Journal of Contemporary Management

Volume 22 Special Issue 1: Business and Financial Markets Resilience and the Fourth Industrial Revolution

A literature review of internal auditing involvement in cybersecurity risk management of the organisation

DOI: https://doi.org/10.35683/jcm24.030.293

MVELO COMFORT SIYAYA*
Department of Accounting Sciences, Cape Peninsula University of Technology, South Africa
Email: siyayam@cput.ac.za
ORCID: https://orcid.org/0000-0002-0987-587X
*corresponding author

JOBO DUBIHLELA
Graduate School of Business and Leadership, University of KwaZulu-Natal, South Africa
Email: dubihlelaj@ukzn.ac.za
ORCID: http://orcid.org/0000-0001-6228-6524

MABUTHO SIBANDA
School of Accounting, Economics, and Finance, University of KwaZulu-Natal, South Africa
Email: sibandam@ukzn.ac.za
ORCID: https://orcid.org/0000-0002-8656-7539

ABSTRACT

Purpose of the study: It is evident that internal auditing plays a crucial role in the governance, risk management and internal control processes of the organisation. Given the recent digitalisation of these processes, cybersecurity risk remains a serious challenge. The involvement of internal auditing in cybersecurity risk management is a new research area that requires urgent attention. Therefore, the purpose of this paper is to investigate the involvement of internal auditing in the cybersecurity risk management of the organisation.

Design/methodology/approach: A non-empirical research study was conducted to examine the involvement of internal auditing in cybersecurity risk management. Data were collected from a variety of sources, including journal articles, books, professional websites, conference papers and theses/dissertations. The PRISMA flow diagram was utilised to guide the selection of relevant data for the study. A thematic qualitative research approach was used for data analysis and guiding the discussion of findings.

Findings: The study found that the internal audit function (third line of defence) is crucial for joining forces with the information technology (IT) function (first line of defence) and risk management function (second line of

defence) in the fight against cybersecurity risk. In addition, the internal audit function has a role in informing the audit committee and the board of directors whether security controls are adequate and operating effectively for mitigating cybersecurity risk.

Recommendations/value: A collaborative effort between internal audit, risk management and IT functions is recommended in the fight against cybersecurity risk within the organisation. A clear set of roles and responsibilities between these functions must be determined in the cybersecurity strategy to minimise duplication of effort and promote good cybersecurity governance.

Managerial implications: A distinct role of internal auditing in cybersecurity risk management was revealed to assist organisational management. Understanding internal audit assurance and its consulting role in cybersecurity risk should assist industry practitioners and policymakers to better utilise internal auditing in the cybersecurity strategy of the organisation.

Keywords: Cybersecurity risk; cybersecurity risk management; governance; internal auditing; internal audit function; internal control; organisation.

JEL Classification: M42

1. INTRODUCTION

Cybersecurity risk is rapidly increasing globally. Organisations around the globe are expected to incur 10.5 trillion US dollars in cybersecurity risk annually by 2025, at a growth rate of 15% year over year (McLean, 2024). Cybersecurity risk is among the top 10 greatest business risks for organisations (Segal, 2023). The report by Panetta (2021) reveals that 88% of board members regard cybersecurity risk as a business risk while only 12% perceive it as a technology risk. The same report reveals that the board of directors may be required to formulate performance requirements concerning cybersecurity risk by 2026 (Panetta, 2021). Organisations are investing heavily in technology and information systems to obtain a competitive advantage over their competitors, indicating that cybersecurity risk will continue to be a threat.

The top five organisational data breaches for the year 2023 were reported to have taken place in countries such as the United Kingdom (UK), the United States of America (USA), India and Kazakhstan (Ford, 2024). The cybersecurity hub on IT governance reported that more than 3.8 billion records of the UK organisation DarkBeam were exposed to a data leak (Powell, 2023). Two of the top 5 data breaches during 2023 were reported to have occurred in the USA. The organisation called Real Estate Wealth Network suffered a data leak of over 1,5 billion records, with a size of 1,16TB (Fowler, 2023). This data leak exposed confidential information relating to property history, addresses, purchase prices, mortgage companies, tax ID numbers and other information that had the potential to put clients' lives at risk. The second

major cyber-attack in the USA involved a ransomware attack that targeted Twitter after a data leak of 220 million email addresses of Twitter users (Irwin, 2023). The Indian Council of Medical Research reported in October 2023 that data relating to at least 815 million Indians who underwent COVID-19 tests had been exposed during a data breach (The Times of India, 2023). In Kazakhstan, the popular parental online application that is used to track children left user records in danger after the App failed to set a password (Okunytė, 2023). It is estimated that over 300 million user records, such as payment information, email addresses and telephone numbers, were left unprotected for more than a month (Okunytė, 2023).

Although all organisations are targeted for cybersecurity risk by hackers, some industries are more vulnerable than others due to the nature of their business. According to Statista (2023), hackers mainly target organisations that are closely involved with people's lives. These organisations may include institutions such as manufacturing, banking and finance, healthcare and higher education. The latest cyber-attacks report across worldwide industries reveals that manufacturing had the highest share of cyber-attacks at 24.8%, followed by banking and finance at 18.9% (Statista, 2023). The professional, business and customer services industry was ranked third at 14.6%, followed by the energy industry at 10.7%. The remaining 31% was spread among the retail and wholesale, education, healthcare, government, transportation, media and telecommunication institutions (Statista, 2023). Cyber-attacks affect all organisations, whether big, medium or small. Palatty (2023) argues that cyber-attacks are becoming more frequent and complex in small to medium-sized organisations – 43% of attacks are aimed at small organisations – unfortunately, 86% of these were found to be unprepared to defend themselves (Palatty, 2023). Insufficient budgets and a lack of critical resources have been identified as the root cause for small organisations being unable to protect themselves against cybersecurity risk (Palatty, 2023).

There are various strategies that management utilises to manage organisational risk, ranging from risk sharing, avoidance, reduction and acceptance (Anderson *et al.*, 2017; Baskerville *et al*., 2022). Risk sharing is the strategy organisations employ to transfer some of their cybersecurity risks to a third party, such as an insurance company. Alternatively, organisations may decide to exit the product/service line that causes the cybersecurity risk; this practice is known as risk avoidance. Various security controls that aim to prevent and/or detect and correct cybersecurity incidents may be adopted to strengthen the cybersecurity risk management programme (Alamri *et al.,* 2022). Lastly, organisations may choose to accept cybersecurity risk should they believe that it is within their risk appetite, or that it will not seriously harm their operations.

According to Camilleri *et al.* (2024) and Deloitte (2021), internal auditing is responsible for providing advice to management and assuring that risk is managed. Internal auditing, in its risk management role, is required to determine whether the cybersecurity risk management strategy designed and implemented by an organisation is adequate and, thus, capable of achieving the planned objectives (Deloitte, 2021). With cybersecurity risk management emerging as a new research area, researchers need to understand the internal auditing perspective in cybersecurity risk management. This study aims to investigate the involvement of internal auditing in cybersecurity risk management, particularly for the protection of critical infrastructure within the organisation.

2. SCOPE OF THE STUDY

This study investigates the involvement of internal auditing in the organisation's cybersecurity risk management processes. It seeks to understand how the internal audit function assists in the management of cybersecurity risk within the organisation as the assurance provider. This study does not focus on the perspectives of other assurance providers, such as external auditors. In addition, the results presented below are not attributed to a specific industry, sector or organisation. Therefore, the effect of industry regulations, laws and standards with respect to internal auditing of cybersecurity risks is not considered. The results of the study are limited to a literature review methodology on the assumption that cybersecurity risk management is an integral part of every organisation's DNA (i.e. innate information for the development and functioning of the organisation).

3. METHODOLOGY

In this study, a non-empirical research design was adopted to understand internal auditing's involvement in the organisation's cybersecurity risk management. Researchers employed a non-empirical research design involving the examination of secondary sources, including journal articles, books, professional websites and theses/dissertations, for data collection (Snyder, 2019). According to Snyder (2019), literature review studies are helpful for the formulation of theory between the research variables. A literature review, using internal auditing and cybersecurity risk management as the research variables was therefore conducted following an interpretive research paradigm. These variables guided the search for the research data necessary for this study. The remainder of this section of the paper details the study research strategy in the form of the two phases used in this study, namely data collection and analysis.

