# Application of Soft Systems Methodology (SSM) to develop Information Systems Security Model for Ethiopian Banking Industry

Dawit Mekonnen
HiLCoE, Computer Science Programme, Ethiopia
dawitmek22@gmail.com

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

**Abstract**

Information Systems (IS) security protects all information assets from misuse, harm or any other unintended results. Literature suggests that focusing on the technical aspects of IS security without due consideration of how a human interacts with the system is insufficient in safeguarding Ethiopian banks' information assets. To fill this gap, this paper adopts a broader perspective and presents an understanding of IS security in terms of a social and organizational perspective using the Checkland's Soft Systems Methodology as an approach in order to achieve a greater insight of the problem situation and with the aim of identifying changes which could improve it. Mixed research method is used as a research paradigm and survey questionnaire and interview are used as methods of data collection. By applying SSM, this paper identified and explored IS security problems and obstacles facing the Ethiopian banking industry. A conceptual model has been proposed. The solutions derived then form the basis upon which recommendations are presented that are both systemically desirable and culturally feasible.

*Keywords:* Soft Systems Methodology; Information Systems; Information Systems Security

## 1. Introduction

Information has become the most valuable asset to protect from insiders, outsiders and competitors. As defined by Lee [1] "an information system is not the information technology alone, but the system that emerges from the mutually transformational interaction between the information technology and the organization". Organizations continue to witness information-related crime and damage becoming the choice of a growing global criminal element. Existing institutions burdened by countless conflicting jurisdictions and inadequate resources have not been successful in reducing the amount or impact of these activities. Maintaining information security requires support and co-operation from all employees within the organization. Even though the technical aspect of IS security needs due attention, a more serious and under-rated aspect of IS security is the human element. Martins and Eloff [2] underline that the behavior of employees and their interaction with computer systems have a significant impact on the security of information. Many losses are not caused by lack of technology or defective technology rather by users of technology and flawed human behavior. The importance of non-technical issues related to information security hasn't been given attention in many studies [3]. Consequently, little attention has been given to the role of human factor like individual choice and behavior or to organizational factors such as national and organizational culture, environment, information security awareness level of employees and how the factors relate to attitudes of employees about information security. However, empirical studies [3, 4, 5] have revealed that non-technical issues are very important in safeguarding an organizational sensitive information.

A bank's ability to take advantage of new opportunities often depends on its ability to provide open, accessible, available, and secure network

services. Having a good reputation for safeguarding information will increase market share and profit. Nowadays, banks are implementing different types of practices to protect information and information systems from fraudulent attacks.

The banking industry in Ethiopia is one of the rapidly growing sectors of the country's economy. In addition, the banking service has shifted from local branch banks to national and global existence and anywhere-anytime banking. The Banking business competition has motivated the advancement of services enabled by IT which in turn increased the information security risk. These threats to information and information systems can include purposeful attacks, environmental disruptions, and human/machine errors and result in great harm to the national and economic security interests of the country [6].

Ethiopian banking system is still underdeveloped compared to the rest of the world regarding electronic payment, Internet banking, Mobile banking, online shopping, etc. Such systems are at early stage. The reasons for this weak or evolutionary development are numerous. The main one that is cited by different scholars is security threat or poor implementation of information systems security [7, 8, 9]. Currently, for the banking industry, there is no information security standard and there is no clear guidance regarding what would establish an acceptable minimum baseline body of information security knowledge for end users [7].

Literature survey and from our experience it is revealed that many Banks in Ethiopia do not have a comprehensive IS security framework or baseline which serves as a guide to develop and implement their own information security policy based on their own requirement in line with notional information security policy. There is no regulatory organ that supervises activities of the banks regarding information security. There is no functional cyberspace security policy in Ethiopia [9]. Security has not been given a considerable attention in Ethiopian banks. Even most of the banks do not have security department or officers [10]. There is lack of research in the area that can support the industry to compete with technologically advanced commercial systems of the rest of the world [10]. A study in [8] revealed that Information security awareness in the banking sector in Ethiopia is unsatisfactory. Consequently, the level of proper information security governance in the banking sector is a critical area for improvement.

