Received 12 October 2021
Revised 4 August 2022
31 August 2022
Accepted 17 November 2022

Maturity of information systems' security in Ethiopian banks: case of selected private banks

Tadele Shimels and Lemma Lessa
School of Information Science, Addis Ababa University, Addis Ababa, Ethiopia

Abstract

Purpose – Information systems' security is more critical than ever before since security threats are rapidly growing. Before putting in place information systems' security measures, organizations are required to determine the maturity level of their information security governance. Literature review reveals that there is no recent study on information systems' security maturity level of banks in Ethiopia. This study thus seeks to measure the existing maturity level and examine the security gaps in order to propose possible changes in Ethiopian private banking industry's information system security maturity indicators.

Design/methodology/approach – Four private banks are selected as a representative sample. The system security engineering capability maturity model (SSE-CMM) is used as the maturity measurement criteria, and the measurement was based on ISO/IEC 27001 information security control areas. The data for the study were gathered using a questionnaire.

Findings – A total of 93 valid questionnaires were gathered from 110 participants in the study. Based on the SSE-CMM maturity model assessment criteria the private banking industry's current maturity level is level 2 (repeatable but intuitive). Institutions have a pattern that is repeated when completing information security operations but its existence was not thoroughly proven and institutional inconsistency still exists.

Originality/value – This study seeks to measure the existing maturity level and examine the security gaps in order to propose possible changes in Ethiopian private banking industry's information system security maturity indicators. This topic has not been attempted previously in the context of Ethiopian financial sector.

Keywords Information systems security, Information systems threat, Information systems security maturity, Maturity level, Maturity model

Paper type Research paper

1. Introduction

A growing body of knowledge addresses information security in developing countries (Saleh, 2012; Ejerssa, 2018; Gera, 2019; Abebe, 2020; Deferew, 2020). This is because information and communication technology (ICT) plays a vital role in the globalized economic sphere. It is widely adopted by various organizations like industrial enterprises, manufacturing companies, health sector, financial sector and educational system in their day-to day operations. The dynamics of events in the current competent financial world is making financial organizations be dependent on this technology (Redlin, 2017). The widespread use of ICT helps financial institutions to meet their customers' needs in various ways. In line with this, banks are widely adopting different technology solutions like core banking, mobile banking, Internet banking, cheque clearance, foreign remittance and so on. Even though

The authors are thankful to all study participants for their willingness to respond to the extensive questionnaire items.

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for- profit sectors.

International Journal of Industrial Engineering and Operations Management
Vol. 5 No. 2, 2023
pp. 86-103
Emerald Publishing Limited
e-ISSN: 2690-6104
p-ISSN: 2690-6090
DOI 10.1108/IJIEOM-10-2021-0014

these dynamically emerging technologies have positive impact on financial institutions, and they are also risky if the organizations fail to protect their information assets from any information security attack (Saleh *et al.*, 2012; Waxman, 2013).

The annual cyber-attacks are rising every year with 27%, from an average of 102–130 (LLC, 2017). Ransomware attacks are increasing by double and information security incidents like WannaCry and Petya have affected thousands of targets and altered the function of public services, financial institutions and large companies across the world (Ponemon Institute, 2015). Based on reported figures, the high rate of increase in information systems' security threats urges organizations to re-examine their information systems' security maturity periodically.

Banking sector is directly impacted by information security threat of different nature. Full or partial disclosure accelerates the diffusion of attacks, increases the penetration of attacks within the target population, and increases the risk of first attack after the vulnerability is reported (Ransbotham, 2015). Hence ensuring the confidentiality, integrity and availability have to be accompanied by the sector. Ejerssa (2018) indicated that information security maturity is a key agenda for developing countries and is not sufficiently addressed. The Ethiopian banking sector information security maturity is below the expected level and their information security is insufficient (Beshah, 2017; Ejerssa, 2018; Gera, 2019; Deferew, 2020). Therefore, resolving the information security agenda requires high priority.

Evaluating the information systems' security capability helps to identify potential threats and existing vulnerabilities (Rainer, 1991). In recent days security threat is rapidly growing and the technological environment requires organizations to continuously adapt to changes and accommodate different kinds of competing mechanisms. Saleh (2012) revealed that the importance of building information systems' security to the organization and regular evaluation of information security maturity level helps to ensure the confidentiality, availability and integrity. This calls for due attention to information systems' security and the need to conduct empirical studies in this area periodically. Hence, analyzing the security maturity level will help financial institutions to take necessary action to protect their environment. The aim of this study is to do systematic investigation on the current information systems' security maturity by analyzing the current working environment and to provide recommendations for improvement. Hence, this research aims to answer two research questions: (1) how is the effectiveness of information security management (ISM) practice in the Ethiopian financial sector? (2) What are the factors prohibiting the effectiveness of ISM toward Payment Card Industry Data Security Standard (PCI-DSS) in the Ethiopian financial sectors?

This research paper is organized as follows. Section 2 briefly discusses the research gap based on extant literature review followed by a brief background on the Information security maturity models. Section 3 presents the research design and methods followed by Section 4 that presents case study results and discusses the implications. Drawing on these results, Section 5 concludes by highlighting the contributions and proposes opportunities for future work.

2. Literature review

This section presents the literature on information security in the banking sector. It starts with a discussion of the research gap, after which literature on information security maturity models is presented.

2.1 The research gap in information security models

These day's financial institutions are in high competition and thus are implementing different technologies to perform better. Since the financial sector is considered as a backbone to the

economy, its information systems' security has to be well designed, implemented and measured periodically. A more secured information sharing in an organization is considered to be good approach in increasing the organizations effectiveness, efficiency, performance and decision-making capability (Olusegun and Ithnin, 2013). However, the behavior of information sharing is very complex and grows dynamically, so it is mandatory to investigate and analyze the potential risks to ensure maturity of information systems' security regularly.

