World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Check for updates

Understanding the role of artificial intelligence in enhancing GRC practices in cybersecurity

Benita Urhobo *

Department of Computer Science, Western Illinois University, Macomb, Illinois, United States.

World Journal of Advanced Research and Reviews, 2024, 22(02), 269–274

Publication history: Received on 20 March 2024; revised on 01 May 2024; accepted on 03 May 2024

Article DOI: https://doi.org/10.30574/wjarr.2024.22.2.1340

Abstract

In cybersecurity, the integrity and security of data and systems can be preserved with governance, risk, and compliance (GRC) practices. As the complexity of cyber threats increases, organizations need to enhance their GRC practices with advanced technologies. This research article studies the role of artificial intelligence in reinforcing GRC practices in cybersecurity. The study provides a comprehensive GRC overview in the context of cybersecurity, highlighting its importance in maintaining a secure and compliant environment. It then examines how AI can enhance GRC practices, including analyzing data, automating compliance processes, and identifying potential threats.

Furthermore, the paper discusses implementing AI-driven GRC solutions, outlining key organizational considerations and best practices. It also addresses ethical and regulatory considerations surrounding AI in GRC in decision-making processes. This study highlights insights into how AI can effectively strengthen cybersecurity GRC practices, ultimately helping governments and organizations mitigate risks and enhance their cybersecurity posture in an increasingly digital world.

Keywords: Cybersecurity; Risk assessment; Data privacy; GRC; Regulatory compliance

1. Introduction

In recent years, the reliance on the Information and Communication Technology (ICT) infrastructure has increased, as have the concerns regarding its security. As ICT systems grow and become complex, they become more vulnerable, making it challenging to prevent opportunities for hackers. In 2015, the cybersecurity outlook in Nigerian cyberspace was an eye-opener, making all the predictions accurate and true. Therefore, we must know that hackers always stay one step ahead of these security systems. The rapid advancement of modern technologies has significantly facilitated global communication through social networking platforms, i.e., Facebook, Twitter, WhatsApp, and Instagram. Over the past few decades, ongoing developmental efforts and research have discovered innovative computer technologies widely used worldwide. Besides the discoveries, cybersecurity threats arise along the way, posing crucial challenges to organizations worldwide.

With the recent advancements, i.e., the Internet of Things (IoT), cybersecurity threats have become more complex. Hackers now utilize advanced techniques such as phishing, zero-day exploits, and ransomware to steal sensitive information. The evolution of these threats led to the implementation of robust Governance, Risk, and Compliance practices, known as GRC practices. GRC practices mitigate risk and ensure regulatory compliance through strategies, processes, and policies that organizations employ to manage their IT environments. Organizations can easily manage cybersecurity for digital assets by stating specific roles and responsibilities and establishing clear governance

* Corresponding author: Benita Urhobo

structures. Robust GRC practices help organizations learn about cybersecurity threats and regulatory requirements. Thus, compliance with regulatory requirements is crucial because non-compliance results in financial penalties.

As artificial intelligence becomes more prevalent, we can improve GRC practices by integrating AI into cybersecurity. AI technologies like national language processing and machine learning analyze data to identify areas vulnerable to cyber threats. AI-powered cybersecurity automates routine tasks such as incident response and threat detection, thus reducing the burden on cybersecurity teams and improving overall efficiency. Recent advancements in AI include Generative Pre-Trained Transformers (GPTs), which are promising for increasing the effectiveness and efficiency of GRC practices in cybersecurity policy development.

The main objective of the research paper is to explore the role of artificial intelligence in enhancing the GRC practices in cybersecurity. This paper discusses the evolution of cybersecurity threats and how AI enhances GRC cybersecurity practices. This study aims to provide insights into how governments can strengthen their cybersecurity and mitigate risk effectively through artificial intelligence.