In addition, major international information security standards applicable in the world are written from a Western perspective, without knowing how applicable Information Security Management (ISM) concepts and practices are to other cultures, which have different social, organizational, and security cultures [11]. The standards do not mention how this can be attained. They do not clearly show the steps or methods that any bank can follow in their requirement identification process when they develop IS security model.

Different literatures and empirical studies have revealed that IS security is unexplored area and complex and dramatically changing. IS security challenges in the banking industry are numerous and inherently diverse [7, 8, 9].

Those kinds of situations are the objectives of this paper, which has been addressed by adopting a holistic system approach which is Soft Systems Methodology (SSM). SSM is a systematic approach for tackling real-world problem situations. It was developed in the 1970s by a team of academics from the University of Lancaster led by Prof. Checkland. SSM is defined by Checkland [12] as *"Soft systems methodology (SSM) is an approach for tackling problematical, messy situations of all kinds. It is an action-oriented process of inquiry into problematic situations in which users learn their way from finding out about the situation, to taking action to improve it."*

The main reasons why we adopt SSM as an approach is to explore problem situations in the banks of Ethiopia and to develop IS security model. SSM by its nature is practical, highly participative,

used as a learning tool and flexible approach to manage changes by perceiving a holistic approach that takes a wider range of factors into account including social and political aspects aiming to suggest change that is meaningful and feasible in the organizational context. In addition, as defined by Checkland, SSM is not a system development methodology rather it is a methodology to identify changes and also it is human problem and process oriented not technique oriented.

From literature and empirical studies, application of SSM for developing IS security model is not implemented so far. Taking these facts into consideration, we apply SSM as an approach to identify and explore IS security issues, assess the current status and practices of IS security processes in the banking industry in Ethiopia and develop IS security model which serves as a guide for developing and implementing IS security baseline.

## 2. Related Work

Ula *et al*. [13] proposed specific Information Security Governance Framework (ISGF) for governing information security in the banking environment. The framework is categorized into three levels which are Strategic, Tactical and Operational, and Technical level. Essentially, the framework is still a general approach to information security governance. It needs to be reviewed by professionals and comprehensively tested in a real banking environment.

The main objective of the work in [14] is to demonstrate the application of SSM to issues and obstacles facing Saudi Arabian government organizations that use ICT. A number of techniques and approaches were used in achieving these objectives including quantitative and qualitative techniques of data analysis. By applying SSM a conceptual model has been proposed. Even if the approach used is useful for our purpose, the proposed model is directly applicable for ICT issues and problems which do not specifically address information security aspects.

SSM is used as a diagnostic tool to analyze a real case information security incident in [15]. The authors used qualitative methodology to collect data by conducting unstructured interview. SSM is used as a diagnostic tool to analyze a real case information security incident not to propose a comprehensive information security conceptual model.

The main objective of the work in [16] is to propose applicable information systems security auditing framework to support people in the area of IT Auditing. It mainly focuses on developing information systems security auditing framework for the respected banks of Ethiopia.

The purpose of the work in [8] is to investigate the extent of information security culture in Ethiopia and indicated that, even big banks in the world that generally do better on security are victims of security breaches. Finally, the authors concluded that there is a significant space to enhance the trust environment between managers and employees that can promote change in information security culture and more rigorous researches are needed to frame practical strategies to enhance the information security culture in the banking sector in Ethiopia.

The work in [17] was to develop and propose Internet banking security framework. The main objective was to develop Internet banking security framework and its major five models aiming to overcome major security issues, specifically for social engineering attacks. However, security breaches and incidents are not only social engineering attacks. There are a variety of attacks, incidents, issues and problems that need to be considered as IS security issues and problems.