Information security measures are designed and implemented in an organization to demonstrate and elaborate the organization's approach to ensure information security. The information security mechanism consists of people, policies and infrastructure (Ejerssa, 2018) designed to address the challenges of security breaches revolving around the secured and valuable asset of an organization. According to Ejerssa (2018), information security maturity level in higher educations in Ethiopia is found unsatisfactory. In fact, organizations are different on their structure, the kind of information they have and the capacity to handle information securely.

According to Houngbo and Hounsou (2015), conducting the measurement on information systems' security using consistent metrics improves the ability to understand it and control it. Measuring the information systems' maturity level leads to control and protect the threats and eventually helps to make improvement in information security handling mechanisms. This is well said by Lord Kelvin's adage, "If you can't measure something, you can't understand it. If you can't understand it, you can't control it. If you can't control it, you can't improve it [1]."

Recent research conducted on information security of financial sectors in Ethiopia revealed that the information security protection and governance culture is unsatisfactory (Yohannes *et al.*, 2019). Other local studies focus on different issues, such as an evaluation of the insider threat in the Ethiopian banking sector (Amare, 2015), cybercrime governance (Hailu, 2015), the policy toward implementing information security (Negussie, 2015), designing framework for information security implementation (Tebkew, 2016), designing framework for information security awareness creation (Kebede, 2019), cyber hygiene practice for employees (Deferew, 2020), information security incident response management (Yohannes *et al.*, 2019) and designing framework to manage human factor toward information systems' security (Abebe, 2020). Other related works by Ejerssa (2018), Gera (2019) tried to address the maturity level of information systems' security on Ethiopian public universities and hospitals in Addis Ababa. Even though those studies contribute to address different information security problems, their intention was not to measure the current maturity level of information security. These authors mentioned that there is a dearth of studies in the area of information security maturity level and recommend conducting the same on a regular basis. Hence, this study attempts to fill this research gap by assessing the information security maturity level in the private banks in Ethiopia and propose possible solutions to fill the gaps. This will help the banks to know their security maturity level and take corrective actions so that they can withstand potential cyber-attacks.

2.2 Information security maturity models

Maturity models are extensively being used as a means of organizational development or measurement in the area of information security. Any framework for performance analysis and improving efficiency can be considered as the basis, and if it incorporates methods for quality assurance, it is referred to as a maturity model (Saleh, 2012). To identify the strengths and weaknesses of an organization's information security maturity level, a variety of frameworks or models may be used to assess and identify the discrepancy between the security criteria standard and the actual working environment layout. The common information security maturity models are summarized below.

The National Institute of Standards and Technology (NIST) has released a framework that will help companies in critical infrastructures to minimize the risk of information security risks. It implements five security measures for institutions. These controls include data and asset identification, detection, security, response and recovery (Osamah and Al-Matari, 2021). The NIST framework establishes rules for the activity of US enterprises. It helps to assess and develop the capability of investigating, preventing and responding to cyber-attacks. The model has five levels, namely: policies, procedures, implementation, testing and integration. In addition, the model is driven by nine key areas that are divided into strategic and technical aspects. According to Nieles *et al.* (2017), higher level of maturity can only be attained if and only if the previous maturity level is attained. Further, the NIST model is oriented to evaluation and documentation of IT systems, and it does not address adequately aspects of nontechnical security services.

ISM maturity model enables an organization's information security maturity level to be divided into five categories of information security capability (namely; unavailable, ad hoc, repeatable, defined, managed or optimized) (Osamah and Al-Matari, 2021). The level of classification is determined by the form of controls and the type of technology enabled by the organization. The maturity level Defined starts by describing the security controls, techniques and technologies needed to protect the organization. The managed maturity level is responsible for developing the technologies required to automate security measures. The optimized maturity level employs access control measures in order to protect the enterprise against both internal and external threats.

De Nederlandsche Bank (DNB) is a maturity assessment framework designed to safeguard financial stability and thus contributes to sustainable prosperity in the Netherlands (Pijpers, 2015). This information system security maturity model is an assessment framework with which financial organizations can perform an assessment to evaluate the maturity of their information systems' security. The DNB information security assessment framework is developed based on COBIT v.4.1 and it includes 21 control objectives which are divided into six areas, i.e. strategy, policies, organization, people, process and technology (Pijpers, 2015; De Haes *et al.*, 2020).

The systems security engineering capability maturity model (SSE-CMM) was created with the goal of advancing security engineering because information security relates to the protection of data against a variety of threats in order to ensure business continuity, minimize risk and maximize profitability and economic opportunities (Kurniawan and Riadi, 2018). Its associated assessment approach are currently available tools for assessing the capability of software vendors of security building materials, programs and services, as well as directing organizations in identifying and developing their security project management (Ferraiolo, 1998).

Levels of maturity for ISM and control in the process ranging from level 0 (none) to level 5 (optimistic), based on the organization's assessment framework. The maturity model is used to identify whether a problem exists and how to prioritize improvements. The five capability maturity levels that represent the process maturity are:

(1) Level 0 indicates that not all base practices are performed.

(2) Level 1 indicates that all the base practices are performed but informally, meaning that there is no documentation, no standards and is done separately.

(3) Level 2 means that the processes are planned and tracked, which indicates commitment to planning process standards.

(4) Level 3 for well defined, meaning standard processing has been run in accordance with the definition.

(5) Level 4 is controlled quantitatively, which means improved quality through monitoring of every process.

(6) Level 5 is improved constantly indicating the standard has been perfect and their focus to adapt to changes.

