Information Technology Governance in Local Government: Audit Committee Responsibilities

Thapelo Lebese, Kgobalale N. Motubatse, and Audrey Legodi

Abstract The study aims to assess the effectiveness of information technology (IT) governance in local government by examining the audit committee's role and capabilities relating to IT governance. This study is prompted by a local government IT infrastructure failing to adequately support service delivery to communities due to poor governance skills and knowledge of audit committees. The risk of mismanagement of resources is therefore increased. The study employs a quantitative research approach and a descriptive research design. A questionnaire survey was used to collect data from the audit committee members, internal auditors, managers and Chief Audit Executives and Council and municipal management. The researcher used descriptive and inferential statistics, Stata/SE version 16 software, descriptive analysis, chi-square test, effect factor analysis and exploratory factor analysis to measure the relationship between two-factor variables. Kaizer criterion was accepted as the extraction method, while the Cronbach alpha coefficient was used to determine the internal consistency of the identified factors. The study reveals that audit committees are ineffective in executing their IT governance activities. Furthermore, there are areas of concern in IT assurance audits. The internal audit function lacks the skills and technical capacity to provide IT assurance services and therefore not add sufficient value to the municipality. The study concludes that there is a significant statistical correlation ($P < 0.001$) between poor IT governance and audit committee skills and expertise. The study recommends that the recruitment of audit committee members should consider their experience in IT governance to ensure that auditors are well-equipped to review IT governance assurance effectively. Also, the importance of IT assurance services by competent, skilled internal auditors was expressed. The study contributes to governance literature by providing empirical evidence on audit committees' IT governance and oversight effectiveness, and also emphasises the need to assess IT engagements by internal auditors. Academic researchers and the National School of Government can use the findings of the study as justification for on minimum required skills and capacity building for audit committee members.

T. Lebese (✉) · K. N. Motubatse · A. Legodi
Tshwane University of Technology, Ga-Rankuwa, South Africa
e-mail: Motubatsekn@tut.ac.za; legodiha@tut.ac.za

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2024

T. Moloi, B. George (eds.), *Towards Digitally Transforming Accounting and Business Processes*, Springer Proceedings in Business and Economics,
https://doi.org/10.1007/978-3-031-46177-4_14

Keywords Audit committee · Governance · Information technology · Municipalities · Internal audit

1 Introduction

Over the years IT has globally influenced how organisations conduct their businesses and municipalities are not exempted from such impacts (Christiansen, 2013). As a result of the fundamental challenges that the world faces, all aspects of modern life are influenced by IT in one way or another (Lloyd, 2004). The development and evolution of IT has influenced how data and information are processed, which then impacts the decision-making processes within corporate spaces (Khemakhem & Fontaine, 2019).

The advent of IT has come with various advantages and disadvantages (Joseph, 2015), which the South African government has also been subjected to. Such advantages include improved productivity, decreased expenses (Grant & Chau, 2005; Mostert & Mutula, 2010) accelerating revenue flows (Tarek et al., 2017) improved information quality (Barnes & Vidgen, 2006) improved promotion of good governance (Bertot et al., 2010) ability to stamp out corrupt and fraudulent activities within organisations (Bertot et al., 2010; Sabani et al., 2019) and enabling innovation (Ravichandran et al., 2017). Kim et al. (2017) and Al-Salmi and Hasnan (2015) believe that the adoption of IT embedded with such advantages will significantly enhance the operational capacity of an organisation.

However, the lack or non-adoption of governance principles might contribute to the perception that IT is adding little or no organisational value despite substantial investments being made (Marnewick & Labuschagne, 2011). Riggins and Wamba (2015); Ndou (2004) highlights that there are significant challenges concerning the adoption and implementation of IT in government, accentuating the lack of skills in the public sector as a significant obstacle. Bakunzibake et al. (2019) emphasise change management as a key challenge to the successful implementation of IT. This constantly changing environment calls for effective governance, risk management and controls, such as cyber security management. Inuwa et al. (2019) believe that ungoverned IT can provide opportunities for corrupt bureaucrats to misuse it for personal gains. Effective governance not only relates to policies but also includes the culture and tone at the top of the governing body and the effectiveness of governance structures (such as internal auditing) in assisting with the assessment of IT related processes. However, with the increased adoption of IT in municipalities, there is limited research on the effectiveness of audit committee in IT governance. Through the lenses of agency theory, the study provides empirical evidence on the effectiveness of audit committees in IT governance and highlights the importance of building the minimum required skills and capacity for audit committee members in IT governance.

The paper begins by outlining the literature review and theory for the study, discussing IT as a concept, IT governance and the impact of effective IT governance. The study then discusses IT risk management and value delivery. Next, the theory on

audit committee is discussed. Followed by examining the effectiveness of the audit committee pertaining to IT. The paper then describes the research design and approach, after which the research findings are presented. Finally, the paper provides concluding remarks and identifies areas for future research.

2 Literature Review and Agency Theory

As a result of the competitive advantage derived from the use of technologies, organisations have since adopted IT as key function of the business. Organisational reliance on IT resulted in challenges, to an extent that corporate governance cannot be addressed without IT governance being considered (Van Grembergen & De Haes, 2007). IT governance is cited as a strategic issue that requires commitment at a strategic level (Mohamed, 2012). Mikalef et al. (2018) support this, arguing that IT governance has been elevated to a primary concern for senior IT officials and business management. It is for these reasons that IT governance is high on the agenda of many organisations (Ali & Green, 2012) and it has similarly received much attention in academic spaces. This is evident in the variety of scholarly definitions of IT governance that exists in the literature the lack of consensus is apparent (Lee & Lee, 2009).

