopia. In line with the issues discussed above, this study has closed the gap by answering the following research questions.

- What is the current information security management maturity level?
- How does it agree with the expected average information security maturity level in the industry?
- What are the challenges in implementing effective information security management?

Previous researchers in the area revealed that most of the Ethiopian banks have not yet implemented information system security management (ISSM) standard and the maturity of information security is not assessed.

2. Related Work

There is few literature on information system security specific to the Ethiopian context. However, related research works are discussed to show their similarities, differences and their contribution to this research.

According to Lema Lessa [1], financial institutions are exposed to threats due to the wide spread of technology and their interconnection to the Internet. Technical controls have been used to minimize the threat. However, using technical controls alone does not help to bring a solution. The author claims that many losses are not caused by lack of technology control. Rather it is caused by faulty human behavior. The researcher aimed at assessing the information security culture and identified the gap that needs management and policy intervention. Therefore, a survey research method was employed to collect quantitative data from 11 banks in Addis Ababa. Using the auditing process, the information security culture was audited. The paper revealed that the information security awareness in the banking industry was unsatisfactory. The findings mainly focused on the need for effective information security culture which enables proper information security governance and implementations that comply with local and international standards.

The work in [3] discusses the benefit of using cloud computing and associated concern. Cloud computing is storing and managing data on virtualized environment so that organizations can have the ability to store data and compute anywhere

and anytime. However, banks are not able to use cloud service due to the security issue and absence of clear standard and framework that guides the banking industry to address compliance and security concerns. The aim of the research was to address this problem by proposing cloud computing security framework for the banking industry. The paper proposed applicable Conceptual Cloud Computing Security Framework for Banking Industry. A model named Sherwood Applied Business Security Architecture (SABSA) is used as a guide for designing the newly proposed security framework based on five basic security questions; namely What, Who, Why, Where, and How. The paper proposed a framework that integrates major components that address security, privacy, legal and compliance and regulatory issues.

Mengistu Bogale and Donald Amoroso [6] addressed the problem of how Ethiopian companies are handling IT Governance program and how IT auditing can be used. First, the authors assessed how IT governance performance influences organizational performance. The aim of the study was to understand the contribution of IT auditing for organizations' overall performance. They used a survey method targeting banking and insurance companies and categorized after clustering into two based on their age and ownership. From the target population, they selected 12 banks and 9 insurance companies for data collection. Quantitative data were gathered with the help of questionnaires. After analyzing the quantitative data gathered, they concluded that IT audit practices are strongly correlated with IT governance performance. IT governance performance and maturity would improve both operational and financial performance of firms.

Kelemie Tebkew [7] assessed the existing Information Security Management (ISM) practices of the banking sector and proposed and developed an ISM framework. The researcher tried to study and compare the available information security management frameworks and best practices. To assess the ISM practices in the banking industry, the researcher used ISO audit checklist and own experience. Both qualitative and quantitative research approaches were used. Data collections were done using questionnaire, document analysis, and interviews. Findings of the assessment show that existing information security management in the surveyed banks lack a formalized comprehensive framework-based information security policy which would result in poor performance in information security management. The researcher proposed an ISM Framework for the banking sector to be used as a starting point to manage information security by developing guidelines and implementing controls to protect banking information assets from threats. The proposed framework has two major components, viz. information security requirement identification mechanism which is the combination of Entity Relationship Model, and Information Security Management System process model with supporting template and countermeasures (controls). Further, 16 main ISM domains are identified. These are further grouped under three categories, viz. Administrative, Technical, and Physical & Environmental security. The suggested framework is still a general approach to ISM. It needs detailed policies and procedures and comprehensive test in a real banking environment. As the researcher stated, the proposed framework requires extra work in order to be implemented. Therefore, it is difficult to conclude the developed framework is valid and applicable in the banking industry to address the challenges related to information security.

3. Approach, Result and the Proposed Solution

This Section discusses the methodology and approaches used to assess the information security maturity level of the banking industry in Ethiopia. Based on the analysis and results of findings, recommendation are made.