There are various information security standards in use around the world, which includes mostly utilized standards like COBIT, ITIL, DNB, PCIDSS, BS7799, etc. Among those standards, ISO27001:2013 serves as an inclusive and most acceptable information security standard around the globe. Yemane (2018), for instance, conducted a study on the ISM system for Ethio Telecom using ISO 27001:2013. This research also adopts the ISO 27001:2013 information security standard with its management practices of selection, implementation, and monitoring of controls (see Table 1). Besides, the SSE-CMM is used to achieve this target. This is because ISO 27001:2013 does not have assessment tools (Rosmiati *et al.*, 2016). So, this research mainly employs ISO 27001:2013 to identify variables that are in the information security assessment areas.

Measuring the security maturity level of information systems with standardized metrics increases the ability to recognize and manage information security safety. Therefore, in order to protect information from various security threats, organizations need to understand their information system security maturity level requirements on a regular basis.

3. Research design and methods

This research followed a quantitative research approach to measure the maturity level of information systems' security of the private banking industry in the country. A case study research strategy was preferred because it allows a composite and multifaceted investigation of the issue or problem (Creswell, 2013). A stratified probability sampling technique was employed to select four banks from a total of 17 private banks in the country. Those banks are grouped into four groups (strata) based on their high-profit achievement 2019/2020 fiscal year. The researchers argue that when the number of customers and financial success grows up, it becomes more vulnerable to security concerns and a prime target for attackers. The banks are divided into four strata and one bank is selected from each stratum.

Table 1.
Domains, objectives and number of controls

No. Annex	Domain of ISO 27001:2013	No of objectives	No of controls
A.5	Information security policies	1	2
A.6	Organization of information security	2	7
A.7	Human resource security	3	6
A.8	Asset management	3	10
A.9	Access control	4	14
A.10	Cryptography	1	2
A.11	Physical and environmental security	1	15
A.12	Operational security	7	14
A.13	Communication security	2	7
A.14	System acquisition, development and maintenance	3	13
A.15	Supplier relationships	2	5
A.16	Information security incident management	1	7
A.17	Information security aspects of business continuity management	2	4
A.18	Compliance	2	8
Total		34	114

Source(s): ISO 27001: 2013, ISO/IEC 27001

Although the banks have a lot of branches all over the country, their information system is mainly managed centrally. Thus, participants for this survey were personnel in the information security division and management information system at headquarters of each sampled private banks. The total number of employees working within information systems and security department for the four sampled banks is 110. Hence, a census is used and 110 questionnaires were distributed to all the staff. The questionnaire was developed using Google Form and distributed to the respondents online through email and Skype. A total of 93 questionnaires were gathered of which two respondents did not answer majority of the questions. Hence, 91 (82.73%) valid questionnaires were used for the analysis. To increase the study's validity and reliability, multiple methods of data collection techniques are used (i.e. questionnaire, document analysis and literature review) to help crosscheck the responses. The questionnaires were adapted from ISO/IEC 27001:2013 and a pilot test was performed by distributing the questionnaires to some IT and network security department's managers.

4. Data presentation and analysis

The questionnaire was developed using an online Google Form and distributed to the respondents through email and Skype. Among the expected total of 110 questionnaires, at least 93 of the respondents completed and returned the questionnaire. This indicates that 84.5% of the questionnaires were returned, and 93 of them are used in this analysis. The data were collected and checked to see if there were any missing or inconsistent answers. Having followed the validation of the questionnaires, the collected data were analyzed using SPSS version 25 to further investigate the results and make recommendations based on the findings. The maturity index is the outcome of determining the level of information security maturity by calculating the maturity level ranging from 0 to 5. Because information security is tied to institution's privacy, the names of any of the sampled banks are not divulged in this study; data are obtained from several private banks, and then stored in one data set for analysis. The mean value of information security controls in Ethiopian private banks in comparison to the four sampled banks is 2.45, while the last predicted information security maturity level is 5 (Optimized). This, in turn, implies that a private banking institution's maturity level score is lies on second level, i.e. repeatable but intuitive (see Table 2).

As it can be seen from Table 2 above, for annex A.9 of ISO/IEC 27001:2013 (Access control), A.11 (Physical and environmental security), A.15 (Supplier relationship) and A.16

Clause	Control objectives	Index	Level
5	Organization of information security	2.47	2
6	Human resource security	2.45	2
7	Asset management	2.34	2
8	Information security policy	2.41	2
9	Access control	2.57	3
10	Cryptography	2.19	2
11	Physical and environmental security	2.73	3
12	Operational security	2.48	2
13	Communication security	2.37	2
14	System acquisition, development and maintenance	2.45	2
15	Supplier relationships	2.57	3
16	Compliance	2.59	3
17	Information security incident management	2.32	2
18	Information security aspects of business continuity management	2.29	2
	Average	*2.45*	*2*

Table 2. Maturity level summary for each control objectives

(Compliance) the average allocated to their equivalent score reaches the maturity level of 3, which is (Defined) and for the rest of control objectives the mean value indicates score level 2 (Repeatable but intuitive) of information security maturity level. This is because the SSE-CMM classifies the score as "Repeatable but intuitive," with a range of 1.51–2.50, whereas if the score ranges from 2.51 to 3.50 entitled with "Defined". Figure 1 depicts the maturity level of information security for private banks in each of fourteen areas derived from ISO 27001:2013. The assessment scale indicates that the organization has a score of less than three in all information security maturity metrics, as seen in Figure 2.