3.1 Phase 1: A data collection phase

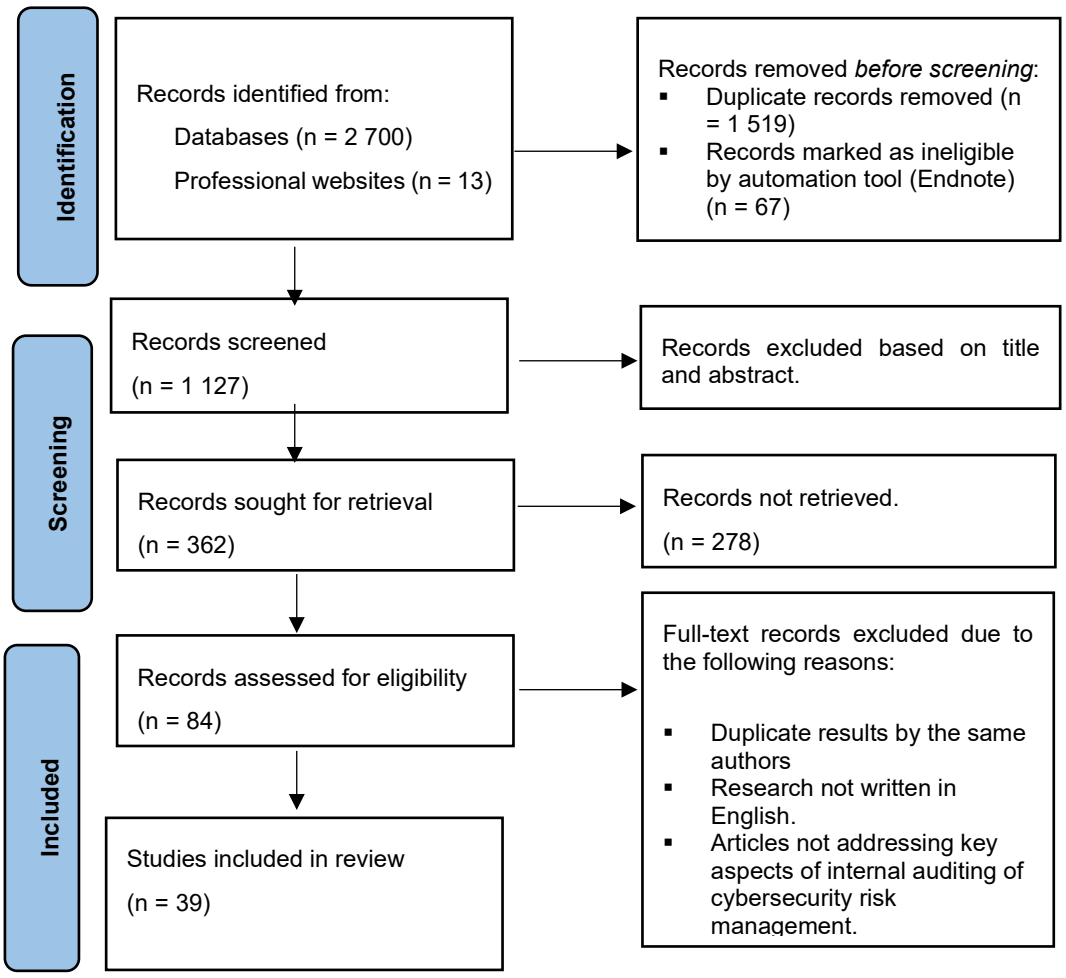
A PRISMA flow chart was chosen in this study to systematically unpack the data collection process. Figure 1 communicates the steps researchers undertook to transparently identify, screen and select data relevant to this study. To reduce possible bias in the selection of studies, reasons are communicated for including and excluding studies, thus enhancing the validity and reliability of the study results. PRISMA flow charts assist the reader in reviewing possible biases in the selection process of studies and examining the generalisability of the study findings (Page *et al.,* 2021).

The search string of the study on databases was limited to 'internal audit*', 'cybersecurity' or 'cyber security' and 'risk management' for the years 2018 to 2023. The years selected were considered sufficiently recent to provide valuable data relating to study variables. With the assistance of a university librarian, the database search was further narrowed to peer-reviewed journal articles with search results limited to relevance, availability and full-text options. The use of the expert librarian allowed the search to cover a larger extent of data, thus enhancing its quality (Noble & Smith, 2015). This search resulted in a total of 2,700 records from databases (Google Scholar, IEEE, Springer LNCS and Web of Science), thus enabling the researchers to obtain a clear understanding of cybersecurity risk, risk management and internal auditing. A total of 13 records were also retrieved from professional websites such as Deloitte, ERM Academy, IT Governance, Embroker and PWC. Duplicate and ineligible studies, as identified by EndNote, were excluded from the analysis (see Figure 1).

The researchers conducted a screening of the remaining records, and some of these articles were excluded based on title and abstract. As shown in Figure 1 below, 278 records were excluded from the analysis as full-text papers could not be retrieved due to access restrictions. In addition, 45 records were excluded from the analysis because they either revealed duplicate results from the same authors, were not written in English or did not address key aspects of internal auditing of cybersecurity risk management. Subsequently, for the purpose of this study, only 39 sources remained relevant to the internal auditing of cybersecurity risk management within the organisation. The consistency in results from the 39 studies that were analysed can be associated with the term 'reliability', and the accuracy of these results can be associated with the term 'validity' (Noble & Smith, 2015). Although non-empirical reviews give access to multiple data sources, they limit researchers to choose studies with caution by strictly aligning the data selection process to the main question of the study (Noble & Smith,

2015). The large sample size cannot, on its own, enhance the generalisability of findings to the population if an appropriate sample design is not chosen (Noble & Smith, 2015; Snyder, 2019). It is further argued by Page *et al.* (2021) that there is no minimum or maximum sample size for systematic literature review studies, however, the study should provide sufficient evidence to achieve its aim.

Figure 1: PRISMA flow chart of the study



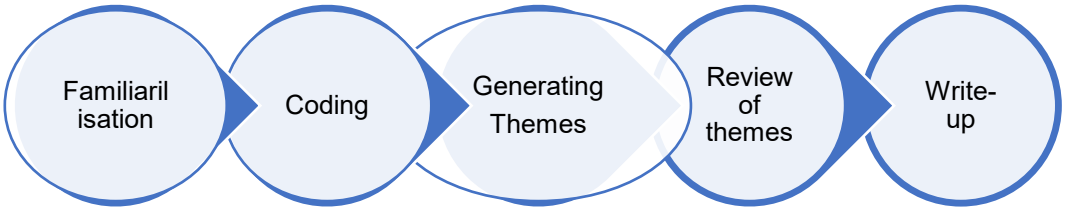
Source: Page *et al.* (2021)

3.2 Phase 2: Data analysis phase

A thematic qualitative analysis strategy was adopted to facilitate the analysis of the data collected from Phase 1. Although, in common with grounded theory, phenomenology and ethnography, the thematic research strategy has not been given much attention by researchers, it can provide meaningful and trustworthy results (Nowel et al., 2017). This strategy was chosen in this study because it is less expensive and requires the researcher to

analyse data objectively (Clarke & Braun, 2017; Nowell et al., 2017). All sources that were chosen for data analysis were independently examined by the researchers to identify common themes that occurred repeatedly across the data. Figure 2 depicts the approach of thematic analysis that researchers followed from the formulation of themes to the writing-up stage.

Figure 2: Thematic analysis method applied



Source: Clarke and Braun (2017)

At the commencement of the analysis process, researchers involved in the study read through the data that remained after phase 1 to become familiar with it. Researchers independently highlighted important sections to develop codes that described their content. Next, researchers met to confirm the codes developed and identify patterns from the codes that were then used to create themes. The validity and accuracy of these themes were enhanced by revisiting the data to review whether the identified themes were a true reflection of the data (Clarke & Braun, 2017; Nowell et al., 2017). The final list of themes and sub-themes was then formulated (see Table 1) to help researchers understand the data systematically. Finally, the findings were recorded, and discussions then took place to address the meaning of each theme in pursuit of achieving the aim of the study. A critical engagement with studies from 2018 to 2023 is presented next.

