

Global Trends in IT Governance for SMEs Cybersecurity (2015-2025): A Bibliometric Analysis

Mpho Mokgathi

Department of Commercial Accounting
School of Accounting
College of Business and Economics
University of Johannesburg
Johannesburg, Republic of South Africa
mmokgathi@uj.ac.za

Olayinka Erin

Department of Accountancy
School of Management
College of Business and Economics
University of Johannesburg
Johannesburg, Republic of South Africa
erin@uj.ac.za

Abstract

In the contemporary digital economy, small and medium-sized enterprises (SMEs) increasingly rely on Information Technology (IT) systems to support their operations, enhance competitiveness, and drive innovation. However, this digital dependence exposes SMEs to escalating cybersecurity threats, while they operate with limited cybersecurity resources, immature governance structures, and inadequate awareness of emerging digital risks. This study maps research trends worldwide on IT governance for cybersecurity in SMEs between 2015 and 2025 through bibliometric analysis, aiming to identify the intellectual structure, thematic evolution, and emerging gaps in knowledge in this field. Data were retrieved from the Scopus database and analysed using VOSviewer to identify keyword co-occurrences, publication patterns, and subject areas. The findings reveal IT governance as the intellectual core linking cybersecurity and risk management, while legal compliance is an emerging concern influenced by regulations such as the General Data Protection Regulation and POPIA. However, decision-making, data security, and cyber-attack response remain under-researched. The study concludes that current literature is concentrated on strategic discourse, lacks operational depth, and shows geographic disparities. It calls for context-sensitive, simplified governance models, cross-country studies, and empirical research integrating cultural, legal, and human dimensions to strengthen SME cybersecurity resilience.

Keywords

IT Governance, Cybersecurity, Small and Medium-Sized Enterprises (SMEs), Risk Management, and Legal Compliance

1. Introduction

In the contemporary digital economy, small and medium-sized enterprises (SMEs) increasingly rely on Information Technology (IT) systems to support their operations, enhance competitiveness, and drive innovation (Opoku, Okafor,

Williams, Aribigbola, & Olaleye, 2024). However, this digital dependence simultaneously exposes SMEs to escalating cybersecurity threats, including data breaches, ransomware, and supply chain attacks (Saeed, Altamimi, Alkayyal, Alshehri, & Alabbad, 2023). Despite these vulnerabilities, many SMEs operate with limited cybersecurity resources, immature governance structures, and inadequate awareness of emerging digital risks. This context highlights the critical importance of IT governance in ensuring the effective management of IT resources, alignment with business objectives, and protection against cyber threats (Judijanto, Hindarto, Wahjono & Djunarto, 2023).

In the last ten years, academic and corporate works studying the meeting point between IT governance and cybersecurity in the context of SMEs have been on a steady rise. However, this body of work is fragmented across disciplines, geographies, and methodologies. AL-Dosari and Fetais (2023) posit that existing studies have a large enterprise emphasis or an extremely narrow focus on technical aspects of security controls to the neglect of such issues as governance mechanisms, strategic alignment, and risk oversight that are critical to SMEs. According to researchers' knowledge, there is little consolidated knowledge pertaining to how IT governance practice has evolved around the world in response to challenges relating to cybersecurity for SMEs. The absence of synthesis acts as a constraint for researchers who want to develop theory and practitioners who intend to implement an evidence-based governance model.

According to researchers' own knowledge, academic output on IT governance and cybersecurity has been growing from 2015 to 2025; there is no consolidated mapping of trends, patterns, and gaps at the global knowledge level specific to SMEs during the period 2015-2025. In the absence of such a review, policymakers, together with researchers and leaders of SMEs, cannot obtain the empirical insights required to guide capacity-building initiatives, inform policy development, or even prioritise research agendas. This is a critical knowledge gap at a time when increasing cyber risks are confronting SMEs, while they also have heightened regulatory and governance expectations imposed on them (Benjamin et al. 2024). Therefore, this study aims to map research trends worldwide on IT governance for cybersecurity in SMEs between 2015 and 2025 by bibliometric analysis, with a view to identifying the intellectual structure, thematic evolution, and emerging gaps of knowledge in this field.

1.1 Research Objectives

- ✓ Analyse the publication pattern, institutions, and countries that are outputting articles about IT governance for cybersecurity in SMEs between 2015 and 2025.
- ✓ To map major research themes, trends, and gaps of knowledge in the literature on IT governance and cybersecurity within the SME context over the past decade.

2. Literature Review

This review of literature critically appraises the body of scholarship that exists on cybersecurity within SMEs with a keen focus on the role IT governance takes in driving digital resilience. More specifically, it adopts five major themes: an overview of cybersecurity from across the globe, adoption practices within SMEs, management of risks relating to cybersecurity, and finally two frameworks - a general cybersecurity framework and a legal one - to discuss knowledge extant, its gaps, and trends toward evolution.

Global view of cybersecurity

Cybersecurity, being the latest wave of global priority adjustment, came about as a response to rapid digital technology proliferation accompanied by increasing parallel cyber threat activities (Safitra, Lubis & Fakhurroja, 2023). Almutairi and Sheldon (2025) posit that in the past decade, there has been great exposure of the attack surface to malicious actors due to continuous integration among systems, cloud computing, and the Internet of Things (IoT). Highly organised ransomware, phishing, and supply-chain attacks against organisations across various geographies, exploiting systemic weaknesses, indicate that an organisation is under assault. These have been driving forces behind increased policy activities on multilateral cooperation and investment in research and innovation for cybersecurity (Judijanto et al. 2023). The highly developed economies of the world have led to such large-scale strategies on cybersecurity (Saeed et al. 2023). However, this gap is now being filled by fast-increasing initiatives in developing regions to match capability gaps with actual threats. Thus, increased awareness notwithstanding considerable differentials in cyber maturity between large enterprises and SMEs or high-income vs low-income countries. Cybersecurity is not a technical issue, it is a governance and socio-economic problem that requires action harmonisation among the public and private sectors (Ijeh, 2021). Increasing digitalisation of trade, finance, and government services over time has deepened global narratives about cybersecurity as components of digital trust, economic resilience, and sustainable development. All this calls for an understanding of how cybersecurity governance

has been conceptualised and brought into practice in different contexts, and particularly where resources fall short, as is the case with SMEs.