The level of information system security maturity among the sampled private banks is also examined. Bank A, Bank B, Bank C and Bank D were ordered in sequence of highest to lowest profit achievement from the four sampled private banks, using stratified probability sampling. As can be seen in Figure 2, the average maturity level for the first high profit Bank A is 2.50, the average maturity level for the second category is 2.48, the average maturity score for the third category sampled bank is 2.39, and the average score result for the final category is 2.43. From the quantitatively collected data the study finding shows that Bank A, Bank B, Bank C and Bank D are on the maturity level of 2. If the maturity metrics range between 1.51 and 2.50, the maturity level is 2, which is Repeatable but intuitive, according to the SSE-CMM maturity level assessment criteria. For all information security areas, the maturity level value is categorized by the range of SSE-CMM maturity level assessment criteria as detailed in Table 3.

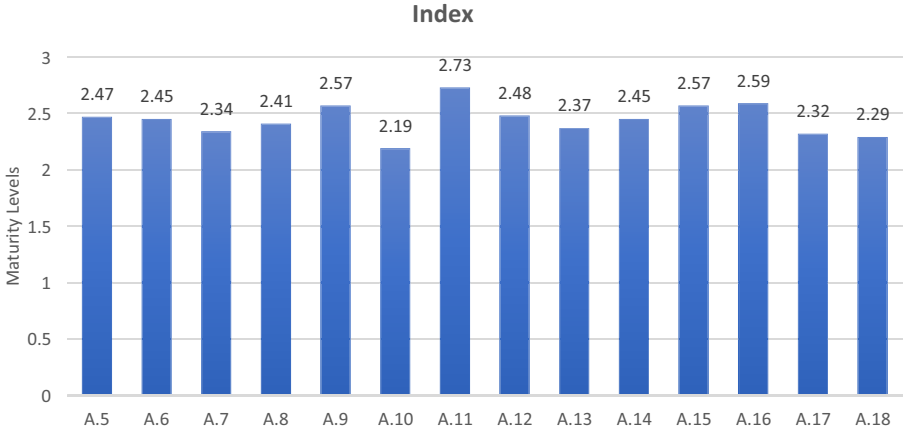

Figure 1.
Maturity level score per each security area

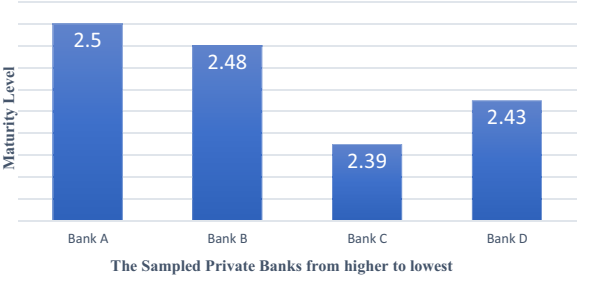

Figure 2.
Maturity level score per Bank

Range	Level	Descriptions
0–0.50	Nonexistent	The company does not care about the importance of information security
0.51–1.50	Initial	The company reactively performs application and implementation of information security, without preceded by prior planning
1.51–2.50	Repeatable/ Intuitive	The company has a pattern that is repeatedly performed in conducting activities security governance, but its existence has not been well defined
2.51–3.50	Define	The company has formal and written standard procedures that have been socialized to employee to be obeyed and worked in daily activities
3.51–4.50	Managed	The company has a number of indicators or quantitative measures that serve as objective performance of every application
4.51–5.00	Optimized	The company has implemented the information technology governance refers to "best practice"

Source(s): Kurniawan and Riadi (2018)

Table 3.
Maturity level criteria assessment index

Thus, the study's finding shows that the sampled private banks' information security maturity level has shown no significant difference. But there is some difference on their attention toward the information system security management criteria of the ISO 27001. Thus, Bank A has achieved the upper score for the maturity level on A.8 (Asset Management), A.11 (Physical and environmental security) and A.16 (Information security incident management), whereas the lowest maturity level score on A.5 (Information security policies), A.10 (Cryptography) and A.17 (Information security aspects of business continuity management). Bank B scored high on A.11 (Physical and environmental security), A.15 (Supplier relationships) and A.16 (Information security incident management) and a low score on A.13 (Communications security), A.14 (System acquisition, development and maintenance) and A18 (Compliance). Bank C scored high maturity level on A.9 (Access control), A.11 (Physical and environmental security) and A.16 (Information security incident management), whereas it scored low maturity on A.8 (Asset management), A.10 (Cryptography) and A.18 (Compliance). Finally, Bank D scored high maturity level on A.5 (Information security policies), A.11 (Physical and environmental security) and A.14 (System acquisition, development and maintenance), but scored low maturity on A.7 (Human resource security), A.17 (Information security aspects of business continuity management) and A.18 (Compliance). Table 4 shows the detailed maturity level results for each bank based on the ISO27001 annex.

4.1 Maturity level gap analysis

The expected maturity level for the SSE-CMM used to calculate the level of information security maturity is 5, which is optimized. First, the value difference for each clause is calculated, and this is the maturity level distance. The total value of the overall difference is calculated by adding all values and dividing them by the number of control objectives. The magnitude of the difference between actual security working conditions and expected security conditions is 2.55, with a 51.1% disparity in overall information security maturity.

From the 14 security areas, three control objectives have scored level 3 (Defined): A.9 – Access Control, A.11 – Physical and environmental protection and A.15 – Supplier relationships, while the vast majority of security control areas are at level 2 (Repeatable but intuitive). In general, the private banking industry has not achieved level 4 (Managed) or level 5 qualification (Optimized). The aggregate outcome of the study to determine the mean value of information security controls in Ethiopian private banks in comparison with the four sampled banks is 2.44, and the last expected information security maturity level is 5 (Optimized). Accordingly, we may deduce that a private banking institution's maturity level

