CAN ARTIFICIAL INTELLIGENCE REPLACE ASSURANCE, GOVERNANCE AND RISK MANAGEMENT PROFESSIONALS?

Phindile R. Nene [*]

[*] PhinHope (Pty) Ltd, Roodepoort, Gauteng, South Africa; PhD Student at the University of South Africa, Pretoria, South Africa
Contact details: PhinHope (Pty) Ltd, 5 Highcliff Estate, Allen's Nek, Roodepoort, Gauteng 1709, South Africa

OPEN ACCESS

How to cite this paper: Nene, P. R. (2024). Can artificial intelligence replace assurance, governance and risk management professionals? *Risk Governance and Control: Financial Markets & Institutions, 14*(2), 25–31.
https://doi.org/10.22495/rgcv14i2p3

ISSN Online: 2077-4303
ISSN Print: 2077-429X

Received: 29.12.2023
Accepted: 29.04.2024

JEL Classification: G32, G34, O16, O32, O33
DOI: 10.22495/rgcv14i2p3

Abstract

The digitalization of most businesses through the integration of artificial intelligence (AI) presents a great threat to many professionals asking themselves if their skill set will still be relevant in the future. The purpose of the research was to understand if AI is ready to replace assurance, governance and risk management professionals in Southern Africa and across the globe. The author critically assessed the role of governance, assurance, and risk management professionals in business and the realities of emerging technology deduced from the author's many years of practical work as an assurance professional. The methodology applied in this study was a narrative approach as the author wanted to gather the views of the conference participants and keep the audience engaged by asking questions during the conference session. The main findings of the paper were that governance, assurance, and risk management play a critical role in business strategy as corporate governance influences investment strategic decisions. This article challenges professionals to embrace and optimise innovative technologies to remain relevant in their areas of influence and expertise. In conclusion, businesses are encouraged to be more innovative and embrace entrepreneurship during the 4th to 5th Industrial Revolution (4IR to 5IR) transformation to improve efficiencies and customer experience (Paschek et al., 2019).

Keywords: Artificial Intelligence, Machine learning, Assurance, Governance, Risk Management

Authors' individual contribution: The Author is responsible for all the contributions to the paper according to CRediT (Contributor Roles Taxonomy) standards.

Declaration of conflicting interests: The Authors declare that there is no conflict of interest.

Acknowledgements: Firstly, the researcher would like to thank the Institute of Risk Management South Africa (IRMSA) for the opportunity and support they have provided in promoting PhinHope (Pty) Ltd. Secondly, the researcher would like to thank the coach Prudence Mokone and the mentor Enzo Scarcella for their support and affirmation during the preparation of this research. The content of this paper was delivered at the 2023 annual conference hosted by the Institute of Risk Management South Africa (IRMSA) at Gallagher Convention Centre Johannesburg on October 10, 2023.

1. INTRODUCTION

The digitalization of most businesses through the integration of artificial intelligence (AI) and the Fourth Industrial Revolution (4IR) to the Fifth Industrial Revolution (5IR) transformation does not only improve efficiencies and customer experience but also presents a great threat to many professionals asking themselves if their skill set will still be relevant in the future (Paschek et al., 2019). This article focuses on what is known and not known about AI and machine learning (ML) in the risk management fraternity. Subsequently, consider the role of good corporate governance in the organisation. The research question is as follows:

RQ1: Can artificial intelligence replace assurance, governance and risk management professionals?

It is true that AI can assure the entire base full end-to-end instead of doing sample testing. This changes the assurance analytical procedures game plan leading to the reduction of the headcount needed to perform analytic assurance functions such as revenue assurance and fraud management. The study conducted by KPMG (n.d.) points out that AI and ML tools are way more advanced than human beings as the machines have the capabilities to utilize large volumes of data and the advanced prediction techniques that are used in financial services as the effective risk management strategy. While Anyoha (2017) from Harvard highlights that even if algorithms remain static, but big data allows AI to learn and perform faster than human beings. Syam and Sharma (2018) regard AI as the 4IR. There is limited research exploring the impact of AI and ML in the risk management fraternity especially in the context of Southern Africa considering the African languages. This research proposes future experimental research testing AI and ML using at least one South African vernacular language such as isiZulu to perform risk and assurance functions. This is very important because Southern Africa is different from Britain, Southern Europe, and the Pacific Rim where the phenomenon of the industrial revolution emanated (Stearns, 2020). This article brings both scholarly and practical contributions as it challenges risk and assurance management professionals to embrace and optimise AI and ML to remain relevant in their areas of influence and expertise.