Understanding Cybersecurity in Small Businesses

The adoption of cybersecurity practices by small and SMEs has been inconsistent and remains at a reactive stage despite increased digital risk exposure (Benjamin et al. 2024). Most SMEs have low financial resources, do not possess IT expertise, and are not aware of cyber threats to them; thus, this accounts for the factors hindering the implementation of proactive security measures (Judijanto et al. 2023). Dahabiyeh (2021) argues that security awareness programs have been identified as critical enablers of adoption by raising the understanding of employees on issues of hygiene elements relating to cyber security and inculcating a culture in behavior disposition towards being security-minded. However, most SMEs do not run organised training programs; therefore, human weaknesses such as inadequate password systems and vulnerabilities to phishing remain highly prevalent (Iqbal & Charles, 2024). Awareness aside, the technical aspects of adopting firewalls, intrusion detection systems, and endpoint security have also been adopted inadequately due to cost impositions, both real and perceived in complexity (Iqbal et al. 2024). Though there has been an emergence of external support mechanisms comprising government grants, vendor solutions, and industry associations to spearhead the adoption drive, much coverage and effectiveness are still wanting (Eggers & Kettl, 2023). This, therefore, leads literature to advocate adaptive, scalable, low-cost cybersecurity models fitting the resource profile of SMEs that can be offered readily. This underscores a pressing need to explore in detail not just what controls are adopted by SMEs but also the governance structures that propel or inhibit such adoption decisions (Seppänen, 2025).

Managing Cybersecurity Risks

According to Mmango and Gundu (2023), cybersecurity risk management consequently forms a pillar of organisational resilience and is most pertinent for SMEs amidst such a dynamic threat environment. Ransomware, business email compromise, and data breaches are the current cyber threats against SMEs that can result in financial loss, reputational harm, or even lead to the closing down of a business (Teymourlouei, 2018). Studies have indicated that most SMEs do not consider the probability or consequences of such threats and hence lag behind in proper planning mechanisms as well as response mechanisms (Marcazzan, Campagnolo & Gianecchini, 2022). Šedukis (2024) posits that effective risk management factors include several critical success factors: top management commitment, organisational awareness, technical competence, continuous monitoring of the cyber environment, etc. However, these factors are largely missing in action within SMEs because of resource and knowledge constraints (Eggunatum & Oboreh, 2022). The assessment process of risks is usually formally or informally identified, evaluated, and prioritised; hence leaving the majority of SMEs in a position where resources cannot be allocated appropriately (Crovini, Santoro & Ossola, 2021). The ISO 31000 and NIST Risk Management Frameworks are very structured but also very complicated, making them less attractive to SMEs (Efe, 2023). This has driven researchers to propose simplified models of risk management that are applicable in context while still maintaining a fair amount of rigor (AL-Dosari et al. 2023). Such approaches would help SMEs move from reactive responses toward proactive risk-based approaches to cybersecurity, ensuring the alignment of security investments with their threat profiles as well as with business priorities (Benjamin et al. 2024).

Understanding Cybersecurity Frameworks

Cybersecurity frameworks define structured approaches towards the design, implementation, and assessment of security practices within organisations. Increasing levels of digital transformation among SMEs require such methodologies (Benjamin et al. 2024). The use of cloud services, e-commerce platforms, and IoT-based operations increases the complexity of the SMEs' digital working environments; therefore, governance and operational controls have to be improved (Chitra, Surianarayanan, Mahamuni, Mohammed, Keno & Boopathi, 2025). Opportunities and risks are thereby fostered by digital transformation since it makes operations more efficient while opening up new threat vectors against SMEs (Straková, Talíř & Váchal, 2022). Efe (2023) posits that such cybersecurity operational frameworks as NIST Cybersecurity Framework and COBIT have been heavily marketed for adoption to corporate organisational process flows as best practices for embedding security into an organisation's workflow. ISO 27001 is among other cybersecurity standards that can be used as international benchmarks for information security management (Eggunatum et al. 2022). Still, its uptake within the SME sector is even lower due to the cost involved in certification activities, coupled with the administrative overhead associated with these activities (Judijanto et al. 2023). This brings to fore an imperative need for an assessment review of how global frameworks are being localised and simplified into the operational realities of SMEs and how governance mechanisms can facilitate their sustained adoption as part of digital transformation strategies (Philbin, Viswanathan & Telukdarie, 2022).

Legal Systems

The second pillar of cybersecurity governance is the legal and regulatory frameworks, which outline standards as well as measures that organisations are obliged to take toward the protection of data and digital assets (Kumar, Bhardwaj & Lather, 2024). Cervi (2022) posits that for many countries across the world, this pillar has been significantly influenced by stringent requirements regarding obligations for data protection and breach notifications akin to those introduced by the General Data Protection Regulation (GDPR) in the European Union member states. In South Africa, this responsibility concerning the processing of information securely falls under POPIA, while cybercrimes are legislated against, including provisions on how to report an incident as well as investigate it, available in a single piece of legislation, the Cybercrimes Act (Watney, 2024). Enforcement regarding accountability improves the facts involved in an incident relating to management of information systems, besides deterring acts related to malicious conduct through cyberspace; nonetheless, practical problems appear when trying to reach compliance due to limited expertise legally and technically present at SME levels (Ezeji, 2024). Non-compliance attracts hefty fines and reputational damage. However, like many other SMEs, compliance is treated as a reactive check-box exercise rather than an integrated part of governance (Ezeji, 2024). Academics advocate that regulatory compliance be institutionalised as part of an organisational culture driven by top management commitment, supported by risk-based policies and continuous employee training. This raises another requirement to investigate more deeply how legal frameworks influence the cybersecurity behaviors of SMEs and what governance models can assist in sustaining compliance (Delso-Vicente, Diaz-Marcos, Aguado-Tevar, & de Blanes-Sebastián, 2025).

3. Methods

This study used the quantitative method. Data was downloaded from the Scopus database. The quantitative approach is defined by Taherdoost (2022) as numerical data collected through observation that describes and interprets the phenomena represented by those observations. As further observed by Pranckutė (2021), since its introduction in 2004, the Scopus database quickly became a strong alternative database and is now considered the largest source for quality peer-reviewed publications. Statistical data were analysed using content analysis, focusing on the years 2015 to 2025, wherein conference papers, journals, articles, and books are included in this data. This selection has been inspired by the characteristics of Volatility, Uncertainty, Complexity, and Ambiguity (VUCA) communities that lead organisations to adopt technology, thereby raising issues on IT Governance and cybersecurity. This method was seen as best for reaching the study goal, which is to map world study trends on IT governance for cybersecurity in SMEs between 2015 and 2025. The aim is to spot the mind setup, theme growth, and new holes in knowing in this field. A cross-sectional approach was used, since the data were collected once off in a single setting.