2. Understanding GRC in Cybersecurity

Cybersecurity and IT together are essential for business. GRC is a new regulation for security systems. Organizations require a framework for securing data and clients. Thus, compliance is a fundamental component of governance. Compliance and regulation issues increase risk. Governance, risk, and compliance begin to move together in an organization (Chhetri, 2022).

With the GRC framework, cybersecurity is associated with working with IT businesses. IT governance frameworks must be integrated to ensure that IT goals align with business goals. GRC frameworks are essential to cybersecurity strategies (Govindji et al., 2018). These provide structured approaches to managing risk for organizations. Furthermore, they ensure compliance with regulations and maintain effective governance over the information systems. IT governance includes rules for monitoring IT risks, compliance with laws and regulations, managing records, and regulating IT assets. Thus, it is a mix of compliance, governance, and risk (Boehm et al., 2020).

Figure 1 GRC Framework

The traditional GRC approaches face several challenges in the context of cybersecurity. This relates to the evolving nature of cyber threats and the complexities of modern IT environments. The traditional GRC approach includes siloed governance, risk management, and compliance systems. As a result, organizations struggle to coordinate their GRC efforts effectively, leading to gaps in risk identification and mitigation (Apeh et al., 2023). Traditional GRC approaches rely heavily on manual risk assessment, compliance monitoring, and reporting processes. These manual processes are error-prone, resource-intensive, and time-consuming. This makes it difficult for organizations to keep pace with the rapidly changing cybersecurity landscape (McIntosh et al., 2023). The regulatory requirements in compliance are a fundamental aspect of GRC. However, the traditional approaches often result in compliance fatigue. Organizations must manage complex regulatory requirements, leading to a compliance burden that can divert resources away from more strategic cybersecurity initiatives. Furthermore, traditional GRC approaches struggle to provide adequate capabilities for risk assessment (Tu et al., 2024).

The importance of GRC practices in mitigating the risk is never overstated. Effective GRC practices help organizations identify and address potential cybersecurity threats. Furthermore, this reduces the likelihood of security and data breaches. These practices enable organizations to demonstrate compliance with the regulatory requirements. Therefore, this fosters trust among stakeholders and enhances their reputation (Meagher and Dhirani, 2023).

3. Role of Artificial Intelligence in GRC Enhancement

Artificial intelligence has developed as a transformative technology, offering significant potential to enhance GRC practices in cybersecurity. Risk management through AI analyzes vast amounts of data to identify real-time risks. These algorithms detect patterns that help indicate cyber threats, thus enabling organizations to mitigate risk regarding cybersecurity proactively. By automating risk assessment processes, AI reduces the reliance on manual intervention, improves accuracy, and allows organizations to respond more effectively to emerging threats (Boehm et al., 2020).

AI technologies streamline compliance monitoring by programming the analysis, reporting, and collection of regulatory requirements. These regulatory systems continuously monitor changes in regulatory landscapes, ensuring that organizations comply with evolving standards and laws (Apeh et al., 2023). AI-powered analytics examine data from several sources, such as external threat intelligence feeds, cybersecurity logs, and employee activities, to identify governance issues and recommend remedial actions. Thus, this facilitates board-level decision-making by gathering cybersecurity risk through real-time insights (Kaur et al., 2023).

While AI offers numerous benefits, adopting GRC practices has significant challenges. Thus, organizations must address concerns related to data privacy, regulatory compliance, and algorithmic bias. Additionally, integrating AI into existing GRC frameworks involves planning and execution to guarantee a smooth operation and maximize the benefits of AI technology (Chakraborty et al., 2023). The role of AI in enhancing GRC practices is expected to expand in the future. The AI advancements that will rise in the future include national learning language, predictive analysis, and machine learning. Organizations are increasingly investing in AI-powered GRC solutions to improve their cybersecurity resilience and regulatory compliance efforts (Dopamu et al., 2024).