The structure of this paper is as follows. Section 2 reviews the relevant literature. Section 3 analyses the methodology that has been used to conduct empirical research on the impact of AI and ML in the risk management fraternity. Section 4 discusses the research results and conference findings. Section 5 provides the research discussion and practical contribution of this study. Section 6 concludes this article.

2. LITERATURE REVIEW

Over the centuries, the industrial revolution has transformed and shaped the history of the world changing the way how things are done. According to Stearns (2020), industrialization is a global phenomenon that first started in the 1770s in Britain followed by Southern Europe countries including Australia and Canada in the 1880s. Subsequently, in the 1960s it expanded to the Pacific Rim followed by countries such as Brazil, Turkey, India, and other parts of Latin America two decades later. Both 4IR and 5IR are characterised by the proliferation of evolving and increasingly complex technologies simultaneously coordinating biological, physical, and digital capabilities such as the Internet of Things (IoT) and robotics (Elayyan, 2021). Nilsson (2009) defines AI as an “activity devoted to making machines intelligent, and intelligence is that quality that enables an entity to function appropriately and with foresight in its environment” (p. 13). While Kaplan and Haenlein (2019) define AI as “a system’s ability to interpret external data correctly, to learn from such data, and to use those learnings to achieve specific goals and tasks through flexible adaptation” (p. 17). Furthermore, AI can be classified as a human-inspired analytical and humanized technology consisting of different evolutionary phases ranging from general, narrow, and superintelligence (Kaplan & Haenlein, 2019).

Several empirical studies, narratives and media sentiment analyses have been conducted in developed countries such as Canada, France, the United States (US), the United Kingdom (UK) and South Korea and in developing countries such as Nigeria, Brazil and India to understand public perception of AI (United Nations Department of Economic and Social Affairs, 2014; Sambasivan & Holbrook, 2018). Kelley et al. (2021) conducted a study assessing the public perception of AI in eight countries namely, Australia, Brazil, Canada, the US, France, South Korea, India and Nigeria and discovered that developed countries have different perceptions about AI compared to developing countries. They further indicated that people from developed countries have different needs compared to the people from developing countries and this contrast is driven by capital income and economic status of each country (Kelley et al., 2021). The consumer research survey conducted across North America, Europe, and Asia in 2017 revealed that AI and ML will improve society by 61% due to increased automation and digitization (Kelley et al., 2021). Public perception is crucial and directly impacts AI ethical issues and policies, how AI is designed, deployed and regulated (Cave et al., 2019).

AI and ML have changed the existing social systems as technology, automation and digitization impact all sectors of the economy (Elayyan, 2021). Paschek et al. (2019) highlighted six advantages of AI, namely: 1) innovation, 2) cost reduction, 3) efficiency, 4) revenue, 5) customer experience, and 6) agility. As much as there are many advantages of AI and ML, however, there are also disadvantages of technological development such as cyber security threats. Cyber security is designed to prevent and protect cyber threats and attacks that can lead to the breach of any confidential information and compromise the integrity of the organisation’s data (Prasetya et al., 2024). According to Bolpagni (2022), cyber security risk is influenced by both geopolitical and socio-economic factors such as peace, democracy, gross domestic product (GDP), and the human development index. Cyber threats can develop into cyber warfare negatively impacting software, hardware, and information (Prasetya et al., 2024). The industrial revolution has truly transformed the world economy. For example, Israel's advanced agricultural technology and construction have transformed traditional agriculture in the desert into a new industry that doubled the Jewish population between 1948 and 1953 (Stearns, 2020). Subsequently, in the Middle East, Israel became an industrial leader through revolutionized commercial agriculture.

