The Quality of Cybersecurity Audits: Do Synergies among the Chief Audit Executive, IT Governance, and Internal Audit Functions Matter?

Dr Abdulaziz Alzeban
Professor in Accounting
Business Department, Applied College, King Abdulaziz University, Jeddah, Saudi Arabia
Email: aalthebyan@kau.edu.sa

Dr Krayyem Al-Hajaya
Associate Professor in Accounting
Mu'tah University
(7) 610170 Mutah, Karak,
Jordan

Email: hajaya@mutah.edu.jo

Dr Nedal Sawan
Associate Professor in Accounting & Finance
Liverpool Business School
Redmonds Building, Brownlow Hill,
Liverpool, UK
L3 5UG
Tell: 01512314743
Email: N.I.Sawan@ljmu.ac.uk

Houda CHAMMAA
Faculty of Economics, Law and Social Sciences
Cadi Ayyad University, Marrakech, Morocco
Email: h.chammaa@uca.ac.ma

Dr Scott Foster
Liverpool Business School
Faculty of Business and Law
/LJMU/ Liverpool/UK- Redmonds Building, Brownlow Hill, Liverpool, UK
L3 5UG
Email: S.Foster@ljmu.ac.uk

Purpose: This study investigates how the internal audit function helps boost an organisation's cybersecurity quality. We focus on the key roles played by the chief audit executive (CAE) competencies in terms of their IT expertise, qualifications and tenure, their interaction with the audit committee (AC), the organisation's IT governance structure, and the role of internal audit (IA) in overseeing cybersecurity.
Methodology and design: Data was collected via a survey questionnaire distributed to internal auditors and audit committee members in UK-listed companies, supplemented by relevant archival data where appropriate.
Findings: Panel regression findings, validated across both CEAs and AC members, reveal that CAE IT expertise, private CAE-AC meetings, and robust IT governance significantly improve cybersecurity quality. Crucially, each additional year of IT audit expertise increases perceived cybersecurity quality by approximately 0.30 units, confirming the high value of deep IT audit expertise. Additionally, IA's role in policy review, regulatory compliance, and risk assessment strengthens cyber resilience.
Originality and value: The study makes an original contribution to the literature by examining how synergies among the CAE's IT competencies, interaction with the audit committee, IT governance, and internal audit functions shape the quality of cybersecurity audits.
Practical implications: The findings carry important practical implications for organisations, regulators, and society. Strengthening IT competencies within internal audit, fostering private dialogue between CAEs and audit committees, and embedding cybersecurity into corporate governance frameworks can significantly improve resilience. Beyond organisational benefits, enhanced cybersecurity audit quality supports consumer protection, safeguards privacy and reinforces public trust in digital infrastructures such as healthcare, banking, and government services, aligning with global standards like the General Data Protection Regulation (GDPR) and the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

Keywords: Internal audit, cybersecurity quality, chief audit executive competences, audit committee, IT governance.

1. Introduction

In the ever-increasingly complicated digital environment, even the threat of cybersecurity has progressively become sophisticated and costly, leveraging attacks on critical organisational infrastructures (Houlden et al., 2023; Al-Shaer et al., 2025). Recent estimates suggest that the global cost of cybercrime could exceed US$ 12 trillion in 2025, driven largely by the increasing sophistication of attacks powered by artificial intelligence and other emerging technologies (Computer Crime Research Center, 2024, as cited in Nairametrics, 2024). Thus, as digitization increasingly becoming an integral part of most processes within organisations, the need for cybersecurity grew exponentially. However, while a lot of faith has been placed in technology-based defences, it is evident that relying on them alone is both questionable and often unreliable (Brenner, 2020; Anderson, 2015). Hence, Effective protection against evolving cyber risks requires organisations to adopt holistic strategies that integrate robust internal audit functions, ensuring that governance, oversight and assurance mechanisms that complement technological safeguards (Vuko et al., 2025; Slapnicar et al., 2022; Wahhab et al., 2022).

Internal audit, once purely seen as a control instrument from the point of view of financial control, has now been transformed into one of the most crucial arms of cybersecurity strategy, which emanating mainly from assessment and evaluation of risks and controls to the assurance

of compliance with cybersecurity principles (Anderson, 2015; Slapnicar et al., 2022; Wahhab et al., 2022; Houlden et al., 2023; Vuko et al., 2025; Al-Shaer et al., 2025). However, despite such transformation, the changing role of the CAE and his competencies, with specific reference to IT expertise, qualifications and tenure, in addition to his relationship with audit committee, have received limited attention in the cybersecurity audit landscape. The ability of internal audits to successfully improve cybersecurity often hinges on the competence of CAE in terms of technical knowledge and experience, as well as their interaction with audit committees (IIA, 2016; Young and Wang, 2014; Sabillon et al., 2017; Islam et al., 2018; Steinbart et al., 2018; Vuko et al., 2025; Al-Shaer et al., 2025). Additionally, the internal audit engagement in regular review of the level of adherence to policies and regulations, the readiness of resources to address cyber risks (Sabillon et al., 2017; Rosati et al., 2019), and its synergy with broader IT corporate governance (Brenner, 2020; Anderson, 2015; Wahhab et al., 2022; Vuko et al., 2025; Cyfert et al., 2025) are all considered vital in enhancing cybersecurity quality.

Although such factors are expected to bear significantly on the quality of cybersecurity audits, the literature has, until now, underexplored the influence of interaction of all aforementioned factors. In this paper, we seek to fill this void by investigating how the internal audit (IA) quality in terms of IT competency of CAE, tenure, and relationships with audit committees, review of cybersecurity polices and regulations, readiness of resources, and IT CG, would affect the quality of cybersecurity audits. By examining these factors, this study seeks to contribute to the growing body of literature on internal audit and cybersecurity with insight into how companies can more effectively protect themselves from the threat of cyber-attacks through better audits and internal control. Four key research questions which this study attempts to answer are as follows:

RQ1: To what extent do the competencies of CAE in terms of IT audit experience, qualifications, and tenure impact on quality cybersecurity audits?

RQ2: Do private meetings between CAE and audit committee improve the quality of cybersecurity audits?

RQ3: Does IT corporate governance affect the quality of cybersecurity audits?

RQ4: To what extent does IA functionality, in terms of reviewing cybersecurity policies and regulation, and readiness of resources, enhances the quality of cybersecurity audits?

Answering these specific questions thus fills an important gap in the existing literature but also offers practical implications to companies that strive to improve cybersecurity through internal audits. The findings highlight that the involvement of IA in assessing cybersecurity readiness and IT governance are key drivers of the quality of cybersecurity. Particularly, proactive involvement in cybersecurity readiness, review of governance policies, and assurance of regulatory compliance all significantly improve quality of cybersecurity, with readiness having the strongest effect. In addition, private meetings between CAEs and audit committees further support cybersecurity, and competencies (experience in the field of IT and professional qualifications) significantly impact the quality of cybersecurity.

The findings of this study carry significant practical implications at multiple levels. For organisations, they highlight the importance of strengthening CAE IT competencies, encouraging private communication channels with audit committees, and embedding cybersecurity into broader governance and risk management structures. These measures not only enhance internal resilience but also enable more strategic allocation of resources and proactive threat mitigation. For regulators and policymakers, the study underscores the value of establishing clear and enforceable frameworks that align internal audit practices with international standards such as the General Data Protection Regulation (GDPR) and the

National Institute of Standards and Technology (NIST) Cybersecurity Framework, thereby ensuring consistency across industries and jurisdictions. At the societal level, improved cybersecurity audit quality directly contributes to protecting consumers' personal data, safeguarding privacy, and preserving public trust in digital systems that underpin critical sectors such as healthcare, banking, and government. By reducing the likelihood and severity of data breaches, organisations strengthen their accountability to stakeholders and help build a more secure digital ecosystem. Collectively, these implications position internal audit not only as a technical safeguard but also as a strategic and ethical pillar in advancing organisational resilience and societal trust in the digital era.

The remainder of this paper is structured as follows. **Section 2** provides a comprehensive literature review and develops the study's hypotheses by drawing on relevant theoretical and empirical insights. **Section 3** outlines the research methodology, including sampling, the data collection process and measurement of variables. **Section 4** presents and discusses the empirical findings, highlighting both the statistical results and their interpretation in the context of prior studies. Finally, **Section 5** concludes the study by summarizing the key findings, outlining practical implications, and discussing limitations alongside avenues for future research.