A variety of scholarly definitions of IT governance available, however according to Webb et al. (2006) that the various definitions do not all reflect crucial elements of the IT governance framework, possibly indicating that authors develop definitions that support their focus at the time of their research. Carr and Hayes (2015) and Alves et al. (2013) say although there is no commonly accepted definition of IT governance, commonly agreed upon definition of IT governance would be very useful and serve to develop and refine IT governance frameworks. These frameworks, as depicted in Fig. 1, would outline the processes and structures that have been put in place that enable IT and business to meet their objectives in terms of risk, resources and performance management while aligning with the business' strategic objectives to enable the business to derive value from its IT investments. The effective functioning of the IT governance framework is reliant on the IT governance structures in place, as depicted in the Fig. 1 below. Audit committee is one of the key pillars of governance in any organisation.

2.1 Governance and Audit Committees

Governance structures and processes are crucial for fostering transparency, accountability, and effective decision-making within organizations (Ananny & Crawford, 2018). Within governance framework, the audit committee holds a key role as part of governance, overseeing and providing guidance on various aspects of organizational operations, including IT governance. IT governance encompasses the framework

Fig. 1 IT Governance Framework and Model. Source: IT Governance Framework and Model, 2020

and processes through which an organization manages and controls its IT systems and operations (Weill & Ross, 2004). The audit committee's responsibility lies in ensuring the presence of appropriate controls and processes that align IT strategically with business needs and objectives, deliver value through IT investments, identify, and manage IT risks effectively, and promote efficient resource and performance management (Iliescu, 2010).

To effectively fulfil their responsibilities, the audit committee must possess the necessary qualifications and skills in IT governance, as emphasized by Chen et al. (2022a, 2022b). This expertise enables audit committee members to comprehend and evaluate IT-related risks and controls, as highlighted by Lankton et al. (2021). The existing literature mainly discuss the importance of expertise and skills in audit committees, but there is limited studies which address IT governance skills. Several studies, including those by Ojeka et al. (2021) and Hadden and Hermanson (2003), emphasize the importance of including IT risk and control discussions in the audit committee agendas. Omer et al. (2020) further assert that the audit committee must have a solid understanding of IT risk management and controls. Additionally, Brand (2016) emphasizes the significance of conducting independent IT audits at regular intervals, separate from financial audits. This separation allows the internal audit function to provide objective and independent evaluations of IT controls and processes, serving as a source of assurance for the audit committee. The capacity and effectiveness of the internal audit function are crucial considerations for the audit committee in fulfilling its responsibilities.

The audit committee plays an advisory role in evaluating the adequacy of disaster recovery and continuity plans, ensuring the organization has robust measures in place to mitigate IT-related disruptions and protect critical systems and data (Contessotto & Moroney, 2014). Additionally, the audit committee actively supports management in addressing IT risks by regularly testing and evaluating cyber security

threats, recovery plans, systems, and processes through the internal audit function (Zanzig & Francia III, 2022). However, while having a well-resourced internal audit function is important, it may not be sufficient for providing valuable if the audit plans are not reviewed and approved by the audit committee. (Herdan, 2008). To address this, the audit committee should review the internal audit function's plans to ensure adequate coverage of IT governance, risks, and controls, as highlighted by Abbott et al. (2010). This assessment helps identify any gaps or areas that require additional attention in the governance of IT within the organization. However, there is a gap in the literature regarding how effective the audit committee is in executing their IT governance role, especially in the South African local municipality context.

2.2 Agency Theory & the Role of Audit Committee in Enhancing IT Governance

The audit committee is a board subcommittee responsible for matters relating to financial reporting and audits (Oji & Ofoegbu, 2017; Spira, 2003). Agency theory, which postulates that conflicts of interest between management and shareholders can arise due to divergent objectives and information asymmetry (McColgan, 2001), can be a useful lens to study IT governance and the role of audit committees in organisations. The literature review in this study highlights the importance of IT governance in maximising the value of IT investments, managing IT risks, and ensuring the overall effectiveness of an organisation's IT systems. In the context of agency theory, these issues can be viewed as potential conflicts between managers, who may seek to maximise their own utility and shareholders, who desire maximum value from their investments.

The role of the audit committee in IT governance can be understood through the lens of agency theory as a mechanism to align the interests of management and shareholders by providing oversight and guidance on IT risk management, internal controls, and IT investment decisions (DeZoort et al., 2002; Moloi, 2014; Oji & Ofoegbu, 2017). The audit committee's expertise in IT and cybersecurity (Ashraf et al., 2020; Legodi, 2021) helps to mitigate the information asymmetry that can exist between management and shareholders with respect to IT-related decisions, thereby reducing the potential for conflicts of interest.

The literature review also highlights the need for a more integrated approach to IT governance, risk management and control, in which the audit committee plays a central role. This aligns with the agency theory perspective that calls for monitoring mechanisms to mitigate conflicts of interest and ensure that management actions are consistent with shareholder interests (Jensen & Meckling, 1976; Fama & Jensen, 1983; McColgan, 2001). By overseeing IT risks and controls, as well as promoting good IT governance practices, the audit committee can help to ensure that management's actions align with the strategic objectives of the organisation, which ultimately benefits shareholders.

Furthermore, the literature review emphasises the importance of IT audit specialists and the use of computer-assisted audit techniques (CAATs) in enhancing the effectiveness of internal audit processes (Janvrin et al., 2008; Asniarti & Muda, 2019). In the context of agency theory, these tools and specialists can be seen as additional mechanisms to reduce information asymmetry and provide greater assurance to shareholders that management is effectively managing IT risks and controls.

The agency theory provides a useful framework for understanding the role of the audit committee in IT governance and the mechanisms through which it can help to align management and shareholder interests. By providing oversight, guidance and expertise in IT-related matters, the audit committee serves as a crucial monitoring mechanism to mitigate potential conflicts of interest and ensure the effective management of IT resources and risks within the organisation.