In a world with evolving technology, we see the hype around AI. Subsequently, organisations are redefining their strategies to automate their governance structures in order to improve their efficiencies. However, from the measures of trustworthiness can we truly confirm the validity, reliability, credibility, resilience, dependability, and transferability of the AI models? According to Saunders (2014), measures of trustworthiness focus on the methods used to access and analyse data. Many people and organisations whether it be public or private, profit or non-profit organisations place reliance on computers to run their daily activities. As such criminals are also relying on technology to spy and terrorize individuals and businesses by manipulating data, stealing, using technological tools to launch attacks, and or refusing service (Putra, 2022). According to Obotivere and Nwaezeigwe (2020) cyberwarriors, cyberspaces, cyberthieves, cyberterrorists, and cyberactivism are the most common cyber threats used by terrorists, spies and criminals. Indonesia is one of the countries that has been terrorized by cyber threats including phishing, ransomware, social engineering, cryptojacking, web defacement and data breaches (Farahbod et al., 2020; Prasetya et al., 2024). Subsequently, the United States has collaborated with Indonesia to address and mitigate cyberterrorism threats in Indonesia (Putra, 2022).

According to Kaplan and Haenlein (2019), the artificial superintelligence of AI can make humans redundant because systems possess general wisdom, and social skills and are also capable of scientific creativity. The reality is technology has disrupted our way of life and professional arenas. Threatening job security results in everyone asking themselves if they are still relevant to the job market or if their roles and professions will be redundant. AI perception can depend on one's experience however, in the field of medical professionals AI has improved repetitive medical imaging practices such as scanning and cancer assessment to improve clinical decision-making (Lewis et al., 2019). AI can support sustainable economic, social and employment efficiencies as the employees can do their jobs faster (Kaplan & Haenlein, 2020).

Both AI and ML indeed can:

- drive proactive risk mitigation through predictive models;
- process and analyse large volumes of data;
- be quicker than human beings;
- automate the repetitive and mundane tasks;
- provide empirical evidence through data-driven insights to allow the professionals to focus on decision-making.

However, the machines cannot:

- make complex decisions because AI cannot make any relationships;
- adhere to King IV's report, other governance standards and codes of ethics as AI cannot make any strategic judgment about corporate governance;
- negotiate with the regulators to align on compliance and ethics matters;
- held accountable for pathetic performance or poor decisions made;
- be agile and innovative considering geopolitical and environmental, social and governance (ESG) risks.

Based on these facts and the advantages of AI and ML, many companies are optimising the evolving technology automating their processes and assurance aspects. To effectively use AI as risk management professionals and optimize technology, we need diverse thinking and strong collaboration with information technology and information security teams. While maintaining our independence within each line of defence, as assurance governors in our organisation; we can effectively collaborate in building one AI platform that allows different capabilities, roles, and permissions instead of having multiple systems. This will not only promote Principles 11 and 15 of the King IV report as they drive the aspects of combined assurance (Institute of Directors South Africa (IDSA, 2016). However, it will improve the economies of scale, internal governance especially data security, and reduce system maintenance and licensing costs. Of course, the author is mindful of the cyber security threats and attacks when the data is centralized. But, when you have more than four independent systems that have similar capabilities, you should consider evaluating your cost to assess the return on investment (ROI) and cut cost.

"*Principle 11: The governing body should govern risk in a way that supports the organisation in setting and achieving its strategic objectives*" (IDSA, 2016, p. 41).

"*Principle 15: The governing body should ensure that assurance services and functions enable an effective control environment, and that these support the integrity of information for internal decision-making and of the organisaztion's external reports*" (IDSA, 2016, p. 41).

The author is not a technician as much as she should worry about responsible design, in terms of:

1. How well the AI model was built?
2. Who is maintaining it?
3. Is it safe and secure to use the platform?

Considering the Protection of Personal Information (POPI) Act, International Organization for Standardization (ISO) standards and other 17 King IV governance principles as the machines are not accountable for good corporate governance in our organisations, but as professionals and business leaders, we are responsible and accountable.