2. Literature review and hypotheses development

2.1. Internal audit and cybersecurity

In today's digital age, the surge in cyber risks calls for strong and proactive measures to protect corporate infrastructures. Internal audit has progressed from its traditional role of financial scrutiny and oversight to becoming a key player in cybersecurity strategies (Al-Shaer et al., 2025). IA functions now encompass risk evaluation, assessment of control effectiveness, and compliance oversight; all of which are crucial in enhancing companies' ability to combat cyber threats (Islam et al., 2018; Jamison et al., 2018). Therefore, internal audits offer recommendations to improve cybersecurity frameworks and address critical protection gaps. However, the degree to which IA can successfully mitigate cybersecurity risks is still up for debate. While many scholars promote an expanded role for IA in cybersecurity, others question whether internal auditors possess the technical and IT skills required to manage these risks effectively. For example, Anderson (2015) and Slapnicar et al. (2022) question whether internal auditors, who are typically focused on compliance, can adequately tackle the complex and changing nature of cybersecurity threats. This raises concerns about whether internal auditors are prepared to handle simultaneously cybersecurity audits in addition to financial and internal control oversight without creating bureaucratic obstacles that could hinder the fast-response and implementation of essential cybersecurity measures.

Despite these concerns, various studies highlight the importance of integrating IA into cybersecurity efforts. IIARF (2015), for instance, emphasizes that internal audits are crucial in fostering organisation-wide readiness for cyber threats. A well-trained and adequately resourced IA function can provide oversight, identify system vulnerabilities, and suggest strategies to close system gaps and bolster corporate defences. Chambers (IIARF, 2015) refers to this as the "home-house advantage," noting that internal auditors are uniquely positioned to work closely with IT and cybersecurity teams to enhance security. Furthermore, studies by Islam et al. (2018) and Steinbart et al. (2014) argue that IA competencies, such as technical IT skills and a strong capacity for risk assessment, are essential for conducting effective cybersecurity audits. These skills allow internal auditors to assess cybersecurity controls and policies more thoroughly, thus improving overall protection and security. Steinbart et al. (2014) also stress the role of audit committees in ensuring that cybersecurity risks are addressed at the highest managerial levels. Conversely, critics such as Wahhab et al. (2022) and Houlden et al. (2023) argue that the gap between cybersecurity requirements and internal auditors' technical capabilities remains a

significant barrier. They contend that cybersecurity is so complex that it demands specialized knowledge that internal auditors often lack. As a result, over-reliance on internal audits for cybersecurity may create a false sense of security, leading companies to overlook more immediate and technical threats. In this regard, Slapnicar et al. (2022) warn that IA's focus on compliance could lead to a false sense of security, with organisations believing they are protected when they remain vulnerable to advanced cyberattacks.

This divergence in viewpoints highlights the need for a balanced approach to IA's role in cybersecurity. While internal audits can enhance organisation preparedness and resilience by identifying weaknesses and ensuring compliance, there is also a risk that audits may focus too heavily on procedural matters and neglect the technical depth required to address cybersecurity threats effectively. Several scholars, including Gatzert and Schmit (2016) Brenner, (2020); Anderson et al., 2024; Wahhab et al., 2022; Vuko et al., 2025; Cyfert et al. 2025, emphasize that internal audits should not be viewed as a cure-all for cybersecurity risks but rather as part of a broader and integrated approach. Internal audits provide substantial value by offering independent assessments and facilitating discussions on cybersecurity strategies. However, this value depends on the auditors' ability to navigate the complexities of cybersecurity, which necessitates ongoing training and collaboration with IT specialists.

While the above discussion elaborate on the impact of the IA on the quality of cybersecurity audit, the effectiveness of the IA function itself remains a central factor. IA effectiveness reflects the ability of the audit function to achieve its objectives, supported by adequate resources, auditor independence, technical competence, and strong relationships with stakeholders. According to Turetken et al., (2020), IA effecrtivness is shaped by both organisational and auditor-level factors, including independence, professional competence, and support from top management. Similarly, Abdelrahim and Al-Malkawi (2022) propose a conceptual model in which organisational support and auditor expertise significantly enhance audit effectiveness. Integrating IA effectiveness into the cybersecurity domain provides a broader explanatory framework, suggesting that CAE competencies, tenure, IT governance, policy reviews, and private meetings all exert their influence through their contribution to overall audit effectiveness. This positions IA effectiveness as both an outcome of these determinants and a mechanism through which audit functions contribute to cybersecurity quality.

2.2. CAE IT Competencies and cybersecurity

CAE expertise in IT audit and information systems is becoming increasingly essential for strengthening an organisation's cybersecurity defences. As cyber threats grow in complexity, auditors need a deep understanding of IT systems to effectively spot vulnerabilities, assess cybersecurity risks and recommend strong controls. Without this specialized IT knowledge, internal audits may lack meaningful insights into the company's cybersecurity defences, leaving the organisation vulnerable to evolving threats (Wahhab et al., 2022; Vuko et al., 2025). Studies suggest that internal auditors with high IT competences had a major effect on the organisation's cybersecurity level. For example, Islam et al. (2018) and Slapnicar et al. (2022) argue that auditors with IT competence have a competitive advantage in being able to control the safekeeping of the cyber-defence function and monitor that it remains resilient and updated. Steinbart et al. (2018) echo this sentiment, in that auditors who have the information on the measured attributes can conduct more detailed risk assessments and suggest targeted improvements, which enhance the organisation's ability to prevent cyberattacks.In the same vein, Cyfert et al. (2025) point out that digital transformation cannot succeed without good digital competencies, including cybersecurity, cloud computing, data management and robotic process automation. These technical skills are critical for ensuring organisational resilience

against cyber threats. Anderson et al. (2024) argue also that competencies in cybersecurity leadership extend beyond purely technical knowledge.

Industry standards also reinforce the importance of IT skills for internal auditors. Certifications like the Certified Information Systems Auditor (CISA) are recognised as a key measure of an auditor's ability to handle complex cybersecurity challenges. According to the Institute of Internal Auditors (IIA, 2016), certified auditors are better prepared to anticipate emerging cyber threats and implement best practices, which is critical for maintaining strong cybersecurity defences. These certifications not only reflect technical capabilities but also ensure ongoing education in the latest cybersecurity trends. However, while IT skills are widely seen as important, some scholars argue that technical expertise alone may not be enough. Sabillon et al. (2017) and Cyfert et al. (2025) suggest that internal auditors also need strong governance skills to ensure that cybersecurity policies align with broader organisational goals. Their research generally shows that auditors who are well-versed in IT governance can better evaluate cybersecurity strategies, helping organisations take a more proactive approach to managing cyber risks. This broader governance perspective ensures that cybersecurity is integrated into the overall risk management framework, rather than being treated as a standalone technical issue.

Despite these findings, there's still a gap in the literature concerning how various competencies interact to improve cybersecurity outcomes. For instance, while IT skills and certifications are critical, there's less understanding of how these abilities impact an ACE engagement with key stakeholders, such as senior management and IT teams. This interaction is fundamental because effective communication between auditors and decision-makers ensures that cybersecurity measures are prioritised and swiftly implemented. Recent studies by Wahhab et al. (2022) and Houlden et al. (2023) stress that the fast-changing nature of cyber threats means auditors must continually update their skills. They emphasize the need for ongoing professional development, especially in emerging technologies such as artificial intelligence and blockchain, which are reshaping cybersecurity. As these technologies become more embedded in business operations, CAE must be prepared to assess the associated risks and recommend suitable security measures. Therefore, the following hypothesis can be formulated:

H1: CAE competencies in IT audit are positively associated with the quality of cybersecurity.