4. Implementing AI-Driven GRC Solutions

The execution of AI-driven GRC solutions in cybersecurity is a complex process. Before implementing AI-driven GRC solutions, organizations must thoroughly assess their cybersecurity risks, compliance requirements, and governance processes (Sunkle et al., 2022). This assessment should include identifying the specific use cases for AI, such as risk assessment, compliance monitoring, and incident response, based on the organization's unique needs and challenges. A study by Kunduru (2023) demonstrated how a financial institution successfully implemented an AI-driven GRC solution to automate its risk assessment process. By leveraging AI algorithms, the institution could analyze data and detect risks more effectively than manual methods.

The right AI technologies and tools are fundamental for successfully implementing AI-driven GRC solutions. Organizations should evaluate different AI platforms, like natural language processing, machine learning, and robotic process automation. This is based on their compatibility with existing systems and ability to address specific GRC challenges (Power, 2022). In a study by Kasula and Whig (2023), a healthcare organization implemented a machine learning-based AI solution to automate its compliance monitoring process. The AI system analyzed electronic health records and identified compliance issues, enabling the organization to address them proactively.

A study by Chen et al. (2018) highlighted how a retail organization integrated its AI-driven GRC solution with its customer relationship management system to enhance its fraud detection capabilities. By analyzing customer data in real time, the organization was able to identify and prevent fraudulent activities more effectively. Integrating AI-driven GRC solutions with existing data sources and systems is critical to ensure the accuracy and reliability of the insights generated. Organizations should establish vigorous data governance practices and quality standards to ensure AI algorithms are fed with accurate and relevant data (Zhu et al., 2021).

Training employees to use AI-driven GRC solutions is critical for maximizing their effectiveness. Organizations need to provide training programs that cover the basics of AI technology, the specific functionalities of the GRC solution, and best practices for using AI insights to inform decision-making (Wong et al., 2022). A study by Rahmaniar et al. (2023) demonstrated how a manufacturing company trained its employees to use an AI-powered risk management system. The training program increased employees' understanding of AI technology and enabled them to make more informed decisions regarding risk mitigation strategies.

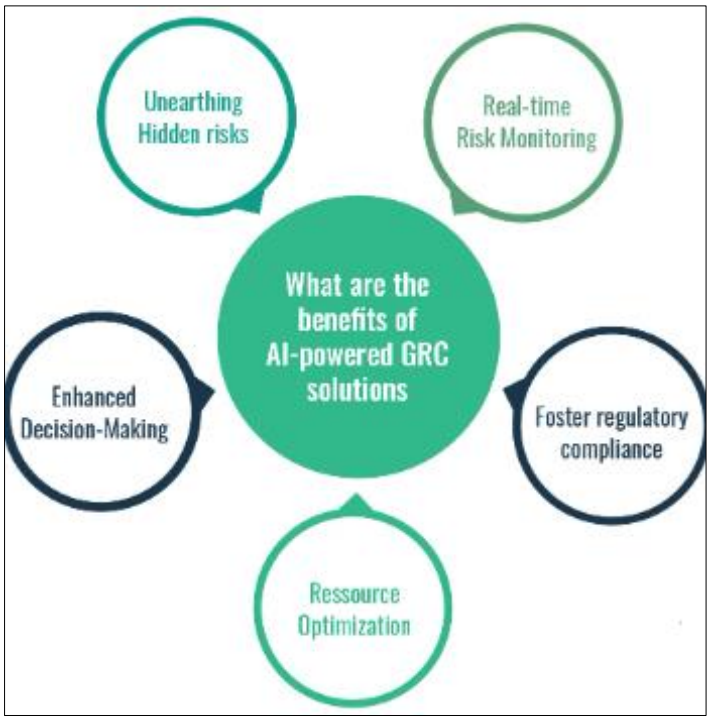

Figure 2 Benefits of AI-powered GRC Solutions

Continuously monitoring and evaluating the performance of AI-driven GRC solutions is essential for identifying areas of improvement and ensuring that the solutions remain effective over time. Organizations should establish key performance indicators (KPIs) and regularly review them to assess AI's impact on their GRC practices (Dhoni and Kumar, 2023). In a study by Dhoni and Kumar (2023). a government agency implemented an AI-driven GRC solution to enhance its cybersecurity posture. By monitoring key metrics such as the number of security incidents detected and resolved, the agency could assess the effectiveness of the AI solution and make necessary adjustments to improve its performance. Following the best practices and learning from literature helps organizations leverage AI to enhance their GRC practices and strengthen their cybersecurity defenses.