3.1 General Approach

We followed DNB's assessment framework, the widely used framework in financial organizations in

the Netherlands. DNB assessment framework was employed to help the information security maturity assessment. It is based on COBIT (Control Objectives for Information and Related Technologies) which includes control objectives and measures to assess the maturity of an organization's IT processes [8]. The DNB framework includes 21 control objectives which are derived from COBIT and ISO and are divided into the following six areas: Strategy, Organization, People, Processes, Technology, and Facility.

Mixed research approach is used and purposive sampling technique was employed to select the respondents from each of the 18 banks that are currently operating in Ethiopia. Data was gathered through survey questionnaire and interview. SPSS is used for data encoding and analysis.

3.2 Information Security Management Maturity Level Result

In this Section, findings related to Information Security Management maturity level of each bank is categorized based on strategic and planning, organization, people, process, technologies, and facilities, as shown in Figure 1.

AS can be seen form Figure 1, 40% of the banks' information security maturity level is at the initial/ad-hoc (level 1) stage, 40% of them are at initiative stage (level 2) and the rest 20% are at the defined stage (level 3).

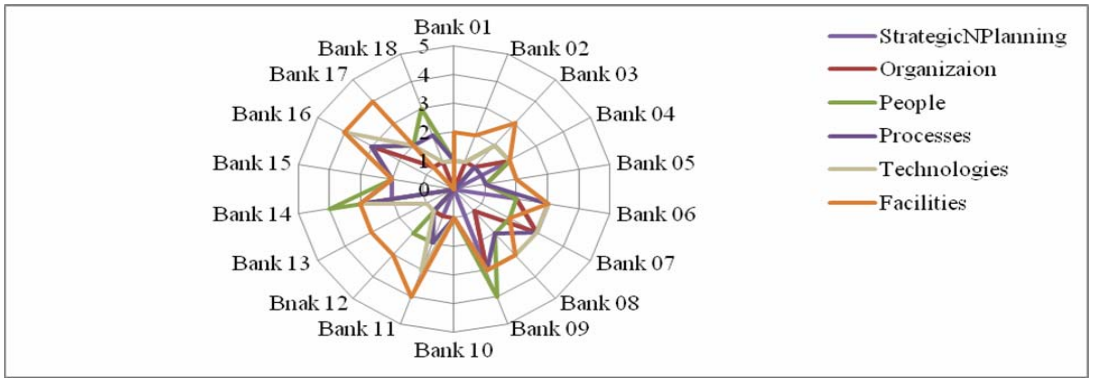

Figure 1: Maturity Level of the Banking Industry in the Aspects of Strategic and Planning, Organization, People, Process, Technologies, and Facilities

Figure 2 shows the mean maturity level of the information security in the banking industry on a radar graph.

As shown in Figure 2, from the total of 18 banks, 4 of them are at level 3 (defined), 7 of them at level 2 (initiative) and the remaining 7 are at level 1 (initial) stage. Generally, there is no bank that passes the industry average information security level.

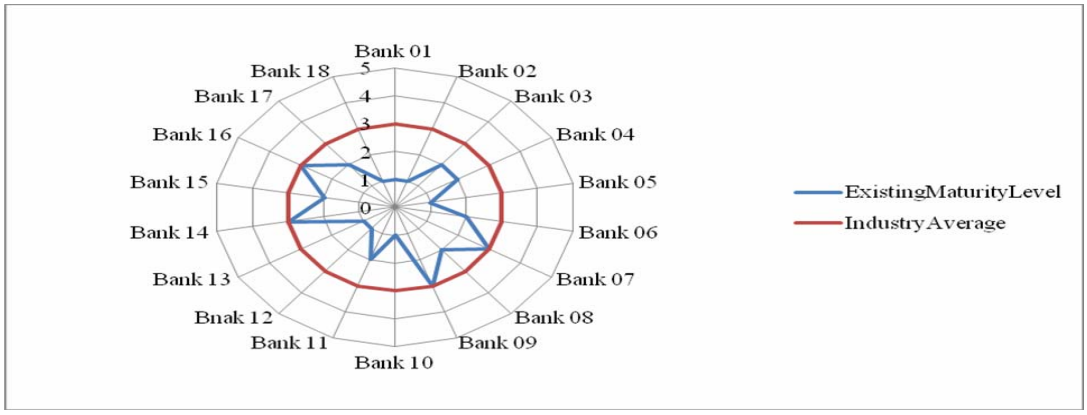

Figure 2: Information Security Management Maturity Level of the Banking Industry

3.3 Suggested Solutions

According to the study result and the concepts learned from the literature review, a recommendation which the Ethiopian banking industry should follow in order to address the stated information security gaps are stated as follows.