Table 4.
Maturity level of each bank as per each ISO 27001 security area

Banks from four different group	A.5	A.6	A.7	A.8	A.9	A.10	A.11	A.12	A.13	A.14	A.15	A.16	A.17	A.18	AVG
Bank A	2.23	2.42	2.5	2.8	2.58	2.1	2.69	2.6	2.52	2.67	2.52	2.71	1.99	2.61	*2.50*
Bank B	2.51	2.51	2.47	2.4	2.57	2.37	2.79	2.41	2.2	2.29	2.77	2.64	2.44	2.34	*2.48*
Bank C	2.44	2.41	2.41	2.01	2.66	1.99	2.8	2.32	2.31	2.23	2.49	2.6	2.54	2.18	*2.39*
Bank D	2.7	2.44	1.97	2.41	2.45	2.42	2.63	2.58	2.58	2.59	2.49	2.41	2.31	2.01	*2.43*
Average per security controls	*2.47*	*2.45*	*2.34*	*2.41*	*2.57*	*2.19*	*2.73*	*2.48*	*2.37*	*2.45*	*2.57*	*2.59*	*2.32*	*2.29*	*2.45*

is on the second level, i.e. repeatable but intuitive. Table 5 shows gap between the current and expected level of information security maturity.

4.2 Document analysis

As per the document analysis, the sampled private banks do have information security policy and protocol in place to protect the company from both external and internal threats. However, only two of the four sampled private banks have agreed to share their information security guidelines. This method of record analysis assisted the researchers in cross-checking the validity of questionnaire responses. The following is a summary of the results for various security control areas:

Access control policy and identity management: This approach applies to all of the institution's current facilities and services. The policy amendment and revision guidelines state that: "Unless there is special enforcement to update the information protection and access policy in the meantime, it should be updated every three years, subject to prior approval of the Board of Directors". The researchers deduce from this declaration that there is a significant gap to revise and review the information security policy.

Security incident management: Information systems that are suspected to be compromised are disconnected from the bank's network before the incident has been reviewed, resolved and the risk has been minimized sufficiently. All information security incidents are reported for later study and evaluation in order to identify areas where policies, processes and information security measures can be improved. If the incident is not adequately resolved, the issue should be escalated to the chief information officer.

Physical and environmental security: Classified information and IT infrastructure, such as the data center, disaster recovery center, server rooms, head office organs switches and all word stations connected to Bank X networks, must be physically secured to reduce business and organizational impacts. For demilitarized zone system, device and network management, equipment and software within the scope of this policy must be administered by support groups authorized by the IT security team. For data security, the data have been divided into four classes.

(1) *High risk*: information assets for which there are legal requirements for preventing disclosure or financial penalties for disclosure, i.e. customers' account information, payroll, personnel and financial information.

No	Information security controls	Maturity		Gap	Gap in %
		Current	Expected		
1	Organization of information security	2.47	5	2.53	50.6
2	Human resource security	2.45	5	2.55	51
3	Asset management	2.34	5	2.66	53.2
4	Information security policy	2.41	5	2.59	51.8
5	Access control	2.57	5	2.43	48.6
6	Cryptography	2.19	5	2.81	56.2
7	Physical and environmental security	2.73	5	2.27	45.4
8	Operational security	2.48	5	2.52	50.4
9	Communication security	2.37	5	2.63	52.6
10	System acquisition, development and maintenance	2.45	5	2.55	51
11	Supplier relationships	2.57	5	2.43	48.6
12	Compliance	2.59	5	2.41	48.2
13	Information security incident management	2.32	5	2.68	53.6
14	Information security aspects of business continuity management	2.29	5	2.71	54.2
Average				2.55	51.1

Table 5. Gap between the current and expected level of information security maturity

(2) *Confidential*: Data that should be protected to prevent unauthorized disclosure. The user access to such data is limited to what he/she needs to do their job and can only be given to staff by role and responsibility.

(3) *Internal use*: this category is for internal business information but if disclosed to external entities, could result in some level of harm or disadvantage for the company, its employees and customers.

(4) *Public*: information that may be freely disseminated without causing any harm to the bank, its customers or shareholders.

Human resource security (During employment and termination): It should be ensured that employees, contractors and third-party users are aware of information security threats and concerns. In the course of their usual employment, their obligations and responsibilities are built to handle organizational security policy. To reduce potential security threats, all employees, contractors and third-party users should get enough safety measures, awareness and orientation in security processes and the proper use of information processing facilities. Management in each division should also ensure that personnel under their supervision are appropriately trained on their information security duties before being provided access to sensitive data or information systems. Employees, contractors and third-party users shall exit the banks in an orderly manner. All equipment and access rights associated to their user role should have to be returned and revoked, and whenever an employee changes role with in the bank, the user's access right also should have to be reviewed. The review includes canceling access rights that are no longer needed, unless it has been explicitly authorized by the information system owner or authorized delegates.

Compliance: Management must ensure that security policies are implemented and that regular checks are conducted to ensure compliance with security policy and standards. Critical information systems should be reviewed at least every two years and the IT auditors shall perform compliance reviews or audit of the implementation of recommendations from information incident reports, when necessary. The researchers recognized from the document analysis that the data collected through the questionnaire are included in the institution's information security policy. However, there is a gap when the strategy is implemented on the ground. Despite the fact that these information security regulations exist, their content is limited in contrast to industry standards, in this case ISO 27001, and they are either not communicated or workers lack sufficient awareness. This in turn shows that the organizations did not revise their security policy in the last two or three years, since higher management has waited for managers to submit proposals on revising the security policy.

4.3 Discussion

This study was carried out to reduce and gradually resolve information security-related difficulties and disasters that arise in a variety of ways by evaluating the existing information security maturity level and identifying security gaps in the Ethiopian private banking industry. Although banking is a key financial organization in the economic sector, it is formally vulnerable to fraud and attacks both internally and externally.

