Cyber-Security Governance Framework and its Effects on Zimbabwe Local Authorities: A Review Paper

Brian Chundu[1], Prof Obert Sifile[1] and Dr Tavengwa Masamha[1]

[1]Chinhoyi University of Technology, Zimbabwe

*Corresponding Author's Email: brianchundu13@gmail.com

Received: 17 February 2025| Accepted: 30 April 2025| Published: 31 May 2025

Abstract

The purpose of this review paper was to analyse literature related to cyber-security governance frameworks effects in Zimbabwe local authorities. Cyber-security governance is a developing subject with an expanding literature. It is founded in information technology governance but is also increasing its recognition in business management. However, there is dearth of literature on the effectiveness of cyber-security governance framework in Zimbabwe local authorities. The authors reviewed journal papers, conference papers, theses and books from various databases namely Google Scholar and ProQuest. The study showed that cyber-security governance enables the formulation of a cyber-security governance framework which has a great impact on the performance of local authorities in Zimbabwe. In addition, a cyber-security governance framework improves organisation's decision making, risk governance and compliance. Conversely, a cyber-security governance framework is inflexible and overly systematic. The paper also contributed to the body of knowledge in the fields of cyber-security governance as well as other related studies thereby supporting literature brought forward by other researchers.

Key words: Cyber-security, Cyber-security governance, Cyber-security governance framework, Local authorities

Introduction

Cyber-security governance is very important in elevating the integrity of security and the effectiveness of organisations together with the business environment in which they operate. The concepts of cyber-security governance and cyber-security works hand in hand. While cyber-security protects network systems and their data against attacks or intrusions, cyber-security governance ensures that organisation's security plans are aligned with its vision, meet the regulations and standards of the nation and attain objectives for achieving security and risk (Albalas et al., 2022). The appropriate use of cyber-security governance improves and supports economic and social development, particularly in empowering employees and organisational systems (Gcaza, 2017). Calderaro (2020) points out that boards and executive leaders ensures that an organisation has a cyber-security governance framework which supports the objectives of the business to manage risk. According to Maleh et al. (2021), cyber-security governance framework is defined as set of values, procedures, and best practices meant to assist companies in handling and mitigating cyber-security risks. Although previous studies have indicated the importance of information technology governance frameworks, there is scarce literature in cyber-security governance framework.

Literature has not fully elaborated the importance of cyber-security governance frameworks particularly in Zimbabwe's local authorities. The attention of most literature has been focused mostly on cyber-security governance in developed countries (Albalas, 2022; De haes et al. 2020a; Maleh et al., 2021; Savas & Karata, 2022). This has resulted in lack of knowledge in cyber-security governance and unsuccessful formulation and implementation of cyber-security policies in Zimbabwe local authorities. Thus, the study reviewed papers related to cyber-security governance framework effects in Zimbabwe local authorities.

Research Methodology

The authors downloaded and reviewed literature from journal papers, conference papers, theses and books which provided quality and relevant cyber-security work and had an impact on the performance of Zimbabwe local authorities. The data bases used for searching literature were Google Scholar and ProQuest. They enabled the authors to have an insight and knowledge on cyber-security governance and analysed cyber-security technical reports.

Results and Discussion

Zimbabwe local authorities are made up of three tiers of the government which are the national or central government at the top, metropolitan and provincial councils in the middle and local authorities at the bottom, the latter of which comprised urban and rural councils (Zimbabwe Constitution, 2013). In addition, the Zimbabwean Constitution (2013) states that there are thirty-two urban and sixty rural local authorities in Zimbabwe which focuses mainly on community engagement, service delivery and devolution. Each local authority has a board which comprises of elected councillors, the town clerk for cities and municipalities, town secretary for town councils and chief executive officers for rural district councils, mayors and executive management (Makunde et al., 2018).

The local authority boards formulate rules and guidelines for making corporate cyber-security decisions (Kabwe et al, 2024). In addition, Kabwe et al. (2024) highlighted that local authority boards align cyber-security with the organisation's vision and mission to fit their strategic effects. In this way, the structure through which the objectives of the company are set, and the means of attaining those objectives and monitoring performance are determined (Savas & Karata, 2022). Thus, the authors suggest that an effective local authority board organ clearly supports significance business processes which add value for the local community and local authorities thereby supporting all the production processes. Therefore, the effects of cyber-security governance framework are that it enables Zimbabwe local authorities to:

a. Outline: a risk management process.