4. Data Collection

This study drew its data from Scopus and adopted bibliometric analysis.

The bibliometric analysis adopted for this study used data from Scopus database. VOSviewer version 1.6.19 was employed for data analysis. The search strings were "IT governance" AND "cybersecurity". In total, 52 documents found between the periods 2015 to 2025 were retrieved. Regarding analysis, the following was done:

VOSviewer:

- Co-occurrence of All Keywords,
- Counting Method – Full counting
- Minimum occurrences are standard at 5
 - 362 are total keywords, and 13 met the threshold
 - The following was excluded from the 13 selected keywords: Information Technology Governance, which occurred 5 times and has a total link strength of 17. This is because information technology is used interchangeably as IT Governance. This made the total number of keywords go from 13 to 12, which were used in the analysis after removing 1 keyword.

Scopus database analysis:

The 52 documents were used to do the analysis. The following was done:

1. Documents by Country or Territory
2. Documents by Affiliation
3. Documents by subject area

5. Results and Discussion

It has found the place of IT governance as the intellectual core of this research domain, but in practical terms, implementation within SMEs is not adequately developed. Most existing studies are about strategic frameworks and high-level risk governance and do not discuss the operational barriers that SMEs face when entering, such as financial constraints on undertaking measures, technical capacity, and levels of awareness. The rest are also from developed nations like the United States, meaning a global research imbalance, hence huge gaps in insight from developing economies, where SMEs are highly vulnerable. It finds risk management to be the crucial link between governance and security, but lacks simplified models; it remains practically adopted by SMEs. Thematic evolution shows a move to governance-centric approaches. In the absence of integration with cultural, legal, and human dimensions, however, they are rendered nugatory. This calls for multi-dimensional frameworks that should, in any case, amalgamate governance with the contextual realities of SMEs.

5.1 Numerical and Graphical Results

VOSviewer highlighted the three clusters (1 & 2). They are categorised as follows: The one painted red is Cluster 1. Cluster 1 includes the following keywords: Cybersecurity, Cyber Security, IT Governance, Decision-Making, Network security, and Cyber-attacks. Cluster 2 is green and consists of the following keywords: Information use, Information Security, Information Systems, Risk Management, Security Data, and Information Technology.

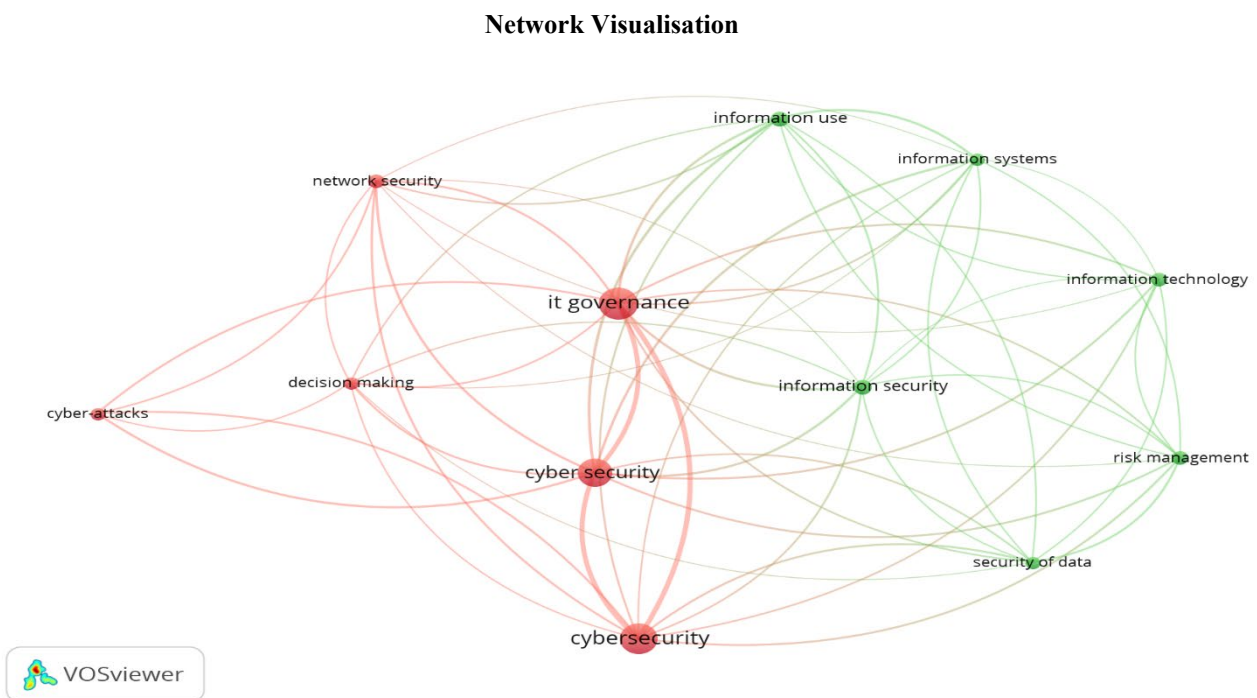


Figure 1. Network Visualisation

Source: Authors' Compilation

Figure 1, above shows the Network Visualisation of all research keywords. This figure shows that IT Governance is a keyword since it is the biggest in network visualisation. IT Governance is in cluster 1, links 11, total link strength 71, and occurrence 31. This is then followed by Cybersecurity, which is in cluster 1, Links 11, total link strength 67, and occurrence 29. Lastly, Cyber Security, which is in cluster 1, links 11, total link strength 76, and occurrence 25. A network places IT Governance at the center of strategy and thereby management as the main theme that could bring unity to the discipline, while placing security and risk, more importantly, as issues for management and strategy rather than just technical issues. IT Governance also makes Cybersecurity the core business since, in experience, this was common; hence, it is highly prioritised as a threat and an area for action. Risk Management has been identified as a path conducting rays from corporate governance to tangible security that will focus on ensuring protection from cyber attacks. The field forms two mutually connected optics: a strategic cluster focusing on governance and security

strategy (Cluster 1) and an applied, institutional cluster focusing on organisational risk implementation (Cluster 2), which are intensely interlinked.