An effective audit committee needs competent and qualified members with the authority and resources to protect stakeholder interests by ensuring reliable financial reporting, internal controls and risk management through its diligent oversight efforts (Moloi, 2014; DeZoort et al., 2002). According to Roussy and Rodrigue (2018) and Moorthy et al. (2011), the audit committee is ultimately responsible for implementing governance structures to evaluate the effectiveness of an organisation's internal control systems, identify errors and inefficiencies and design system controls that prevent defects. However, the role of the audit committee has evolved over the years since the emergence of IT. As a result, IT expertise has become an integral component of the audit committee's skill set that is essential to its effective advisory and oversight role.

Ashraf et al. (2020) examined whether IT expertise of audit committees impact the reliability and timeliness of financial reporting through the difference-in-differences analysis. The study found that audit committee IT expertise resulted in a reduction in the likelihood of material restatement and a reduction in the likelihood of IT-related material weaknesses. The findings supported their assertion that the quality of financial reporting is significantly improved by the presence of an IT expert in the audit committee.

Additionally, audit committees IT skills must include cyber security insight (Legodi, 2021). Ojeka et al. (2017) shared similar sentiments rising from their study that assessed whether a relationship exists between cyber security and audit committee effectiveness using audit committee independence, technological expertise, and financial expertise characteristics as independent variables. The variable used to measure the dependent variable is cyber security compliance. 13 banks listed on the Nigerian stock exchange were selected. The empirical analysis was carried out using product moment correlation and ordinary least square regression analysis methods. The results showed that audit committee characteristics measured by independence, financial expertise and technological expertise all have a nonsignificant negative relationship to cyber security in the Nigerian banking sector. The study recommended that the composition of the audit committee in Nigeria be worked on to deliberately incorporate needed technological and financial experts who can ask probing questions and offer their wealth of experience in safeguarding the shareholder's interest. The severe impacts of cybercrime and the growth of cyber

threats have resulted in a need for organisations' boards of directors to be involved in IT governance (Corradini, 2020); such involvement by the board may better equip the organisation to deal effectively with the challenges that come with IT. However, little is known about the audit committee's role in IT governance (Lankton et al., 2021).

In organisations, a documented audit committee charter defines the purpose, structure, internal controls and roles and responsibilities of audit committee members (Deloitte, 2017). Lankton et al. (2021) investigated the influence of security breaches and board-level technology committees on disclosing IT general controls roles in the audit committee charter using efficiency and institutional theories using a sample of 189 firms. The finding pointed out that those organisations with an IT committee that experienced a data breach are more likely to disclose IT governance roles in the audit committee charter. The findings suggest that firms experiencing a data breach realise their vulnerability and because they already have oversight at the board level, it is more natural for them to increase oversight by assigning IT governance roles to the audit committee.

The audit committee should scrutinise IT-related risks (Ashraf et al., 2020). Turel et al. (2017); Ramamoorti and Weidenmier (2004) point out that the role of the audit committee and internal auditors nowadays lies in scrutinising IT solutions brought into the business environment (Abu-Musa, 2008). An audit committee should be a team of experts with sufficient skills, abilities and knowledge to recommend the most effective systems (Chen & Komal, 2018; Bierstaker et al., 2001). In other words, most authors suggest that the audit committee should now move from the traditional role of only overseeing accounting reports and principles to include overseeing the IT solutions of an organisation (CFA Institute, 2021; Moorthy et al., 2011; Jackson, 2004).

According to Moorthy et al. (2011), the change of role for the audit committee has been a challenge. Huff et al. (2006) conducted a study to determine if the audit committee gives attention to their new roles related to IT governance. Their study interviewed board chairs and members of 17 medium-to-large corporations, most with global operations. The findings suggested that the audit committee is not allocating adequate attention to its role in IT governance. The study further suggests ways in which the audit committee can adopt and adapt to the newly transferred oversight role in IT governance, one of them being to include IT controls and risk as agenda items for discussion in board meetings. Legodi (2021) concurs to the recommendation, stating that IT should be a standing agenda item in the audit committee meetings (Legodi, 2021). This recommendation is in line with the guidelines of King IV, that the audit committee should discuss the IT related risks and controls (IoD, 2010).

According to Moorthy et al. (2011), the audit committee is ultimately responsible for implementing governance structures to evaluate the effectiveness of an organisation's internal control systems, identify errors and inefficiencies and design system controls that prevent defects. This applies even with regard to IT control environments. With the increasing adoption of information systems and technology, independent IT audits should be carried out at regular intervals and given special

attention (Byrnes et al., 2018). Internal audit reviews are regarded as audit committee comfort providers (Susanto, 2020). IT audits are regarded as an integral part of internal audits. Thus, the audit committee should discuss these in their meetings and be in a position to support the audit department in being able to conduct the internal audit reviews relating to the IT environment of the municipality. This can be achieved by ensuring that the internal audit department of the municipality has and uses efficient IT audit resources to enable them to review the municipality's IT related controls effectively and efficiently (Weidenmier & Ramamoorti, 2006). Resources include the use of IT audit specialists where necessary. Janvrin et al. (2008) found that the use of IT specialists is common, even among auditors who are assigned to examine complex IT systems. According to Asniarti and Muda (2019), operational internal audit reviews of IT are improving due to better CAAT use. This may be the root cause of why studies have found that the IT audit may not be conducted to the required level and depth (Hadden et al., 2003).

Muchenje (2013) says that there are advantages to using IT; however, there are inherent business risks that must be managed effectively. According to Tarek et al. (2017), ensuring that the right people oversee IT risks at an organisation is essential and the audit committee is rightfully charged with this oversight role by the charter. The audit committee is responsible for setting the tone for the risk culture in the organisation (Cassidy et al., 2001). Seale (2017) studied factors influencing the decision to adopt an IT risk management framework at universities in South Africa. The study used a deductive approach and found that the key staff members responsible for ratifying the adopted enterprise risk management framework were audit committees, risk committees and senior IT management committees, amongst others.