NIST (2024) asserts that developing a cyber-security governance framework enables the organisation to outline its risk management process in the overall work settings. Cyber-threats are all over the environment in which companies manage their operations. Many organisations rely on cyber-security governance to identify and mitigate risks (Albalas, 2022). To add on, organisations today challenge all weak information technology links which can cause a major cyber-threat (Maleh et al, 2021). As such, failure to conduct a root cause analysis and classify cyber-risk can lead to inadequate responsiveness being paid to the most vulnerability (Aliyu et al., 2020). To commend this viewpoint, Zimbabwe local authorities benchmark their information technology governance with NIST and COBIT frameworks to achieve a smooth understanding of cyber-security risk management processes and the potential cyber-security attacks (ISO, 2015; NIST, 2024). Thus, the local authorities are dividing risks and putting their attention on effective and efficient cyber-risk management

b. Be inclusive

Chundu et al. (2025) note that organisations with cyber-security governance frameworks safeguards cyber-risks at domestic and global levels. For a global organisation, regional contemplation makes imposing steady principles a challenge, since functions in diverse topographies frequently use diverse policies and severance systems (Maleh et al., 2021). However, most companies nowadays are in disarray as to how best to accomplish an international stability as they are caught between on either captivating a consolidated method or enabling each region to work independently (Sagala & Őri, 2024). De Haes et al. (2020b) asserts that the goal should be to collect data and enable governance and inclusivity both at local and international levels providing continuous input and analysis of security and compliance.

c. Support production processes

Graham et al. (2011) argues that cyber-threats are continual risks for all business operations despite the industry in which they function. Mitigating cyber-risk requires a culture of cyber-security with management obligation to, and demonstrating of good cyber security decision-making (Kabanda, 2018). Correspondingly, this can be steered by the board which contemplates risks and involves them into crucial working and strategic decision-making process including the espousal of cyber-security governance framework as a regular agenda item for full board meetings (Levstek et al., 2022).

d. Fit in cyber-security into a corporate structure.

Lowry et al. (2024) argue that corporate structure creates a governance brand which enables the construction of cyber-security goals. Besides, this includes outlining well-defined proprietorship, influence, and tasks among all internal stakeholders for serious threat controlling and tasks recording (Shaker et al., 2023). In the context of Zimbabwe local authorities, the board evaluates the corporate structure to guarantee that the cyber-security function is sufficiently signified across the business, internal and external stakeholders, and management (Kabwe et al., 2024). Additionally, Amarilli et al. (2023) explains that the board set prospects that cyber-security and cyber-risk functions are to obtain satisfactory enrolment, support and monitor the effectiveness of these elements.

e. Supports cyber-security expertise

Joyce et al. (2021) argues that cyber-security governance allows boards to recognise various bases of cyber-security know-how including directors, internal and external stakeholders which successfully superintend the company's cyber-security. Correspondingly, Zimbabwe local authorities' boards guarantee that cyber-security expertise is signified, participate in occasions to upsurge their base level of understanding on cyber-risk, search for third-party consultants who advise them, contemplate intermittent audits reviews of cyber-security and benchmark organisational cyber-security operations with self-governing third parties (Sofyani et al., 2020).

f. Cooperate information technology in business operations

A study conducted by Burch et al. (2024) points out that an active cyber-security governance framework enables flexibility in organisational operations. However, there is a general agreement that local authorities which are well linked to technological ways of executing business are more disposed to cyber-attacks hence, they need to co-operate and align their business approaches with organisational information technology governance polices (Kabwe, 2024). This assertion is supported by Chundu et al. (2025) who argues that leaders must inspire collaboration across their portfolio's and with their stakeholders to make sure that their institutions promote the overall spirit of cyber-security governance.

g. Protect information

According to Gcaza (2017), information security is a system of securing information by alleviating information risks. Correspondingly, Peltier (2013) points out that information security involves the safeguarding of restricted data both private and monetary from cyber-attacks and crimes. Literature put forward by Shaker et al (2023) asserts that active information security involves a complete and cross-functional method, including people, processes, and technology. On this basis, Bada et al (2019) argues that adopting a cyber-security governance framework enables the placement of programmes which inhibit unlawful people from retrieving business or personal information. To add on, confidential information can be safeguarded from any unlawful activities. Thus, the aim of information security in Zimbabwe local authorities is to enhance the protection and confidentiality of sensitive information such as client account details, monetary information, or trade secrets.