Overlay Visualisation

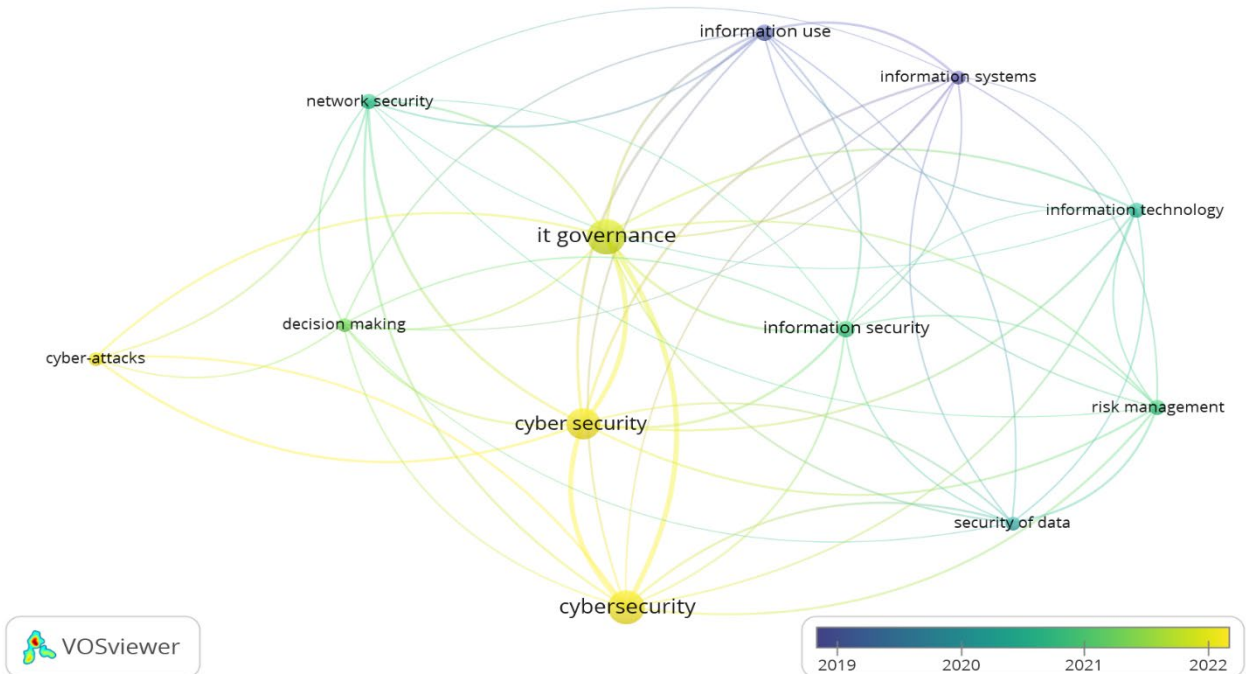


Figure 2. Overlay Visualisation

Source: Authors' Compilation

Figure 2, above illustrates an overlay visualisation of all keywords, highlighting their average publication year and indicating the chronological evolution of Global research trends. IT Governance is in cluster 1, with 11 links, a total link strength of 71, and the highest occurrence at 31, with an average publication year of 2021:77. This suggests that IT Governance remains the core and most established research theme and trend. Then followed by Cybersecurity in cluster 1, with 11 links, a total link strength of 67, and an occurrence of 29, with an average publication year of 2022:41. Lastly, Cyber Security, which is in cluster 1, links 11, total link strength 76, and occurrence 25, with an average publication year of 2022:12. The overlay visualisation shows how research priorities have changed. The field moved from a focus on tech IT systems to work on IT Governance, which forms the strategic paths used in digital risk management around 2021. The newest studies, going into 2022 and later, deal with work inside this setup to face the urgent issue of Cybersecurity. This change shows a field that is actively changing based on threat landscapes by making more complex management-based answers, where governance becomes the steady heart, enabling the best response to new types of cyber threats.

