Journal of Digital Science

ISSN 2686-8296

Volume 4 Issue 1 **June 2022**

CONTENTS

A conceptual framework for assessing information security management practices in selected universities in Uganda

Benjamin Ahimbisibwe [1][0000-0002-0570-1274],
Peter Nabende [1][0000-0003-2141-7940]

[1] Makerere University, Kampala, Uganda

https://doi.org/10.33847/2686-8296.4.1_2

Received 21.04.2022/Revised 03.05.2022/Accepted 22.05.2022/Published 12.06.2022

Abstract. The purpose of this paper is to present a conceptual framework for assessing managerial level information security practices, governance, and activities in selected university institutions in Uganda. Extant literature was drawn from existing information security management practices in different organizations. The proposed conceptual framework consisted of four manageable areas, namely, information security governance practices, information security practices, personnel management practices, and physical security practices. These areas are further subdivided into 25 categories that provide a formal checklist for assessing existing information security management practices in university institutions in Uganda.

Keywords: Conceptual framework, information security management practices, university institutions in Uganda.

1. Introduction

A conceptual framework describes the state of knowledge, identifies gaps in the phenomena under study, and outlines methodological underpinnings. Bilsky et al. [7] sum it up with two questions: why is the research important? and what contributions might a conceptual framework add to the body of knowledge? A conceptual framework is important because it helps to identify and clarify the central aspects of a study, connecting these aspects and their influence on the research being carried out [17].

Although several studies have been conducted in the information security management (ISM) domain, these studies did not provide a comprehensive guidance on specific practices to be followed by universities in the Ugandan context. None of them provides an adequate checklist of standards for assessing existing information security management practices (ISMPs) adopted by universities in Uganda. This paper proposes a conceptual framework that specifies such a checklist of standards. The conceptual framework was developed based on a generic inductive approach. The conceptual framework evolved during the study as new ideas, insights and knowledge concerned with the assessment of information security management practices got established [28]. At the beginning of the study, a tentative framework was constructed based on initially identified concepts and their relationships. Adjustments to the framework were then made as we gained a deeper understanding of the subject on information security management practices in organizations until the proposed conceptual framework that specifies 25 items for use as a checklist.

2. Literature Review

Several studies have been conducted to guide organizations to develop effective information security programs. The studies conducted in the Information Security Management (ISM) domain have focused mainly on individual aspects and the

application of different conceptual frameworks in various organizations. Current literature is limited in the explicitness to managerial level aspects of information security in organizations. This paper aimed at developing a conceptual framework that explicitly covers managerial level aspects of information security in selected universities in Uganda. In this section, we review some considerably related studies and discuss their relevance to the Ugandan context. We focus on the wider perspective of the ISM domain, information security management practices (ISMPs), and ISMPs at Kabale University and Bishop Barham University College both located in the western region of Uganda.

Information security is a multidimensional problem that is continually evolving and changing. Studies have evolved from approaching information security in a one-sided technical perspective to a managerial perspective with the view to providing a holistic and comprehensive approach [31]. A shared characteristic of existing studies is the aim to provide guidance to organizations by identifying activities that constitute a security program. The different studies use different terminologies such as processes, principles, practices, activity or theory to present their advice. Furthermore, existing studies use different levels of detail and analysis in describing the activities that organizations should implement. It is from the review of these studies that we identify gaps in terms of completeness, specificity, and implementation of ISMPs.

2.1. Information Security Management Practices in Organizations

In a study conducted by Keller et al. [9] about ISM in small organizations, nine best practices were recommended. These include: installation and proper configuration of firewalls; updated software; protection against viruses, worms, and trojans; implementation of strong password policy; implementation of physical security measures to protect computer assets; implementation of company policy and training; connecting remote users securely; locking down servers; and implementation of intrusion detection services. These practices are technological practices with the exception of implementation of policy and training.

Qingxiong and Pearson [16] proposed an ISM framework with the following five steps: assess organizational environment, establish information security objectives, analyze information security requirements, develop information security controls, and train or evaluate information security controls. However, due to ever changing information security patterns, new challenges associated with rising use of mobile and wireless systems have sprung up. Thus, the framework by Qingxiong and Pearson [16] does not adequately cover for new developments and new vulnerabilities.

