OPEN ACCESS

Saudi Journal of Engineering and Technology
Abbreviated Key Title: Saudi J Eng Technol
ISSN 2415-6272 (Print) | ISSN 2415-6264 (Online)
Scholars Middle East Publishers, Dubai, United Arab Emirates
Journal homepage: https://saudijournals.com

Original Research Article

A Framework to Enhance Information Security Governance in SMEs

Derrick Mwanje[1*], Ocen Samuel[1], Godfrey Tumwebaze[1], Moses Bukenya[1]

[1]Mountains of the Moon University, Fort Portal, Uganda

DOI: 10.36348/sjet.2023.v08i12.002 | **Received:** 08.11.2023 | **Accepted:** 14.12.2023 | **Published:** 28.12.2023

***Corresponding author:** Derrick Mwanje
Mountains of the Moon University, Fort Portal, Uganda

Abstract

In the modern organizational landscape, information technology plays a pivotal role in shaping business processes. The increasing reliance on IT necessitates a focus on the confidentiality, availability, and integrity of both enterprise and customer data, making information security a paramount concern. This study delves into the challenges faced by Small and Medium-sized Enterprises (SMEs) in Fort Portal Central Division during their information security governance efforts, highlighting issues such as limited resources, budget constraints, time limitations, and a lack of expertise in drafting and ensuring compliance with security policies. To address these challenges, a comprehensive framework for improving Information Security Governance in SMEs was developed and evaluated. Primary data were collected from 351 respondents, including Proprietors, Directors, CEOs, Managers, and operations personnel, shedding light on the specific hurdles faced by SMEs. The proposed framework underwent rigorous evaluation based on design science parameters, demonstrating efficiency and usability. The results of the evaluation revealed that the developed framework effectively addressed the identified challenges, fulfilling the study's objective. The study recommends SMEs in Fort Portal City to implement the framework to enhance their Information Security Governance efforts. Additionally, policy makers in Uganda, including the National Information Technology Authority Uganda (NITA-U) and Uganda Investments Authority (UIA), can leverage the designed framework to make informed decisions regarding SMEs and information security management and governance. This research contributes valuable insights to the broader discourse on information security governance in SMEs, particularly within the context of Fort Portal City.

Keywords: Information Security Governance, SMEs, Framework, Fort Portal City, Data Integrity, Cybersecurity, Small and Medium-Sized Enterprises, Information Technology, Policy Implementation.

Introduction

In developing nations, the rise of e-business, e-services, and e-governance has amplified dependence on business data and information technologies, making this data vulnerable to continuous threats and potential security breaches, thereby impacting the fragile economic structures of these countries [1]. The COVID-19 pandemic in 2020 forced a transformative shift, compelling organizations worldwide to adopt remote working strategies. While some adapted swiftly, SMEs in Africa, especially Uganda, faced challenges securely transitioning to remote work, necessitating the revitalization of IT environments, procedures, and workforce [2].

The Africa Cybersecurity Report 2020 reported a significant surge in cybercrime during the pandemic, with a 300% increase in 2020. Despite efforts to fortify ICT resources and cybersecurity plans in Uganda, Information Security Management often took precedence, overshadowing the crucial aspect of Information Security Governance (ISG) [3].

SMEs, crucial to the growth process in emerging countries, constitute a substantial portion of global economies. In Uganda, SMEs make up 67% of the commercial sector and 99% of businesses, including micro-businesses. The technological reliance in this sector underscores the need for safety and security measures. Existing frameworks for Information Security Governance, proposed by Walters and Jacques, may prove unsuitable for SMEs due to their complexity [4].

While COBIT 5 for Information Security, part of a recognized Governance Framework, offers a globally accepted approach, its comprehensive nature may pose challenges for SMEs operating under constraints of time and resources. Despite available frameworks, SMEs often lack the necessary resources and expertise to address information security governance components effectively [5].

Theoretical perspectives, including the Integrated System Theory (IST), emphasize the necessity for a comprehensive approach aligning with organizational objectives. Recognized ISG frameworks, such as ISO standards and NIST practices, often lack theoretically grounded methods and empirical evidence on efficiency.