The work in [18] focuses on the effect of strong corporate culture and organizational commitment as important aspects for enhancing information security. The research tries to examine the extent to which information security behaviors, as part of an organizational culture, relate to a common work attitude variable known as organizational commitment. The authors used survey questionnaire for employees of a large sized bank in Greece. They

concluded that in order to ensure effective and proactive information security, all staff must be active participants rather than passive observers of information security. However, no model, guideline, or framework is proposed to be followed or practiced.

## 3. The Proposed Solution

By applying SSM we developed a conceptual model for Information Systems Security for the Ethiopian banking industry as shown in Figure 1. In the proposed model there are nine inter dependent activities that must be performed for modeling Information systems security system for the banking sectors.

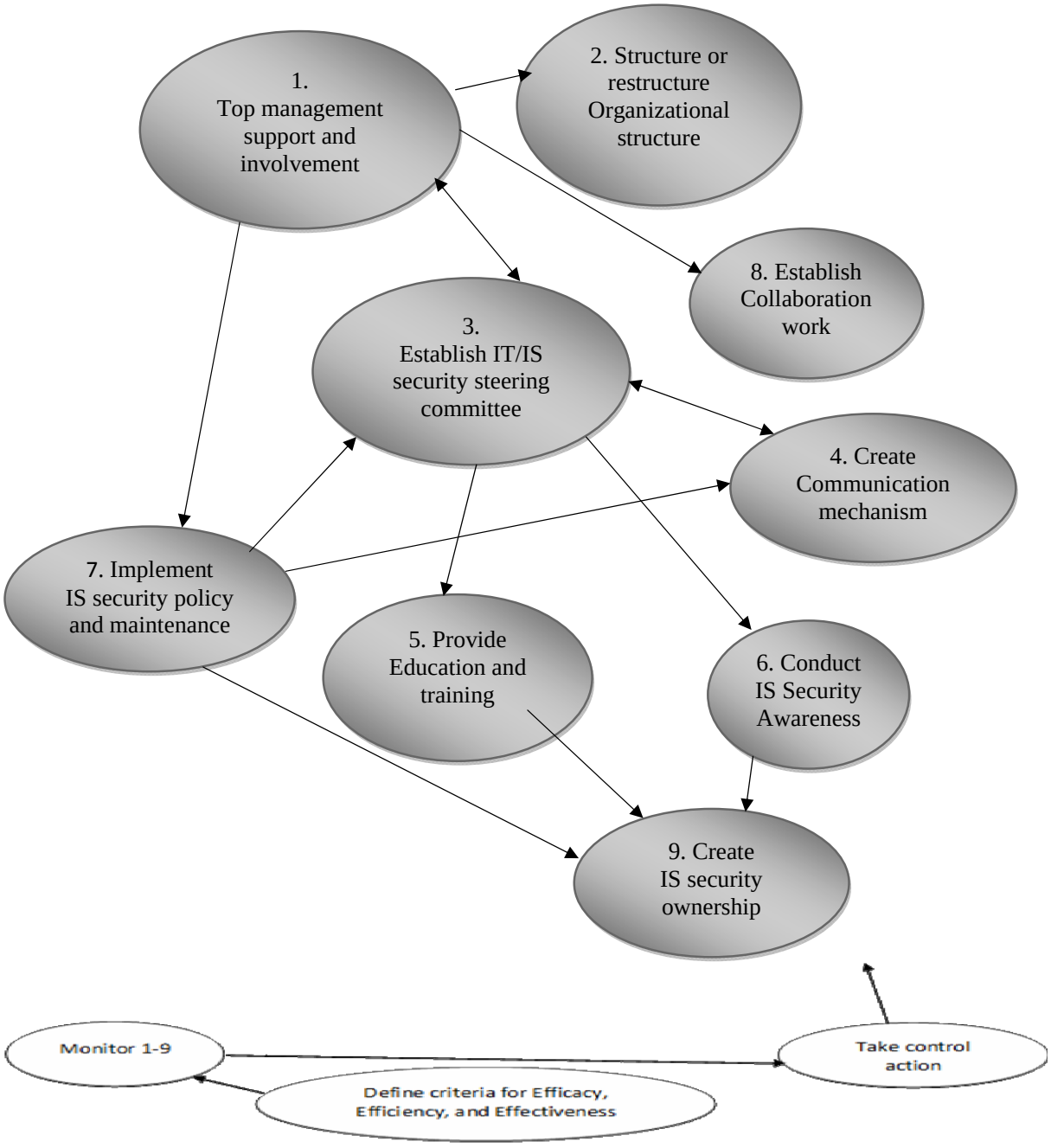


*Figure 1:* Conceptual Model of Information Systems Security for the Ethiopian Banking Industry