The total number of private banks in Ethiopia is 16, according to data acquired from the National Bank of Ethiopia (NBE), and the researchers divided them into four groups based on their high-profit achievement in the 2019/2020 fiscal economic year. Theoretically, the banks with the highest economic achievement are more vulnerable to security attacks, whereas those with the lowest economic achievement are less important to attackers. As a result, when the bank makes a large profit, it becomes a more attractive target for attackers. As a result, Bank A, Bank B, Bank C and Bank D have been arranged in order from highest to lowest profit attainment, from A to D.

The information security maturity level is not a one-time task; institutions founded on information systems must evaluate their security maturity level on a regular basis, as several researchers suggest. This research aimed at answering two research questions, which are discussed below.

RQ1. "Where is the information systems' security maturity level of Ethiopian private banking industry?"

The assessment of information security maturity levels helps in determining the organizations' relevant security processes that must be enforced in order to achieve information and information security system. Maturity level values scale from zero to five are used to measure the level of maturity in line with the Maturity Level Performance Objectives.

According to the study's results, the average value of the information security maturity level on the Ethiopian private banking industry in terms of the selected banks is 2.45, and the maximum result on information security maturity level is five (Optimized). This level of significance suggests that information security maturity is at the second level, and that is repeatable but intuitive. And, according to the SSE-CMM assessment criteria, level 2 means that information security controls exist and are carried out in an ordered and controlled way, but in an unstructured manner.

The value of the difference between the actual information security maturity level and expected information security requirements is 2.55. There is a legitimately significant disparity in terms of value in relation to current maturity level as the expected maturity level's worth. There is an action cycle that is repeated when doing duties connected to information security governance management, but its presence has not been explicitly proven or properly defined, and formal inconsistency exists. As stated in the prior section, private banks must be more secure and knowledgeable on the subject because they handle financial information and must address security.

According to Beshah, (2017), the Ethiopian banking industry's maturity level of ISM is lower than what is predicted, with weak information security control and management. According to the study, there is also no information security system or standard used by banks as well as no legislative framework enforced by the banking regulatory body. According to the report, the majority of the banks surveyed lack a structured information security standard, 83.3% lack an ISM standard and 16.7% have implemented COBIT, ISO and PCI DSS independently. The analysis did not calculate maturity and did not define it with a number, and it was carried out using the DNB maturity level evaluation system. Finally, based on the research findings, the researcher suggests that the maturity level gap should be filled by performing an assessment of information security maturity level on a regular basis. Furthermore, banks should offer security awareness training to employees as well as enforce security policies and procedures. In our research, however, majority of the respondents (more than 70%) agreed that their bank has adopted an information security policy, even though there are no institutional framework criteria imposed by regulatory body NBE. The information security division is organized at a department level and has security staff, which was not the case couple of years ago. There is a noticeable difference between the two studies. However, the information security maturity level must be assessed on a regular basis in order to compare the research results and close the gap.

Although not in financial sector, related local research studies were conducted to assess the maturity level of Ethiopian public universities (Ejerssa, 2018). The ISO27001:2013 information security control priorities were used by the researcher, and the study was carried out using the SSE-CMM maturity model evaluation criteria. According to the findings of the study, the majority of the security domain has a maturity level of 2 (Repeatable but intuitive). Another study conducted by Gera, (2019) on assessing the information security maturity

level of hospitals in Addis Ababa using the ISO27002, shows the outcome of maturity level 2 based on the SSE-CMM maturity assessment model.

The sensitive nature of the data handled by financial institutions distinguishes them from hospitals and educational institutions. Hence, in this research, the financial sector's maturity level is nearly identical to that of the other sectors. In recent years, the banking industry has shown an increase in the implementation of electronic e-banking services, and the market is now focused on providing superior customer service. In order to provide high-quality service, banks must safeguard the confidentiality, integrity, and availability of their information systems. Financial services have become one of the most common targets for electronic criminals as technology has advanced.

RQ2. "How can the security gaps be improved to enhance the information security maturity of the private banks?"

The maturity levels are assessed in order to decide the necessary security changes that a company can implement in order to create a better information and information security framework. Using the results of the questionnaire data, the average value of information security maturity level in Ethiopian private banks was measured. The four sampled banks' average maturity level is 2.45, which is level 2, and the estimated maturity level is 5. Knowing an organization's information security maturity level gives you more trust that its data assets are adequately protected against persistent attacks. It also provides a standardized and systematic mechanism for identifying and assessing information security threats, designing and enforcing appropriate controls and monitoring and improving the effectiveness of the major security areas specified in ISO 27001 information security control criteria.

Several international standards have also emphasized the importance of an organization's information security strategy. According to ITIL, ISO and SAN, information security standards should be implemented within the organization, and employees should be familiar with the policy. Bank X has put in place an information security policy, but it does not seem to be well applied across the whole branches. Some employees are unsure of what they are and are not supposed to do. According to quantitative statistics, 30% of employees are unaware that their company has an information security standard.

According to the study results, the banking industry is facing both internal and external information security threats. A total of 40.7% of respondents reported internal attacks, 22% reported external attacks and 37.3% say all types of attacks. To defend against such attacks, private bank top management must understand the value of information security and pay careful attention to information security maturity on a regular basis. They must focus on creating and coordinating information security teams, as well as allocating an appropriate budget to meet the department's technological requirements. Furthermore, any employee should follow the ISM system protocol and lock his or her computer whenever he or she leaves the workplace, during lunch or break time, or even when he or she goes to another office and there should be a policy in place to protect his or her data from desktop change, including the use of strong passwords and frequent changes, which must be implemented by policy.

According to the study's findings, critical infrastructures such as financial institutions, Internet service providers and national security institutions face challenges, such as a lack of in-house expertise, difficulty identifying the correct security warning sign, a lack of enabling technologies and violation of existing security controls. For information security, expertise or trained professionals are required. According to recent studies, technologies do not work independently. Technological solutions make use of people, procedures and job practices. Trained professionals should use information security software as part of a larger security activity. Besides, based on the interview responses, the following are challenges in relation to information system security maturity in the case private banks:

(1) The information security manual lacks standardized risk analysis and security guidelines.