As the end user, the author just needs a tool that is reasonable enough to help gather empirical evidence to identify the root cause, support in decision making and advance risk mitigation strategies. Yampolskiy (2015) suggests that the poor design of the AI systems can be dangerous as they can be used for malicious purposes such as spyware, hazardous software, worms, and viruses. Bostrom (2011, p. 67) defines AI hazards as "computer-related risks in which the threat would derive primarily from the cognitive sophistication of the program rather than the specific properties of any actuators to which the system initially has access". The security risk exposures increase as the technology and intelligence of the systems continue to evolve however, there are conflicting views on what can be classified as AI hazards because the risk identified by a certain group or organisation is an opportunity for another organisation (Yampolskiy, 2016).

Despite the level of automation, the author is very sure that manual intervention and human intellect will always be needed, as we all just agreed that robots cannot make any governance and ethical judgments. Therefore, they will miss some of the steps in the assurance process leaving the business vulnerable to risk exposures. For example, you might have an excellent AI tool that is well-maintained with fantastic capabilities that allow you to generate real-time monitoring and drive proactive risk management. However, in the author's view, as the tool owner, you will still be required to develop risk tolerance and priorities that are relevant to your environment to support your organisation's strategic objectives. That is what the author is referring to when she highlights the aspect of manual intervention and human intellect to support AI in analysing large volumes of data and generating meaningful insights. Some researchers call this manual intervention hybrid intelligence (Akata et al., 2020; Cavalcanti et al., 2023).

We have discussed and agreed on AI's permanent disadvantages. The author is sure the readers will agree that assurance, governance and risk management professionals deal with complex tasks almost every day. Furthermore, to ensure the best practice, professionals are always required to engage with various stakeholders such as clients, regulators, and professional bodies. Considering all these facts, the researcher would like us to zoom into the future fit of the assurance space considering what will improve when we optimize AI.

3. RESEARCH METHOD

The research methodology provides insight into the research process to be followed and how the specific tasks will be executed (Mouton, 2022). This article was conducted within the interpretivism paradigm and applied the narrative approach. According to Saunders et al. (2019), the interpretive process is key and highly recommended for the researcher to follow when developing new knowledge, exploring new rich understanding and meaningful experiences. During the conference session, the author used a narrative approach to gather the views of the conference participants and continuously asked questions during the conference session to understand if there were any other views from the audience. From the three available research methods, namely quantitative, qualitative, and mixed-method research, the latter being a combination of the quantitative and qualitative methods; narrative research from part of the qualitative method. The majority of the narrative work is found in the interdisciplinary journals that followed distinctively post-structural and qualitative approaches (Jones et al., 2023). Narrative research is perfect for researchers who are interested in "constructivist-oriented, qualitative research that examines people's experiences from their perspectives" (Barkhuizen & Consoli, 2021, p. 2). According to Parks (2023), narrative research is an adequate method to collect and tell the stories about people's life experiences. Furthermore, the author assured the audience that the information shared during the conference such as the email address was a pseudonym and therefore, as the governance community there was no need to be concerned about the POPI Act 4 of 2013 (South African Government, 2013).

The 2023 IRMSA conference was attended by various risk management professionals from various organisations within Southern African countries such as Namibia, Zimbabwe, Uganda, South Africa, Eswatini and Zambia. The conference theme was "Limitless" and the conference sponsors included but were not limited to Marsh, Barnowl, Exclaim, LexisNexis, Old Mutual PAX Resilience, PhinHope, SAIPA, Riskonet, Veeam, Trialogue, Morgan Solus, Milpark Education, Institute of Vetting Africa. There were also significant representations from various national and local government departments. The in-person attendance was tracked via real-time check-in at the venue on the day while online attendance was tracked via the app where a specific ID was associated with each registered email (this information was provided by the 2023 IRMSA content provider via email).

As the conference organisers, IRMSA monitored and kept the attendance register, and the attendance stats were directly obtained from the IRMSA's events manager. The narrative approach methodology assisted the author in gathering the views of the conference participants and keeping the audience engaged during the conference session. Due to limited research of this nature, the author proposed future research to be conducted and apply the experimental research methodology as currently there is limited experimental research presenting practical analysis within the risk and assurance profession. The list of the proposed topics is provided in Section 5.