According to Tryfonas [26], information security encompasses both managerial and technical aspects with issues emanating from internal and external sources. Tryfonas identified managerial practices such as establishment and use of policy, compliance with security standards, copyright protection, risk analysis and information security audits; and recommended technological practices such as requisite skills, cryptographic solutions, network security and use of firewalls, access control mechanisms, software security practices and intrusion detection techniques. Although Tryfonas identifies both managerial and technical issues, his recommendations are virtuously technological. Tryfonas further stated that simply deploying frameworks alone cannot solve all the information security and IT governance requirements. Therefore, organizations need to develop frameworks with elements that also include support from senior management, that include staff awareness and that include training in order to achieve all the intended benefits.

Other scholars like Oyelami and Ithnin [15] conducted a study on establishing a sustainable information security management policy in organizations. They proposed a guideline to ISMPs describing main processes and the activities of each process as

security management practices to be implemented in organizations to secure information. Accordingly, Oyelami and Ithnin [15] argued that an effective ISM process should consist of six sub-processes: policy, awareness, access, monitoring, compliance, and strategy; Oyelami and Ithnin [15] went ahead to describe each process and the activities undertaken thereof. Their study suggested that a policy process is a repetitive process continuously updated that starts by identifying what to secure, and document a draft policy that is to be published upon approval. However, a policy is exclusively managerial and therefore cannot handle all information security related issues of an organization.

In a study conducted to investigate ISM and its influence in the Nigerian banking sector by Babatunde and Selamat [5], a conceptual framework consisting of technological, organizational, and environmental factors was proposed. This framework identified factors that influence ISM practices among bankers from the perspective of reducing frauds and errors. If properly implemented, it could lead to improvement of information systems security and create a better investment climate in the banking industry.

A recent study was conducted by Zaini et al. [32] and was aimed at determining the extent to which ISM practices impact on the organizational agility. Zaini et al.'s [32] findings indicated that operational agility is significantly related to ISM practices in the sampled Malaysian organizations. Their study conceptualized three factors based on practices including: administrative security, technical security, and physical and environmental security controls. However, the suggested guidelines seemed to be complex to implement for some organizations especially those with difficulties in distinguishing security practices that influence agility [32].

2.2. Information Security Management Practices in Uganda

Uganda like most countries in the world has embraced the use of new Information Communication Technologies (ICTs) in all institutions including universities. This has been attained through introduction of information systems that ease handling of information in university institutions [13]. The adoption of information systems calls for a shift in the information handling mechanisms to match the new trends. There are some studies that have been carried out about information security related issues in Uganda. For instance, an investigation was conducted by Kisakye [10] into information security practices implemented by the Research and Education Networks of Uganda (RENU). Another study by Bogere et al. [8] was on the influence of ICT security to academic environment in universities in Uganda. Mbabazi et al. [12] assessed the implementation of information security policy in Ugandan universities. However, most of the Ugandan studies do not cover the attributes associated with the conceptual framework in this paper.

With the increased integration of ICTs in daily life, universities have also increased utilization of technology induced operations in their systems. This has encouraged the implementation of information systems security with corresponding practices to secure them. A number of university institutions have adopted reforms aimed at improving the implementation of information security measures. These include laws governing information security like the Computer Misuse Act 2011, Electronic Transactions Act 2011, Electronic Signatures Act 2011, Data protection and privacy Act 2019, etc. However, these laws have not been fully operationalized and incorporated in the information security management framework. To supplement these laws, the government of Uganda has developed an information security governance policy with elements of all activities required to manage information, personnel, equipment and physical security [27].

However, information management is still a big challenge to university institutions in Uganda. This is evidenced by the existing under developed information

management practices and strategies to guide information management processes and operations. These include but are not limited to information security governance practices, information security practices, personnel management practices, and physical security practices for information systems security as covered in the proposed conceptual framework in this paper.

3. Methodology

The purpose of this paper was to develop a conceptual framework with enhanced information security management practices in corporate organizations. It was motivated by lack of a comprehensive managerial-based information security framework for enhancing information security in organizations within the Ugandan context. In order to attain the intended objective, it was imperative that a conceptual framework suitable for the proposed solution be developed along the way.