Furthermore, audit committees should oversee and advise on hardware and software security. Software security should be prioritised in an organisation (Reeder et al., 2017; Mead et al., 2008). Software security measures such as encryption can be used to control access to files, as can firewalls that help give access only to authorised users. Physical security should also be improved, such as by locking doors and restricting computer room access (Alqatamin, 2018). Such physical and software risks and controls, therefore, need to be addressed by the audit committee in fulfilling its fiduciary role (Cohen et al., 2017; Hadden, 2002). The other responsibility of the audit committee is to provide confidence to customers involved in e-commerce transactions with the organisation. Moreover, it is an internal control measure to provide reliable financial statements (Bananuka et al., 2019). In addition, there is enterprise risk management, which the audit committee must deal with in real-time (Ojeka et al., 2017). According to Tarek et al. (2017), ensuring that the right people oversee IT risks at an organisation is always essential.

Therefore, based on the literature review, it is critical that the audit committee has IT knowledge and can provide adequate oversight. Limited studies have been conducted on the effectiveness of audit committee in providing IT governance oversight, especially in the South African local municipality context. Based on the above discussion, the study aims to provide empirical evidence.

on the effectiveness of audit committees in IT governance and highlights the importance of building the minimum required skills and capacity for audit committee members in IT governance.

3 Research Methodology

The data of the audit committee activities in enhancing IT governance were collected by means of a Likert scale survey questionnaire at the Sekhukhune District municipality in the Limpopo province of South Africa. The municipality consists of four local municipalities, namely Fetakgomo/Tubatse, Ephraim Mogale, Elias Motsoaledi and Makhuduthamaga. The questionnaires were distributed to all local municipalities and primarily completed by the audit committee members, internal audit staff, municipal management officials and the operation staff members who are exposed to the work of the audit committees. The largest group of respondents (74.4%) had more than 5 years of working experience in the similar position while 17% consisted of those with at least 3 years' experience. This indicates that the responses come from knowledgeable and experienced individuals, making them reliable. Furthermore, 44.7% of the respondents have undergraduate qualifications (up to NQF level 7), while 34% possess postgraduate qualifications at NQF level 8 and 21.3% of the respondents hold master's degrees. Effectively, most respondents have at least the minimum required qualifications for their respective positions. This ensured that the data obtained were reliable to address the research problem and to achieve the research objectives. The target population of the study is displayed in Table 1 below.

The researcher is knowledgeable about the audit committee activities and their working relationships with other stakeholders; hence, the purposive sampling of stakeholders was used. Participants were drawn from all the municipalities and consisted of the members of the audit committees, the Chief Financial Officers, Accounting Officers, Chief Audit Executives, internal auditors, and the Heads of Departments/divisions.

The study applied positivist paradigm and quantitative methodology. Quantitative research is predicated on the assumption that there is an objective to study, a research problem to examine and an obligation to manage and measure the data collected (Babbie, 2020). Data were analysed through descriptive and inferential

Table 1 Target population and sample size in selected municipalities

	Municipality					
Participant Groupings	A	B	C	D	E	Total
Audit committee	5	5	5	5	5	25
Internal auditors/managers	2	2	2	2	2	10
Municipal council & management	17	18	8	17	4	64
Total						99

statistics employed by the researcher. Stata/SE version 16 software was used to analyse the statistical data obtained through the survey questionnaires.

Descriptive analysis was produced using frequency tables. The chi-square test was used for inferential statistics to measure the significant relationship between two factor variables. The effect factor analysis and correlations were measured to understand how the different underlying factors influence the variance amongst the variables. Exploratory factor analysis was used as the extraction method with varimax rotation conducted to determine the dimensionality of each of the sub-sections; factors with Eigen values above 1 (Kaizer criterion) were accepted. The Cronbach alpha coefficient was used to determine the internal consistency (reliability) of each of the identified factors using the agreed thresholds stated in the literature as 0.5 (acceptable); 0.6 (satisfactory for exploratory research) and 0.7 (most used instrument) (George & Mallery, 2003).

4 Findings

The literature section of this study outlined the existing literature regarding the role of the audit committee in IT governance. The literature was used to inform the development of the questionnaire used to collect the data on the audit committee activities in enhancing IT governance. The results of the response analysis are presented in Fig. 2 and further discussed in this section.

Figure 2 illustrates that a significant majority of respondents (65.9%) agreed or strongly agreed that at least one member of the audit committee must have appropriate qualifications and skills in IT and governance, A larger majority (83.3%) agreed that audit committee meeting agendas include the IT risk and controls as discussion points, 20.4% were neutral, 64.6% agreed that independent IT audits are carried out at regular intervals, 71.5% agreed with the municipality on the appropriateness of its disaster recovery and continuity plans, 51% disagreed with the security audit committee's substantive reports on the organisation's top cyber-threat risk management priorities and 38.8% argued that internal audit uses efficient IT audit tools to enable them to effectively review the municipality's IT related controls. A solid majority of the respondents (68.7%) agreed either way.

The main findings form the results illustrate that participants are concerned about the audit committee's effectiveness in enhancing IT governance where it concerns cyber security and in ensuring that the internal audit function is adequately resourced and skilled to assist in proving assurance regarding the IT risks and control environment of the municipalities. As outlined in the literature review, Brand (2016) and Abbott et al. (2010), it is important for audit committees to ensure that the internal audit function is adequately resourced to address IT governance issues.