4. RESULTS

To provide meaningful insights regarding AI and ML in the assurance, governance and risk management fraternity, the author comprehensively reviewed the existing literature to explore what is known and not known about AI and ML in the risk management fraternity. Subsequently, consider the role of good corporate governance in the organisation. Even though AI and ML have disrupted the risk management fraternity however, in Southern Africa currently, no robot is using any of the eleven vernacular languages such as isiZulu which is one of the most dominating languages used in South Africa. Furthermore, within the risk and assurance profession, no robot is programmed to perform any of the risk and assurance functions such as internal audit, compliance, and risk assessments.

As much as technology drives economies of scale but maintaining AI in the long run will be very costly because you continuously need to improve the AI versions, enhance the scripts to be relevant to your environment, and mitigate emerging risks. However, the way we perform the assurance will never ever be the same again. Ladies and gentlemen, we better gear up for an augmented future.

The author further envisions our future lives not only training human beings but also training robots in order to serve us since emerging risks are dynamic. The evolving risk exposures not only pose challenges to us but also present great opportunities to us as professionals. The reality is change is inevitable and the old business operating systems will reach the end of life. During the change management process critical thinking, negotiations with the project team or partners in the case of merger and acquisition, sound judgment, and decision-making will always be needed (Nene, 2023). Furthermore, AI cannot independently develop multiple scenarios that need to be tested before the new system goes live and different use cases considering the sensitivity of the customer data, ethics code of conduct, regulatory requirements, and compliance risk exposures. Lastly, AI and ML will not possess the human capabilities or superperform the human capital but rather give professionals a more competitive advantage in performing their jobs (Misra, 2023).

5. DISCUSSION

This article considers the role of good corporate governance in the organisation by analysing what is known and not known about AI and ML in the risk management fraternity. Even though AI and ML have changed the existing social systems through technology, automation and digitization since the transition directly impact all sectors of the economy (Elayyan, 2021). However, AI and ML cannot make any strategic and ethical decisions as only human intellect possesses such capabilities (Misra, 2023). Furthermore, during the 2023 IRMSA conference, over 400 conference attendees asserted with the author that AI and ML are disruptive to the risk management fraternity. The next subsections will highlight the known temporally limitations of AI followed by the proposed future research.

5.1. Temporary artificial intelligence limitations

Now let us zoom into the temporal limitations of AI and use the telecommunication industry as a case study. Let us assume one of the mobile operators is in the process of migrating their billing platform from the old system to the new system and they are using AI to perform change assurance. In the context of South Africa, we have eleven official languages (Lastrucci et al., 2023) and at this point, in time there are no robots that are speaking vernacular languages unless the author is outdated.

The only available technology is interactive voice response (IVR). Then during the data sanitization, AI performs a spell check on the non-English words from the customer's personal information such as name, surname, address, and email address because in English you hardly find the words that have duplicated consonants, but in the African languages you do get them frequently. For example, we have communities staying at Qhudeni, Nquthu, Gqeberha and Kwaqumbu.

Please close your eyes and imagine how AI will read the following email address: "Nomtshomi@mhlahlamehlo.co.za". The author is convinced that the risk and assurance colleagues would agree that the information transferred to the new system as a part of data migration will be biased and inaccurate leading to frustration on both sides — the customer and the mobile operator as well. Imagine the impact this will have on the customer experience and on the mobile operator's revenue and reputation. As much as it is easy to quantify revenue impact and those goodwill credits that are often granted to customers when they complain. However, reputational damage goes far beyond what one can imagine as the organisations' share price is also driven by the perception (Nene, 2023).

This is the opportunity that presented itself for PhinHope to offer customer experience and change management assurance services in order to help the businesses meet their strategic objectives without exposing their customers to fraud and poor customer experience that will lead to high customer churn, revenue leakages and reputational risks (Nene, 2023).

It is difficult to eliminate fraud but through internal controls and proactive fraud prevention mitigation strategies, the organisation can combat and detect potential fraud (Rinaldo et al., 2022). We all know that ML and robotics are using the scripts, and once the fraudsters have mastered the script and the balance scorecard that the organisation has put in place as their risk mitigation strategy by default that organisation is exposed to vulnerabilities. Fraudsters and hackers will exploit the areas that are outside the script. Subsequently, fraud will increase, and great exposure to non-compliance and customer complaints will also increase (Nene, 2023). Therefore, there will be a demand for assurance, governance and risk management professionals for organisations will always want someone with an eagle eye.