4. FINDINGS AND DISCUSSION

Table 1 presents all the themes and subthemes generated for this study. All the 39 sources considered for data analysis are also presented as they relate to the identified themes. Reference to sources outside the scoped period of 2018 to 2023 is made to facilitate the discussion of results. These sources, such as the Institute of Internal Auditors (2024), set the theoretical foundation for the field of internal auditing to understand its involvement in the emerging area of cybersecurity risk management.

Table 1: Themes and sub-themes derived from relevant sources.

THEMES	SUB-THEME	RELEVANT SOURCE
Perspectives	Integrated risk management IT team Risk committee Independent assessment	Alamri *et al.* (2022); Albalas *et al*. (2022); Kamariotou & Kitsios (2023); Kure *et al*. (2022); NIST, (2018). I
Processes and controls	Administrative control Physical control Technical control	Baskerville *et al.* (2022); Keerthana *et al.* (2023); Malatji (2023); Sawik & Sawik (2022); Shaikh & Siponen (2023).
Practices	Cybersecurity strategy Risk identification Risk prioritisation Security controls Cyber insurance liability Cyber risk programme	Arafa *et al.* (2023); Alamri *et al.,(*2022); Baskerville *et al.* (2022); Boeding *et al*. (2022); Gale *et al*. (2022); Kamariotou & Kitsios (2023); NIST, (2018); Sawik & Sawik (2022).
Challenges	Cybersecurity talent Innovative cyber risks Third-party risk governance Budget	Arafa *et al*. (2023); Holmes (2021); Oltsik (2019); Palatty (2023); Pooja & Damle (2023).
Internal audit role	Assurance Consulting	Alarcon *et al.* (2023); Bozkus Kahyaoglu & Caliyurt (2018); Deloitte (2021); Khelil & Khlif (2022); Lois *et al.* (2021); NIST (2018); Oyewumi *et al.* (2023); Simić (2022); Slapničar *et al.* (2022).
Internal audit focus	Governance Risk management Internal control	Al-Matari, *et al.* (2021); Al-Sartawi (2020); Alarcon *et al*. (2023); Brazngi *et al.* (2023); Bozkus Kahyaoglu & Caliyurt (2018); Christ *et al*. (2022); Daidj (2022); Davis (2021); Deloitte (2021); Dikokoe (2021); Gunawan *et al.* (2023); Hepworth *et al*. (2022); Islam *et al*. (2022); Lois *et al*. (2021); Mwim & Mtweni (2022); NIST, (2018); Rosati *at al.* (2022); Sabillon (2022); Shaikh & Siponen (2023); Simić (2022); Slapničar *et al.* (2022); Todorović *et al.* (2020); Usman *et al.* (2023).

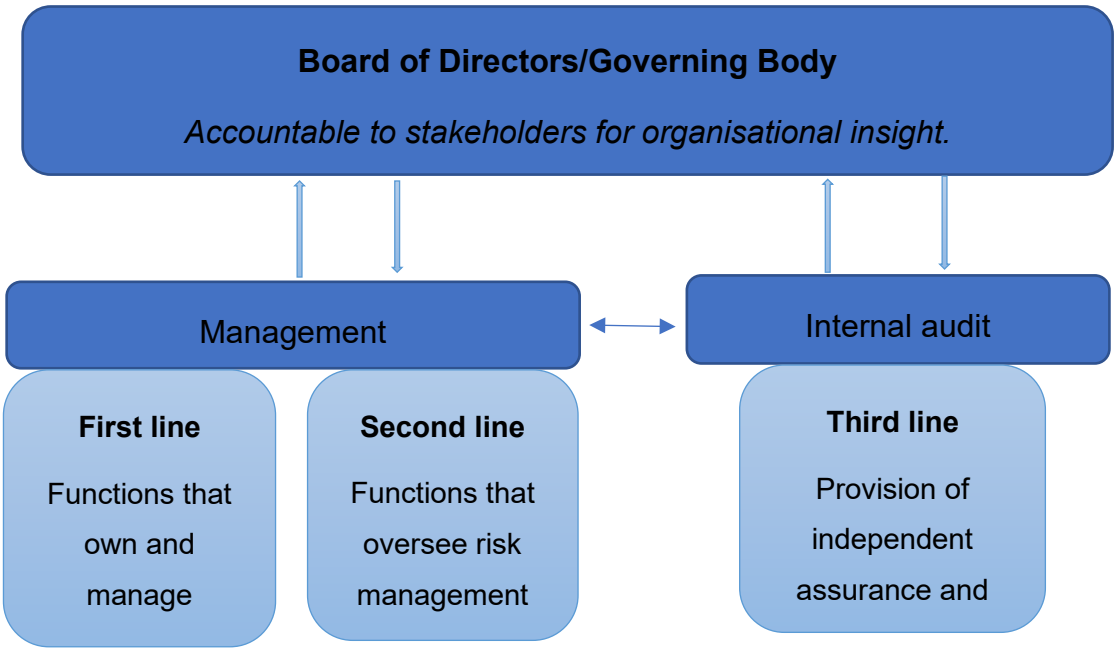
4.1 Perspective on cybersecurity risk management

The process that organisations undertake to identify, examine, prioritise and respond to cybersecurity risks is known as cybersecurity risk management (Alamri *et al.,* 2022; NIST,

2018). Arguably, cybersecurity risk management should be an integral part of organisation-wide risk management (Alamri *et al.,* 2022; Albalas et al, 2022). The IT team is primarily responsible for the management of cybersecurity risk (Kamariotou & Kitsios, 2023; Kure *et al.,* 2022). The design of security controls and processes is normally facilitated by the information security function of the IT team (Kure *et al,* 2022). Where possible, organisations can formally establish a risk committee that is primarily dedicated to monitoring cybersecurity risks and overseeing the implementation of security controls by the IT team to manage cybersecurity risk (Camilleri *et al.,* 2024). Arguably, organisations are at risk because the implemented security controls may not be sufficiently robust or may not operate as intended by the executive management and the board. Consequently, an independent assessment should be conducted to ensure that cybersecurity controls are adequate and operate effectively to achieve the intended objectives (Camilleri *et al.,* 2024).

The diagram below shows a typical structure of those parties involved in the management of cybersecurity risk within the organisation. It depicts the interaction among the board of directors, management and the internal auditing section in their efforts to manage cybersecurity risk. The IT function/information security function is shown as the first line of defence that owns and manages cybersecurity risk. The risk management function is depicted as the second line of defence, and internal auditing as the third line of defence.

Figure 3: Three Lines of Defence Theory – cybersecurity risk management



Source: Culp and Thompson (2016)

4.2 Processes and controls for cybersecurity risk management

Several processes and controls for managing cybersecurity risk exist, including administrative, physical and technical controls (Keerthana, 2023; Sawik & Sawik, 2022; Shaikh & Siponen, 2023). The reviewed literature reveals that preventing, detecting and correcting cybersecurity incidents are the major functions of the cybersecurity risk management processes and controls (Baskerville *et al.*, 2022; Keerthana, 2023; Shaikh & Siponen, 2023). Preventative security controls aim to avert security incidents from occurring (Keerthana, 2023). Antivirus programs, passwords and locking devices are the commonly used preventative security controls within the organisation (Baskerville *et al.,* 2022; Keerthana, 2023). Preventative controls do not provide absolute assurance that cybersecurity risk is managed. Detective controls, such as surveillance cameras, review of access rights and audit logs, are used to detect unwanted activities within the IT environment (Baskerville *et al.,* 2022; Keerthana, 2023). Measures, known as corrective controls, must be taken to correct unwanted activities that are detected in the IT environment (Baskerville *et al.,* 2022; Keerthana, 2023). Examples of corrective security controls may include rebooting a system, an incident response plan and the implementation of a business continuity plan.