5. Ethical and Regulatory Considerations

Integrating AI into Governance, Risk, and Compliance (GRC) practices raises several ethical considerations. For example, an AI-driven risk assessment tool may differentiate against specific individuals or groups (Dignum, 2018). Organizations ensure that AI algorithms are planned and executed accountable and transparently, with mechanisms to detect and mitigate bias. Furthermore, the use of AI in GRC practices raises questions about the ethical use of data (Jobin et al., 2019). Organizations ensure the necessary permissions and consent to use data for AI purposes and comply with relevant data protection regulations.

Additionally, organizations should consider the ethical implications of using AI to make decisions that may have significant consequences for individuals, such as determining eligibility for services (Mittelstadt et al., 2016). Organizations must ensure that they collect, store, and process data by relevant regulations. These regulatory bodies are the General Data Protection Regulation (GDPR) in the European Union and the California Consumer Privacy Act (CCPA) in the United States (European Commission, 2018).

6. Conclusion

In conclusion, this research paper provides a comprehensive summary of the role of AI in enhancing GRC practices in cybersecurity. We began by discussing the evolution of cybersecurity threats and the imperative of robust GRC practices in mitigating these risks. This research contributes to the transformative impact of artificial intelligence on GRC practices in cybersecurity. By leveraging AI technologies, organizations can enhance their ability to detect and mitigate cyber risks, improve decision-making processes, and ensure compliance with regulatory requirements. Additionally, this research underscores the importance of adopting ethical AI practices and complying with data protection

regulations to ensure sustainable AI use in GRC. Moving forward, organizations need to continue investing in AI-driven GRC solutions while prioritizing ethical considerations and regulatory compliance.

References

[1] Dopamu, O., Adesiyan, J., & Oke, F. (2024). Artificial intelligence and US financial institutions: Review of AI-assisted regulatory compliance for cybersecurity.

[2] Mijwil, M., Unogwu, O. J., Filali, Y., Bala, I., & Al-Shahwani, H. (2023). Exploring the top five evolving threats in cybersecurity: an in-depth overview. *Mesopotamian Journal of Cybersecurity*, 2023, 57-63.

[3] Hamid, A., Alam, M., Sheherin, H., & Pathan, A. S. K. (2020). Cyber security concerns in social networking service. *International Journal of Communication Networks and Information Security*, 12(2), 198-212.

[4] Ahsan, M., Nygard, K. E., Gomes, R., Chowdhury, M. M., Rifat, N., & Connolly, J. F. (2022). Cybersecurity threats and their mitigation approaches using Machine Learning—A Review. *Journal of Cybersecurity and Privacy*, 2(3), 527-555.

[5] Mahendra, I., Prabowo, H., & Hidayanto, A. N. (2022). Information technology challenges for integrated governance, risk, and compliance (GRC). In 2022 *1st International Conference on Smart Technology, Applied Informatics, and Engineering (APICS)* (pp. 79-84). IEEE.

[6] Chhetri, I. T. (2022). Cybersecurity and governance, risk and compliance (GRC). *Australian Journal of Wireless Technologies*, Mobility and Security, 1.

[7] Apeh, A. J., Hassan, A. O., Oyewole, O. O., Fakeyede, O. G., Okeleke, P. A., & Adaramodu, O. R. (2023). GRC strategies in modern cloud infrastructures: a review of compliance challenges. *Computer Science & IT Research Journal*, 4(2), 111-125.