Density Visualisation

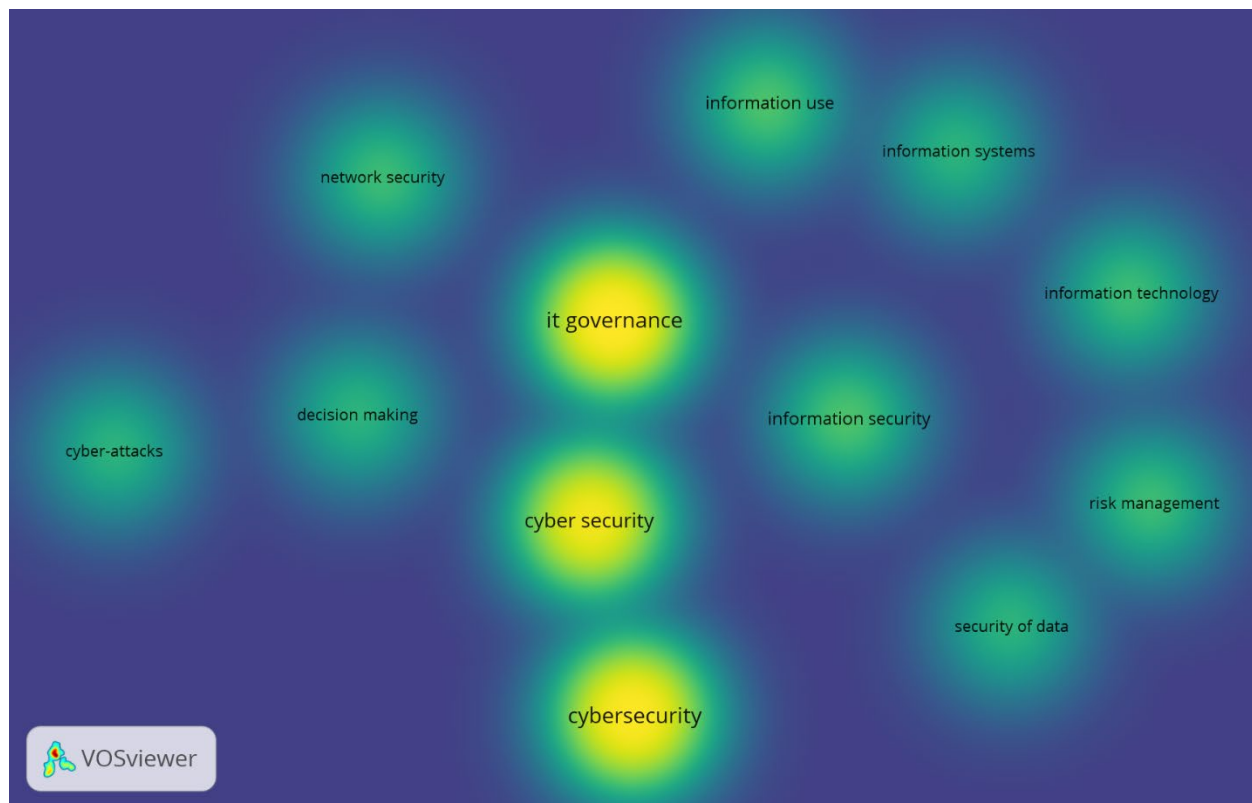
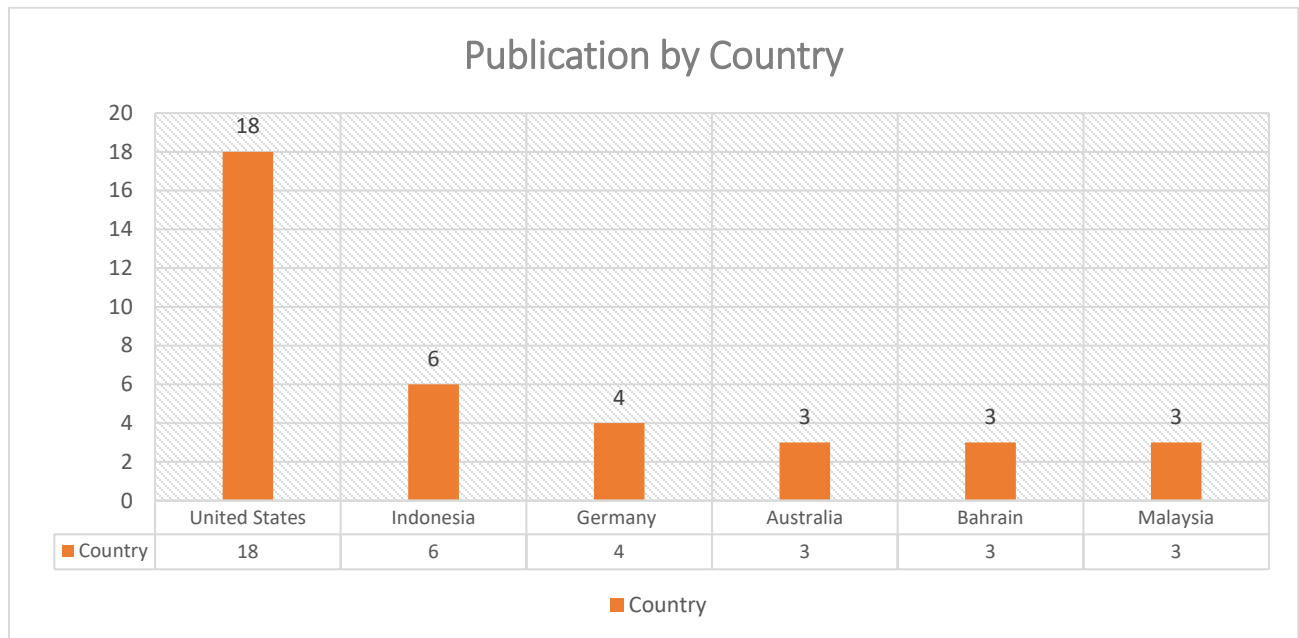


Figure 3. Density Virsualisation

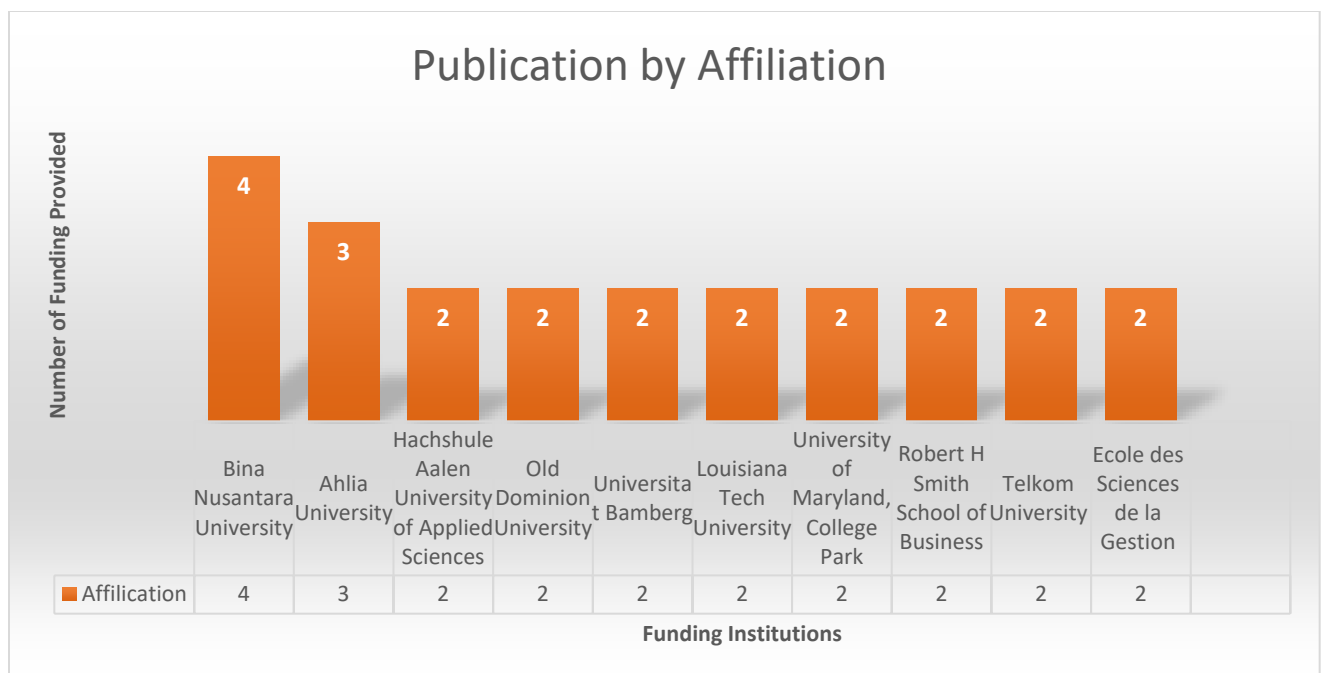
Figure 3, illustrated above, shows that the hotspot regarding the topic under study is IT Governance. It shows that many researchers are writing about it. This is followed by cybersecurity and Cyber security, which are emerging research trends. Decision-making, Security of data, Cyber-attacks, and information systems are under-researched in relation to the topic at hand since they all have an occurrence of 5 each. The density visualisation presents a mature core IT Governance with strong, growing applications with Cybersecurity, but is surrounded by large thematic gaps. This area shows more about big strategies and top results, missing details on the real steps and parts that make that plan work. This viewpoint points out a need for later studies to go further from the main strategy area to look into these less-studied but very important connecting pieces.