- Increase IT security maturity level by setting a benchmark and assessing the maturity of information security periodically.
- Develop information security policy and procedure.
- Train both users and technical staff periodically.
- Empower information security management.
- Periodically make a risk assessment and penetration testing.
- Establish Security Operation Center to centrally manage, analyze and mitigate an information security attack.
- Adapt an information security standard as outlined below.

Recommended Information Security Standard for The Banking Industry

Information security standards and best practices can be the best solution for effective information security management [10]. This is because they have their own focus areas, advantages, and drawbacks. The existing preferable standards which are mostly used for information security management and compliance are ISO 27K, COBIT and PCI DSS [9]. Usability of ISO and COBIT standards have scored 163 and 160 respectively out of the total of 203 countries in the world. Payment Card Industry Data Security Standard (PCI DSS) has scored 125 and ranked third [9]. PCI DSS controls are mandatory for organizations that collect and store credit card data. Therefore, financial institutions are required to be compliance with this requirement in order to give an international card payment service. To manage information system security effectively and to comply with the regulation requirement, many organizations adopt different information security management models but each information security management model or standard has its own advantages and drawbacks. So, best practices should be adopted based on the business context focusing where their use benefits the organization most [10]. Therefore, there is no any information security model that fulfills the entire organization's requirement. However, an organization can adopt the three major standards by aligning the security control requirements of one on another.

To suit information security management to the business needs, formal processes with good IT governance support should be used. So, COBIT can be used at a higher level of IT governance providing an overall control framework process model that generally suits every enterprise [10]. ISO 27001 and PCI DSS can be mapped into COBIT to address concerns that have special focus on security and cardholder data. The purpose of the mapping is providing an integrated way for complementary use of COBIT, ISO 27001, and PCI DSS for information security management [11, 12].

In order to align ISO 27001 to COBIT 4.1, an approach in [11] shows how to use both standards' functionality by mapping ISO into COBIT control objectives. This result combines an aligned COBIT 4.1 and ISO 27001 control objectives in one. Finally, PCI DSS control requirements were identified and mapped to the correspondent domain of the two control objectives. This will create an alignment between the control objectives of COBIT, ISO 27001, and PCI DSS.

4. Discussion

According to the survey we made, the majority of the banks interviewed do not have a formal information security standard adopted, 83.3% of the banks have not implemented information security management standard, while 16.7% of them have implemented COBIT, ISO and PCI DSS separately. A previous study by Kelemie Tebkew [7] also corresponds to this finding. This finding shows lack of use of information security management standard

in the banking industry in Ethiopia. The study also identified the challenges in adopting information security which are lack of understanding of the value of information security standard, lack of training, lack of technical staff, and lack of management support.

As per the assessment made based on the DNB assessment framework, the Information security maturity assessment indicators are categorized as Strategic and Planning, Organization, People, Process, Technology, and Facility [8] from 18 banks. All the indicators are below the expected industry average, whereas physical security is relatively in a better state, which also corresponds with previous studies [7].

Generally, we found that Information Security Management Maturity level of the banking industry is unsatisfactory or below the expected average. This is due to weak information security controls and poor information security management.

5. Conclusion and Future Works

In recent years, the banking industry in Ethiopia has been on the rise in delivering new technological e-banking products, currently the competition has become delivering quality service to customers. To provide a good service quality, banks should maintain the confidentiality, integrity and availability of their information systems. Financial service has been one of the major targets for electronic criminals along with the advancement of technology. Preserving the information security will help banks to increase their market share, customer trust and to keep their business reputation.