This research aims to address the governance challenge of information security in SMEs. It seeks to evaluate the current state of information security governance, gathering requirements to design a framework tailored to the specific needs of organizations and businesses. Information security is not merely a technical matter; it poses a governance challenge, and this research endeavors to contribute to the development of a suitable information security governance framework for SMEs and other organizations.

EXPERIMENTAL SECTION/MATERIAL AND METHODS

The research methodology employed a Design Science Research Process (DSRP) model, consisting of six steps, to address information security governance challenges in SMEs [6]. The process involved a comprehensive literature review on information security governance in SMEs to identify existing gaps. Data collection was carried out to determine the needs for a solution, with a focus on compliance monitoring and strategic-level management involvement. An information security governance framework was then designed, developed, and proposed for implementation, emphasizing simplicity and resource efficiency in the SMME environment.

The study targeted legally registered SMEs in Fort Portal central division, selecting stakeholders such as Directors, CEOs, Managers, Accountants, and IT managers for participation. Sample size determination, using Krejcie and Morgan's formula, resulted in a sample of 351 respondents out of 4487 from registered enterprises. Purposive sampling was employed to select individuals with unique characteristics for the study. Data collection methods included document review and questionnaires, aiding in analyzing existing frameworks and establishing requirements for the proposed framework. Ethical considerations were paramount throughout the research, with adherence to guidelines and obtaining informed consent from participants.

The Information Security Governance Framework was designed through modeling, utilizing Unified Modeling Language (UML) diagrams. Its development followed the rapid prototyping model, using MySQL for the database, PHP for scripting, and HTML, CSS (Bootstrap framework), and JavaScript for the front end. The framework support system aimed to target organizational goals, manage checklists, assess implementation progress, facilitate information sharing, and improve communication among stakeholders.

The framework underwent evaluation using structured walkthroughs and a Likert scale validation approach, involving experts in information security management and governance. Ethical considerations were meticulously followed, ensuring confidentiality and proper data handling throughout the study. All works from other authors used in the study were duly acknowledged, adhering to academic integrity principles.

RESULTS AND DISCUSSION

The study aimed to develop a framework for improving Information Security Governance in SMEs, guided by four specific objectives: 1) analyzing existing frameworks, 2) gathering requirements, 3) designing the framework, and 4) evaluating the proposed framework. Demographic characteristics of respondents were assessed to ensure relevance to SMEs. The targeted numbers of the SMEs were 351, in Fort Portal City.

Response Rates and Demographics

The study engaged 351 SMEs; response Rates was 300 with a notable 85.4% response rate. Demographics revealed a majority of male respondents (65.3%), aged 36-50 years (47.7%), and predominantly holding degrees (26.0%). Experience-wise, most SMEs had operated for 6-10 years (35.0%).

Existing Frameworks Analysis

The study examined existing frameworks, highlighting strengths and weaknesses:

1. **NIST Standards:** Generic and comprehensive, yet neglects SME-specific needs.
2. **COBIT 5:** Detailed but considered too large for SMEs.
3. **ITIL Practices:** Guides ISG but lacks a practical implementation framework.
4. **Jacques C Model:** Supports security requirements but lacks specific methods.

Framework Requirements

Organizational Reliance on IT: Respondents expressed concerns about inadequate infrastructure and processes for IT reliance, suggesting a need for digitization and budgeting for technology.

Security Program Administration: Findings revealed deficiencies in configuration management and patch strategy, emphasizing the importance of robust security programs.

Risk Management Process: Only 18% conducted risk assessments, indicating a significant gap in managing information security risks, necessitating a tailored framework.

Policy Development and Enforcement: Most SMEs lacked consistent, communicated, and enforceable security policies, emphasizing the need for tailored policies.