To develop the conceptual framework, a systematic review of related literature in the domain area is recommended as the best approach ([4]; [24]) and it is the approach that was adopted for this paper. The systematic review involved identification of relevant studies, appraisal of their quality, and summarization of the evidence such that reasonable conclusions are reached [24]. This approach was followed to identify key concepts and develop the framework that identifies the different variables and their relationships as shown in Table 1.

4. Proposed conceptual framework for assessing ISMPs

The proposed framework identifies four manageable areas, namely: information security governance practices, information security practices, personnel management practices, and physical security practices. These four areas are further subdivided into 25 closely related subsections (activities) that form the checklist for collecting data and describing the status of ISMPs in an organization and their contribution to an organization's information security.

The proposed conceptual framework shows the relationship between dependent and independent variables (Table 1). The framework describes the connection between the four main categories of ISMPs as well as the activities performed in each (as independent variables), against the organization's information security (as a dependent variable).

Table 1. A conceptual framework for assessing information security management practices in selected universities in Uganda

Main practices	**Sub practices (activities)**	
Independent variables		Dependent variable
Information security governance practices	• Policy statement on information security • Information security organization • Information systems risk management • Information security awareness, education and training among stakeholders • Have Business Continuity & Disaster Recovery mechanisms • Information systems incident risk management • Compliance with information system guidelines	Organization's information security
Information security practices	• Information system asset management • Secure information sharing • Information systems supply chain security • Access management to information systems • Install network security controls	

	• Ensure portable and removable media security • Enhance remote access security • Ensure protective monitoring of information systems • Implement information back-ups • Secure accreditation for IS	
Personnel management practices for information systems security	• Describe staff responsibilities and clear security roles • Ensure baseline security clearance for all users of information systems • Ensure Top secret clearance for all the users	
Physical security practices for information systems security	• Install physical security measures • Install physical entry controls • Design internal data centre & physical access controls • Enhance information systems equipment security • Ensure secure equipment disposal & re-use	

Source: Primary data

In the following subsections, we provide general descriptions of the different independent variables in Table 1 which are critical towards achieving an organization's information security.

4.1. Information Security governance practices

One of the factors that influence how organizations manage an information security program is information security governance ([29]; [31]). Information security governance is a subset of the overall cooperate governance that include the adoption of a comprehensive approach to organize efforts and integrate various information security practices [30]. Adopting it would provide the right strategic direction, achieve objectives set, manage threats appropriately and use organizational resources correctly. However, this would require involvement of senior management and board of directors in information security governance issues. Therefore, implementing information security governance practices with support from higher organizational echelons would help to address the organization's information security issues. This is an implication that involving senior management and board of directors to be held accountable for information security governance practices would provide necessary leadership. According to Trim et al. [25], good information security governance practices can be ensured if it is viewed as an integral part of corporate governance, processes and structures. Therefore, information security governance practices can serve as a major element to secure organization's information. Such a scenario would require a clear policy statement on information security indicating information security aspects, systems risk management approaches, systems incident risk management strategies, education and training among stockholders, well stipulated Business Continuity and Disaster Recovery plans and measures for non-compliancy with information systems security set guidelines.

4.2. Information Security Management

Information security practices are structured processes implemented to manage information security in organizations ([2];[3]). The aim is to maintain adequate levels of confidentiality, integrity and availability of information. This process involves planning, organizing, coordinating and controlling in order to establish acceptable level of security. The information security practices covered in the proposed

framework would entail activities performed to provide protection of information assets in organizations. These activities included asset management, secure information sharing, supply chain security, access management, network security controls, security of portable and removable media, remote access security, protective monitoring of information systems, implementation of information security back-ups as well information system accreditation by professional bodies. These activities if well implemented, would help organizations to maintain acceptable levels of integrity, confidentiality and availability of organization's information security [22]. Therefore, information security practices are regarded as an important element in the proposed information security management conceptual framework for selected universities in Uganda.