2.3. CAE Tenure and Cybersecurity

The length of time a chief executive auditors (CAEs) serves in their role can impact how well an organisation protects itself against cyber threats (Anderson et al., 2024). CAEs with longer tenures have more time to gain a deeper understanding of the organisation's specific challenges, its risk landscape, and the rapidly changing digital environment. This accumulated knowledge enables experienced CAEs to make more informed decisions and provide stronger strategic advice on cybersecurity matters. Empirical studies suggest that the tenure of the CAE positively influences their capacity to detect potential cybersecurity vulnerabilities and to align security strategies with the organisation's overarching objectives (Brenner, 2020; Anderson, 2015). Experienced CAEs are often better at spotting gaps in cybersecurity measures and recommending effective improvements. Brenner (2020) notes that seasoned CAEs have a deep familiarity with both the organisation's technical infrastructure and its long-term objectives, which allows them to create cybersecurity plans that support not only immediate needs but also the organisation's overall vision. This alignment ensures that cybersecurity initiatives address current threats while also advancing the organisation's strategic goals. Anderson et al. (2024) further reinforce the strategic advantage of accumulated tenure in developing tailored cybersecurity frameworks.

Moreover, CAEs who have been in their roles for an extended period tend to build strong relationships with key stakeholders, such as the board of directors and audit committees. These relationships are critical for keeping cybersecurity a top priority within the organisation. Anderson et al. (2024) confirm that such relationships of the leadership enhance cross-functional cybersecurity coordination. This might create trust between the CAE and stakeholders, which fosters more open discussions about cybersecurity vulnerabilities, leading to quicker decisions and faster responses to emerging threats (Anderson, 2015). This close collaboration also helps ensure that cybersecurity measures are implemented and further continuously refined to meet different forms of cyber risks.

However, the potential downsides of long CAE tenures should not be ignored. While experience is valuable, longer tenures can also result in complacency. CAEs may become normalized and too comfortable in their routinized roles, potentially overlooking new and emerging threats by relying on familiar practices. Scholars like Wahhab et al. (2022) warn that long-tenured CAEs must remain proactive, continuously updating their knowledge of the latest cybersecurity trends and challenges. Staying informed about developments such as artificial intelligence, machine learning and blockchain is indispensable to keeping cybersecurity strategies effective and up to date. Striking a balance between experience and continuous learning is crucial for ensuring that long-tenured CAEs can lead effectively in the cybersecurity space. While their experience helps them navigate the organisation's complex risk environment, ongoing education ensures they can stay responsive to the fast-changing nature of cyber threats. Scholars such as Houlden et al. (2023) suggest that organisations should encourage CAEs to participate in professional development programs focused on emerging technologies and cybersecurity trends, thereby reducing the risk of complacency.

Accordingly, CAEs with longer tenures have accumulated more organisational knowledge, making them better equipped to assess cybersecurity risks and implement effective defences. However, it also considers the importance of continuous learning to avoid complacency and ensure that cybersecurity measures stay adaptable to new threats (Brenner, 2020; Anderson, 2015; Wahhab et al., 2022; Anderson et al., 2024). As CAEs strengthen their relationships with the board and audit committees, their ability to influence cybersecurity decisions grows, resulting in more comprehensive and effective cybersecurity strategies. Hence, we can hypothesize:

H2: CAE tenure is positively associated with a higher quality of cybersecurity.

2.4. IT Corporate Governance and Cybersecurity

IT corporate governance is a key in improving an organisation's ability to manage cybersecurity risks. Well-designed governance mechanisms, such as board-level oversight, comprehensive policies, and effective risk management practices, create a strong foundation for addressing cybersecurity challenges (Cyfert et al., 2025; Kamiya et al., 2021). Sabillon et al. (2017) argue that effective IT governance frameworks allow organisations to proactively prepare for and mitigate cyber threats through coordinated and strategic efforts. By integrating cybersecurity into the broader governance structure, IT corporate governance strengthens the organisation's ability to identify, assess, and respond to potential cyber risks. Recent studies have further reinforced the link between corporate governance and cybersecurity by demonstrating its strategic and economic impact. For instance, Cyfert (2025) show that organisations with strong cybersecurity governance benefit from higher corporate market value, primarily due to increased investor trust and supply chain confidence. Their findings emphasizes that cybersecurity, when embedded within broader governance mechanisms, contributes to long-term value creation and reputational strength. Similarly, Cortez and Dekker (2022) sheds light on the presence of cybersecurity expertise within boards significantly enhances the quality of

cybersecurity oversight and disclosure. These findings suggest that governance structures must evolve to include technological competence at the highest level of decision-making.

The involvement of the board of directors in managing cybersecurity risks is particularly emphasized in the literature. Rothrock et al. (2018) assert that active board engagement is vital for building strong cybersecurity frameworks. They argue that when boards are directly involved in overseeing cybersecurity strategies, organisations are better equipped to prioritise cybersecurity at the highest levels of decision-making. This ensures that cybersecurity aligns with the organisation's long-term objectives and that sufficient resources are allocated to maintain strong defences against different types of cyber threats. Similarly, Islam et al. (2018) stress the importance of board-level support for IT corporate governance, claiming that proactive board engagement reduces security risks by ensuring that cybersecurity measures are constantly monitored and updated. Building on this perspective, Al-Shaer et a. (2025) argue that cybersecurity should be treated as a strategic and ethical concern rather than a purely technical matter. Their empirical study shows that powerful CEOs and effective audit committees strengthen oversight of cybersecurity risk management, thereby reinforcing the governance dimension of cyber resilience. This evidence supports the view that IT corporate governance must extend beyond structural mechanisms to include leadership dynamics and board-level engagement in shaping cybersecurity outcomes. This aligns with findings from Radu and Smaili (2022), who demonstrate that board diversity and engagement positively influence cybersecurity transparency and preparedness. Moreover, Kamiya et al. (2021) argue that risk management and governance quality directly affect a firm's reputation after a cyberattack, emphasizing the idea that governance is not only preventative but also plays a crucial role in post-crisis resilience.

While prior studies show that strong governance practices can significantly support better cybersecurity outcomes, with board oversight playing a key role in implementing effective strategies for cybersecurity, some scholars, however, argue that IT corporate governance alone may not be enough to manage cybersecurity effectively. Haislip et al. (2017) caution against overreliance on governance frameworks, suggesting that such structures can create a false sense of security. They believe that while governance provides valuable oversight, it may lack the specialized focus necessary to address the technical complexities of cybersecurity. Organisations that depend solely on governance without incorporating specialized cybersecurity measures may become complacent, leaving themselves vulnerable to sophisticated cyberattacks. Rosati et al. (2019) also echo these concerns, criticizing the generic nature of many IT corporate governance frameworks. They argue that while governance provides broad oversight, it often fails to address the specific challenges posed by cybersecurity. Cyber threats are dynamic and complex, requiring tailored approaches that go beyond standard governance practices. According to Rosati et al. (2019) effective cybersecurity management demands customized strategies that address the unique risks organisations face in today's digital world. Adiloglu and Gungor (2019) also bring to light concerns about the agility of IT corporate governance in responding to emerging cybersecurity threats. They argue that governance structures can be slow to adapt to the fast-paced and constantly evolving nature of cyber risks, potentially leading to vulnerabilities. Their research suggests that more dynamic and responsive governance practices are needed to ensure organisations can quickly adapt to new risks and implement timely cybersecurity measures. Without such flexibility, even well-governed organisations may struggle to keep up with continuously emergent and changing cyber-attacks.

Thus, while strong IT corporate governance and active board involvement are essential for improving cybersecurity, relying solely on governance frameworks has limitations. The complexity and ever-changing nature of cyber threats require more specialized and flexible approaches to cybersecurity management. Organisations need to balance leveraging

governance structures for oversight with incorporating technical expertise and adaptable strategies to ensure resilience against advanced cyberattacks. Based on the above discussion, the hypothesis can presented as follows:

H3: The quality of cybersecurity is positively associated with strong IT corporate governance.

2.5. Role of IA in reviewing policies, regulations and readiness of cybersecurity

Internal audit plays an increasingly strategic role in reinforcing cybersecurity quality by conducting independent assessments of governance frameworks, ensuring compliance with evolving regulations, and evaluating organisational preparedness for cyber threats. Recent academic literature (Al-Shaer et al., 2025; Elmaasrawy & Tawfik, 2025; Adesokan-Imran (2025); Alhawtmeh, 2025) provides compelling evidence that effective internal auditing enhances cybersecurity resilience across these three core pillars.