Security rules, policies, procedures and guidelines (known as administrative security controls) are set at the board level to protect confidential information from access by unauthorised users (Malatji, 2023; Shaikh & Siponen, 2023). These administrative controls should govern the user management access of the organisation to limit unauthorised admission to the organisation's confidential data (Malatji, 2023). Management of user access and privileges, protection of employees, clearance and evaluation and employee training and awareness are identified as fundamental areas that administrative controls must implement and supervise (Malatji, 2023; Shaikh & Siponen, 2023). Administrative controls alone are not adequate to manage cybersecurity risk. Physical controls are also essential to physically protect critical infrastructure through which sensitive data is stored (Shaikh & Siponen, 2023). Physical controls protect security infrastructure from theft by unauthorised users. These controls may include, but are not limited to, biometric systems, the use of identity cards for access, surveillance cameras and alarm systems (Malatji, 2023; Shaikh & Siponen, 2023). Additionally, technical controls are designed to protect organisational data that travels over the network (Shaikh & Siponen, 2023). Technical controls such as access controls, network authentication, encryption and firewalls are essential to prevent unauthorised users from corrupting sensitive data via the internet (Malatji, 2023; Shaikh & Siponen, 2023). Table 2 below present types of security controls that were found across the reviewed literature, together with their functions in cybersecurity risk management.

Table 2: Cybersecurity controls and their functions

Control Type	Preventative	Detective	Corrective
Administrative	❖ Policies for hiring and termination ❖ Division of duties ❖ Classification of data	❖ Review access rights ❖ Audit logs & unauthorised changes	❖ Incident response plan ❖ Organisational continuity plan
Physical	❖ Gates ❖ Fences ❖ Locks	❖ Surveillance cameras ❖ CCTV	❖ Reissue of access cards ❖ Repair of physical damage
Technical	❖ Firewalls ❖ IPS ❖ Antivirus ❖ MFA	❖ Honeypots ❖ IDS	❖ System rebooting ❖ Virus quarantine ❖ Vulnerability patching

Sources: Keerthana (2023), Sawik and Sawik (2022)

4.3 Practices and challenges in cybersecurity risk management

Although cybersecurity risk management processes may differ from one organisation to the next, some steps, practices and considerations remain constant across all environments. It is considered a standard practice to commence the management of cybersecurity risk by developing a comprehensive cybersecurity strategy (Arafa *et al*., 2023; Kamariotou & Kitsios, 2023). These scholars believe that such a strategy should outline clear cybersecurity objectives, policies and procedures to protect sensitive data (Arafa *et al.*, 2023; Kamariotou & Kitsios, 2023). Arguably, the organisational cybersecurity management process commences with understanding the IT environment and identifying the critical infrastructure to protect against cybersecurity risk (Boeding *et al.*, 2022; NIST, 2018). A comprehensive understanding of the IT environment and organisational assets facilitates the process of identifying all cyber risks within the IT environment. These risks may include phishing, malware, denial of access and ransomware attacks (Alamri *et al.,* 2022). Resources to mitigate risks are limited. Thus, the prioritisation of cyber risks that organisations face is common in cybersecurity risk management. Risk assessment is normally conducted for the impact and likelihood of all those risks that need urgent attention (Baskerville *et al.,* 2022). The enforcement of strict cybersecurity controls often follows to manage the prioritised risks in the cybersecurity risk management programme. Most scholars consider the implementation of cybersecurity controls and consideration of cyber insurance liability as the most common risk responses to cybersecurity risk (Kohnke *et al.,* 2016; Sawik & Sawik, 2022). Scholars argue that a cybersecurity risk management programme is effective when it is communicated to all organisational stakeholders (Arafa *et al.*, 2023; Gale *et al.,* 2022). A well-communicated cybersecurity programme gives insight to organisational stakeholders regarding their position in cybersecurity risk management (Gale *et al.*, 2022). Informed employees are in a better position to understand their security role in enhancing the cybersecurity risk management effectiveness of the organisation.

Organisations struggle with cybersecurity talent, innovation of cybersecurity risks, lack of vendor governance framework and budgets in cybersecurity risk management (Holmes, 2021; Oltsik, 2019; Pooja & Damle, 2023). Developing, recruiting and retaining top cybersecurity talent is a major challenge for most organisations (Pooja & Damle, 2023). The inability to find skilled cybersecurity professionals has become a threat that organisations must deal with. Cybersecurity risks are evolving and dynamic. The lack of proliferation of solutions to deal with the consistently evolving cybersecurity threats undermines the effectiveness of a cybersecurity risk programme in most organisations (Oltsik, 2019; Pooja & Damle, 2023).

Although small organisations are more susceptible, the issue of a deficient cybersecurity budget is common to all organisations, whether small, medium or large (Oltsik, 2019; Palatty, 2023). Another serious challenge identified is the lack of vendor governance frameworks for cybersecurity management. Interconnectivity of organisational systems with those of the vendor poses third-party cyber risks for many organisations (Holmes, 2021). Organisations often fail to track third-party risks in line with their internal cybersecurity policies and compliance processes (Arafa *et al.*, 2023; Holmes, 2021). In the absence of a vendor governance framework and communication of such a framework, organisations experience gaps in the awareness and expectations of vendors in cybersecurity risk management (Arafa *et al.*, 2023; Holmes, 2021).

4.4 Internal auditing role in cybersecurity risk management

Internal audit engagements comprise either assurance or consulting (Institute of Internal Auditors, 2024). From the data analysis undertaken, *'assurance'* and *'consulting'* emerged as the sub-themes necessary for understanding the nature of internal auditing services on cybersecurity risk management.

4.4.1 Assurance role

The Three Lines of Defence Theory explains that the IT function and its team (security engineers, information security officers and chief information security officers) should take the primary ownership of cybersecurity matters within the organisation, as the first line of defence (Simić, 2022; Slapničar *et al.*, 2022). Additionally, the risk management function and/or the risk committee, as the second line of defence, is responsible for the management and monitoring of cybersecurity risks within the organisation (Alarcón Cotrina *et al*., 2023; Slapničar *et al*., 2022). Members of the governing body and its subcommittees, such as the audit committee, are not involved in the daily operation of the organisation and, as a result, these structures may need assurance that approved security policies and procedures are adhered to within the organisation (Camilleri *et al.,* 2024; Deloitte, 2021). According to NIST (2018), assurance engagements increase the board's confidence that the availability, confidentiality and integrity of data have been met.

There are a number of mechanisms within the three lines of defence that support assurance activities within the organisation, including risk assessments, risk treatments, risk management, security assurance and auditing (Culp & Thompson, 2016). Various researchers (Bozkus Kahyaoglu & Caliyurt, 2018; Lois *et al.,* 2021; Slapničar *et al.*, 2022) argue that the traditional auditing framework must be updated to reflect the modern digital business

environment. Auditing frameworks of the recent era should incorporate continuous internal audits, cybersecurity affirmation and control monitoring to allow the organisation to revise its new assurance services (Bozkus Kahyaoglu & Caliyurt, 2018; Lois *et al.*, 2021). The independence of internal auditing qualifies this activity to conduct assurance on the cybersecurity risk management of the organisation (Deloitte, 2021). As the third line of defence, internal auditing is required to conduct an independent assessment of organisational cybersecurity risk management processes to assure the governing body and the audit committee that cybersecurity risk is managed. The International Professional Practices Framework (IPPF) of internal auditing regards assurance as the process of independently examining organisational processes for evidence to determine their effectiveness (Institute of Internal Auditors, 2024).

Internal auditing is an autonomous, impartial activity that is designed to help organisations achieve their objectives by providing assurance activities (Institute of Internal Auditors, 2024). In its assurance role, internal auditing conducts an independent examination of cybersecurity risk management processes and recommends areas that need improvement (Khelil & Khlif, 2022; Lois *et al.,* 2021). Internal audit assurance engagements aim to provide the governing body with reasonable confidence that the planned cybersecurity objectives will be achieved (Khelil & Khlif, 2022). Camilleri *et al.* (2024) and Deloitte (2021) both claim that the assurance role of internal auditing makes this function remain involved in the whole cyber incident management lifecycle. While management reviews the root cause and the quality of the response during the incident management lifecycle, an internal audit activity provides assurance that the overall operational resilience of the organisation is at appropriate levels (Camilleri *et al.*, 2024).