EFA was used to summarise the variables included on the questionnaire and develop factors and make meaningful factors for further analysis. Table 2 presents the factor loadings, and the discussion then follows:

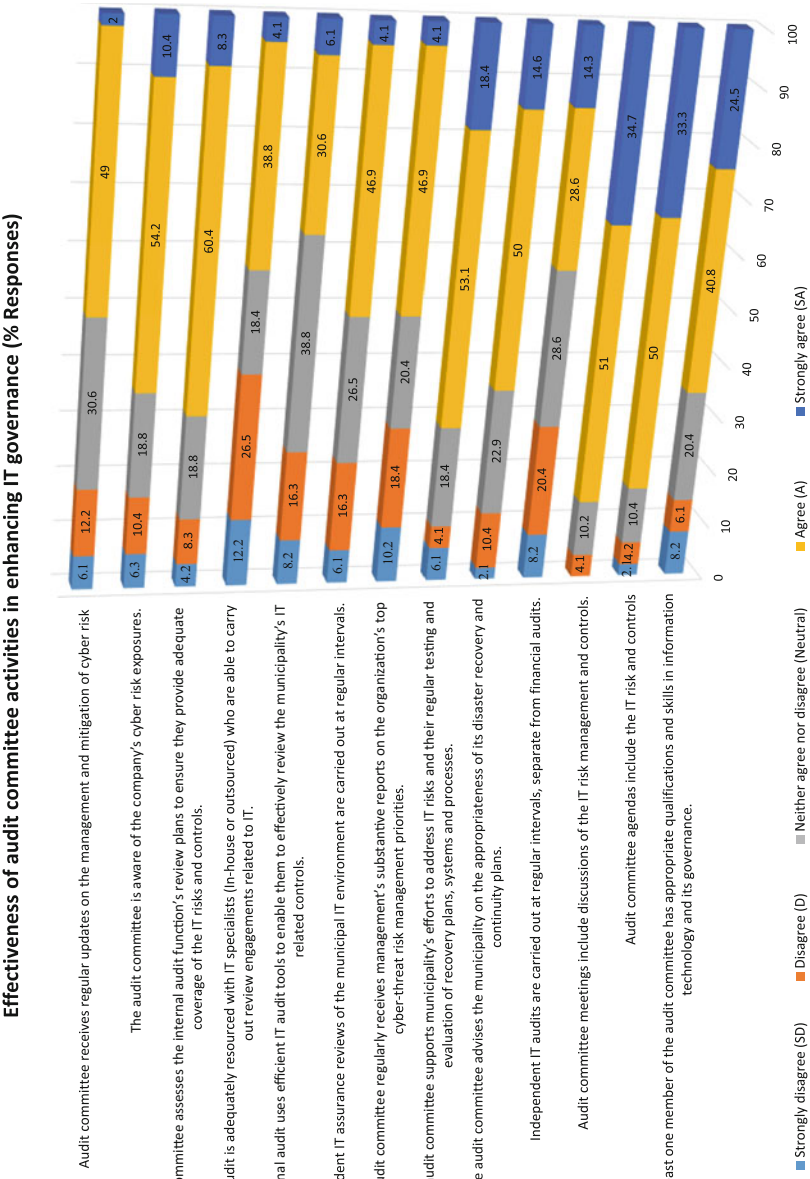

Fig. 2 Descriptive statistical presentation of the responses. Source: Researcher's own illustration

Table 2 Exploratory factor analysis for IT and audit committee

Factor	KMO & Bartlett's test (sig. value)	% Variance explained	Factor loadings		Cronbach's alpha
IT and Audit Committee	0.858 $P < 0.001$	77.8%	Factor 1	Factor 2	0.9291
At least one member of the audit committee has appropriate qualifications and skills in IT and its governance.				0.7572	
Audit committee agendas include the IT risk and controls				0.7784	
Audit committee meetings include discussions of the IT risk management and controls.				0.8014	
Independent IT audits are carried out at regular intervals, separate from financial audits.			0.4782		
The audit committee advises the municipality on the appropriateness of its disaster recovery and continuity plans.				0.7219	
The audit committee supports municipality's efforts to address IT risks and their regular testing and evaluation of recovery plans, systems, and processes.				0.7014	
The audit committee regularly receives management's substantive reports on the organisation's top cyber-threat risk management priorities.			0.6391		
Independent IT assurance reviews of the municipal IT environment are carried out at regular intervals.			0.6701		
Internal audit uses efficient IT audit tools to enable them to effectively review the municipality's IT related controls.			0.6785		
Internal audit is adequately resourced with IT specialists (In-house or outsourced) who are able to carry out review engagements related to IT.			0.6080		
Audit committee assesses the internal audit function's review plans to ensure they provide adequate coverage of the IT risks and controls.			0.7135		
The audit committee is aware of the company's cyber risk exposures.			0.6080		
Audit committee receives regular updates on the management and mitigation of cyber risk			0.8521		

Source: Researcher's own illustration

Table 2 shows that the audit committee's influence on the original variables for IT and audit committee is shown to be significant, with two factors accounting for 77.8% of the variance. The first factor is the direct correlation between independent IT audits, management's top cyber-threat risk management priorities, internal audit tools and internal audit resourced with IT specialists. The second factor is a positive correlation between variables, with at least one member of the audit committee having appropriate qualifications and skills in IT and its governance, activities including IT risk and controls, meetings, discussions, disaster recovery and continuity plans and supports municipality's efforts to address IT risks. This factor represents the audit committee's IT governance skills, experience, and expertise.

Table 3 Descriptive statistics for factor variables

Factors	Minimum	Maximum	Mean	Std. Deviation	Skewness	Kurtosis
Audit committee IT Governance oversight responsibility	1.00	4.63	3.2500	0.80309	−1.094	1.345
Audit committee IT Governance skills, experience and expertise.	1.60	5.00	3.8936	0.78779	−1.015	1.233

Source: Researcher's own tabulation

Table 4 The relationship between factor variables correlations

Factor	Audit committee IT governance oversight responsibility.	Audit committee IT governance skills, experience, and expertise
Audit committee IT governance oversight responsibility.	1	
Audit committee IT governance skills, experience, and expertise	0.685**	1

Correlation is significant at the 0.01 level (2-tailed). **
Source: Researcher's own tabulation

Table 3 shows that each factor variable had instances where either all the respondents or none of the respondents agreed with the individual variables that were encompassed by the questionnaire's statements. Instances where not a single participant agreed with the statement should raise red flags because this may be an indication of ineffective performance on the part of the audit committee. The relationship between factor variables was determined using a Pearson correlation coefficient, which indicates the direction and strength of the relationships between the factors (Table 4).