5.2. Future research directions

Based on the limitations of AI and ML and the fact that robots cannot make any strategic and ethical decisions as only human intellect possesses such capabilities (Misra, 2023). Furthermore, currently, there is no robot using any of the eleven vernacular languages such as isiZulu which is one of the most dominating languages used in South Africa neither perform any of the risk and assurance functions such as internal audit, compliance, and risk assessments. Many countries have evolved in digital technology (United Nations Department of Economic and Social Affairs, 2014; Sambasivan & Holbrook, 2018; Paschek et al., 2019; Elayyan, 2021; Kelley et al., 2021), but for the purpose of the IRMSA conference, the author only focused on the Southern Africa region. Therefore, future research and articles are required to:

- explore whether the robots are ready to independently develop new controls to mitigate emerging risks and perform risk assessments in the African context;
- investigate whether the robots are ready to independently develop new controls to mitigate emerging risks and perform risk assessments in the world at large;
- study the development of AI and ML that will communicate in isiZulu followed by any other African vernacular languages dominating within the

Southern African region such as Swahili;

- explore the development of AI and ML that can perform the full end-to-end risk and assurance functions such as internal audit and risk assessments;
- assess the return on investment from the implemented AI and ML platforms within the combined assurance functions in the organization;
- assess and quantify the risk exposures associated with multiple assurance tools implemented by a single organization.

6. CONCLUSION

The increase in complex technologies and integration of IoT, digitalization and robotics has improved efficiencies and customer experience however in contrast these technologies have also presented a great threat to many professionals causing doubt if the current skill set will still be relevant in the future (Paschek et al., 2019; Elayyan, 2021). However, governance, assurance, and risk management play a critical role in the success of business strategy and corporate governance influences investment strategic decisions. Therefore, to improve efficiencies, stakeholder satisfaction, and customer experience businesses are encouraged to be more innovative and embrace entrepreneurship during the 4IR and 5IR transformation. The embracement and optimisation of innovative technologies will ensure that assurance, governance and risk management professionals remain relevant in their areas of influence and expertise not only in the Southern African context but across the globe.

There is still a lot of work to be done in order to improve cybersecurity threats while developing AI and ML to be compatible with risk and assurance domains. The author is not in denial of the progressive technology. However, all that the author is saying, this is a great time to live if it is not an exciting time for us to unlearn what we know, relearn, and learn new things to ensure that we remain relevant in our areas of influence and expertise. Lastly, AI and ML are not assurance, governance and risk management strategies or strategists, but they are just enablers. While the professionals are the strategic drivers with God-given strategic thinking and intellect that supersede robots' capabilities. Misra (2023) concurred that AI and ML will not steal our jobs, but they are giving us a competitive advantage to do our jobs faster and improve decision-making which is supported by empirical evidence. Therefore, let us take the courage to optimize every opportunity to upscale our services and add value to our stakeholders as we strengthen the internal controls and ensure sound governance. In conclusion, due to the limitations within the risk and assurance profession as there is no robot currently programmed to perform any of the risk and assurance functions such as internal audit, compliance, and risk assessments. Therefore, the author proposed future research to be conducted and apply the experimental research methodology and this can be done through quantitative or qualitative or mixed methods.

REFERENCES

Akata, Z., Balliet, D., de Rijke, M., Dignum, F., Dignum, V., Eiben, G., Fokkens, A., Grossi, D., Hindriks, K., Hoos, H., Hung, H., Jonker, C., Monz, C., Neerincx, M., Oliehoek, F., Prakken, H., Schlobach, S., van der Gaag, L., van Harmelen, F., … Welling, M. (2020). A research agenda for hybrid intelligence: Augmenting human intellect with collaborative, adaptive, responsible, and explainable artificial intelligence. *Computer*, *53*(8), 18–28. https://doi.org/10.1109/MC.2020.2996587

Anyoha, R. (2017, August 28). *The history of artificial intelligence. Science* in the News. https://sitn.hms.harvard.edu/flash/2017/history-artificial-intelligence/

Barkhuizen, G., & Consoli, S. (2021). Pushing the edge in narrative inquiry. *System, 102*, Article 102656. https://doi.org/10.1016/j.system.2021.102656