(2) There are no systems in place to track the level of information security maturity.

(3) Professional and certified information security specialists are in short supply.

(4) Disaster recovery is not adequately planned for server environments that are in the same location.

(5) Security guidelines for information systems are not adequately updated and reviewed on a regular basis.

(6) There is no distinction or separation between the information security strategy and the IT governance system.

(7) There are no industry norms or best practices on a financial system governor.

(8) Employees are not aware of the security requirements for information systems.

(9) Information is needed to bridge the gap between departments and to improve the detection of emerging risks.

(10) Budget and manpower allocations are inadequate.

The information security areas such as access control, physical and environmental protection, supplier relationships and compliance are all information security measures that are rated at a higher maturity level, which is level 3 of maturity (Define) procedure. This research also aimed to evaluate the security control objectives with the lowest maturity levels, which were shown to be extremely weak, and these are: cryptography, information security incident management and information security aspects of business continuity management. These security control zones, on the other hand, need to be improved.

5. Conclusion and recommendations

5.1 Conclusion

According to the SSE-CMM, the average result is 2.4 for all of the ISO 27001 controls. Hence, we conclude that the banks do not have a predefined and distinct information protection disaster recovery strategy or risk reduction techniques. However, they are partly consistent with international requirements and guidelines such as ITIL, COBIT and ISO. Some processes, such as data classification and incident escalation to the chief information officer, are well executed, whereas some other processes and practices are not well-established, such as awareness and training programs, operational risk prevention systems, teamwork, risk assessment processes and post-incident practices such as sharing of experience are examples of factors that limit maturity.

Human resources, especially technical workers, are not well-versed in technological innovations. This increases the company's exposure to information system security threats. Besides, failure to conduct regular risk analysis and maturity level measurements exposes IT systems to various attacks caused by emerging technology and incidents. Security solutions from different software suppliers and device providers in the banking industry are not adequately tested for possible risks. As per the survey results, private banks do not get their systems evaluated by third parties that have the appropriate resources and experience for risk assessment. Besides, they do not perform comprehensive risk assessments on their own.

5.2 Recommendations for practice

Maturity of information systems' security indicates the degree of development and strength of an organization's security measures to mitigate risks threatening its assets. This study, thus, can help banks to visualize their current information protection capacity and identify security gaps that need to be addressed. Other banks and related financial institutions can also evaluate their information systems' security level using the assessment tool and technique used in this study.

Although the private banks have an information security policy in place, security guidelines and procedures are not well documented and security-related activities are exercised on an ad hoc basis. The information security policy should also be reviewed periodically for its adequacy and completeness. Besides, the user access rules and rights for each user should be expressly stated in a policy guideline. In the event of a transition or promotion, each employee's access privileges must be changed. Employees' information security awareness should also be assessed during the hiring process and on the job periodically. Rules governing information security requirements should also be included in the contract of employment. When an employee, contractor or third-party leaves the organization, he or she must return all of the institution's assets that were used for work under the terms of the contract.

A growing number of information security threats have been reported in recent years. Malware, virus and power outage as well as minor errors with serious consequences are all common occurrences. Financial institutions are highly vulnerable to threats that can damage their operations in various ways and jeopardize their survival. Any kind of attack in the financial sector cannot be tolerated. This study revealed that information security incident management in private banking is found inadequate (i.e. 2.3) and classified at level 2 (repeatable but intuitive). To avoid asset loss and disruption of institute operations, information systems should be monitored and physically well secured. Thus, there must be a well-organized and skilled incident management response team, and this team must practice daily to obtain experience. The banks should focus mainly on difficult areas such as response time, user report process and knowledge gap. All IT staff, managers, incident management team members and other company employees with essential positions must participate in the emergency preparedness practice.

The researchers also recommend that banks should execute the following system security standards specified for each level to have regular improvement and monitoring:

Banks should undertake the following to reach level 3 from their current maturity level of 2:

(1) Create a security standard methodology and follow it.

(2) When both internal and external security-related incidents are noticed and tracked, coordinate practices to resolve the issue.

(3) Organize security awareness, education and training programs.

(4) Control and manage security services and mechanisms.

(5) Changes in the operational security posture should be tracked and dealt in accordance with security goals.

(6) Implement, monitor and update information security standards on a regular basis.

Banks should do the following to reach level 4 from their current maturity level of 3:

(1) They should set measurable information security targets and manage threat protection performance objectively.

(2) The activities and processes clearly show that the customer's security requirements were met.

(3) Implement proper physical security controls to guarantee that all facilities housing key systems/equipment, as well as physical areas.

Banks should undertake the following to reach level 5 from their current maturity level of 4:

(1) Increasing organizational capability in terms of process efficiency by gathering, synthesize and monitor vulnerabilities and their attributes using a threat risk analysis method.

(2) To the extent essential to accomplish their roles, all members of a security project team are aware of and involved with security engineering efforts.

(3) Implement and administer a centralized system for detecting, removing and protecting against harmful code in all forms.

(4) Banks should focus their improvement efforts on the required commitment at all levels in order to achieve all incremental maturity levels.

5.3 Suggestions for future research

To have a regular enhancement of the maturity of information systems' security and to have a capability to protect the institution's information system from technological advancement threat, the researchers believe that conducting a more detailed research studies can better benefit financial institutions. Accordingly, this research considered limited private banks. If a future study considers all private banks, the results of this study can be improved which again can provide additional insights. Assessing the security maturity level of an information system is not a one-time activity. As a result, evaluating maturity level over time and comparing the result with this study can help management to trace the progress and find areas of focus. Construct a framework that allows the financial sector to self-assess the maturity level of information systems' security.