4.4.2 Consulting role

Apart from assurance activities, internal auditing needs to accommodate consulting activities in its audit plan. In its consulting role, internal auditing helps management by performing a requested task that should add value to improve organisational performance (Institute of Internal Auditors, 2024; Siyaya *et al.*, 2021). Moodley (2019) asserts that consulting activities of internal auditing consist of services such as information technology, project management and business reengineering. In general, internal auditing consulting activities require a high degree of competence because their purpose is to advise and to make recommendations to the auditee (Bozkus Kahyaoglu & Caliyurt, 2018; Moodley, 2019). Likewise, both *Camilleri et al.* (2024) and Oyewumi *et al.* (2023) believe that internal auditing professionals must be

equipped with adequate knowledge and skills to understand the cybersecurity threats and risks facing the organisation. Additionally, competent internal auditing professionals understand the process, communicate effectively and help management solve complex cybersecurity problems (Camilleri *et al.*, 2024).

In its consulting role, the internal audit function collaborates with other lines of cybersecurity defence, including the IT and risk management functions, to improve their understanding of cybersecurity risk management (Simić, 2022). Such collaboration assists both parties in focusing on strategic cybersecurity matters and knowledge-sharing (Bozkus Kahyaoglu & Caliyurt, 2018; Simić, 2022). Arguably, the independence and objectivity of internal audit professionals could be a downside in consulting engagements (Lois et al., 2021; Moodley, 2019). It is for this reason that the Institute of Internal Auditors advises internal auditing professionals to refrain from examining processes in which they were previously involved, with a time frame of one year being taken into consideration (Institute of Internal Auditors, 2024).

4.5 Internal audit focuses on cybersecurity risk management

Although internal auditing does not assume the primary ownership of cybersecurity risk management, scholars argue that internal auditing has a crucial role to play in this regard (Camilleri *et al.*, 2024; Deloitte, 2021; Lois *et al.,* 2021; Slapničar *et al.,* 2022; Usman *et al.*, 2023). Internal auditing plays a vital role in examining the appropriateness and operational effectiveness of cybersecurity governance, risk management and internal control processes (Camilleri *et al*., 2024; Deloitte, 2021). As a result, '*governance', 'risk management'* and *'internal control'* are the sub-themes that emerged to guide internal auditing focus areas in the cybersecurity management of the organisation.

4.5.1 Governance

According to IPPF, governance consists of structures and systems that are compiled by the board of directors to achieve organisational objectives (Institute of Internal Auditors, 2024). Likewise, cybersecurity governance can be viewed as a system of structures and processes that help organisations achieve their security goals, namely: confidentiality, integrity and availability of information assets (NIST, 2018). The study of Simić (2022) reveals that internal auditing is tasked with examining cybersecurity governance for alignment with organisational governance in pursuit of achieving organisational objectives. Organisational management and the board decide on security policies, structures and processes to protect organisational critical assets (Al-Sartawi, 2020). They decide on a cybersecurity strategy that they believe will enable the organisation to achieve the organisational objectives (Al-Sartawi, 2020).

Numerous standards and frameworks are helpful in the development of the organisational strategy, including NIST and ISO/IEC 27000, to mention a few. The first two lines of defence pursue the setting of the right tone at the top with respect to cybersecurity governance so that cybersecurity fraud and other security-related incidents will not be tolerated within the organisation (Mwim & Mtsweni, 2022; Penno, 2022). The right tone at the top creates an enabling environment in which the organisation's employees tend to understand what is expected of them concerning cybersecurity governance (Mwim & Mtsweni, 2022). It also generates awareness and the obligation for organisational employees to comply with security controls (Mwim & Mtsweni, 2022).

As part of its governance function, internal auditing plays a role in reviewing the security governance processes of the organisation (Simić, 2022). Internal auditing assists organisations by independently reviewing whether the organisation's cybersecurity governance programme complies with the required security regulations (Hepworth *et al.,* 2022). Internal auditors also test whether the adopted security strategy conforms to the applicable cybersecurity frameworks (Bozkus Kahyaoglu & Caliyurt, 2018; Hepworth *et al*., 2022). During the auditing process, internal auditors identify loopholes in the organisation's security governance programme and suggest how it can be improved (Camilleri *et al.*, 2024; Hepworth *et al.*, 2022). The reviewed literature suggests that internal auditors need to partner with information security functions to improve cybersecurity governance within the organisation (Islam *et al.,* 2018; Simić, 2022). Islam *et al.* (2018) found that collaboration between internal auditors and information security professionals is positively correlated with the detection of security risk incidents.

4.5.2 Risk management process

The risk management process is the strategy that is used by management to identify risks that may hinder the achievement of organisational objectives (NIST, 2018). The aim of this practice is for management to respond to the identified risks to protect the organisation from threats. Individual managers identify risks and design responses in their business units to contribute to the organisation-wide risk management process (Dikokoe, 2021). According to Anderson *et al.* (2017) and Shaikh and Siponen (2023), risk management is the ultimate responsibility of senior management within the organisation. Cybersecurity risks are unique; thus, most organisations have decided to formulate a committee that focuses on managing cybersecurity risk (Alarcón Cotrina *et al.,* 2023; Shaikh & Siponen, 2023). Internal auditing is thought to be of value in helping organisations in the management of cybersecurity risk. Scholars believe

that internal auditing can independently examine the organisation's cybersecurity risk management programme and advise the board and the audit committee on its effectiveness (Brazngi & Al-Saqa, 2023; Sabillon, 2022; Todorović *et al.,* 2020).

According to Camilleri *et al.* (2024) and Deloitte (2021), internal auditing helps organisations with the identification of vulnerabilities that may result in cybersecurity incidents. Internal auditing conducts a cybersecurity risk assessment on a wide range of organisational processes, and the findings of the assessment are reported to the board and audit committee. Such an assessment is of value to the organisation because all areas that require immediate attention by management and security providers are identified (Christ *et al.,* 2021; Rosati *et al.,* 2022). A respondent in the study of Simić (2022) reported that the internal audit report on cybersecurity risk assessment, which is later reviewed by the board, is of great significance to auditors because they are taken more seriously as a result of this practice. Camilleri *et al.* (2024) argued that a cybersecurity risk assessment activity conducted by internal auditors not only identifies vulnerabilities within organisational processes, but also points out opportunities for strengthening the organisation's security programme. During the risk assessment process, internal auditing can assist the organisation by classifying and ranking all the identified risks into high, medium and low categories (Davis, 2021). A comprehensive cybersecurity risk assessment assists internal auditors in designing their internal audit plan, owing to their having taken into consideration a broader view of organisational processes. Likewise, security assessments can in turn assist organisations to focus their limited resources on cybersecurity risks that are ranked as high (Davis, 2021; Deloitte, 2021).

4.5.3 Internal control processes

Organisational management is responsible for the design and implementation of internal security controls that aim to mitigate cybersecurity risks (Al-Matari *et al.,* 2021). A comprehensive security control design should consist of administrative, technical and physical controls (Camilleri *et al.,* 2024; Deloitte, 2021). In the battle to fight cybersecurity risks within the organisation, the collaborative effort of internal auditing is crucial for independently examining whether the controls are adequately designed and operate effectively to achieve their objectives, i.e. to mitigate cyber risks within the organisational risk appetite *(*Al-Matari *et al.,* 2021; Daidj, 2022). Organisations are often in a hurry to introduce new business processes and, in doing so, critical cybersecurity risks may be ignored (Camilleri *et al.,* 2024; Gunawan *et al.,* 2023). Such practices may have devastating effects. Internal auditing can help prevent incidents of this nature by proactively examining whether precautions have been exercised on

all cybersecurity risks that could emerge from the launch of the new business activity, service or product (Gunawan *et al.,* 2023).