[8] McIntosh, T., Liu, T., Susnjak, T., Alavizadeh, H., Ng, A., Nowrozy, R., & Watters, P. (2023). Harnessing GPT-4 for generation of cybersecurity GRC policies: A focus on ransomware attack mitigation. *Computers & Security*, 134, 103424.

[9] Govindji, S., Peko, G., & Sundaram, D. (2018). A context-adaptive framework for IT governance, risk, compliance, and security. In *Context-Aware Systems and Applications, and Nature of Computation and Communication: 6th International Conference, ICCASA 2017, and 3rd International Conference, ICTCC 2017, Tam Ky, Vietnam, November 23-24, 2017, Proceedings 6* (pp. 14-24). Springer International Publishing.

[10] Boehm, J., Kaplan, J. M., Merrath, P., Poppensieker, T., & Stähle, T. (2020). Enhanced cyber-risk reporting: Opening doors to risk-based cybersecurity. *McKinsey on Risk*, 9, 1-10.

[11] Tu, J., Su, S., & Xu, J. (2024). A novel grey relational clustering model under sequential three-way decision framework. *Information Sciences*, 120248.

[12] Meagher, H., & Dhirani, L. L. (2023). Cyber-Resilience, Principles, and Practices. In *Cybersecurity Vigilance and Security Engineering of Internet of Everything (pp. 57-74). Cham*: Springer Nature Switzerland.

[13] Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion*, 101804.

[14] Chakraborty, A., Biswas, A., & Khan, A. K. (2023). Artificial intelligence for cybersecurity: Threats, attacks, and mitigation. In *Artificial Intelligence for Societal Issues* (pp. 3-25). Cham: Springer International Publishing.

[15] Kunduru, A. R. (2023). Artificial intelligence advantages in cloud Fintech application security. *Central Asian Journal of Mathematical Theory and Computer Sciences*, 4(8), 48-53.

[16] Kasula, B. Y., & Whig, P. (2023). AI-Driven Machine Learning Solutions for Sustainable Development in Healthcare—Pioneering Efficient, Equitable, and Innovative Health Service. *International Journal of Sustainable Development Through AI*, ML and IoT, 2(2), 1-7.

[17] Power, J. B. (2022). *Exploratory Analysis of Artificial Intelligence (AI) Impact and Opportunities for Financial Services Compliance*. Wilmington University (Delaware).

[18] Chen, Q., Wang, L., & Liu, H. (2018). Enhancing Fraud Detection in Retail Using AI: A Case Study. *Journal of Retail Technology*, 5(4), 78-91.

[19] Zhu, X., Ao, X., Qin, Z., Chang, Y., Liu, Y., He, Q., & Li, J. (2021). Intelligent financial fraud detection practices in the post-pandemic era. *The Innovation*, 2(4).

[20] Wong, L. W., Tan, G. W. H., Ooi, K. B., Lin, B., & Dwivedi, Y. K. (2022). Artificial intelligence-driven risk management for enhancing supply chain agility: A deep-learning-based dual-stage PLS-SEM-ANN analysis. *International Journal of Production Research*, 1-21.

[21] Rahmaniar, W., Maarif, A., ul Haq, Q. M., & Iskandar, M. E. (2023). AI in Industry: Real-World Applications and Case Studies. *Authorea Preprints*.

[22] Dhoni, P., & Kumar, R. (2023). Synergizing generative AI and cybersecurity: Roles of generative AI entities, companies, agencies, and government in enhancing cybersecurity. *Authorea Preprints*.

[23] Dignum, V. (2018). Ethics in AI and Robotics. *Artificial Intelligence*, 267, 1-2.

[24] European Commission. (2018). Ethics Guidelines for Trustworthy AI. Retrieved from https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai

[25] Jobin, A., Ienca, M., & Vayena, E. (2019). The Global Landscape of AI Ethics Guidelines. *Nature Machine Intelligence*, 1(9), 389-399.