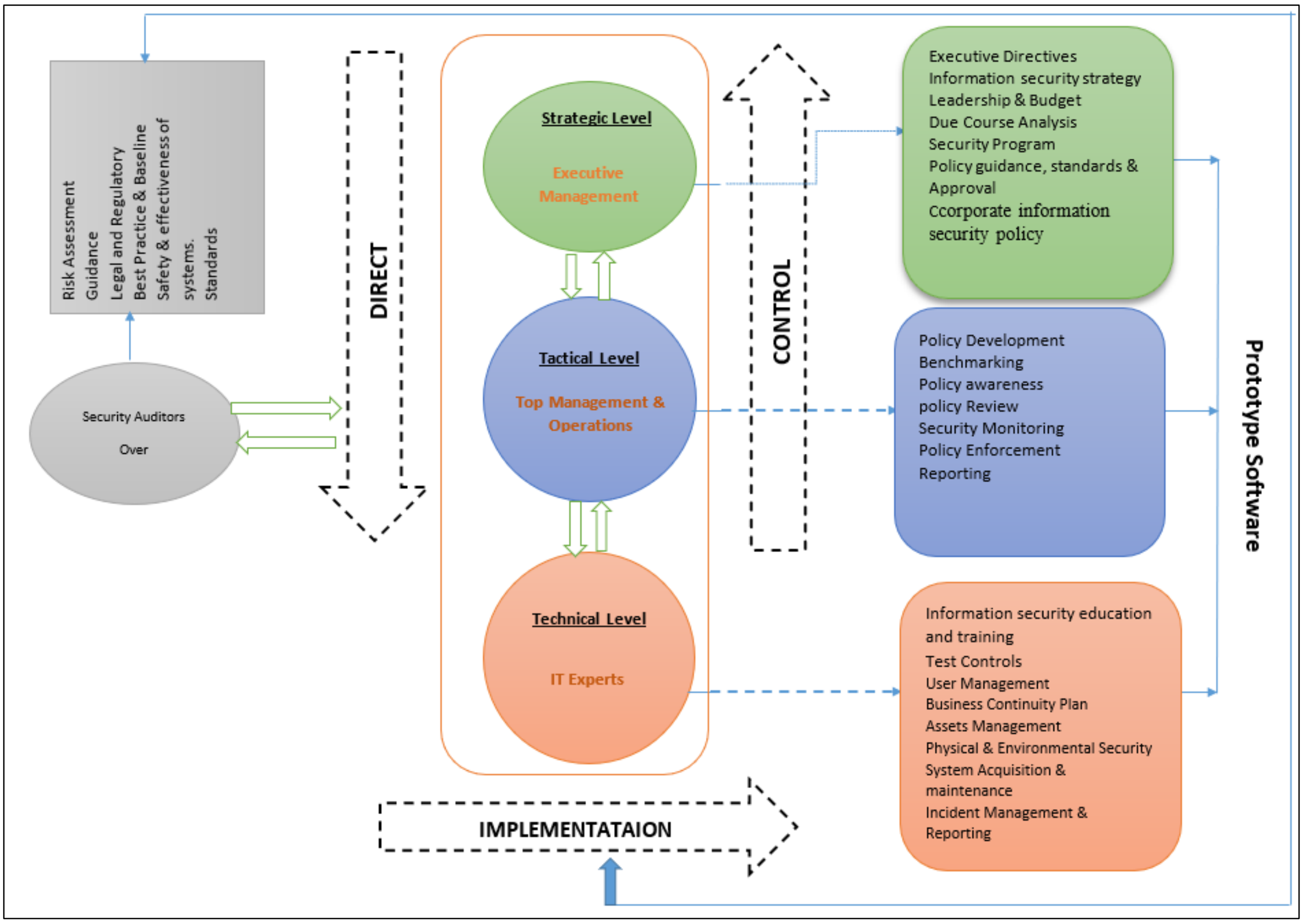
Information Security Policies and Procedures: Critical areas like disaster recovery and incident response lacked formalized policies, requiring focused attention in the proposed framework.

User Requirements Gathering: Survey results suggested a need for clear incident response plans and expert guidance in information security governance, indicating a gap in SME capabilities.

User Opinions on Information Security Governance: Respondents emphasized the importance of clear security incident plans, expert guidance, and management commitment to information security initiatives.