4.3. Personnel security practices

Information technology professionals are facing challenging tasks, analyzing, designing, and deploying solutions to protect information resources. This not-with-standing, previous studies concede that human beings are the major sources of many security failures ([11]; [1]). Human beings are vulnerable to a wide range of security attacks ranging from deliberate violation of security policy to circumvention of physical and technical security controls [23]. In addition, practitioners tend to underestimate the likelihood of occurrence of security breaches caused by human beings. A key area in information security research is understanding ways of motivating employees to participate in more secure behaviors [21].

Personnel security practices can address the problems associated with human oriented behaviors. The human resource practices of employee recruitment and selection, training and development, performance monitoring and appraisals are very important to improving organizational security routine [14]. Investing in staff training, awareness and development can motivate them to support attainment organizational goals. Staff training in information security management can serve as critical measure to safe guard an organization's information resources [6].

However, to achieve the best results, security training and awareness programs should be regularly evaluated to match the security threat levels [19]. Similarly, involving employees in overall security programs through commitment and engagement can be seen as a critical factor in improving job performance [18]. This is coupled with employee monitoring as an effort to maintain the high levels of productivity.

In order to ensure baseline security clearance for all users of information systems, employee background checks are important to ascertaining possible criminal records, character, and fitness for the position [20]. For staff to be held accountable and liable for their omissions or commissions with regard to their actions related to information security, their responsibilities and roles should be clearly described and clearance obtained to access top secret information in organizations.

4.4. Physical security

With regard to this conceptual framework, physical security meant activities aimed at installing physical security measures, installing physical security entry controls, designed internal data centre and physical access, all aimed at enhancing information systems equipment security. Physical security practices would stop unauthorized physical access, damage, and interference to information, premises and resources. This would curtail a range of physical security threats like crime, espionage, natural disasters, acts of terrorism and protecting personnel against violence and other harmful acts.

According to ISO/IEC 27001, organizations must protect equipment and personnel against physical and environmental threats. Such security measures help reduce the risk of unauthorized access to information and loss or damage to equipment. Physical security measures have strong importance to equipment, personnel and information. Organizations should also protect supporting facilities such as electricity supply and cabling infrastructure in order to reduce associated security threats or outcomes. Based on the proposed conceptual framework, a comprehensive managerial level framework would help to enhance an organization's information security.

5. Conclusion

The objective of this study was to develop a framework with a checklist of items for assessing information security practices and their relationship to an organization's information security. An in-depth examination of information security management practices in literature revealed lack of comprehensive guidance on assessing information security management practices in organizations. In this paper, we identify variables that constitute the proposed conceptual framework for information security management practices in organizations. We provide a summary of the contributions of the paper as follows:

- Information security has been known to be inadequate in most institutions including universities. This has been blamed mainly on the inadequacy of information security management practices. In this paper, we have presented a conceptual framework that would provide guidance for appropriate information security management practices for universities in Uganda.
- We also suggest that if the enacted laws to govern information security in Uganda like the Computer Misuse Act 2011, Electronic Transactions Act 2011, Electronic Signatures Act 2011, Data protection and privacy Act 2109, were fully operationalized and incorporated in the information security management framework, then system threats would be minimized.
- The proposed conceptual framework specifies an adequate checklist of standards that can be used to assess existing information security management practices adopted by universities in Uganda.

References

1. Abawajy, J. (2014). User preference of cyber security awareness delivery methods. Behaviour & Information Technology, 33(3), 237-248.
URL: https://doi.org/10.1080/0144929X.2012.708787
2. Alshaikh, M., Ahmad, A., Maynard, S. B., & Chang, S. (2014). Towards a taxonomy of information security management practices in organisations. ACIS.
URL: https://openrepository.aut.ac.nz/handle/10292/8174
3. Alshaikh, M. (2018). *Information security management practices in organisations*. PhD thesis, The University of Melbourne. URI: http://hdl.handle.net/11343/208934
4. Aromataris, E. (2014). The systematic review: an overview. *American Journal of Nursing*, March 2014, Vol. 114(3).URL: https://doi.org/10.1097/01.naj.0000444496.24228.2c
5. Babatunde, D. A., & Selamat, M. H. (2012). Investigating information security management and its influencing factors in the Nigerian banking industry: a conceptual model. *International Journal on Social Science & Art*, 2(2), 55-59. URL:
https://www.researchgate.net/profile/Dorcas-Adebola-Babatunde-2/publication/264884940
6. Baxter, R. J., Holderness Jr, D. K., & Wood, D. A. (2016). Applying basic gamification techniques to IT compliance training: Evidence from the lab and field. *Journal of information systems*, 30(3), 119-133. URL: https://doi.org/10.2308/isys-51341
7. Bilsky, S. A., Cole, D. A., Dukewich, T. L., Martin, N. C., Sinclair, K. R., Tran, C. V. & Maxwell, M. A. (2013). Does supportive parenting mitigate the longitudinal effects of peer victimization