Possible recommendations which are systemically desirable and culturally feasible solutions for the situation are proposed for the Ethiopian banking industry as follows.

- Conducting an awareness about IS security objectives to the top management is very essential in order to get top management's attention, because top management is the one to have the most influence in a bank. The awareness program must focus on business benefits that can be gained from improving IS security activities of a bank.
- Top management support and involvement is also the main activity for the success of effective implementation of IS security in a bank. This activity is also accepted and suggested by the SSM group discussion as a primary change in the banking industry.
- Another area of possible change in the banking industry in Ethiopia suggested by the SSM group discussion is organizational structure of IT security office. IT security office should report directly to the President or Chief Executive Officer of a bank.
- Result obtained from the discussion and data collected shows that there is no IT security steering committee in the Ethiopian banking industry. Discussion in the SSM group strongly suggested the need to establish IT/IS security steering committee that has actors from the concerned departments and executives of a bank.
- It has been manifested from group discussion and data collected (questionnaire and interview findings) that the banking industry in Ethiopia encounters a problem in implementing and enforcing IS security policy. The SSM group discussion agreed and suggested to establish and implement IS security policy, guidelines, procedure, manuals, etc. throughout policy enforcement, review and update the policy periodically.
- It has been marked from the group discussion and data collected (questionnaire and interview findings) that banks in Ethiopia are weak in providing advanced education and training for IT security experts. Therefore, banks of Ethiopia should provide sufficient tools and facilitate information security related training for IT security experts, and supply instruction guidance and manuals that can be easily understood.
- SSM group discussion agreed on an acceptable idea and suggested that Banks in Ethiopia should deliver strong and consistent communication mechanisms for communicating IS security policy, procedures, guidelines, manuals, etc.
- The SSM group discussion suggested that it is advisable for top management to establish strong and consistent cooperation and collaboration among the three business units of a bank which are IT department, IT security office and IT audit division.
- Participants of the SSM group discussion suggested that it is a must to aware and train all staff of a bank about their IS security roles and responsibilities continuously and to hold them accountable in order to enhance their bank's performance.

## 4. Discussion

We obtained a clear picture through a discussion with key participants (SSM group) and from the data collected (questionnaire and interview) at each site of the surveyed banks of Ethiopia. This research clearly identifies IS security issues and challenges in banks of Ethiopia which are: absence of IT security steering committee, communication gap with the management and staff, lack of IS security awareness, lack of financial and human (IS security qualified experts) resource, lack of IS security governance, inefficiency of IS security risk management processes, lack of advanced training for IT security experts, disorganization of IT security office in the

organizational structure, and implementation of informal and unapproved IS security policy.

By applying SSM we identified social and political issues and obstacles in the Ethiopian banks like: lack of IS security awareness, high level of power distance cultural factor within the top management and IT security office of the bank resulted a challenge in order to convince and aware top management of the banks of Ethiopia about the importance and necessity of IS security objectives in safeguarding the banks data and the need for continual improvement, lack of policy enforcement due to lack of IT security office empowerment and so on.

## 5. Conclusion

When banks in Ethiopia want to develop and implement information systems security framework or baseline, it is advisable to consider the following issues primarily which means without the issues listed below, it is difficult to construct or develop any organizations Information Systems Security model. Therefore, the basic nine concerns to develop Information Systems Security model for an organization are listed below:

1. Top management support and involvement.
2. Structuring or restructuring IT security office.
3. Establishing IT/IS security steering committee for the bank.
4. Creating a Communication mechanism throughout the bank.
5. Providing adequate education and training for IT security experts.
6. Conducting IS security awareness.
7. Implementing IS security policy through policy enforcement.
8. Establishing a strong collaboration with three business units (IT security office, IT audit division and IT/IS department).