2.5.1 Governance Policy Reviews

Internal auditors are key players in assessing whether cybersecurity governance structures are robust, up-to-date, and effectively implemented. According to Babiker (2025), internal audit functions that frequently review governance frameworks contribute to better-defined cybersecurity strategies, clearer risk ownership, and more structured incident escalation protocols. Alhawtmeh (2025) further demonstrates that organisations with proactive internal audit teams exhibit stronger information security governance maturity and reduced risk exposure. These evaluations help ensure that cybersecurity is not treated as a purely technical issue but is embedded within the broader organisational governance design. Internal audit also ensures that these governance mechanisms remain aligned with international standards and are capable of addressing dynamic threat environments.

2.5.2 Ensuring Regulatory Compliance

The regulatory landscape surrounding cybersecurity is becoming increasingly complex, with organisations facing obligations under laws such as the GDPR, NIST guidelines, and sector-specific standards. Internal audit plays a crucial role in helping organisations navigate this complexity. Adesokan-Imran (2025) note that internal auditors help implement compliance frameworks by conducting thorough audits of internal controls, vendor agreements, and operational practices. These efforts do more than ensure legal conformity; they further elevate security maturity and enhance stakeholder confidence. Moreover, audit-driven compliance reviews lead to more consistent application of security measures across departments and third-party interfaces, reducing potential gaps in the organisation's cyber-defence systems.

5.2.3 Assessing Cyber Readiness and Resilience

Beyond policy and compliance, IA evaluates whether the organisation is adequately prepared to detect, respond to, and recover from cyber incidents. This includes reviewing business continuity plans, incident response protocols and conducting scenario-based simulations. Elmaasrawy and Tawfik (2024) found that the dual assurance and advisory roles of IA lead to improved organisational, human and technical preparedness. Their findings underline the importance of IA in building a culture of proactive cyber risk management. Alhawtmeh (2025) adds that organisations with mature internal audit functions demonstrate stronger response coordination during cyber crises and tend to report fewer severe disruptions. These benefits have even been reflected in lower cyber insurance premiums, which serve as external indicators of reduced organisational cyber risk.

The convergence of findings from these recent studies supports the development of a new hypothesis and sub-hypotheses as follows:

H4: The involvement of IA in cybersecurity leads to higher quality of cybersecurity, and the following sub-hypotheses are proposed:

- ***H4a:*** When IA reviews the organisation's governance policies and procedures, the quality of cybersecurity is more likely to be higher.
- ***H4b:*** When IA ensures that cybersecurity regulations are met, the quality of cybersecurity is more likely to be higher.
- ***H4c:*** The involvement of IA in assessing cybersecurity readiness leads to higher quality of cybersecurity.

2.6. Private meetings between the audit committee and CAE and cybersecurity

Private meetings between the audit committee (AC) and the CAE are critical for fostering a confidential environment where sensitive issues, including cybersecurity, can be discussed openly and in depth (Young and Wang, 2014). These meetings provide a platform for candid discussions that might not occur in a more formal board meeting setting. By enabling direct communication, private meetings allow for a thorough exploration of cybersecurity weaknesses and the strategies needed to address them. Scholars like Bissell (2013) point out that private meetings between the AC and the CAE promote transparency and trust, two essential components for effectively tackling complex cybersecurity concerns. In these private settings, the CAE has the freedom to speak more openly, which leads to a more accurate and detailed presentation of the organisation's cybersecurity status. Bissell (2013) argues that this setting is especially valuable because it gives the CAE the opportunity to raise concerns that might otherwise be downplayed or overlooked in larger meetings. This direct line of communication ensures that potential cybersecurity risks are examined thoroughly, and tailored solutions are discussed. In response, the AC can offer appropriate guidance, helping to ensure that cybersecurity strategies are in line with the organisation's overall priorities. Private meetings also enhance the organisation's cybersecurity quality by allowing the CAE to provide detailed updates on the state of the organisation's defences. KPMG (2015) concluded that these interactions give the AC deeper insights into the organisation's cybersecurity risks, which leads to better-informed decision-making.

Recent literature underscores the importance of open and frequent communication between the audit committee and the CAE. According to the Institute of Internal Auditors (IIA, 2024), private exchanges enhance trust, independence, and the quality of oversight, especially in areas involving fast-evolving threats like cybersecurity. The updated Global Internal Audit Standards emphasize that informal and private conversations are essential to maintaining a robust relationship between internal audit and key stakeholders (IIA, 2024). Such meetings enable the CAE to present an honest and nuanced view of the organisation's cybersecurity posture. Islam (2018) argue that direct communication with the AC allows the CAE to voice concerns that might otherwise be filtered or downplayed, facilitating more accurate risk assessments and tailored remediation plans. This improves the quality of oversight by encouraging the audit committee to allocate resources and guide strategy based on informed insights.

Accordingly, Regular and private consultations between the AC and the CAE are crucial to maintaining cybersecurity as a top priority and ensuring that the necessary resources are allocated to protect the organisation's information systems (Lanz, 2014). Private meetings also strengthen cybersecurity by enabling strategic alignment between the AC and the CAE. Vuko et al. (2025) highlight that these interactions promote informed decision-making and the prioritisation of cybersecurity investments. When audit committees are engaged in these dialogues, they are better positioned to ensure that cybersecurity strategies are not only reactive but also resilient and proactive. Furthermore, Haislip et al. (2017) emphasizes the importance

of empowering the CAE to report cyber risks independently and directly to the board. His empirical study demonstrates that organisations where the CAE has such access tend to have significantly better cybersecurity preparedness. In these cases, internal audit plays a crucial role in early warning and systemic risk identification. The meetings also facilitate multi-stakeholder coordination. Vuko et al. (2025) stress that internal audit effectiveness, and its collaboration with the first and second lines of defence, correlates positively with improved cyber controls. Private dialogues serve as a bridge between operational risk management and board-level oversight.

Based on the above discussion, the following hypothesis is posited:

H5: Private meetings between the audit committee and the CAE are positively associated with higher quality of cybersecurity.

3. Research Method

To achieve the objectives of the study, data were gathered from two surveys. Both surveys were used to obtain information related to IA and cybersecurity. Such information is typically not disclosed in annual reports; therefore, the survey serves as a key source for obtaining data related to IA and the study's variables. First survey was directed to CAE in the UK-listed companies, and the second survey was directed to AC. First section of the survey was related to general background including some demographic data pertaining to the respondent, the staff within the IA department, the resources allocated to IA, private meetings between CAE and AC. Second section covers cybersecurity. And the third section covers IT governance, policies, regulations, and readiness of cybersecurity. Fourth section covers IA role and IA annual plan. Survey directed to the ACs is slightly different than the one directed to CAEs in terms of the scales used to measure IA competencies and IA resources, whereas measures of other variables remain the same (i.e. private meetings between CAE and AC, cybersecurity, IT governance, policies, regulations, readiness of cybersecurity, IA role and annual plan). Regarding competencies, participants were asked to give their perceptions of the level of CAE experience in the field of IT audit and internal audit using scale of 7 points. Participants were also asked to give their perceptions of the level of sufficiency of IA resources in terms of number of staff and annual budget allocated to IA department, using scale of 7 points (1 = not sufficient, and 7 = totally sufficient).[1]

Company contact details were sourced from the London Stock Exchange and official corporate websites. The survey was distributed to CAEs across all listed UK companies – approximately 1,538 in total. Companies lacking valid contact information were excluded from the sample.[2]

---

[1] To ensure the validity and reliability of the survey instrument, several procedures and tests were conducted. Initially, a pre-test was carried out to confirm that the questionnaire was clear and comprehensible to the target respondents, thereby supporting its validity. Content validity was established by consulting experts in the field – who reviewed the instrument and provided feedback – leading to targeted modifications. These adjustments focused on areas such as cybersecurity, IT governance, policies, regulations, cybersecurity readiness, the role of internal audit, and the annual audit plan. Construct validity was addressed by carefully designing the survey to ensure that each question effectively measured its intended construct. Consistent with best practices in the literature, questions were formulated using straightforward language to encourage participation. The pre-test results confirmed that the wording was sufficiently simple, the questions followed a logical sequence, and the overall survey length was appropriate – all contributing to strong construct validity. Regarding reliability, internal consistency was assessed using Cronbach's alpha. The results indicated high reliability, with scores of 0.82 for the cybersecurity-related items and 0.86 for the IT governance items.