on depressive thoughts and symptoms in children? *Journal of abnormal psychology*, 122(2), 406-419. URL: https://doi.org/10.1037%2Fa0032501
8. Bogere A., Haolader, F. A., & Mahbubur, R. A. (2013). The influence of ICT security to academic environment at universities, case study Uganda: *International Journal of Innovative Research in Science, Engineering and Technology*, Vol 2, 4866-4873. ISSN: 2319-8753. URL: http://www.rroij.com/open-access/the-influence-of-ict-security-to-academicenvironment-at-universities-case-study-uganda.pdf
9. Coventry, W.L. & Keller, M. C. (2005). Estimating the extent of parameter bias in the classical twin design: A comparison of parameter estimates from extended twin-family and classical twin designs. *Twin Research and Human Genetics*, 8(3), 214-223.
URL: https://doi.org/10.1375/1832427054253121
10. Kisakye, A. (2012). *An investigation into information security practices implemented by Research and Education Networks of Uganda (RENU)*. Masters thesis, Rhodes University. URL: https://research.ict.ru.ac.za/snrg/Theses/Kisakye%202012%20MSc.pdf
11. Komatsu, A., Takagi, D., & Takemura, T. (2013). Human aspects of information security: An empirical study of intentional versus actual behavior. *Information Management & Computer Security*, 21(1), 5-15. URL: https://doi.org/10.1108/09685221311314383
12. Mbabazi, B. P., Kareyo, M. and Muwanga–Zake, J.W.F. (2016). Assessing the implementation of information security policy in Ugandan Universities. *Global Journal of Engineering Science and Researches*, 3(11), 1-7. ISSN 2348-8034. URL: http://www.gjesr.com/Issues%20PDF/Archive-2016/November-2016/1.pdf
13. Mugyenyi,R. (2017). Analysing information systems security in higher learning institutions of Uganda. *International Journal of Scientific & Technology Research*, 6(10), 385-392. ISSN: 2277-8616. URL: https://www.ijstr.org/final-print/oct2017/Analysing-Information-Systems-Security-In-Higher-Learning-Institutions-Of-Uganda.pdf
14. Naz, F., Aftab, J., & Awais, M. (2016). Impact of human resource management practices (HRM) on performance of SMEs in Multan, Pakistan. *International Journal of Management, Accounting and Economics*, 3(11), 699-708. URL: https://www.ijmae.com/article_116565.html
15. Oyelami, J. O., & Ithnin, N. B. (2015). Establishing a sustainable information security management policy in organization: A guide to information security management practice (ISMP). *International Journal of Computer and Information Technology*, 4(01), 44-49. URL: https://www.ijcit.com/archives/volume4/issue1/Paper040107.pdf
16. Qingxiong, M., Schmidt, M. B., & Pearson, J. M. (2009). An Integrated Framework for Information Security Management. Review of Business, 30(1). URL: link.gale.com/apps/doc/A220136074/AONE?u=googlescholar&sid=bookmark-AONE&xid=19347e2e
17. Ravitch, S. M., & Riggan, M. (2016). Reason & Rigor: How conceptual frameworks guide research. Sage Publications. URL: https://doi.org/10.1177/105268461602600504
18. Radhakrishna, A., & Raju, R. S. (2015). A Study on the effect of human resource development on employment relations. IUP Journal of Management Research, 14(3), 28. URL: https://www.iupindia.in/1507/Management%20Research/A_Study_on_the_Effect.html
19. Rantos, K., Fysarakis, K., & Manifavas, C. (2012). How effective is your security awareness program? An evaluation methodology. Information Security Journal: A Global Perspective, 21(6), 328-345. URL: https://doi.org/10.1080/19393555.2012.747234
20. Sarode, A. P., & Deore, S. S. (2017). Role of third-party employee verification and background checks in HR management: An overview. Journal of Commerce and Management Thought, 8(1), 86. URL: https://indianjournals.com/ijor.aspx?target=ijor:jcmt&volume=8&issue=1&article=006
21. Solaiman, B., Bosse, E., Pigeon, L., Gueriot, D., & Florea, M. C. (2015). A conceptual definition of a holonic processing framework to support the design of information fusion systems. Information Fusion, 21, 85-99. URL: https://doi.org/10.1016/j.inffus.2013.08.004
22. Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. International Journal of Information Management, 36(2), 215-225. URL: https://doi.org/10.1016/j.ijinfomgt.2015.11.009
23. Stewart, J. M., Chapple, M., & Gibson, D. (2015). *Certified information systems security professional study guide.* John Wiley & Sons. 7th Edition. URL: https://www.wiley.com/en-us/CISSP+%28ISC%292+Certified+Information+Systems+Security+Professional+Official+Study+Guide%2C+7th+Edition-p-9781119042716
24. Tawfik, G. M., Dila, K. A. S., Mohamed, M. Y. F., Tam, D. N. H., Kien, N. D., Ahmed, A. M., & Huy, N. T. (2019). A step-by-step guide for conducting a systematic review and meta-analysis