Source: Authors' Compilation

Figure 4. Type of publication

The above Figure 4 illustrates the type of publications by Country. The majority of the contributions are from the United States, accounting for 18 publications. This is followed by Indonesia, which has 6 publications. The third largest publication is Germany, accounting for 4 publications. The following countries, Australia, Bahrain, and Malaysia, have 3 publications each.



Source: Authors' Compilation

Figure 5. Funding sponsors

Figure 5 above shows the publications by affiliation Bina Nusantara University is the top-affiliated University with 4 publications. Followed by Ahlia University with 3 publications. Hachshule Aalen University of Applied Sciences, Old Dominion University, Universitat Bamberg, Louisiana Tech University, University of Maryland, College Park, Robert H Smith School of Business, Telkom University, and Ecole des Sciences de la Gestion have 2 publications each.

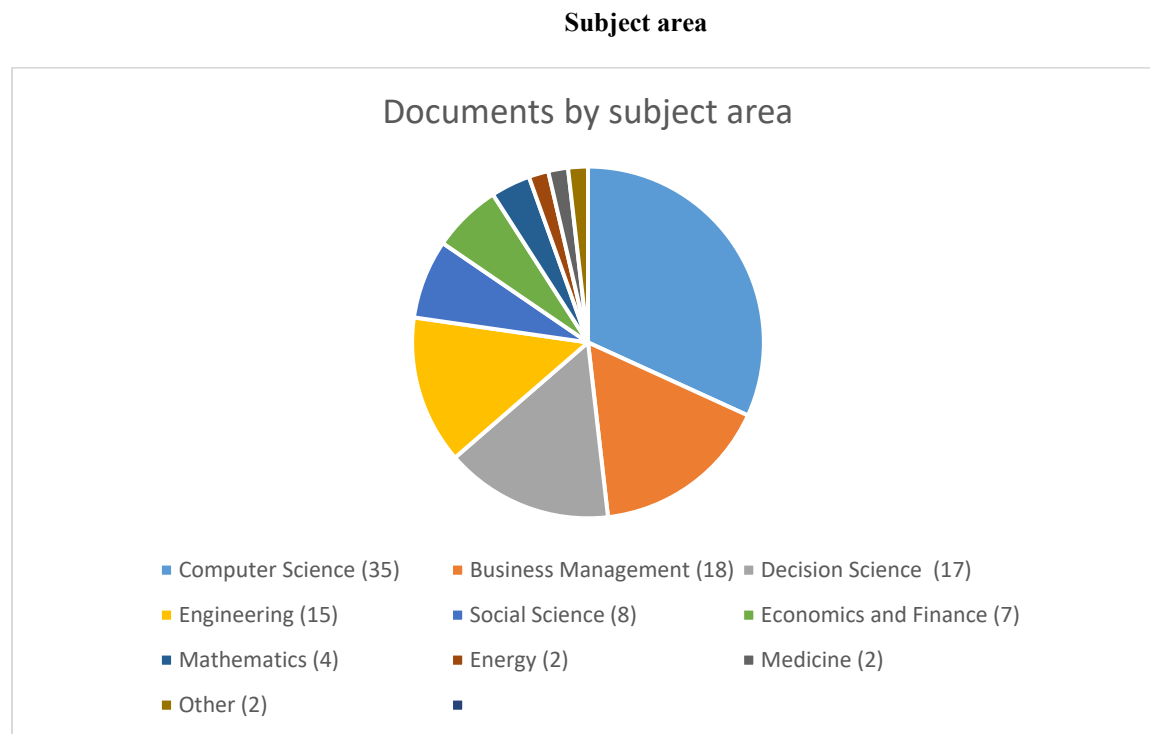


Figure 6. Subject area

Figure 6 above shows publications by subject type. Nine major subjects contribute to the body of knowledge as far as IT Governance and Cybersecurity are concerned globally. Computer Science is the highest contributor with 35 documents. The second highest contributor is Business Management with 18 documents, the third highest contributor is Decision Science with 17 documents, and the fourth highest contributor is Engineering with 15 documents, the fifth highest contributor is Social Science with 8 documents, the sixth highest contributor is Economics and Finance with 7 documents and the eighth highest contributor is Mathematics with 4 documents then followed by Energy and Medicine as the least contributors with 2 documents each.

5.2 Emerging Themes

The main theme is that IT governance should serve as a strategic base for managing cybersecurity, illustrating developing management-based approaches to sustain resilience. Related is growing an interest in risk management that helps connect corporate governance with concrete security outcomes. Other important themes include reframing cybersecurity not just as a technical issue but rather as a governance and socio-economic problem, plus the shift from purely technical security controls to more management-oriented frameworks involving decision-making, organisational strategy, and oversight of risks. The research discovered increasing trends toward legal compliance interest, where acts such as GDPR and POPIA play critical roles in influencing security practices among SMEs. The density visualisation highlights under-researched areas, including decision-making, data security, and response to a cyber-attack. Thus, thematic gaps, when taken together, underline the gradual shift in the field from fragmented technical studies to more comprehensive governance-oriented paradigms.