In the modern digital world, internal audit functions must plan to conduct audits on administrative, technical and physical controls that intend to protect their organisation from cybersecurity risk (Camilleri *et al.,* 2024). Internal auditing of administrative security controls should consider the review of cybersecurity policies and procedures that aim to protect critical organisational infrastructure (Dikokoe, 2021). Internal auditing of technical security controls, on the other hand, should entail the examination of technical controls such as intrusion detection policies, firewall policies and data backups (Camilleri *et al.,* 2024; Dikokoe, 2021). Most people, including auditors, are often frightened when they hear IT concepts such as intrusion detection, firewalls and vulnerability testing (ERM Academy, 2024). However, scholars claim that, while internal auditors should focus their work on the process of internal auditing, a basic understanding of these IT concepts is essential (Deloitte, 2021; ERM Academy, 2024; Usman *et al.,* 2023). These scholars believe that auditors with appropriate knowledge and skills should perform technical security controls' audits. In addition, the CEO and president of the Institute of Internal Auditors elucidated that cybersecurity audits do not solely concern IT issues, but are mainly about business issues (ERM Academy, 2024). Lastly, internal auditors should focus their attention on examining the appropriateness and operational effectiveness of physical controls that protect the critical organisational infrastructure, such as computer servers, computer rooms and data centres (Camilleri *et al.,* 2024).

5. EMERGING TRENDS IN AUDITING OF CYBERSECURITY RISK

Undoubtedly, the cybersecurity audit market is anticipated to rise globally. The modern business environment warrants auditors to expand their scope to include the monitoring of technological issues that hinder the achievement of organisational objectives, such as cybersecurity risk. This section of the study summarises cybersecurity audit trends identified throughout the reviewed literature that were found to have a severe impact on the organisation's ability to respond to security risk.

5.1 Nature of internal audits

Traditionally, organisations would prioritise business audits and give less focus to IT audits. The current digitalisation of organisational processes shifts the focus of audit work programmes to prioritise IT audits (Bozkus Kahyaoglu & Caliyurt, 2018). Scholars believe that cybersecurity audits now have as fair a chance of being included in the audit work programme

as any other audit area that needs attention (Kearney, 2022; Omotunde & Ahmed, 2023). In addition, current audit work programmes tend to incorporate more consulting audits than in the past (Simić, 2022). Through consulting audits, auditors are given an opportunity to engage with other cybersecurity risk management role players (Simić, 2022).

5.2 Skill shortage

A new skill set is now required by both IT professionals and internal auditors because of the need for cybersecurity risk management (Catal *et al.,* 2023). Kearney (2022) claims that the majority of employees lack technical skills in cybersecurity risk management, and measures for improving this deficit must be taken. Organisations are either training, recruiting or outsourcing cybersecurity talent in response to the lack of internal technical skill (Catal *et al*., 2023; Kearney, 2022). This evolution requires organisations to find the means to recruit and retain competent professionals in cybersecurity risk management.

5.3 Third-party audits

The dependence on third-party controls and processes has risen in recent years. Organisations engage in relationships with third parties to share cybersecurity risks and resources to manage these risks. Cybersecurity risks such as data loss, identity theft and misuse of systems may take place (Arafa *et al.,* 2023). Modern audit work programmes incorporate assessment of third-party processes to assure the board and executive management that cybersecurity processes are secured (Arafa *et al.,* 2023; Gale *et al.,* 2022).

5.4 Continuous auditing

Unlike traditional risks, cybersecurity risks are dynamic and changing consistently (Islam *et al.,* 2018). Conducting risk assessment across organisational processes is no longer a once-off task. Assessments are conducted at a point in time. The automation of business processes has changed the landscape of risks and their behaviour (Islam *et al.,* 2018; Slapničar *et al.,* 2022). Automation warrants auditors to consistently assess the behaviour of the identified risks and the possibility that others could emerge (Sabillon, 2022; Slapničar *et al.,* 2022). Automation and data analytics are on the rise in auditing and cybersecurity.

Automation and analytics methods are incorporated across audit work programmes to strengthen data within all organisations (Sabillon, 2022). The testing of automation practices is increasing due to heavier reliance on automation by organisations (Sabillon, 2022). Audit functions are implementing continuous auditing to flag unwanted activities in the IT environment and encourage adherence to established procedures.

5.5 Cybersecurity governance

The pressure for governance teams to efficiently govern organisational processes is increasing. The board and the audit committee require assurance that governance processes respond to the management of cybersecurity risk (Camilleri *et al.,* 2024; Deloitte, 2021). Assessment of mechanisms to strengthen cybersecurity governance, such as cyber education, policies and procedures, is gaining attention in response to the current threat to the business cybersecurity landscape (Camilleri *et al.,* 2024; Deloitte, 2021).

6. MANAGERIAL IMPLICATIONS

The findings of this study revealed the strategic importance of internal auditing in improving an organisation's cybersecurity risk management efforts. For management, recognising internal audit not only as an assurance provider but also as a strategic partner in cybersecurity is essential. By fostering collaboration between the internal audit function and both IT and risk management teams, organisations can strengthen their defence against cybersecurity threats. Managers should leverage the internal audit function's insights to identify vulnerabilities and support proactive risk mitigation. Furthermore, this study equips industry practitioners with emerging trends and practical insights that can inform decision-making, drive innovation, and improve audit efficiency. Policymakers and management are encouraged to invest in strengthening the internal audit function's capacity to support cybersecurity initiatives, thereby ensuring resilience and competitiveness in an increasingly digital environment.

7. CONCLUSION

This paper aimed to examine the involvement of internal auditing in the cybersecurity risk management of organisations. A non-empirical review of studies for the period 2018 to 2023 was conducted to achieve the aim of the study. A PRISMA flow diagram was utilised for data collection. A thematic qualitative research strategy was used to analyse the data collected and guide the discussion of the study results. The study results revealed that the internal audit function (third line of defence) is crucial for joining forces with the IT function (first line of defence) and risk management function (second line of defence) in the fight against cybersecurity risk. From the assurance perspective, internal auditing conducts an independent examination of organisational cybersecurity risk management processes to assure the board and the audit committee that cybersecurity risk is effectively managed. It conducts a comprehensive cybersecurity risk assessment that helps the organisation identify vulnerabilities within its cybersecurity risk management programme. From the consulting

perspective, internal auditing may be requested by the board and management to assist with specific cybersecurity tasks. Consulting engagements allow internal auditors to focus on strategic matters of the organisation, while building professional relationships with other cybersecurity role players.

It is crucial that policymakers and industry practitioners understand the involvement of internal auditing in cybersecurity risk management. Hence, the internal audit role in cybersecurity risk management is an emerging research area. It is anticipated that industry practitioners can use the results of this study to motivate the need for support from management. Management may also want to better understand the involvement of internal auditing in the cybersecurity risk management dilemma. In addition, emerging trends in auditing of cybersecurity risk were discovered and consolidated in the study results. These trends are crucial for industry internal audit practitioners and policymakers to drive innovation, reduce disruption of risks and maximise the efficiency of internal audits while staying competitive in the market. Therefore, this paper considers its contribution to the existing body of knowledge to include educating both industry internal audit practitioners and policymakers concerning the involvement of internal auditing in cybersecurity risk management. Limitations and considerations for future research are outlined below.

8. RECOMMENDATIONS FOR FUTURE STUDIES

The research concerning the involvement of internal auditing in cybersecurity risk management of the organisation is in its infancy. With respect to future research work, it would be appropriate to conduct a survey on the involvement of internal auditing in cybersecurity risk management to allow for greater accuracy. For example, a survey may consist of understanding the determinants of cybersecurity audit effectiveness within the organisation. Apart from a survey, case studies could be more appropriate for developing a framework for auditing cybersecurity risks, as part of the cybersecurity risk management programme. Undoubtedly, more research work in this area could allow for a greater degree of generalisation and comparative conclusions.

Conflict of interest: The authors declare no conflict of interest with respect to the research, authorship and publication of the article.

Data availability: This article draws extensively from secondary data from various published literature and other sources.

Ethical clearance and informed consent statement: Ethical clearance was neither applicable nor required, as the study is based on a review and synthesis of existing literature and publicly available academic works. No human participants were directly involved.

Funding: The authors did not receive any financial support for research, authorship and publication of the article.

Prior publication: This article represents a substantial reworking (more than 50%) of Mvelo Siyaya, PhD thesis, which is not yet submitted, entitled 'framework for auditing cybersecurity within metropolitan municipalities: The case of eThekwini Municipality, at the School of Accounting, Economics, and Finance, College of Law and Management Studies, University of KwaZulu-Natal, Durban, with Professor M Sibanda (supervisor) and Professor J Dubihlela (co-supervisor).