The table reveals a strong positive relationship between audit committee IT governance skills, experience and expertise and oversight responsibility. This suggests that more audit committees are more likely to effectively execute their roles and activities in a way that enhances IT governance in the municipalities. These findings are consistent with literature as outlined by Chen et al. (2022a, 2022b) in saying that IT expertise enhances the audit committee's monitoring ability and oversight of cybersecurity risks.

5 Conclusion and Recommendations

The study found that the audit committee is effectiveness is limited as a result of inadequate IT audits and assurance reviews, under-resourced IT audit department and inadequate auditing tools. Furthermore, statistical analysis revealed a

relationship between audit skills and expertise, audit committee interpersonal skills and how the audit committee execute their oversight role in IT governance. These results are consistent with the findings of Ashraf et al. (2020) and Chen et al. (2022a, 2022b), who found that financial and risk monitoring responsibilities are enhanced by the presence of IT governance skills, experience, and expertise. The findings validate the Agency theory to some extent. They suggest that deficiencies in IT audits, under-resourced IT audit departments, inadequate auditing tools, and the importance of audit skills and expertise all influence the effectiveness of audit committees in IT governance. These findings highlight the significance of appropriate monitoring and control mechanisms in mitigating agency problems and aligning the interests of principals and agents within organizations.

In order for audit committees to effectively fulfil their role and responsibilities in IT governance, it is crucial for them to continuously enhance their skills and knowledge in IT risks, particularly cyber threats. Additionally, it is essential for these committees to ensure the efficient functioning of the internal audit function by providing adequate resources, both in terms of technology and human capital, to conduct IT assurance reviews. By doing so, audit committees can effectively contribute to the overall IT governance organizations.

6 Recommendations for Future Research

Audit committee roles could be studied further in South Africa to expand their role beyond traditional internal control, financial reporting, and IT areas. Qualitative research could be used to gain an in-depth understanding of the impact of audit committee activities on local government governance. This could help to identify the strengths and weaknesses of audit committees, as well as improve audit outcomes despite the introduction of Operation Clean Audit Outcomes in 2014. Based on the findings of the study, a study can be conducted to assess the effectiveness of internal audit functions in conduct IT audit assurance, with specific focus in local government.

References

Abbott, L. J., Parker, S., & Peters, G. F. (2010). Serving two masters: The association between audit committee internal audit oversight and internal audit activities. *Accounting Horizons, 24*(1), 1–24.

Abu-Musa, A. A. (2008). IT and its implications for internal auditing. *Managerial Auditing Journal, 23*(5), 438–466. https://doi.org/10.1108/02686900810875280

Ali, S., & Green, P. (2012). Effective IT(IT) governance mechanisms: An IT outsourcing perspective. *Information Systems Frontiers, 14*(2), 179–193.

Alqatamin, R. M. (2018). Audit committee effectiveness and company performance: evidence from Jordan. *Accounting and Finance Research, 7*(2), 48–60.

Al-Salmi, A., & Hasnan, A. P. D. N. B. (2015). E-Government contributions and advantages: A review of sultanate of Oman. *International Journal of Scientific and Research Publications, 5*(12), 214–219.

Alves, C. R., Riekstin, A. C., Carvalho, T. C. & Vidal, A. G. (2013). IT governance frameworks: A literature review of Brazilian publications. *CONF-IRM 2013 Proceedings*. 34. https://aisel.aisnet.org/confirm2013/34

Ananny, M., & Crawford, K. (2018). Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability. *New Media & Society, 20*(3), 973–989.

Ashraf, M., Michas, P. N., & Russomanno, D. (2020). The impact of audit committee IT expertise on the reliability and timeliness of financial reporting. *The Accounting Review, 95*(5), 23–56.

Asniarti, A., & Muda, I. (2019, May). The effect of computer assisted audit tools on operational review of IT audits. In *1st International Conference on Social Sciences and Interdisciplinary Studies (ICSSIS 2018)* (pp. 23–27). Atlantis Press.

Babbie, E. R. (2020). *The practice of social research*. Cengage learning. Retrieved from https://books.google.co.za/books?hl=en&lr=&id=5mf6DwAAQBAJ&oi=fnd&pg=PP1&dq=Babbie,+E.+R.+(2020).+The+practice+of+social+research.+Cengage+learning&ots=Bmw8b4JsdU&sig=x6BTO2GjNyD5Hz1PasmqoQmqerc&redir_esc=y#v=onepage&q&f=false.

Bakunzibake, P., Grönlund, Å., & Klein, G. O. (2019). Organisational challenges in the implementation of 'one-stop' e-Government in Rwanda. *Electronic Journal of e-Government, 17*(1), 1–19.

Bananuka, J., Kadaali, A. W., Mukyala, V., Muramuzi, B., & Namusobya, Z. (2019). Audit Committee effectiveness, isomorphic forces, managerial attitude and adoption of International Financial Reporting Standards. *Journal of Accounting in Emerging Economies, 9*(4), 502–526. https://doi.org/10.1108/jaee-08-2018-0084

Barnes, S. J., & Vidgen, R. T. (2006). Data triangulation and web quality metrics: A case study in e-government. *Information & Management, 43*(6), 767–777.

Bertot, J. C., Jaeger, P. T., & Grimes, J. M. (2010). Using ICTs to create a culture of transparency: E-government and social media as openness and anti-corruption tools for societies. *Government Information Quarterly, 27*(3), 264–271.

Bierstaker, J. L., Burnaby, P., & Thibodeau, J. (2001). The impact of IT on the audit process: An assessment of the state of the art and implications for the future. *Managerial Auditing Journal, 16*(3), 159–164. https://doi.org/10.1108/02686900110385489

Brand, D. (2016). A global look at IT audit best practices. *EDPACS, 54*(2), 8–9.