with simulation data. Tropical medicine and health, 47(1), 1-9. URL: https://tropmedhealth.biomedcentral.com/articles/10.1186/s41182-019-0165-6
25. Trim, P. R. J., Lee, Y. I., & Weston, D. (2014). An interdisciplinary approach and framework for dealing with security breaches and organizational recovery. British Embassy Seoul. URL: http://www.iaac.org.uk/media/1067/reporttrimyoumcybersecuritymarch14.pdf
26. Tryfonas, T. H. E. O. (2010). Information security management and standards of best practice. Handbook of Electronic Security and Digital Forensics. World Scientific Publishing Co, 207-236. URL: https://doi.org/10.1142/7110
27. National Information Technology Authority (NITA) Uganda (2014). National Information Security Policy. National Information Security Framework (NISF) Publication, Uganda.
28. Varpio, L., Paradis, E., Uijtdehaage, S., & Young, M. (2020). The distinctions between theory, theoretical framework, and conceptual framework. Academic Medicine, 95(7), 989-994. URL: https://doi.org/10.1097/ACM.0000000000003075
29. Whitman, M., & Mattord, H. J. (2014). Information security governance for the non-security business executive. URL: https://digitalcommons.kennesaw.edu/facpubs/3204/
30. Williams, G. M., Kroes, R., & Munro, I. C. (2000). Safety evaluation and risk assessment of the herbicide Roundup and its active ingredient, glyphosate, for humans. Regulatory toxicology and pharmacology, 31(2), 117-165. URL: https://doi.org/10.1006/rtph.1999.1371
31. Yaokumah, W., & Brown, S. (2014). An empirical examination of the relationship between information security/business strategic alignment and information security governance domain areas. Journal of Law and Governance, 9(2). URL: https://doi.org/10.15209/jbsge.v9i2.718
32. Zaini, M. K., Masrek, M. N., & Sani, M. K. J. A. (2020). The impact of information security management practices on organisational agility. Information & Computer Security. URL: https://doi.org/10.1108/ICS-02-2020-0020

Aims and Objectives

Published online by ICS two times a year, Journal of Digital Science (JDS) is an international peer-reviewed journal which aims at the latest ideas, innovations, trends, experiences and concerns in the field of digital science covering all areas of the scholarly literature of the sciences, social sciences and arts & humanities. The main topics currently covered include: Artificial Intelligence Research; Digital Economics, Education, Engineering, Finance, Health Care.

The main goal of the journal is the effective dissemination of original incites/results generated by the human brain and presented/reflected in articles using modern information/digital technology.

Contact information

Website: https://ics.events

Email: conf@ics.events