REFERENCES

Al-Matari, O.M., Helal, I.M., Mazen, S.A. & Elhennawy, S. 2021. Integrated framework for cybersecurity auditing. *Information Security Journal: A Global Perspective,* 30(4):189-204. [https://doi.org/10.1080/19393555.2020.1834649].

Al-Sartawi, A.M.M. 2020. Information technology governance and cybersecurity at the board level. *International Journal of Critical Infrastructures,* 16(2):150-161. [https://doi.org/10.1504/IJCIS.2020.107265].

Alamri, B., Crowley, K. & Richardson, I. 2022. Cybersecurity risk management framework for blockchain identity management systems in Health IoT. *Sensors,* 23(1):1-38. [https://doi.org/10.3390/s23010218].

Alarcón Cotrina, W.E., Delgado Canales, M.E., Gutiérrez Mariño, E.M., Crespo Buquich, D.A. & Ogosi Auqui, J.A. 2023. Computer security and audits as a measure to protect our information. In *Intelligent Sustainable Systems: Selected Papers of World,* S4 2022(2):511-520. Springer. [https://doi.org/10.1007/978-981-19-7663-6_48].

Albalas, T., Modjtahedi, A., & Abdi, R. 2022. Cybersecurity governance: a scoping review. *International Journal of Professional Business Review, 7*(4):01-19. [https://doi.org/10.26668/businessreview/2022.v7i4.e629].

Anderson, U.L., Head, M.J. & Ramamoorti, S. 2017. Internal auditing: Assurance and advisory services. 4th ed. USA: Internal Audit Foundation.

Arafa, A., Sheerah, H.A. & Alsalamah, S. 2023. Emerging digital technologies in Healthcare with a spotlight on cybersecurity: A Narrative Review. *Information,* 14(12):1-15. [https://doi.org/10.3390/info14120640].

Baskerville, R.L., Kim, J. & Stucke, C. 2022. The cybersecurity risk estimation engine: A tool for possibility based risk analysis. *Computers & Security,* 120:102752. [https://doi.org/10.1016/j.cose.2022.102752].

Boeding, M., Boswell, K., Hempel, M., Sharif, H., Lopez Jr, J. & Perumalla, K. 2022. Survey of cybersecurity governance, threats, and countermeasures for the power grid. *Energies,* 15(22):8692. [https://doi.org/10.3390/en15228692].

Bozkus Kahyaoglu, S. & Caliyurt, K. 2018. Cyber security assurance process from the internal audit perspective. *Managerial Auditing Journal,* 33(4):360-376. [https://doi.org/10.1108/MAJ-02-2018-1804].

Brazngi, S.Y.A.A. & Al-Saqa, Z.H.Y. 2023. Internal audit requirements to enhance cybersecurity in economic units in considering the Institute of Internal Auditors (IIA) guidelines. *Tikrit Journal of Administration and Economics Sciences,* 19:(63,2)N94-112. [http://dx.doi.org/10.25130/tjaes.19.63.2.5].

Camilleri, J., Isnoo, V. & Cremona, K. 2024. The role of internal audit in cyber security. [Internet: https://www.pwc.com/mt/en/publications/cybersecurity/the-role-of-internal-audit-in-cyber-security.html; downloaded 22 February 2024].

Catal, C., Ozcan, A., Donmez, E. & Kasif, A. 2023. Analysis of cyber security knowledge gaps based on cyber security body of knowledge. *Education and Information Technologies,* 28(2):1809-1831. [https://doi.org/10.1007/s10639-022-11261-8].

Christ, M.H., Eulerich, M., Krane, R. & Wood, D.A. 2021. New frontiers for internal audit research. *Accounting Perspectives,* 20(4):449-475. [https://doi.org/10.1111/1911-3838.12272].

Clarke, V. & Braun, V. 2017. Thematic analysis. *The Journal of Positive Psychology,* 12(3):297-298. [https://doi.org/10.1080/17439760.2016.1262613].

Culp, S. & Thompson, C. 2016. The convergence of operational risk and cyber security. Accenture & Chartis Research Ltd. [https://asbaweb.net/es/bibl/x-lecturas-recomendadas/1329-la-convergencia-del-riesgo-operacional-y-la-seguridad-cibernetica/file].

Daidj, N. 2022. The digital transformation of auditing and the evolution of the internal audit: Taylor & Francis. [https://doi.org/10.4324/9781003215110].

Davis, R.E. 2021. Auditing information and cyber security governance: A controls-based approach. CRC Press, Taylor & Francis. [https://doi.org/10.1201/9781003099673].

Deloitte. 2021. Cybersecurity and the role of internal audit - an urgent call to action. [Internet: https://www2.deloitte.com/us/en/pages/risk/articles/cybersecurity-internal-audit-role.html; downloaded on 22 February 2024].

Dikokoe, T. 2021. Role of internal audit in managing cyber security risks. South Africa: University of Johannesburg. [https://www.proquest.com/openview/a178a3c484f0611b62963c9b16a733d0/1?pq-origsite=gscholar&cbl=2026366&diss=y].

ERM Academy. 2024. The role of internal audit in strengthening cyber security. [Internet: https://www.erm-academy.org/publication/risk-management-article/role-internal-audit-strengthening-cyber-security/; downloaded on 22 February 2024].

Ford, N. 2024. List of Data Breaches and Cyber Attacks in 2023 – 8,214,886,660 records breached. [Internet: https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-2023#top-data-breach-stats; downloaded on 17 January 2024].

Fowler, J. 2023. 1.5 Billion Records Leaked in Real Estate Wealth Network Data Breach. [Internet: https://www.vpnmentor.com/news/report-realestatewealthnetwork-breach/; downloaded on 17 January 2024].

Gale, M., Bongiovanni, I. & Slapnicar, S. 2022. Governing cybersecurity from the boardroom: challenges, drivers, and ways ahead. *Computers & Security,* 121:102840. [https://doi.org/10.1016/j.cose.2022.102840].

Gunawan, B., Ratmono, B., Kurniasih, D. & Setyoko, P. 2023. Cybersecurity effectiveness: The role of internal auditor certification, risk assessment and senior management. *International Journal of Data and Network Science,* 7(4):1805-1814. [https://doi.org/10.5267/j.ijdns.2023.7.011].

Hepworth, L.R., Greenman, C., Esplin, D. & Johnston, R. 2022. Cybersecurity and data privacy: the rising expectations within internal audit. *Journal of Forensic and Investigative Accounting,* 14(3):454-465.

Holmes, A.E. 2021. Exploring the challenges of the risk management framework implementation for cybersecurity professionals. California: Northcentral University. (DBA-thesis).

Institute of Internal Auditors. 2024. Global internal audit standards. [Internet: https://www.theiia.org/globalassets/site/standards/globalinternalauditstandards_2024january9.pdf; downloaded on 22 February 2024].

Irwin, L. 2023. Criminal Hackers Leak Email Addresses of 220 Million Twitter Users. [Internet: https://www.itgovernance.co.uk/blog/criminal-hackers-leak-email-addresses-of-220-million-twitter-users; downloaded on 17 January 2024].

Islam, M.S., Farah, N. & Stafford, T.F. 2018. Factors associated with security/cybersecurity audit by internal audit function: An international study. *Managerial Auditing Journal,* 33(4):377-409. [https://doi.org/10.1108/MAJ-07-2017-1595]

Kamariotou, M. & Kitsios, F. 2023. Information Systems Strategy and Security Policy: A Conceptual Framework. *Electronics,* 12(2):1-12. [https://doi.org/10.3390/electronics12020382].

Kearney, J. 2022. Top five cybersecurity and IT audit trends that most impact an organization's ability to respond to today's challenges. [internet: https://www.bakertilly.com/insights/top-five-cybersecurity-it-audit-trends; downloaded on 17 January 2024].

Keerthana, E. 2023. Types of Security Controls. [Internet: https://www.infosectrain.com/blog/types-of-security-controls/; downloaded on 22 February 2024].