Considering this fact, the research assessed the current maturity level of information security management in the banking industry and recommended a suitable information security management standard to close the gap. Related researches and documents have been reviewed to compare and inspect the information security management standards widely used. This research used DNB assessment framework which consists COBIT 4.1 and ISO 27001 standards for the purpose of maturity level assessment. The findings of the assessment indicate that the information security maturity level of the banking industry is very low or below average. The banking industry has weak information security controls and management system due to lack of technical experts, absence of management support and user awareness.

This study has been carried out on information security maturity assessment which is not studied in this area in the Ethiopia context. There are pieces of literature in information security in general. However, it is difficult to find literature specific to this purpose. There are limitations on this research. So in future work further studies will be done on assessing the maturity level after a period of time and compare the result, study on how to implement security operation center in the banking industry in Ethiopia, and incorporating Information Technology Infrastructure Library (ITIL) control objectives on the proposed framework to address IT Service management requirement.

References

[1] Lema Lessa, “Information Security Culture in the Banking Sector in Ethiopia”, 2012, retrieved from https://www.researchgate.net/profile/Lemma_Lessa/publications, last accessed on May 12, 2016.

[2] Abdullah Alshboul, “Information Systems Security Measures and Countermeasures: Protecting organizational assets from Malicious Attacks", 2010, retrieved from http://www.ibimapublishing.com/journals/CIBIMA/2010/486878/486878.pdf, last accessed on May 13, 2016.

[3] Meskerem Alemu and Abrehet Omer, “A Cloud Computing Conceptual Security Framework for Banking Industry", Journal of Emerging Trends in Computing and Information Sciences, Vol. 5, No. 12, December 2014.

[4] Balcha Reba, "State of CyberSecurity in Ethiopia", June 2005, retrieved from

http://itu.int/osg/spu/cybersecurity/contributions/Ethiopia_Reba_paper.pdf last accessed on May 12, 2016.

[5] National Bank of Ethiopia, retrieved from http://www.nbe.gov.et/financial/banks.html. Last accessed on May 10, 2016.

[6] Mengistu Bogale and Donald L. Amoroso, “Auditing IT and IT Governance in Ethiopia” September 2015, retrieved from, https://www.researchgate.net/publication/281321417_Auditing_IT_and_IT_Governance_in_Ethiopia

[7] Kelemie Tebkew, "Information Security Framework for Banking Industries in Ethiopia" retrieved from http://etd.aau.edu.et/bitstream/123456789/8702/1/Kelemie%20Tebkew%20Yirdaw.pdf, last accessed on August 10, 2016

[8] Torben Bijpers, "DNB Framework for Financial Institutions to Achieve a Maturity Level 4 using DNB Framework", retrieved from http://www.vurore.nl/images/vurore/downloads/scripties/2042-Def.scriptie_ TorbenPijpers.pdf. last accessed on may 22, 2016.

[9] Heru Susanto, Mohammad Nabil Almunawa, and Yong Chee Tuan, "Information Security Management System Standards: A Comparative Study of the Big Five", 2011, retrieved from, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.673. 9909&rep=rep1&type=pdf, last accessed on August 10, 2016

[10] ISACA "Aligning-COBIT-ITIL-V3-ISO27002", retrieved from http://www.isaca.org/Knowledge-Center/Research/Documents/Aligning-COBIT-ITIL-V3-ISO27002-for-Business-Benefit_res_Eng_1108.pdf, last accessed on December 2, 2016.

[11] Razieh Sheikhpour and Nasser Modiri, "An Approach to Map COBIT Processes to ISO/IEC 27001 Information Security Management Controls", retrieved from http://www.sersc.org/journals/IJSIA/vol6_no2_2012/2.pdf, last accessed on December 2, 2016.

[12] Pritam Bankar, CISA, CISM, and Sharad Verma, retrieved from, "Mapping PCI DSS v2.0 With COBIT 4.1", http://www.isaca.org/Knowledge-Center/Documents/Mapping-PCI-DSS-v2.0-With-COBIT-4.1.pdf, last accessed on December 2, 2016.