Bolpagni, M. (2022). Cyber risk index: A socio-technical composite index for assessing risk of cyber attacks with negative outcome. *Quality & Quantity*, *56*, 1643–1659. https://doi.org/10.1007/s11135-021-01199-3

Bostrom, N. (2011). Information hazards: A typology of potential harms from knowledge. *Review of Contemporary Philosophy, 10*, 44–79. https://nickbostrom.com/information-hazards.pdf

Cavalcanti, J. H., Kovacs, T., Ko, A., & Pocsarovszky, K. (2023). Production system efficiency optimization through application of a hybrid artificial intelligence solution. *International Journal of Computer Integrated Manufacturing*. https://doi.org/10.1080/0951192X.2023.2257661

Cave, S., Coughlan, K., & Dihal, K. (2019). "Scary robots": Examining public responses to AI. In *AIES'19: Proceedings of the 2019 AAAI/ACM Conference on AI, Ethics, and Society* (pp. 331–337). Association for Computing Machinery. https://doi.org/10.1145/3306618.3314232

Elayyan, S. (2021). The future of education according to the fourth industrial revolution. *Journal of Educational Technology and Online Learning*, *4*(1), 23–30. https://doi.org/10.31681/jetol.737193

Farahbod, K., Shayo, C., & Varzandeh, J. (2020). Cybersecurity indices and cybercrime annual loss and economic impacts. *Journal of Business and Behavioral Sciences*, *32*(1), 63–71. http://asbbs.org/files/2020/JBBS_32.1_Spring_2020.pdf#page=63

Jones, M. D., Smith-Walter, A., McBeth, M. K., & Shanahan, E. A. (2023). The narrative policy framework. In C. M. Weible (Ed.), *Theories of the policy process* (5th ed., pp. 161–195). Routledge. https://doi.org/10.4324/9781003308201-7

Institute of Directors South Africa (IDSA). (2016). *King IV report on corporate governance for South Africa 2016*. https://www.adams.africa/wp-content/uploads/2016/11/King-IV-Report.pdf

Kaplan, A., & Haenlein, M. (2019). Siri, Siri, in my hand: Who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence. *Business Horizons, 62*(1), 15–25. https://doi.org/10.1016/j.bushor.2018.08.004

Kaplan, A., & Haenlein, M. (2020). Rulers of the world, unite! The challenges and opportunities of artificial intelligence. *Business Horizons*, *63*(1), 37–50. https://doi.org/10.1016/j.bushor.2019.09.003

Kelley, P. G., Yang, Y., Heldreth, C. M., Moessner, C., Sedley, A., Kramm, A., Newman, D. T., & Woodruff, A. (2021). Exciting, useful, worrying, futuristic: Public perception of artificial intelligence in 8 countries. In *AIES'21: Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics, and Society* (pp. 627–637). Association for Computing Machinery. https://doi.org/10.1145/3461702.3462605

KPMG. (n.d.). *Artificial intelligence in risk management*. Retrieved October 2, 2023, from https://kpmg.com/ae/en/home/insights/2021/09/artificial-intelligence-in-risk-management.html

Lastrucci, R., Dzingirai, I., Rajab, J., Madodonga, A., Shingange, M., Njini, D., & Marivate, V. (2023). Preparing the Vuk'uzenzele and ZA-gov-multilingual South African multilingual corpora. In *Proceedings of the Fourth Workshop on Resources for African Indigenous Languages (RAIL 2023)* (pp. 18–25). Association for Computational Linguistics. https://doi.org/10.18653/v1/2023.rail-1.3

Lewis, S. J., Gandomkar, Z., & Brennan, P. C. (2019). Artificial intelligence in medical imaging practice: Looking to the future. *Journal of Medical Radiation Sciences*, *66*(4), 292–295. https://doi.org/10.1002/jmrs.369

Misra, S. (2023, January 2). How AI can be the secret sauce to your risk management strategy. *Forbes*. https://www.forbes.com/sites/forbestechcouncil/2023/01/02/how-ai-can-be-the-secret-sauce-to-your-risk-management-strategy/?sh=5cbe14dc1a19

Mouton, J. (2022). *How to succeed in your master's and doctoral studies: A South African guide and resource book*. Van Schaik.