Khelil, I. & Khlif, H. 2022. Internal auditors' perceptions of their role as assurance providers: a qualitative study in the Tunisian public sector. *Meditari Accountancy Research, 30*(1):121-141. [https://doi.org/10.1108/MEDAR-04-2020-0861].

Kohnke, A., Shoemaker, D. & Sigler, K.E. 2016. The complete guide to cybersecurity risks and controls. CRC Press, Taylor & Francis. [https://doi.org/10.1201/b19631]

Kure, H.I., Islam, S. & Mouratidis, H. 2022. An integrated cyber security risk management framework and risk predication for the critical infrastructure protection. *Neural Computing and Applications,* 34(18):15241-15271. [https://doi.org/10.1007/s00521-022-06959-2].

Lois, P., Drogalas, G., Karagiorgos, A., Thrassou, A. & Vrontis, D. 2021. Internal auditing and cyber security: audit role and procedural contribution. *International Journal of Managerial and Financial Accounting,* 13(1):25-47. [https://doi.org/10.1504/IJMFA.2021.116207].

Malatji, M. 2023. Management of enterprise cyber security: A review of ISO/IEC 27001: 2022. Bangkok: Thailand. (2023 International Conference on Cyber Management and Engineering; 26-27 January). [https://doi.org/10.1109/CyMaEn57228.2023.10051114].

McLean, H. 2024. 2024 Must-Know Cyber Attack Statistics and Trends. [Internet: https://www.embroker.com/blog/cyber-attack-statistics/; downloaded on 17 January 2024].

Moodley, A. 2019. Organisational performance management as a mechanism to improve service delivery in the South African public sector: the contribution of internal auditing as an enabler. Pretoria: University of South Africa. (PhD-thesis).

Mwim, E. N. & Mtsweni, J. 2022. Systematic review of factors that influence the cybersecurity culture. *International Symposium on Human Aspects of Information Security and Assurance*, pp. 147-172. Cham: International Publishing 2022. [https://doi.org/10.1007/978-3-031-12172-2_12].

NIST. 2018. Framework for improving critical infrastructure cybersecurity. [Internet: https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf; downloaded on 25 February 2024].

Noble, H. & Smith, J. 2015. Issues of validity and reliability in qualitative research. *Evidence-based Nursing,* 18(2):34-35. [https://doi.org/10.1136/eb-2015-102054].

Nowell, L.S., Norris, J.M., White, D.E. & Moules, N.J. 2017. Thematic analysis: Striving to meet the trustworthiness criteria. *International Journal of Qualitative Methods,* 16(1):1609406917733847. [https://doi.org/10.1177/1609406917733847]

Okunytė, P. 2023. *KidSecurity's user data compromised after app failed to set password*. [Internet: https://cybernews.com/security/kidsecurity-parental-control-data-leak/; downloaded on 17 January 2024].

Oltsik, J. 2019. Cyber risk management challenges are impacting the business. [Internet: https://www.csoonline.com/article/567049/cyber-risk-management-challenges-are-impacting-the-business.html; downloaded on 25 January 2024].

Omotunde, H. & Ahmed, M. 2023. A comprehensive review of security measures in database systems: Assessing authentication, access control, and beyond. *Mesopotamian Journal of Cybersecurity, 5(3)*15-133. [https://doi.org/10.58496/MJCSC/2023/016].

Oyewumi, H. K., Ayoib, C.-A. B. & Popoola, O.M.J. 2023. Internal auditors without proficiency: a giraffe without a neck. *International Journal of Accounting, Auditing and Performance Evaluation,* 19(1):1-21. [https://doi.org/10.1504/IJAAPE.2023.130526].

Page, M.J., Moher, D., Bossuyt, P.M., Boutron, I., Hoffmann, T.C., Mulrow, C.D. & Brennan, S.E. 2021. PRISMA 2020 explanation and elaboration: updated guidance and exemplars for reporting systematic reviews. *BMJ Journal*, 372:1-36. [https://doi.org/10.1136/bmj.n160].

Palatty, V. 2023. 51 Small Business Cyber Attack Statistics 2023 (And What You Can Do About Them). [Internet: https://www.getastra.com/blog/security-audit/small-business-cyber-attack-statistics/; downloaded on 17 January 2024].

Panetta, K. 2021. Six key takeaways from the Gardner board of directors survey. [Internet: https://www.gartner.com/en/articles/6-key-takeaways-from-the-gartner-board-of-directors-survey; downloaded on 17 January 2024].

Penno, M. 2022. A theory of assurance: Balancing costly formal control with tone at the top. *Management Science,* 68(1):654-668. [https://doi.org/10.1287/mnsc.2020.3861].

Pooja, M. & Damle, M. 2023. Information Security Issues and Challenges: Perspective of Industry 4.0 Paradigm. Uttarakhand: India. (International Conference on Innovative Data Communication Technologies and Application; 14-16 March).

Powell, O. 2023. More than 3.8 billion records exposed in DarkBeam data leak. [Internet: https://www.cshub.com/data/news/darkbeam-data-leak; downloaded on 17 January 2024].

Rosati, P., Gogolin, F. & Lynn, T. 2022. Cyber-security incidents and audit quality. *European Accounting Review,* 31(3):701-728. [https://doi.org/10.1080/09638180.2020.1856162].

Sabillon, R. 2022. Audits in cybersecurity. *Research Anthology on Business Aspects of Cybersecurity*, 1-18. [https://doi.org/10.4018/978-1-6684-3698-1.ch001].

Sawik, T. & Sawik, B. 2022. A rough cut cybersecurity investment using portfolio of security controls with maximum cybersecurity value. *International Journal of Production Research,* 60(21):6556-6572. [https://doi.org/10.1080/00207543.2021.1994166].

Segal, L. 2023. The 10 Biggest Risks And Threats For Businesses In 2023. *Forbes*. [Internet: https://www.forbes.com/sites/edwardsegal/2023/01/01/the-10-biggest-risks-and-threats-for-businesses-in-2023/?sh=49d2cc8830c0; downloaded on 18 January 2024].

Shaikh, F.A. & Siponen, M. 2023. Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity. *Computers & Security,* 124:102974. [https://doi.org/10.1016/j.cose.2022.102974].

Simić, N. 2022. The Internal Auditor's Role in Cybersecurity Governance: A qualitative study about the internal auditor's influence on the people factor of cybersecurity. Uppsala University. (MBA-thesis).

Siyaya, M.C., Epizitone, A., Jali, L.F. & Olugbara, O.O. 2021. Determinants of internal auditing effectiveness in a Public Higher Education Institution. *Academy of Accounting and Financial Studies Journal,* 25(2):1-18.

Slapničar, S., Vuko, T., Čular, M. & Drašček, M. 2022. Effectiveness of cybersecurity audit. *International Journal of Accounting Information Systems,* 44:100548. [https://doi.org/10.1016/j.accinf.2021.100548].

Snyder, H. 2019. Literature review as a research methodology: An overview and guidelines. *Journal of Business Research,* 104:333-339. [https://doi.org/10.1016/j.jbusres.2019.07.039].

Statista. 2023. Distribution of cyber attacks across worldwide industries in 2022. [Internet: https://www.statista.com/statistics/1315805/cyber-attacks-top-industries-worldwide/; downloaded on 18 January 2024].

The Times of India. 2023. Government probing 'data breach' of 8 crore Indians from ICMR Covid site. [Internet: https://timesofindia.indiatimes.com/india/government-probing-data-breach-of-8-crore-indians-from-icmr-covid-site/articleshow/104835828.cms; downloaded on 17 January 2024].

Todorović, Z., Todorović, B. & Tomaš, D. 2020. The role of internal audit in the fight against cyber crime. *EMC Review-Economy and Market Communication Review* 20(2):514-529. [https://doi.org/10.7251/EMC2002514T].

Usman, A., Che-Ahmad, A. & Abdulmalik, S.O. 2023. The role of internal auditors characteristics in cybersecurity risk assessment in financial-based business organisations: A Conceptual Review. *International Journal of Professional Business Review,* 8(8):1-31. [https://doi.org/10.26668/businessreview/2023.v8i8.2922].