[2] The survey targeted two key corporate governance actors: the CAEs and ACs. Initially, invitations were sent to 1,538 UK-incorporated companies listed on the London Stock Exchange, where the internal audit function is either established formally or integrated (if any) within risk and compliance structures. For the ACs segment, the sample was refined to 1,207 companies. This adjustment was necessary due to the absence of publicly available or

The first online survey was conducted in November 2023 and from which 512 responses were received from CAEs and 345 from AC members. A follow-up request was sent out in January 2024 which generated a further 31 responses from CAEs, making a total of 543 CAE surveys, and 16 additional responses AC members, creating a total of 361 responses from AC members. [3] Additional data were obtained from responding companies' annual reports as sources of information relating to the other variables included in the study such as data related to AC. [4]

The survey instrument underwent a two-step validation process. First, the questionnaire was reviewed by a panel of three experts with academic and professional expertise in IA and cybersecurity to ensure content validity, clarity, and alignment with the study's objectives. Based on their feedback, several items were revised for clarity. Second, a pilot test was conducted with 12 internal auditors from UK-listed firms to assess the clarity and face validity of the survey items. Minor adjustments were made following this pilot.

To address potential non-response bias, we compared early and late respondents on key variables (e.g., policies, IT governance scores), and found no statistically significant differences, suggesting limited response bias. In addition, follow-up reminders were issued to enhance participation.

3.1. Model and variables measures

The following regression model is developed to test the hypotheses of the study, which include test variables and control variables.

$$CYBER\text{-}SEC = b_0 + b_1 IACOMP + b_2 ITGOV + b_3 TENURE + b_4 AC\text{-}CAE + b_5 POLICIES + b_6 REGULATIONS + b_7 RESOURCES + b_8 ACINDEP + b_9 ACEXP + b_{10} READINESS + b_{11} IAROLE + b_{12} PLAN + Industry + Year + \varepsilon \quad (1)$$

The dependent variable is cybersecurity (CYBER-SEC). CYBER-SEC is measured by a number of proxies using scale of 7 points. Table 1 presents definition of the variables of the study. The main test variables are: IA competencies (IACOMP), CAE tenure (TENURE), IT governance (ITGOV), private meetings between CAE and AC (AC-CAE), reviewing organisations policies and procedures (POLICIES), ensuring that cybersecurity regulations are met (REGULATIONS), and the involvement of IA in the readiness of cybersecurity (READINESS).

Table 1: definitions of the variables

Variables	Definitions

verifiable contact information for some audit committees, and/or the lack of clarity in governance disclosures as to whether certain AIM-listed or smaller firms had formal audit committees in place.

[3] The response rates (35.3% and 29.9%) are considered acceptable for corporate-level online surveys compared to other studies in the internal audit field; for example, the response rate of Ismael and Kamel study (2021) is 62%, and the rate of Al-Sukker et al. study (2018) is 43.3%. Our response rate can be attributed to that the surveys were short, clearly structured, and easy to complete, which reduced respondent burden and encouraged participation. A follow-up strategy was also employed, including reminder emails that were professionally worded and sent at appropriate intervals, which is known to significantly improve response rates.

[4] Data for this study were collected from two primary sources: (1) two surveys administered CAE and AC, and (2) publicly available annual reports from the same companies. To enable meaningful analysis, survey responses were matched with the corresponding company's annual reports. As a result, the data cannot be considered fully anonymous. However, all data were treated with strict confidentiality, and no identifying information was disclosed in the analysis or reporting of results. The research protocol ensured that any potentially identifying details were excluded from the results, and the study was conducted in accordance with ethical research standards.

CYBER-SEC	Cybersecurity: using scale of 7 points, a number of indicators are used as proxies to measure cybersecurity, these being: ✓ Cybersecurity combines technological solutions, robust policies and procedures, ongoing education, and a proactive stance towards emerging threats. ✓ To what extent does cybersecurity system protect against known and unknown threats? (e.g. malware, phishing attacks, data breaches, and other cyber threats). ✓ To what extent is cybersecurity able to adapt to new threats and vulnerabilities as they emerge (e.g. regular updates, patches, and staying informed about the latest cybersecurity trends). ✓ To what extent can cybersecurity withstand attacks, minimize damage, and recover quickly in case of a breach or cyber incident? ✓ To what extent does company perform regular training and awareness programs educate employees about cybersecurity best practices? ✓ Proactive cybersecurity involves continuous monitoring, threat hunting, and preemptive measures to prevent attacks before they occur. ✓ Cybersecurity is scalable to accommodate growth and changes in an organisation's IT infrastructure and operations. CAE perception:
IACOMP	Internal audit (IA) competency: several proxies are used as indicator of IA competency, these are: number of years of work experience in the field of IT audit, and professional qualifications equals one if staff possess a professional certification, and zero otherwise. AC perceptions: The level of CAE experience in the field of IT audit and internal audit using scale of 7 points (1 = not expert, and 7 = very expert).
ITGOV	Using scale of 7 points, IT governance is measured by a number of proxies including: (1) the extent of aligning IT strategy with business objectives; (2) IT governance ensures that cybersecurity strategies are aligned with overall business objectives; (3) the extent of establishing transparent processes for allocating and managing IT resources; (4) the extent that IT governance involves the processes, structures, and policies that ensure IT resources are aligned with business goals, managed efficiently, and controlled effectively; (5) the extent of endorsing and mandating IT policy by the board; (6) the extent that IT governance frameworks include risk assessment and management processes; (7) the extent of integrating IT controls with enterprise risk management; (8) the extent that IT governance defines roles and responsibilities related to IT and cybersecurity; (9) the extent that IT governance frameworks establish policies and procedures for IT and cybersecurity; (10) the extent that IT governance includes mechanisms for measuring and reporting IT performance; (11) the extent that IT governance frameworks include compliance controls to adhere to regulations and industry standards.
TENURE	CAE tenure is the number years CAE held in his/her position.
AC-CAE	Private meetings between audit committee (AC) and chief audit executive (CAE) are measured by two indicators: Annual number of private meetings between AC and CAE; and The proportion of private meetings (number of private meetings divided by the annual number of AC meetings).
POLICIES	Reviewing organisation's governance policies and procedures using scale of 7 points.
REGULATION	IA ensures that cybersecurity regulations are met using scale of 7 points.
RESOURCES	IA resources are number of internal audit staff in the department. AC perception: The level of sufficiency of IA resources in terms of number of staff and annual budget allocated to IA department, using scale of 7 points (1 = not sufficient, and 7 = totally sufficient).
ACINDEP	Coded 1 if all AC members are independent, and zero otherwise.
ACEXP	AC financial expertise is the proportion of members who possess financial expertise.
READINESS	The extent of IA involvement in cybersecurity readiness using scale of 7 points.
IAROLE	Using scale of 7 points, two indicators are used, these being: the extent of IA role to strengthen organisation security, and the extent of IA to aid in assuring the effectiveness of the organisational cybersecurity.

PLAN	Cybersecurity is included in the IA annual plan using scale of 7 points.
Industry	Industry is dummy variable.
Year	Year is dummy variable.

4. Results

4.1. Descriptive analysis

Table 2 presents an overview of the descriptive statistics of the variables used in this study, providing initial insights into the characteristics of the sample and the overall distribution of responses across key constructs. The dependent variable, CYBER-SEC, has a mean of 5.20 (on a scale from 1 to 7), suggesting a moderately high perception of cybersecurity audit quality across the sample (i.e. most organisations perceive their cybersecurity audit quality as good), with relatively low standard deviation (SD = 0.97) indicates limited variation in this perception among respondents. The median of 5.00 indicates that half of the organisations rate cybersecurity audit quality at 5 or higher, supporting this observation.

IT governance (ITGOV) scores a mean of 4.80 (SD = 1.18) on a 7-point scale, highlighting that IT governance is moderately implemented across the sample. The standard deviation indicates some variation, although organisations vary in the robustness of their governance frameworks. The mean scores of policy reviews (POLICIES = 5.25), regulatory compliance efforts (REGULATION = 4.50), and cybersecurity readiness (READINESS = 4.25) show that IA is relatively active in reviewing cybersecurity-related governance policies and ensuring regulatory compliance, although IA involvement in cybersecurity readiness is somewhat lower.