Nilsson, N. J. (2009). *The quest for artificial intelligence*. Cambridge University Press. https://doi.org/10.1017/CBO9780511819346

Nene, P. R. (2023). Value-added tax change implementation aftermath: A case of MTN. *Open Journal of Business and Management, 11*(6), 2966–2987. https://doi.org/10.4236/ojbm.2023.116164

Obotivere, B. A., & Nwaezeigwe, A. O. (2020). Cyber security threats on the internet and possible solutions. *International Journal of Advanced Research in Computer and Communication Engineering*, *9*(9), 92–97. https://doi.org/10.17148/IJARCCE.2020.9913

Parks, P. (2023). Story circles: A new method of narrative research. *American Journal of Qualitative Research*, *7*(1), 58–72. https://www.ajqr.org/article/story-circles-a-new-method-of-narrative-research-12844

Paschek, D., Mocan, A., & Draghici, A. (2019). Industry 5.0 — The expected impact of next industrial revolution. In *Thriving on future education, industry, business, and society: Proceedings of the MakeLearn and TIIM International Conference 2019* (pp. 125–132). ToKnowPress. http://www.toknowpress.net/ISBN/978-961-6914-25-3/papers/ML19-017.pdf

Prasetya, A. W. Y., Suhardjo, B., & Munir, R. (2024). Regression analysis of the national cyber security index in the Southeast Asia Region. *Asian Journal of Social and Humanities*, *2*(5), 1206–1216. https://doi.org/10.59888/ajosh.v2i5.249

Putra, B. A. (2022). Cyber cooperation between Indonesia and the United States in addressing the threat of cyberterrorism in Indonesia. *International Journal of Multicultural and Multireligious Understanding, 9*(10), 22–33. https://ijmmu.com/index.php/ijmmu/article/view/4058

Rinaldo, N. S. M., Oktavia, R., & Amelia, Y. (2022). Fraud triangle perspective on the tendency of fraudulent financial statements in non-financial state-owned enterprises. *Asian Journal of Economics and Business Management*, *1*(2), 58–66. https://doi.org/10.53402/ajebm.v1i2.86

Rotatori, D., Lee, E. J., & Sleeva, S. (2021). The evolution of the workforce during the fourth industrial revolution. *Human Resource Development International*, *24*(1), 92–103. https://doi.org/10.1080/13678868.2020.1767453

Sambasivan, N., & Holbrook, J. (2018). Toward responsible AI for the next billion users. *Interactions*, *26*(1), 68–71. https://doi.org/10.1145/3298735

Saunders, M. (2014). *Research methods for business students* (6th ed.). Pearson.

Saunders, M., Lewis, P., & Thornhill, A. (2019). *Research methods for business students* (8th ed). Pearson.

South African Government. (2013). *Protection of Personal Information Act 4 of 2013*. https://www.gov.za/documents/protection-personal-information-act

Stearns, P. N. (2020). *The industrial revolution in world history*. Routledge.

Syam, N., & Sharma, A. (2018). Waiting for a sales renaissance in the fourth industrial revolution: Machine Learning and artificial intelligence in sales research and practice. *Industrial Marketing Management, 69*, 135–146. https://doi.org/10.1016/j.indmarman.2017.12.019

United Nations Department of Economic and Social Affairs. (2014). *World economic situation and prospects*. United Nations. https://doi.org/10.18356/ad0c5772-en

Yampolskiy, R. V. (2015). The space of possible mind designs. In J. Bieger, B. Goertzel, & A. Potapov (Eds.), *Artificial general intelligence* (Lecture Notes in Computer Science: Vol. 9205, pp. 218-227). Springer. https://doi.org/10.1007/978-3-319-21365-1_23

Yampolskiy, R. V. (2016). Taxonomy of pathways to dangerous artificial intelligence. In *Proceedings of the Workshops at the Thirtieth AAAI Conference on Artificial Intelligence* (pp. 143–148). Association for the Advancement of Artificial Intelligence. https://cdn.aaai.org/ocs/ws/ws0156/12566-57418-1-PB.pdf