However, the adoption of a cyber-security governance framework may encounter resistance from employees and stakeholders who are accustomed to existing practices (Saha & Anwar, 2024). In addition, this resistance could stem from concerns about changes in job roles, responsibilities, and processes as this could lead to job losses for some employees. This could occur if new structures and policies result in redundancies or if certain roles are deemed unnecessary in the context of the framework (Dhillon et al., 2017). In the same vein, De Haes et al. (2020b) further adds that cyber security governance frameworks bring in sophistications, inflexibility, excessive focus on documentation and high costs including training. This implies that a lot of time and resources is provided to a framework that reduces information technology processes and doesn't match with employees' competencies (von Solms, 2005; De Haes et al., 2013; ISO/IEC, 2015; NIST, 2024)

In view of the above assertions, the authors suggest that adopting a framework for cyber-security in Zimbabwe's local authorities ensures obedience of the local authorities with legislations. As highlighted by Joyce et al. (2021) obeying legislations, standards and procedures can be done through incorporating a cyber-security governance framework. To add on, fulfilling with legislations involves following the recognised guiding principles, standards and procedures. Based on this view, the authors concurs that a cyber security governance framework in Zimbabwe local authorities can be established in agreement with stipulations formed by local authority boards and then positioned in agreement with operating standards and procedures. Thus, compliance incorporates exertions to confirm that local authorities are standing by business guidelines and government legislation.

Conclusion and Recommendations

The paper discussed the concepts of cyber-security and effects of cyber-security governance framework in Zimbabwe's local authorities. Overally, the paper touched on both the potential benefits and challenges associated with implementing a cyber-security governance framework within Zimbabwe local authorities. The paper asserted that a cyber-security governance framework has a positive effect to local authorities because it enables them to manage cyber-security risk. Furthermore, the paper highlighted that cyber-security governance frameworks enable Zimbabwe local authorities to have a standardised policy, reduce cyber-attacks, improve cyber-security, and promotes e-governance. Thus, the paper recognises cyber security governance frameworks as a critical aspect of organisational performance, especially in the context of protecting data assets and ensuring compliance with regulatory requirements. Conversely, the paper underscored the importance of considering various implications including organisational resistance, resource constraints, costs, complexity, workforce impacts, and the imperative of information protection, when introducing such frameworks.

References

Albalas, T., Modjtahedi, A., Abdi, R. (2022) Cybersecurity governance: A scoping review *International Journal of Professional Business Review.* v. 7, 01-19

Aliyu, A., Maglaras, L., He, Y., Yevseyeva, I., Boiten, E., Cook, A., & Janicke, H. (2020). A Holistic Cybersecurity Maturity Assessment Framework for Higher Education Institutions in the United Kingdom. *MDPI, Applied Sciences,* 10(10), 3660.

Amarilli, F., van den Hooff, B., & van Vliet, M. (2023). Business-it alignment as a coevolution process: An empirical study. Journal of Strategic Information Systems, 32(2), 101776.

Bada, M., Solms, B., & Agrafiotis, I. (2019). Reviewing National Cybersecurity Awareness for Users and Executives in Africa. *International Journal on Advances in Security*, 12(2), 108–118.

Burch, G., Burch, J. & McGarry, M. (2024). Cybersecurity Risk Management Governance: An Agency Theory Perspective. *ISACA Journal. Issues* 2024 Volume 5

Calderaro, A., & Craig, A. J. S. (2020). Transnational governance of Cyber-security: Policy challenges and global inequalities in cyber capacity building. *Third World Quarterly*, 0(0), 1– 22.

Chundu, B., Masamha, T. & Sifile, O. (2025). Cyber-security governance framework for Zimbabwe local authorities. Law, Criminology and Criminal Justice, *Cogent Social Science Journal,* Vol 11 (1), 1-10

De Haes, S., Van Grembergen, W., & Debreceny, R. S. (2013). COBIT 5 and enterprise governance of information technology: Building blocks and research opportunities. *Journal of Information Systems,* 27(1), 307-324.