Table 2: Descriptive results

Variable	Max	Min	Mean	Median	S.D.
CYBER-SEC	7.00	1.00	5.20	5.00	0.97
IACOMP:					
EXPERIENCE	25.00	10.00	14.50	14.00	3.11
QUALIFICATIONS	1.00	0.00	0.91	1.00	0.35
ITGOV	7.00	1.00	4.80	5.00	1.18
TENURE	18.00	5.00	11.25	11.00	3.47
AC-CAE	5.00	1.00	2.80	3.00	1.12
POLICIES	7.00	1.00	5.25	5.00	0.92
REGULATION	7.00	1.00	4.50	4.00	1.01
RESOURCES	40.00	3.00	6.50	5.00	3.22
ACINDEP	1.00	0.00	0.92	1.00	0.21
ACEXP	1.00	0.00	0.79	0.76	0.28
READINESS	7.00	1.00	4.25	4.00	1.18
IAROLE	7.00	1.00	5.40	5.00	0.95
PLAN	7.00	1.00	5.75	5.00	0.87
N: 543					

CYBER-SEC quality of cybersecurity; IACOMP is IA competencies using two proxies: (1) EXPERIENCE is number of years of work experience in the field of IT audit, and (2) QUALIFICATIONS is professional qualifications equals one if staff possess a professional certification, and zero otherwise; ITGOV IT governance is the average scores of a number of indicators; TENURE is the number years CAE held in his/her position; AC_CAE is annual number of private meetings between AC and CAE; POLICIES is reviewing organisation's governance policies and procedures using scale of 7 points; REGULATION is IA ensures that cybersecurity regulations are met using scale of 7 points; RESOURCES IA resources is number of internal audit staff in the department; ACINDEP coded 1 if all AC members are independent, and zero otherwise; ACEXP is the proportion of AC members who possess financial expertise; READINESS is the extent of IA involvement in cybersecurity readiness using scale of 7 points; IAROLE is the average scores of two indicators: the extent of IA role to strengthen organisation security,

and the extent of IA to aid in assuring the effectiveness of the organisational cybersecurity; PLAN is that cybersecurity is included in the IA annual plan.

Table 3 presents Pearson correlation coefficients between quality of cybersecurity (CYBER-SEC) and the independent variables examined in the study. The correlation results reveal meaningful and statistically significant relationships between the quality of cybersecurity (CYBER-SEC) and several key governance and IA factors. Notably, IA involvement in cybersecurity readiness (READINESS) exhibits the strongest positive correlation ($r = 0.50$, $P < 0.01$), indicating that active involvement of IA in assessing organisational preparedness for cyber threats significantly enhances the quality of cybersecurity. IT governance (ITGOV) also shows a substantial positive correlation ($r = 0.45$, $P < 0.01$), underscoring the importance of robust governance structures in supporting cybersecurity strategy. IA assurance that cybersecurity regulations are met (REGULATION) is similarly associated with improved cybersecurity ($r = 0.41$, $P < 0.01$), suggesting that the role of IA in ensuring adherence to cybersecurity regulations is a critical driver of cyber resilience. Furthermore, CAE IT audit experience (EXPERIENCE) and professional qualifications (QUALIFICATIONS) are positively related to cybersecurity quality ($r = 0.28$ and $r = 0.17$, respectively), confirming the significance of technical competencies in the IA function.

By contrast, CAE tenure (TENURE) demonstrates a weak and statistically insignificant correlation with cybersecurity ($r = 0.03$), suggesting that the length of time a CAE serves in their role does not inherently translate into improved cybersecurity outcomes. This finding supports the notion that experience must be complemented by continuous professional development to remain effective in the rapidly evolving cybersecurity landscape. Likewise, IA resources (RESOURCES) show a weak positive correlation with cybersecurity ($r = 0.08$), which, although positive, is not statistically significant. This implies that simply increasing staff size or budget may not be sufficient unless accompanied by targeted training, effective governance alignment, and strategic prioritisation of cybersecurity activities.

Table 3: Correlation results

Variables	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1. CYBER-SEC	1													
2. EXPERIENCE	***0.28***	1												
3. QUALIFICATIONS	**0.17**	**0.19**	1											
4. ITGOV	***0.45***	***0.30***	***0.25***	1										
5. TENURE	0.03	-0.12	-0.08	0.11	1									
6. AC-CAE	***0.25***	0.09	-0.04	0.10	***0.19***	1								
7. POLICIES	***0.22***	***0.33***	***0.26***	**0.15**	0.09	***0.23***	1							
8. REGULATION	***0.41***	***0.29***	***0.24***	**0.12**	0.01	***0.27***	0.10	1						
9. RESOURCES	0.08	-0.01	-0.13	**0.14**	**0.12**	0.11	**0.15**	-0.01	1					
10. ACINDEP	**0.14**	-0.05	-0.10	***0.20***	-0.12	***0.52***	**0.17**	**0.13**	***0.28***	1				
11. ACEXP	**0.16**	-0.02	-0.07	***0.22***	-0.08	***0.40***	**0.18**	0.05	-0.04	-0.09	1			
12. READINESS	***0.50***	***0.24***	***0.21***	**0.17**	-0.06	***0.36***	0.04	0.10	0.10	**0.15**	***0.24***	1		
13. IAROLE	***0.32***	0.10	0.04	***0.19***	-0.03	**0.16**	0.13	**0.18**	-0.03	**0.14**	***0.22***	***0.29***	1	
14. PLAN	***0.38***	**0.19**	**0.16**	**0.18**	-0.04	**0.18**	0.06	***0.20***	**0.14**	**0.17**	***0.27***	***0.38***	***0.19***	1

Bold significant at 0.05; **Bold** and ***Italic*** significant at 0.01

4.2. Testing Hypotheses

Table 4 presents the results of the first set of regression models, examining the determinants of cybersecurity audit quality from both CAE and AC perspectives (Panels A and B respectively). The models explain a substantial proportion of variance in the dependent variable (*Pseudo* R^2 = 0.592 for Panel A and 0.611 for Panel B), indicating strong model fit. To test the first hypothesis, regression test was run to test the impact of competency on cybersecurity. Table 4 (Panel A) shows that IACOMP are positively associated with CYBER-SEC at level of $P < 0.05$, and thus supporting *H1*. When breaking the competency data into individual variables for additional consideration, results indicate that both EXPERIENCE and QUALIFICATIONS show positive and statistically significant coefficients at level of $P < 0.01$ (*Coef*. 0.295) and $P < 0.05$ (*Coef*. 0.208) respectively. Key findings reveal that EXPERIENCE significantly enhances cybersecurity audit quality, with coefficients of 0.295. It can be said that each additional year of IT audit experience increases perceived cybersecurity audit quality by approximately 0.30 units, highlighting the value of deep IT audit expertise. These results imply that among IA competency indicators, experience in IT audit is more likely to be an important indicator in leading to effective cybersecurity[5].

Table 4: Regression results – testing hypotheses

Variable	Panel A – CAE Perceptions			Panel B – AC Perceptions		
	Coef.	*Wald*	*VIF*	*Coef.*	*Wald*	*VIF*
EXPERIENCE	0.295	7.869**	1.871	0.431	9.896**	1.864
QUALIFICATIONS	0.208	5.634*	1.807	0.229	6.809*	1.976
ITGOV	0.935	9.215**	1.520	1.034	11.659**	1.481
TENURE	0.056	1.697	1.615	0.064	1.871	1.738
AC-CAE	0.351	6.145*	1.783	0.294	5.018*	1.691
POLICIES	0.241	6.603*	1.672	0.385	5.952*	1.612
REGULATION	0.862	10.481**	1.469	0.806	10.815**	1.387
RESOURCES	0.102	2.471	1.359	0.082	3.185	1.436
ACINDEP	0.117	2.672	1.451	0.097	2.866	1.472
ACEXP	0.081	2.275	1.461	0.070	2.149	1.518
READINESS	1.109	12.258**	1.529	1.277	13.247**	1.461
IAROLE	0.470	7.372**	1.534	0.674	8.021**	1.502
PLAN	0.687	8.320**	1.683	0.733	9.596**	1.595
INDU		Yes		Yes		
YE		Yes		Yes		
N		543		361		
Pseudo R^2		0.592		0.611		
P		< 0.01		< 0.01		