Discussion of Findings

The study successfully addressed four key research questions, shedding light on the existing gaps and challenges in information security governance frameworks, the requirements for implementing a suitable framework, the design process of the framework, and the evaluation of frameworks. The findings emphasized the generic nature of existing frameworks, the lack of validation in many ISG models, and the need for practical implementation and measurement guidelines.



Figurer 1: Framework for ISG

ISG Framework description

The Information Security Governance Framework is designed to align with corporate governance principles, emphasizing the integration of information security and IT governance. The framework introduces a Direct Control Cycle, encompassing strategic, tactical, and technical levels of management [7]. It recognizes the crucial role of the board and executive management in providing strategic directives that cascade down to operational levels. The framework above introduces an Audit Function at the technical level, addressing the lack of expertise in SMEs by incorporating IT and security experts. Components such as the Audit Function, Risk Assessment, Legal and Regulatory Compliance, and Incident Handling contribute to a comprehensive approach, ensuring effective information security governance. The framework supports a risk-based approach to budgeting, policy development and enforcement, awareness training, and reporting at various levels, addressing specific challenges faced by SMEs. The framework's development is supplemented by the Information

Security Governance Framework support system, facilitating organization-wide implementation and monitoring

RECOMMENDATIONS

The recommendations emanating from the study target different stakeholders. Small and medium-sized enterprises (SMEs) are encouraged to implement the proposed Information Security Governance framework to enhance their cybersecurity efforts. Leadership within SMEs is urged to provide support and demonstrate commitment to information security initiatives, ensuring direct control actions across various management levels. Additionally, policymakers, such as the National Information Technology Authority Uganda (NITA-U) and Uganda Investments Authority (UIA), are advised to consider the framework when making decisions related to SMEs and information security management.

Limitations of the Study

While the study contributes valuable insights, its limitations must be acknowledged. The focus on SMEs in Fort Portal City narrows the scope, leaving a broader perspective unexplored. Recognizing this limitation is crucial in understanding that the findings may not be universally applicable to SMEs across the entire nation or globe. To address potential biases resulting from the limited geographical scope, future research is recommended to include SMEs from other cities and regions. Expanding the study beyond the selected SMEs in Fort Portal City will provide a more comprehensive understanding of the framework's applicability. Moreover, empirical studies in enterprises beyond Uganda will contribute to assessing the efficiency and usability of the framework in diverse contexts.

CONCLUSION

Despite the acknowledged limitations, the study successfully achieved its main goal of developing an Information Security Governance framework tailored for SMEs. The evaluation results indicate positive perceptions regarding the framework's efficiency and usability within the selected SMEs [8]. The study sets the stage for future research and implementation efforts to validate the framework in various organizational settings and geographical locations.

REFERENCES

1. Coertze, J., & Von Solms, R. (2013). A Model for Information Security Governance in Developing Countries.
2. Africa Cybersecurity Report Uganda. (2020). *Local Perspective on Data Protection and Privacy Laws: Insights from African SMEs.*
3. Posthumus, S., Von Solms, R., & King, M. (2010). The board and IT governance: The what, who, and how. *South African Journal of Business Management, 41*(3), 23–32. https://doi.org/10.4102/sajbm.v41i3.23
4. Walters, R., & Wills, G. (2017). A Proposed Best-practice Framework for Information Security Governance. In *Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security (IoTBDS 2017).* https://doi.org/10.5220/0006303102950301
5. Koornhof, H. (2009). A Framework for IT Governance in Small Businesses. *Information Security.* Nelson Mandela Metropolitan University.
6. Yildirim, E., Akalp, G., Aytac, S., & Bayram, N. (2010). Factors influencing information security management in small- and medium-sized enterprises: A case study from Turkey. *International Journal of Information Management.* https://doi.org/10.1016/j.ijinfomgt.2010.11.005
7. Brotby, K. (2009). *Information Security Governance: A Practical Development and Implementation Approach.* Honoken, New Jersey: John Wiley & Sons.
8. Wilson, M., Wnuk, K., Silvander, J., & Gorschek, T. (2018). A literature review on the effectiveness and efficiency of business modeling. *E-Informatica Software Engineering Journal, 12.* https://doi.org/10.5277/e-Inf180111.