5.3 Proposed Improvements

Future research should fill the identified thematic gaps. Studies should drill down beyond high-level governance strategies to the operational and behavioral facilitators of cybersecurity in SMEs. In particular, studies should elaborate on how decision-making structures, human factors, and organisational culture constrain or facilitate the adoption and sustainability of security frameworks. A simplified, context-sensitive governance model that reflects their resource limitations is urgently needed in the study, as existing ISO27001 and COBIT frameworks are always too complex or resource-intensive to implement. A cross-country study would provide a comparison of the socio-economic and regulatory environments that influence SME cybersecurity practices in different countries. Bibliometric analysis combined with qualitative research will allow for a much finer understanding of issues, motivations, and risk perceptions on the part of SMEs. Subsequent studies could assess the real-world impact of legislative enactments as a legal impetus on behavioural compliance dispositions of SMEs, particularly POPIA and the Cybercrimes Act in South Africa. This study will go a long way in forming an enhanced, practical, and evidence-based knowledge base toward an SME-focused IT governance framework.

6. Conclusion

This study provides a synthesised worldwide trend of IT governance for SMEs' cybersecurity intellectual structure, thematic evolution, and research gaps between 2015 and 2025. Therefore, it shows that IT governance has become the main theme that would develop into an umbrella concept accommodating cybersecurity strategy, and meanwhile, risk management plus legal compliance are moving on the rise as tracks. The discipline is poorly grounded theoretically, with a focus on strategic talk, insignificant attention paid to practicalities, and geographic disparity in academic contributions. Thus, context-sensitive models integrated from various international standpoints, empirically tested, would set new knowledge frontiers. In turn, such a study will provide baseline content for filling bars to raise SME resilience in highly digitised, unpredictable settings through scholars, policymakers, and practitioners.

References

- AL-Dosari, K. and Fetais, N., Risk-management framework and information-security systems for small and medium enterprises (SMES): A meta-analysis approach. *Electronics*, Vol.12,no.17, pp.3629. 2023. <https://doi.org/10.3390/electronics12173629>
- Almutairi, M. and Sheldon, F.T., IoT–Cloud Integration Security: A Survey of Challenges, Solutions, and Directions. *Electronics*, Vol.14, no. 7, pp.1394. 2025. <https://doi.org/10.3390/electronics14071394>
- Benjamin, L.B., Adegbola, A.E., Amajuoyi, P., Adegbola, M.D. and Adeusi, K.B., Digital transformation in SMEs: Identifying cybersecurity risks and developing effective mitigation strategies. *Global Journal of Engineering and Technology Advances*, Vol.19, no.2, pp.134-153. 2024.DOI: <https://doi.org/10.30574/gjeta.2024.19.2.0084>
- Cervi, G.V., Why and how does the EU rule global digital policy: An empirical analysis of EU regulatory influence in data protection laws. *Digital Society*, Vol.1, no.2, pp.18. 2022.<https://doi.org/10.1007/s44206-022-00005-3>
- Chitra, M., Surianarayanan, R., Mahamuni, V.S., Mohammed, S., Keno, M.T. and Boopathi, S., Study on cloud computing-empowered small and medium enterprises. In *Essential Information Systems Service Management* pp. 189-220. 2025. DOI: 10.4018/979-8-3693-4227-5.ch008
- Crovini, C., Santoro, G. and Ossola, G., Rethinking risk management in entrepreneurial SMEs: towards the integration with the decision-making process. *Management Decision*, Vol.59,no.5, pp.1085-1113. 2021.<https://doi.org/10.1108/MD-10-2019-1402>
- Dahabiyeh, L., Factors affecting organizational adoption and acceptance of computer-based security awareness training tools. *Information & Computer Security*, 29(5), pp.836-849. 2021. <https://doi.org/10.1108/ICS-12-2020-0200>
- Delso-Vicente, A.T., Diaz-Marcos, L., Aguado-Tevar, O. and de Blanes-Sebastián, M.G., Factors influencing employee compliance with information security policies: a systematic literature review of behavioral and technological aspects in cybersecurity. *Future Business Journal*, Vol.11, no.1, p.28. 2025. <https://doi.org/10.1186/s43093-025-00452-7>
- Efe, A., A comparison of key risk management frameworks: COSO-ERM, NIST RMF, ISO 31.000, COBIT. *Denetim ve GÜvence Hizmetleri Dergisi*, Vol.3, no.2, pp.185-205. 2023.
- Eggers, W.D. and Kettl, D.F., *Bridgebuilders: How government can transcend boundaries to solve big problems*. Harvard Business Press. 2023.
- Egwunatum, S.I. and Oboreh, J.C., Factors Limiting Knowledge Management among Construction Small and