De Haes, S., Van Grembergen, W., Joshi, A., & Huygh, T. (2020b*). Enterprise Governance of IT, Alignment, and Value* (Third ed.). Springer International Publishing.

Dhillon, G., Syed, R., & de Sa′-soares, F. (2017). Information security concerns in IT outsourcing: Identifying (in) congruence between clients and vendors. *Information & Management,* 54(4), 452–464.

Government of Zimbabwe (2013). *Constitution of Zimbabwe Amendment (No. 20).* Government Printers Harare: Harare

Graham, J., Howard, R., & Olson, R. (2011). *Cyber Security Essentials.* Taylor and Francis Group, LLC

ISO/IEC 38500 (2015). *Information Technology Governance of IT for the organisation.* Retrieved from https://www.itgovernanceusa.com/iso38500.

Joyce, S. Dobrygowski, D., & Van der Oord, F. (2021). *Principles for Board Governance of Cyber Risk. Harvard Law School Forum on Corporate Governance.* Retrieved from https://corpgov.law.harvard.edu/2021/06/10/principles-for-board-governance-of-cyber-risk/

Kabanda, G. (2018). A Cyber - security Culture Framework and Its Impact on Zimbabwean Organisations. *Asian Journal of Management, Engineering & Computer Sciences* (AJMECS) Vol. 3(4), 17-34

Kabwe, K., Zhou, C., Jardim, L. & Surguladze, E. (2024). Empowering Societal Digital Transformation at the Local Level. A Case Study of Pemba Town Council. *Digital Policy Studies (DPS).* 3(1)2024

Levstek, A., Pucihar, A.& Hovelja, T. (2022). Towards an Adaptive Strategic IT Governance Model for SMEs. *Journal of Theoretical Applied Electronic Commerce Research.* 17, 230–252.

Lowry, M. R., Lowry, P. B., Chatterjee, S. ("Suti"), Moody, G. D., & Richardson, V. J. (2024). Achieving Strategic Alignment Between Business and Information Technology with Information Technology Governance: The Role of Commitment to Principles and Top Leadership Support. *European Journal of Information Systems,* 1–26.

Makunde, G., Chirisa, I., Mazorodze, C., Matamanda, A., Pfukwa, C. (2018). Local Governance System and the Urban Service Delivery in Zimbabwe: Issues, Practices and Scope. *International Journal of Technology and Management.* 3(1) p. 13

Maleh, Y., Sahid, A. & Belaissaoui, M. (2021). A Maturity Framework for Cybersecurity Governance in Organisations, *Edpacs,* 63:6, 1-22.

National Institute of Standard and Technology. (2024). *NIST Cybersecurity Framework 2.0.* Retrieved from https://www.nist.gov/news-events/news/2024/02/nist-releases-version-20-landmark-cybersecurity-framework.

Peltier, T. R. (2013). *Information security fundamentals* (2nd ed.). (CRC Press (ed.). Taylor & Francis.

Sagala, G. H., & Őri, D. (2024). Exploring Digital Transformation Strategy to Achieve SMEs Resilience and Antifragility: A Systematic Literature Review. *Journal of Small Business & Entrepreneurship,* 1–30.

Saha, B. and Anwar, Z. (2024) A Review of Cybersecurity Challenges in Small Business: The Imperative for a Future Governance Framework. *Journal of Information Security,* 15, 24-39.

Savas, S., & Karata, S. (2022). Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity governance. *Int. Cybersecurity. Law Rev*, 3, 7–34.

Shaker, A. S., Al-Shiblawi, G. A. K., Union, A. H., Hameed, K. S. (2023) The Role of Information Technology Governance on Enhancing Cybersecurity and its Reflection on Investor Confidence. *International Journal of Professional. Business Review.*89(6) p. 01-23.

Sofyani, H., Riyadh, H.A., & Fahlevi, H. (2020) Improving service quality, accountability and transparency of local government: The intervening role of information technology governance, *Cogent Business & Management,* 7:1

von Solms, S. H. (2005). Information security governance - compliance management vs operational management. *Computers and Security,* 24(6), 443–447.