* and ** indicate *P*-value is significant at the 5 and 1 percent levels, respectively; IACOMP is IA competencies using two proxies: (1) EXPERIENCE is number of years of work experience in the field of IT audit, and (2) QUALIFICATIONS is professional qualifications equals one if staff possess a professional certification, and zero otherwise; ITGOV IT governance is the average scores of a number of indicators; TENURE is the number years CAE held in his/her position; AC_CAE is annual number of private meetings between AC and CAE; POLICIES is reviewing organisation's governance policies and procedures using scale of 7 points; REGULATION is IA ensures that cybersecurity regulations are met using scale of 7 points; RESOURCES IA resources is number of internal audit staff in the

[5] To ensure the validity of our regression models, standard diagnostic checks were conducted. Variance Inflation Factors (VIFs) for all predictor variables were calculated and are reported in Table 4. All VIF values fall well below 2.0, indicating that multicollinearity is not a concern. Additionally, although normality and homoscedasticity assumptions apply strictly to regression, we examined Pearson and deviance residuals from the models to assess model fit. The residuals did not display systematic patterns, skewness, or heteroscedasticity, suggesting that the model is well specified and robust. These diagnostics support the reliability of the estimated coefficients.

department; ACINDEP coded 1 if all AC members are independent, and zero otherwise; ACEXP is the proportion of AC members who possess financial expertise; READINESS is the extent of IA involvement in cybersecurity readiness using scale of 7 points; IAROLE is the average scores of two indicators: the extent of IA role to strengthen organisation security, and the extent of IA to aid in assuring the effectiveness of the organisational cybersecurity; PLAN is that cybersecurity is included in the IA annual plan; INDU is an industry dummy variable; YE is a year dummy variable.

Contrary to expectations, TENURE is not statistically significant (*Coef.* 0.056, $P > 0.05$), and therefore, *H2* is not supported – suggesting that length of CAE tenure alone does not directly impact the quality of cybersecurity. While tenure reflects stability in leadership, these results suggest that duration alone does not directly translate to improved cybersecurity quality. It may be that competencies and active engagement in IT and cybersecurity practices are more critical than length of service per se.

ITGOV exhibits a strong positive and highly significant association with the quality of cybersecurity (*Coef*. 0.935, $P < 0.01$) – a strong effect emphasizing that robust IT governance substantially enhances cybersecurity. A one-unit improvement in IT governance could boost the quality of cybersecurity audit by nearly one full point. These findings provide support for *H3*. The relatively large coefficients suggest that robust IT governance frameworks exert a substantial positive effect on cybersecurity audit outcomes – underscoring the importance of governance structures and practices in managing cybersecurity risk.

The analysis provides strong evidence in support of *H4* and its sub-hypotheses. POLICIES shows significant positive association (*Coef.* 0.241, $P < 0.05$) confirming that IA review of governance policies enhances the quality of cybersecurity audit, providing support to *H4a*. REGULATION is significant at $P < 0.01$ (*Coef.* 0.862) – suggesting that IA assurance on regulatory compliance is a critical driver of the quality of cybersecurity, hence, *H4b* is supported. READINESS shows the largest effect among variables (*Coef.* 1.109, $P < 0.01$) and most impactful levers for enhancing the quality of cybersecurity, thus supporting *H4c* – highlighting that IA involvement in cybersecurity readiness has a major positive impact on cybersecurity quality. These findings imply that the quality of cybersecurity is more likely to be higher when IA review cybersecurity regulations and organisations comply with those regulations, IA involves in cybersecurity readiness, and IA has a role to strengthen organisation security.

Further, the analysis demonstrated that private meetings between AC and CAE (AC-CAE) is positively influence cybersecurity (*Coef*. 0.351, $P < 0.05$), and thus H5 is supported – implying that each additional private meeting improves quality of cybersecurity by approximately 0.35 units, underscoring the importance of AC-CAE interaction. It also indicates that private meetings between AC and CAE give more chances for CAE to discuss sensitive issues related to cybersecurity, and hence, improve the quality of cybersecurity, and reinforcing the value of strong communication and alignment between AC and CAE. These results offer practical guidance for organisations seeking to elevate their cybersecurity assurance practices.

In terms of the control variables, IAROLE and PLAN are positively associated with CYBER_SEC (*Coef.* 0.470 $P < 0.01$; *Coef.* 0.687 $P < 0.01$) respectively – implying that including cybersecurity in the IA annual plan increases the quality of cybersecurity, whereas the coefficients for IA resources (RESOURCES), AC independence (ACINDEP), AC expertise (ACEXP), are not significant.

It is worth mentioning, while CAE tenure and IA resources were hypothesized to influence cybersecurity quality, they did not yield statistically significant results in our models. Several statistical and contextual explanations may account for this. First, CAE tenure showed relatively low variance (mean = 11.25 years; SD = 3.47), potentially limiting its discriminative power. Moreover, tenure may have curvilinear effect, where moderate tenure enhances performance

while extremely short or long tenure has diminished influence. It is also probable that strategic engagement and influence, rather than duration of service, are the true drivers of the quality of cybersecurity. In other words, non-significance of CAE tenure across models may suggest that time in role alone may not be a sufficient predictor of cybersecurity. Regarding IA resources, the lack of significance may stem from the fact that the current measure reflects resource quantity (e.g., staff size, budget) rather than quality or strategic deployment. Resource sufficiency alone may be a necessary but insufficient condition for cybersecurity enhancement. Organisations with lean but highly skilled IA teams may achieve stronger outcomes than those with larger but less specialized teams. Additionally, the relationship between resources and cybersecurity might be moderated by organisational priorities, IT maturity, or the level of integration between IA and cybersecurity strategy. These factors suggest that future research should consider more nuanced or interactive measures of both tenure and resource.

Furthermore, to enhance the accessibility of the results, we summarize below the practical meaning of key coefficients. The findings indicate that each additional year of CAE experience in IT audit increases perceived the quality of cybersecurity audit by approximately 0.30 points (on a 7-point scale), which underscores the importance of deep IT expertise. Similarly, a one-point improvement in IT governance (e.g., stronger alignment of IT with business goals, enhanced policy enforcement) boosts the quality of cybersecurity by nearly 1.0 point. Notably, READINESS had the strongest effect; organisations with higher IA involvement in cybersecurity readiness (e.g., pre-established response protocols and cybersecurity awareness) experienced over 1.1 points higher the quality of cybersecurity. These findings illustrate that not all factors carry equal weight – some (e.g., readiness, IT governance, regulations, IA plan) are particularly influential.

Figure 1 summarizes the significant predictors identified in the regression model (based on the CAE perceptions). Bars represent the magnitude of the effect (regression coefficients), illustrating the relative weight of each factor in influencing the quality of cybersecurity. READINESS and ITGOV exhibit the largest impact, followed by IA assurance that cybersecurity regulations are met, and cybersecurity is included in the IA annual plan (PLAN).