- Medium Enterprises. *Journal of Engineering, Project, and Production Management*, Vol.12,no.1, p.25. 2022.DOI 10.32738/JEPPM-2022-0003
- Ezeji, C.L., Cyber policy for monitoring and regulating cyberspace and cyber security measures for combating technologically enhanced crime in South Africa. *International Journal of Business Ecosystem & Strategy* (2687-2293), Vol.6, no.5, pp.96-109. 2024.<https://doi.org/10.36096/ijbes.v6i5.670>
- Ijeh, A.Cis, it a Cyber Security Strategy for Social Development?. In *Crime Science and Digital Forensics*, pp. 202-217. ., 2021.
- Iqbal, J. and Charles, H., Reducing Cybersecurity Risks in SMEs: Custom Training Programs to Combat Human-Error Vulnerabilities. 2024.
- Judijanto, L., Hindarto, D., Wahjono, S.I. and Djunarto, A., Edge of enterprise architecture in addressing cyber security threats and business risks. *International Journal Software Engineering and Computer Science (IJSECS)*, Vol.3,no.3, pp.386-396. 2023. DOI: <https://doi.org/10.35870/ijsecs.v3i3.1816>
- Juneja, A., Goswami, S.S. and Mondal, S., Cyber security and digital economy: opportunities, growth and challenges. *Journal of technology innovations and energy*, 3(2), pp.1-22. 2024. <https://doi.org/10.56556/jtie.v3i2.907>
- Kumar, V.A., Bhardwaj, S. and Lather, M., Cybersecurity and Safeguarding Digital Assets: An Analysis of Regulatory Frameworks, Legal Liability and Enforcement Mechanisms. *Productivity*, Vol.65,no.1, pp.1-10. 2024. DOI:10.32381/PROD.2024.65.01.1
- Manning, L. and Kowalska, A., The threat of ransomware in the food supply chain: a challenge for food defence. *Trends in Organized Crime*, pp.1-29. 2023. <https://doi.org/10.1007/s12117-023-09516-y>
- Marcazzan, E., Campagnolo, D. and Gianecchini, M., 2022. Reaction or anticipation? Resilience in small-and medium-sized enterprises. *Journal of Small Business and Enterprise Development*, Vol.29,no.5, pp.764-788. <https://doi.org/10.1108/JSBED-07-2021-0271>
- Mmango, N. and Gundu, T., November. Cyber resilience in the entrepreneurial environment: a framework for enhancing cybersecurity awareness in SMEs. In *2023 International Conference on Electrical, Computer and Energy Technologies (ICECET)* pp. 1-6. 2023, DOI: 10.1109/ICECET58911.2023.10389226
- Opoku, E., Okafor, M., Williams, M., Aribigbola, A. and Olaleye, A., 2024. Enhancing small and medium-sized businesses through digitalization. *World Journal of Advanced Research and Reviews*, Vol.23,no.2, p.222. 2022, DOI: 10.30574/wjarr.2024.23.2.2313
- Philbin, S., Viswanathan, R. and Telukdarie, A., Understanding how digital transformation can enable SMEs to achieve sustainable development: A systematic literature review. *Small Business International Review*, Vol.6,no.1, pp.473. 2022. <https://doi.org/10.26784/sbir.v6i1.473>
- Pranckutė, R., 2021. Web of Science (WoS) and Scopus: The titans of bibliographic information in today's academic world. *Publications*, Vol.9,no.1, pp.12. <https://doi.org/10.3390/publications9010012>
- Saeed, S., Altamimi, S.A., Alkayyal, N.A., Alshehri, E. and Alabbad, D.A., Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. *Sensors*, Vol.23,no.15, pp.6666. 2023.<https://doi.org/10.3390/s23156666>
- Safitra, M.F., Lubis, M. and Fakhurroja, H., Counterattacking cyber threats: A framework for the future of cybersecurity. *Sustainability*, Vol.15,no.18, pp.13369. 2023. <https://doi.org/10.3390/su151813369>
- Šeduikis, L., 2024. *Factors of successful it project risk management in the organization and their influence on it project success* (Doctoral dissertation), Vilniaus universitetas.
- Seppänen, S., 2025. Digital transformation in SMEs: drivers, challenges, and the impact of emerging technologies on decision-making and management control.
- Straková, J., Talíř, M. and Váchal, J., Opportunities and threats of digital transformation of business models in SMEs. *Economics and Sociology*, Vol.15,no.3, pp.159-171. 2022.doi:10.14254/2071-789X.2022/15-3/9
- Taherdoost, H., What are different research approaches? Comprehensive review of qualitative, quantitative, and mixed method research, their applications, types, and limitations. *Journal of Management Science & Engineering Research*, Vol.5,no.1, pp.53-63. 2022. DOI: <https://doi.org/10.30564/jmser.v5i1.4538>
- Teymourlouei, H., Preventative Measures in Cyber & Ransomware Attacks for Home & Small Businesses' Data. In *Proceedings of the international conference on scientific computing (CSC)*, pp. 87-93. 2018.The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).
- Watney, M., Exploring South Africa's Cybersecurity Legal Framework Regulating Information Confidentiality, Integrity, and Availability. In *International Conference on Cyber Warfare and Security*, pp. 430-438. 2024.

Academic Conferences International Limited.

Biographies

Mpho Mokgathi holds Postgraduate Diplomas in Risk Management and Business Management from Mancosa. He enrolled for an MCom in Computer Auditing at the University of Johannesburg. He has been in the higher education sector for eight years; he started his teaching career at the University of Johannesburg in 2017, where he served as a Cost and Estimating and Marketing Management tutor for several years. Later, he joined Rosebank College as a lecturer and currently works at the Department of Commercial Accounting in the School of Management at the College of Business and Economics, University of Johannesburg as an Assistant Lecturer. Mpho's research areas are IT risk management, the protection of personal data management, cyber security, and computer auditing. He recently published research papers at the international conferences globally, held in Cape Town, South Africa, Bali, Indonesia, and Bangkok, Thailand. He has been actively engaged in community service since he was a student, and as a result, the University recognised his efforts. Mpho served as a project manager at the Enactus office, where he did a lot of work assisting the community, tutoring and training them in entrepreneurship. He taught many SME owners how best to leverage ICT in their businesses. Currently, he is involved in a Day Care project at Soweto. Mpho Mokgathi is a young, promising, and emerging academic who is well-rounded.

Olayinka Erin is an Associate Professor of Accounting at the University of Johannesburg. Prior to this appointment, he served as a Postdoctoral Research Fellow at the University of South Africa, where he became the first postdoctoral fellow in the College of Accounting Sciences to attain the prestigious National Research Foundation (NRF) C-rating as an established researcher. He earned his PhD in Accounting from Covenant University, Nigeria, in 2020 and brings over twenty (20) years of extensive professional and academic experience spanning the financial services sector, multinational organisations, consulting, and higher education. At the University of Johannesburg, he currently teaches Empirical Accounting and IT Risk and Risk Management at the Master's level. Prof. Erin has published extensively in high-impact, ABS/ABDC-ranked journals, including the *International Journal of Disclosure and Governance (IJDG)*, *Journal of Accounting and Organizational Change (JAOC)*, *International Journal of Accounting, Auditing and Performance Evaluation (IJAAPE)*, *International Journal of Business Governance and Ethics (IJBGE)*, *Public Organization Review (POR)*, *Journal of Public Affairs (JPA)*, *Sustainability Accounting, Management and Policy Journal (SAMPJ)*, *Journal of Financial Reporting and Accounting (JFRA)*, *Journal of Accounting in Emerging Economies (JAE)*, *Measuring Business Excellence (MBE)*, *Meditari Accounting Research (MEDITARI)*, and the *Journal of Cleaner Production (JCLP)*. His research focuses on risk governance, corporate governance, and non-financial reporting, with particular emphasis on integrated reporting, biodiversity reporting, sustainability reporting, and the Sustainable Development Goals (SDGs).