Byrnes, P. E., Al-Awadhi, A., Gullvist, B., Brown-Liburd, H., Teeter, R., Warren, J. D., & Vasarhelyi, M. (2018). *Evolution of auditing: From the traditional approach to the future audit. In Continuous auditing*. Emerald Publishing.

Carr, C. T., & Hayes, R. A. (2015). Social media: Defining, developing, and divining. *Atlantic Journal of Communication, 23*(1), 46–65.

Cassidy, D., Goldstein, L., Johnson, S. L., Mattie, J. A., & Morley, J. E., Jr. (2001). *Developing a strategy to manage enterprise-wide risk in higher education*. NACUBO and Price Waterhouse Coopers LLP.

CFA Institute. (2021). *Audit committee role & responsibilities*. Retrieved from https://www.cfainstitute.org

Chen, C., Hartmann, C. C. & Gottfried, A. (2022a, June 21). *Impact of audit committee IT expertise on data breaches*. Retrieved from: https://meridian.allenpress.com/jis/article/doi/10.2308/ISYS-2020-076/483224/The-Impact-of-Audit-Committee-IT-Expertise-on-Data.

Chen, C., Hartmann, C., & Gottfried, A. (2022b). The impact of audit committee IT expertise on data breaches. *Journal of Information Systems, 36*(3), 61–81.

Chen, S., & Komal, B. (2018). Audit committee financial expertise and earnings quality: A meta-analysis. *Journal of Business Research, 84*(1), 253–270.

Christiansen, B. (Ed.). (2013). *Cultural and technological influences on global business*. IGI Global.

Cohen, J., Krishnamoorthy, G., & Wright, A. (2017). Enterprise risk management and the financial reporting process: The experiences of audit committee members, CFO s, and external auditors. *Contemporary Accounting Research, 34*(2), 1178–1209.

Contessotto, C., & Moroney, R. (2014). The association between audit committee effectiveness and audit risk. *Accounting & Finance, 54*(2), 393–418.

Corradini, I. (2020). *Building a cybersecurity culture in organizations* (Vol. 284). Springer.

Deloitte Access Economics. (2017). *Soft skills for business success*. Deakin.

Fama, E. F., & Jensen, M. C. (1983). Separation of ownership and control. *The Journal of Law and Economics, 26*(2), 301–325.

DeZoort, F. T., Hermanson, D. R., Archambeault, D. S., & Reed, S. A. (2002). Audit committee effectiveness: A synthesis of the empirical audit committee literature. *Journal of Accounting Literature, 2002*(21), 38–75.

George, D., & Mallery, P. (2003). SPSS for Windows step by step: A simple guide and reference. 11.0 update—4th ed. Boston: Allyn & Bacon.

Grant, G., & Chau, D. (2005). Developing a generic framework for e-government. *Journal of Global Information Management (JGIM), 13*(1), 1–30.

Hadden, L. B. (2002). *An investigation of the audit committee and its role in monitoring IT risks*. Nova Southeastern University.

Hadden, L. B., & Hermanson, D. R. (2003). Is your audit committee watching IT risks? *Journal of Corporate Accounting & Finance, 14*(5), 35–39.

Hadden, L. B., Hermanson, D. R., & DeZoort, F. T. (2003). Audit Committees Oversight of IT risk. *Review of Business Information Systems (RBIs), 7*(4), 1–12.

Herdan, A. (2008). The relationship between the audit committee and the internal audit function: Evidence from UK. *Studia i Prace Uniwersytetu Ekonomicznego w Krakowie, 1, t. 1*, 446–455.

Huff, S. L., Maher, P. M., & Munro, M. C. (2006). IT and the board of directors: Is there an IT attention deficit? *MIS Quarterly Executive, 5*(2), 55–68.

Iliescu, F. M. (2010). Auditing IT governance. *Informatica Economica, 14*(1), 93.

Institute of Directors (South Africa). (2010). King Report on Governance for South Africa 2009: King Code of Governance Principles for South Africa 2009; Companies Act 71 of 2008. Juta and Company Ltd. IoDSA refers to the Institute of Directors in Southern Africa (2016).

Inuwa, I., Kah, M. M., & Ononiwu, C. G. (2019). Understanding how the traditional and IT anti-corruption strategies intertwine to Curb public sector corruption: A systematic literature review. In *PACIS* (p. 15).

Jackson, R. A. (2004). *Get the most out of audit tools*. www.findarticles.com/ (Accessed 4 April 2021).

Janvrin, D., Bierstaker, J., & Lowe, D. J. (2008). An examination of audit IT use and perceived importance. *Accounting Horizons, 22*(1), 1–21.

Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal of Financial Economics, 3*(4), 305–360.

Joseph, S. R. (2015). Advantages and disadvantages of E-government implementation: literature review. *International Journal of Marketing and Technology, 5*(9), 18–34.

Khemakhem, H., & Fontaine, R. (2019). The audit committee chair's abilities: Beyond financial expertise. *International Journal of Auditing, 23*(3), 457–471.

Kim, S. H., Jang, S. Y., & Yang, K. H. (2017). Analysis of the determinants of software-as-a-service adoption in small businesses: Risks, benefits, and organisational and environmental factors. *Journal of Small Business Management, 55*(2), 303–325.

Lankton, N., Price, J. B., & Karim, M. (2021). Cybersecurity breaches and the role of information technology governance in audit committee charters. *Journal of Information Systems, 35*(1), 101–119.

Lee, J., & Lee, C. (2009). IT governance-based IT strategy and management: Literature review and future research directions. In *Information technology governance and service management: Frameworks and adaptations* (pp. 44–62).

Legodi, A. H. (2021). *Enhancing audit committee effectiveness in South African municipalities* (Doctoral dissertation).

Lloyd, I. J. (2004). *Information technology law*. Oxford University Press.