Note

1 Quote by Lord Kelvin. "To measure is to know."

References

Abebe, G. (2020), "A framework for human factors influence on information systems security at commercial banks in Ethiopia", MSc. Thesis, Addis Ababa University (unpublished).

Amare, B. (2015), "Assessment of insider threat in Ethiopian banking industry", MSc. Thesis, Addis Ababa University (Unpublished).

Beshah, E.B. (2017), *An Investigation on the Current Information System Security Maturity Level of the Banking Industry in Ethiopia*.

Creswell, J.W. (2013), *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*, Sage Publications, Los Angeles.

De Haes, S., Van Grembergen, W., Joshi, A. and Huygh, T. (2020), *Enterprise Governance of Information Technology: Achieving Alignment and Value in Digital Organizations*, Springer Nature Switzerland AG, Cham.

Deferew, B. (2020), "*Cyber hygiene practices amongst employees of ethiopian commercial banks*", MSc Thesis, Addis Ababa University (unpublished).

Ejerssa, N. (2018), "Assessment of information security maturity level on Ethiopian public universities", MSc. Thesis, Addis Ababa University (Unpublished).

Ferraiolo, K. (1998), "The systems security engineering capability maturity model", available at: https://csrc.nist.rip/nissc/1998/proceedings/tutorB5.pdf

Gera, E. (2019), "Assessment of maturity level of information security management using ISO 27002 at hospitals in Addis Ababa, Ethiopia", MSc. Thesis, Addis Ababa University (Unpublished).

Hailu, H. (2015), "The State of Cybercrime Governance in Ethiopia", available at: file:///C:/Users/lemma/Downloads/Cyber-Crime2015.pdf

Houngbo, P.J. and Hounsou, J. T. (2015), "Measuring information security: understanding and selecting appropriate metrics", *International Journal of Computer Science and Security (IJCSS)*, Vol. 9 No. 2, pp. 108-120.

Kebede, A. (2019), "Designing a framework for selecting effective information security awareness delivery method", MSc. Thesis, Addis Ababa University (unpublished).

Kurniawan, E. and Riadi, I. (2018), "Security level analysis of academic information systems based on standard iso 27002: 2013 using SSE-CMM", *International Journal of Computer Science and Information Security (IJCSIS)*, Vol. 16 No. 1, pp. 139-147.

LLC, P.I. (2017), *Cost of Cyber Crime Study: Insights on the Security Investments that Make a Difference*, Accenture Security.

Negussie, A. (2015), "Practices, challenges and prospects of information security policy in Ethiopian banking industry", MSc. Thesis, Addis Ababa University (Unpublished).

Nieles, M., Dempsey, K. and Pillitteri, V.Y. (2017), *An Introduction To Information Security (NIST Special Publication (SP) 800-12 Rev. 1 (Draft))*, National Institute of Standards and Technology, US Department of Commerce.

Olusegun, O.J. and Ithnin, N.B. (2013), "Enhancing the conventional information security management maturity model (ISM3) in resolving human factors in organization information sharing", *International Journal of Computer Science and Information Security*, Vol. 11 No. 8, pp. 65-76.

Osamah, M.M. and Al-Matari, I.M. (2021), "Adopting security maturity model to the organizations' capability model", *Egyptian Informatics Journal*, Vol. 22 No. 2, pp. 193-199, doi: 10.1016/j.eij.2020.08.001.

Pijpers, T. (2015), *A framework for Financial Institutions to Achieve Maturity Level 4 based on the DNB Assessement Framework*, De Nederlandsche Bank N.V.

Ponemon Institute LLC (2015), "2014: a year of mega breaches", Sponsored by Identity Finder, available at: https://www.ponemon.org/local/upload/file/2014%20The%20Year%20of%20the%20Mega%20Breach%20FINAL_3.pdf

Rainer, J.R. (1991), "Risk analysis for information technology", *Journal of Management Information Systems*, Vol. 8 No. 1, pp. 129-147.

Ransbotham, S. (2015), "Information disclosure and the diffusion of information security attacks", *Information Systems Research*, Vol. 26 No. 3, 150818112523008.

Redlin, T.G. (2017), "Innovations, growth and participation in advanced economies - a review of major concepts and findings", *International Economics and Economic Policy*, Vol. 14, pp. 293-351.

Rosmiati, Riadi, I. and Prayudi, Y. (2016), "A maturity level framework for measurement of information security performance", *International Journal of Computer Applications (0975-8887)*, Vol. 141 No. 8, pp. 1-6.

Saleh, M. (2012), "Information security maturity model", *International Journal of Computer Science and Security (IJCSS)*, Vol. 5 No. 3, p. 21.

Saleh, M.F., Abbad, M. and Alghazo, J.M. (2012), "Compliance to the information security maturity model in Saudi Arabia", *Journal of Computer Science and Engineering*, Vol. 14 No. 2, pp. 1-8.

Tebkew, K. (2016), "Information security framework for banking industries in Ethiopia", MSc. Thesis, Addis Ababa University (Unpublished).

Waxman, M.C. (2013), "Self-defensive force against cyber attacks: legal, strategic and political dimensions (March 19, 2013)", *International Law Studies*, Vol. 89, available at: https://ssrn.com/abstract=2235838

Yemane, G. (2018), "Assessing information security management using an ISO 27001:2013 framework: a case study at Ethio Telecom", MSc. Thesis, Addis Ababa University (Unpublished).

Yohannes, T., Lessa, L. and Negash, S. (2019), "Information security incident response management in an Ethiopian bank: a gap analysis", *AMCIS*.

Corresponding author
Lemma Lessa can be contacted at: lemma.lessa@aau.edu.et