## References

[1] Lee, A. S., “Thinking about Social Theory and Philosophy for Information Systems”, John Willey and Sons, Ltd, Chichester, England, 2004, pp. 1-26.

[2] Martins and Eloff, “Information Security Culture in Public Hospitals: the case of Hawassa Referral Hospital”, The African Journal of Information Systems, Vol. 3, Issue 3, 2011, pp. 72-86.

[3] Siponen, M. and Oinas –Kukkonen, H., “A Review of Information Security Issues and Respective Research Contribution”, SIGMIS Database, 38(1), 2007, pp. 60-80.

[4] Dhillon and Torkzadeh, “Value-focus Assessment of Information Systems Security in Organizations”, Information System Journal, 2006, pp. 293-314.

[5] Vroom, C. and von Solms, R., “Towards Information Security Behavioral Compliance”. Computers and Security, 23 (3), 2004, pp. 191-198.

[6] Patrick, D. G., “Managing Information Security Risk: Organization, Mission, and Information System View”, U.S. Special Publication 800-39, 2011.

[7] Ayana Gemech, “Adoption of Electronic Banking System in Ethiopian Banking Industry: Barriers and Drivers”, May 14, 2012, retrieved from http://www.papers.ssrn.com/so13/papers.cfm?abstract_id=2058202.

[8] Abiy Woretaw and Lemma Lessa, “Information Security Culture in the Banking Sector in Ethiopia”, 5th ICT 2012 Ethiopian Conference, June 08, 2012.

[9] Balcha Reba, “State of Cybersecurity in Ethiopia”, June 2012, retrieved from http://www.itu.int/osg/spu/cybersecurity/contributions/Ethiopia _Reba_paper.pdf.

[10] Yigezzu Belay, “Information Systems Security Audit Readiness in case of Ethiopian

Government Organization", 2011, retrieved from http://www.spidercenter.org/sites/default/files/master_thesissponsored/Ms_Thesis_Yigezzujorro.pdf.

[11] Mohammed, A., and Karen, N., "A Proposed Framework for Understanding Information Security Culture and Practices in the Saudi Context", in Proceedings of the 7th Australian Information Security Management Conference, 2009.

[12] Checkland, P. and Poulter, J., "Systems Approach to Managing Change, A Practical Guide", London, Springer-Verlag, 2010, pp. 191-242.

[13] Munirul Ula, Zuraini BT Ismail and Zailani Mohamed Sidek, "A Framework for the Governance of Information Security in Banking System", Journal of Information Assurance and Cyber Security, 2011).

[14] Saleh Al Zhrani, Al Imam Muhammad bin, "Development of a Soft System Model to Identify Information and Communications Technology Issues and Obstacles in Governmental Organization in Saudi Arabia", Journal of Theoretical and Applied Information Technology, pp. 93-104.

[15] A. Bilal, K. Stewart. "Security from a System Thinking Perspective: Applying SSM to the Analysis of Information Security Incident". Stockholm University.

[16] Shemlse. Gebremedhin, "Information Systems Security Audit Framework for Banking Industry", Unpublished Masters Thesis, HiLCoE School of Computer Science and Technology, Addis Ababa, Ethiopia, 2013.

[17] Aychiluhim Dessisa, "Internet Banking Security Framework: the case of Ethiopian Banking Industry", Unpublished Masters Thesis, HiLCoE School of Computer Science and Technology, Addis Ababa, Ethiopia, 2014.

[18] Ioannis Koskosas, Konstantinos Kakoulidis, and Christos Siomos, "Information Security: Corporate Culture and Organizational Commitment", International Journal of Humanities and Social Science, Vol. 1, No. 3, pp. 192-198, March 2011.