Marnewick, C., & Labuschagne, L. (2011). An investigation into the governance of IT projects in South Africa. *International Journal of Project Management, 29*(6), 661–670.

McColgan, P. (2001). Agency theory and corporate governance: A review of the literature from a UK perspective. *Department of Accounting and Finance working paper, 6*, 0203.

Mead, N. R., Viswanathan, V., & Padmanabhan, D. (2008, July). Incorporating security requirements engineering into the dynamic systems development method. In *In 2008 32nd Annual IEEE International Computer Software and Applications Conference* (pp. 949–954). IEEE.

Mikalef, P., Krogstie, J., van de Wetering, R., Pappas, I., & Giannakos, M. (2018, January). Information governance in the big data era: Aligning organisational capabilities. In *Proceedings of the 51st Hawaii International Conference on System Sciences*.

Mohamed, N. (2012). A conceptual framework for IT governance effectiveness in private organisations. *Information Management & Computer Security, 20*(2), 88–106. https://doi.org/10.1108/09685221211235616

Moloi, T. (2014). Disclosure of risk management practices in the top South African mining companies: An annual/integrated report disclosure analysis. *African Journal of Business Management, 8*(17), 681–688.

Moorthy, M. K., Mohamed, A. S. Z., Gopalan, M., & San, L. H. (2011). The impact of IT on internal auditing. *African Journal of Business Management, 5*(9), 3523–3539.

Mostert, J., & Mutula, S. M. (2010). Challenges and opportunities of e-government in South Africa. *The Electronic Library, 28*(1), 38–53.

Muchenje, T. (2013). *An Analysis of the impact of emerging technology on organisations' internal Controls*. University of Johannesburg (South Africa).

Ndou, V. (2004). E-Government for developing countries: Opportunities and challenges. *The Electronic Journal of Information Systems in Developing Countries, 18*(1), 1–24.

Ojeka, S., Adeboye, A. B., & Dahunsi, S. O. (2021). Does audit committee characteristics promote risk management practices in Nigerian listed firms? *Accounting and Finance Research, 10*(2), 70–77.

Ojeka, S., Ben-Caleb, E., & Ekpe, E. O. I. (2017). Cyber security in the Nigerian banking sector: An appraisal of audit committee effectiveness. *International Review of Management and Marketing, 7*(2), 340–346.

Oji, O., & Ofoegbu, G. N. (2017). Effect of audit committee qualities on financial reporting of listed companies in Nigeria: A perspective study. *International Journal of Scientific and Research Publications, 7*(10), 278–290.

Omer, W. K. H., Aljaaidi, K. S., & Al-Moataz, E. S. (2020). Risk management functions and audit report lag among listed Saudi manufacturing companies. *The Journal of Asian Finance, Economics and Business (JAFEB), 7*(8), 61–67.

Ramamoorti, S., & Weidenmier, M. L. (2004). *Opportunities in internal auditing: Chapter 9 The pervasive impact of information technology on internal auditing (supplemental chapter)*. The Institute of Internal Auditors Research Foundation (IIARF).

Ravichandran, T., Han, S., & MIT has, S. (2017). Mitigating diminishing returns to R&D: The role of IT in innovation. *Information Systems Research, 28*(4), 812–827.

Reeder, R. W., Ion, I., & Consolvo, S. (2017). 152 simple steps to stay safe online: Security advice for non-tech-savvy users. *IEEE Security & Privacy, 15*(5), 55–64.

Riggins, F. J., & Wamba, S. F. (2015, January). Research directions on the adoption, usage, and impact of the internet of things through the use of big data analytics. In *In 2015 48th Hawaii international conference on system sciences* (pp. 1531–1540). IEEE.

Roussy, M., & Rodrigue, M. (2018). Internal audit: Is the 'third line of defense' effective as a form of governance? An exploratory study of the impression management techniques chief audit executives use in their annual accountability to the audit committee. *Journal of Business Ethics, 151*(3), 853–869.

Sabani, A., Farah, M. H., & Dewi, D. R. S. (2019). Indonesia in the spotlight: combating corruption through ICT enabled governance. *Procedia Computer Science, 161*, 324–332.

Seale, T. (2017). *Factors influencing the decision to adopt an IT risk Management framework at universities in South Africa* (Master's thesis, University of Cape Town).

Spira, L. F. (2003). The audit committee: performing corporate governance. *European Accounting Review, 12*(3).

Susanto, D. (2020). The triangle defense for financial reporting quality: The interplay between internal auditing, the audit committee, and the external auditor. *Wahana: Journal Economics, Managements and Accountants, 23*(1), 112–130.

Tarek, M., Mohamed, E. K., Hussain, M. M., & Basuony, M. A. (2017). The implication of IT on the audit profession in developing country. *International Journal of Accounting & Information Management, 25*(2), 237–255.

Turel, O., Liu, P., & Bart, C. (2017). Board-level IT governance effects on organisational performance: The roles of strategic alignment and authoritarian governance style. *Journal of Information Systems Management, 34*(2), 117–136.

Van Grembergen, W., & De Haes, S. (Eds.). (2007). *Implementing information technology governance: Models, practices and cases: models, practices and cases*. IGI Global.

Webb, P., Pollard, C. & Ridley, G. (2006, January). Attempting to define IT governance: Wisdom or folly? In *Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06)* (Vol. 8, pp. 194a). IEEE.

Weidenmier, M. L., & Ramamoorti, S. (2006). Research opportunities in information technology and internal auditing. *Journal of Information Systems, 20*(1), 205–219.

Weill, P., & Ross, J. W. (2004). *IT governance: How top performers manage IT decision rights for superior results*. Harvard Business Press.

Zanzig, J. S., & Francia, G. A., III. (2022). Auditor evaluation and reporting on cybersecurity risks. In *Research anthology on business aspects of cybersecurity* (pp. 19–38). IGI Global.