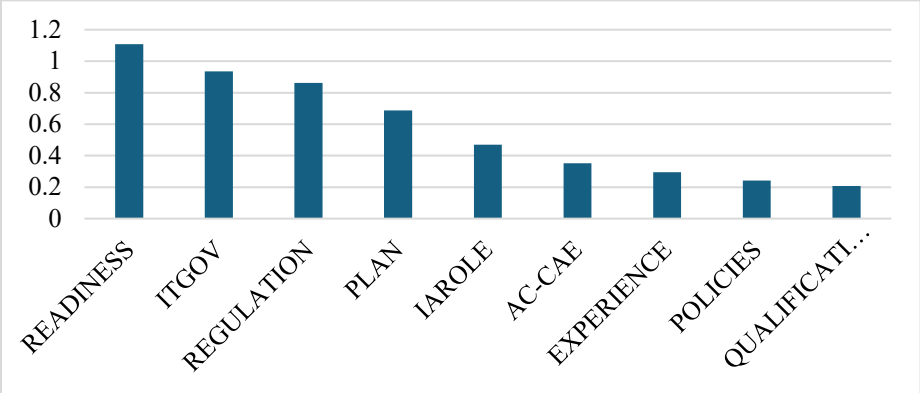

Figure 1: Key predictors of the quality of cybersecurity coefficient

4.3. Audit Committee (AC)

Further investigation is performed to test the hypotheses and re-run Model (1) using the perceptions of AC members. The results reported in Table 4 (Panel B) show similar outcomes

to the main findings presented in Panel A, indicating their robustness. Outcomes show a positive impact of READINESS (*Coef.* 1.277, $P < 0.01$) IA's involvement in cybersecurity readiness exhibited the largest effect, underscoring the strategic importance of proactive IA engagement in building cybersecurity resilience. Moreover, findings confirm the importance of IT governance, which exhibited one of the strongest positive effects on the quality of cybersecurity (*Coef.* 1.034, $P < 0.01$). This finding highlights that robust governance structures provide a critical foundation for managing cybersecurity risks and supporting audit effectiveness. Results also confirm that IA review of organisation's governance policies and procedures enhances the quality of cybersecurity (*Coef.* 0.385, $P < 0.05$). The results provide strong support for the role of CAE competencies (H1), where both IT audit experience and professional qualifications are positively and significantly associated with the quality of cybersecurity $P < 0.01$ (*Coef*. 0.295 $P < 0.01$; and *Coef*. 0.208 $P < 0.05$) respectively. Importantly, CAE experience had a larger effect from the AC perspective, emphasizing its perceived value in strengthening cybersecurity assurance. The economic effect of EXPERIENCE is particularly notable in Panel B (AC perceptions), where the effect size is larger, suggesting that ACs value experience in IT audit even more strongly when assessing cybersecurity outcomes. This highlights the importance of both formal qualifications and accumulated IT audit experience in enhancing the quality of cybersecurity audit. Findings also show that private meetings between AC and CAE (AC-CAE) are significant (*Coef*. 0.294 $P < 0.05$), whereas TENURE is not significant (*Coef*. 0.064 $P > 0.05$) – supporting outcomes reported in Panel A. In summary, the regression results provide robust support for *H1*, *H3*, *H4*, and *H5*, while *H2* is not supported. Further, IAROLE and PLAN are significantly associated with CYBER-SEC (*Coef*. 0.674, and *Coef*. 0733) respectively – providing additional evidence of the significant impact of IA role on the quality of cybersecurity. Overall, these further checks indicate the robustness of the results obtained in the main analysis, depicting an association between quality cybersecurity and IA function.

4.4. Robustness and additional tests

Several tests are conducted using interaction tests, additional variables, alternative measures of the variables.

First, further investigations to confirm the robustness of the results obtained were also made. Moderations tests were performed between IA competency (EXPERIENCE) and three variables, these being: REGULATION, READINESS, and ITGOV. We posit that when IA staff are skilled in IT audit and information system security are more likely to strengthen organisation security and ensure the readiness of cybersecurity, and hence improve effectiveness of the security. Hence, model (1) is produced to test whether the effects of REGULATION, READINESS, and ITGOV on CYBER-SEC are increased/decreased when they are interacted with EXPERIENCE. Secondly, an investigation was also carried out to determine whether the effects of these three variables (REGULATION, READINESS, and ITGOV) increased or decreased with the interaction with private meetings between AC and CAE (AC-CAE). For this purpose, models (2&3) are estimated:

(2)

$$CYBER\text{-}SEC = b_0 + b_1 EXPERIENCE + b_2 QUALIFICATIONS + b_3 ITGOV$$
$$+ b_4 TENURE + b_5 AC\text{-}CAE + b_6 POLICIES + b_7 REGULATIONS$$
$$+ b_8 RESOURCES + b_9 ACINDEP + b_{10} ACEXP + b_{11} READINESS$$
$$+ b_{12} IAROLE + b_{13} PLAN + b_{14} REGULATIONS*EXPERIENCE$$
$$+ b_{15} READINESS*EXPERIENCE + b_{16} ITGOV*EXPERIENCE$$
$$+ Industry + Year + \varepsilon$$

(3)

$$CYBER\text{-}SEC = b_0 + b_1 EXPERIENCE + b_2 QUALIFICATIONS + b_3 ITGOV + b_4 TENURE + b_5 AC\text{-}CAE + b_6 POLICIES + b_7 REGULATIONS + b_8 RESOURCES + b_9 ACINDEP + b_{10} ACEXP + b_{11} READINESS + b_{12} IAROLE + b_{13} PLAN + b_{14} REGULATIONS*AC\text{-}CAE + b_{15} READINESS*AC\text{-}CAE + b_{16} ITGOV*AC\text{-}CAE + Industry + Year + \varepsilon$$

Table 5 (Panels A&B) extends the analysis through interaction effects to further unpack the determinants of the quality of cybersecurity. The models exhibit improved explanatory power (*Pseudo* R^2 = 0.614 and 0.640 respectively), reflecting better model fit. Although the coefficients of EXPERIENCE (*Coef.* 0.302, and 0.293) are slightly different than these reported in Table 4, it remains a significant positive predictor.[6]

Table 5 (Panels A&B) reports the results of Model (2&3) determining whether the effects of REGULATION, READINESS, and ITGOV on CYBER-SEC increase when it is combined with EXPERIENCE. The findings reveal that the effects of these three variables increased when IA staff are experts in IT audit, and CYBER-SEC is more likely to be higher (*Coef.* 1.083, 0.816, and 1.370 respectively) the significance level is $P < 0.01$, thereby supporting the results reported in Table 4. Consequently, evidence is offered that competent IA staff ensure cybersecurity regulations are met and its readiness, hence, enhancing quality of cybersecurity. Further, interaction effects provide novel insights – implying that experienced IT auditors amplify the benefits of regulatory compliance, and that experienced in IT audit more effectively improve readiness of cybersecurity.

Table 5: Regression results – additional analysis

Variable	Panel A – Model 2		Panel B – Model 3	
	Coef.	*Wald*	*Coef.*	*Wald*
EXPERIENCE	0.302	6.319*	0.293	6.481*
QUALIFICATIONS	0.205	4.572*	0.211	4.463*
ITGOV	0.742	8.360**	0.785	8.694**
TENURE	0.069	1.894	0.053	1.736
AC-CAE	0.233	6.129*	0.251	6.022*
POLICIES	0.184	5.548*	0.176	5.411*
REGULATION	0.620	9.366**	0.601	8.314**
RESOURCES	0.107	2.892	0.091	2.739
ACINDEP	0.098	2.581	0.101	2.664
ACEXP	0.087	2.239	0.073	2.188
READINESS	0.761	8.972**	0.743	9.671**
IAROLE	0.273	7.105**	0.258	7.311**
PLAN	0.429	7.661**	0.395	7.633**
REGULATIONS*EXPERIENCE	1.083	11.379**		
READINESS*EXPERIENCE	0.816	12.085**		
ITGOV*EXPERIENCE	1.370	14.237**		
REGULATIONS*AC-CAE			1.106	10.431**
READINESS*AC-CAE			0.902	13.148**
ITGOV*AC-CAE			1.413	17.173**
INDU	Yes		Yes	
YE	Yes		Yes	

[6] The regression models reported in Table 5 are estimated using log regression. Accordingly, we report *Pseudo* R^2, which evaluates model fit by comparing the log-likelihood of the full model to that of a null model. Values of *Pseudo* R^2 between 0.20 and 0.40 are typically considered excellent in social science applications. The values reported in Table 5 (0.614 and 0.640) indicate that the models explain a substantial proportion of variation in cybersecurity quality, suggesting robust explanatory power for models of this type.

N	543	543
Pseudo R^2	0.614	0.640
P	< 0.01	< 0.01

* and ** indicate *P*-value is significant at the 5 and 1 percent levels, respectively; IACOMP is IA competencies using two proxies: (1) EXPERIENCE is number of years of work experience in the field of IT audit, and (2) QUALIFICATIONS is professional qualifications equals one if staff possess a professional certification, and zero otherwise; ITGOV IT governance is the average scores of a number of indicators; TENURE is the number years CAE held in his/her position; AC_CAE is annual number of private meetings between AC and CAE; POLICIES is reviewing organisation's governance policies and procedures using scale of 7 points; REGULATION is IA ensures that cybersecurity regulations are met using scale of 7 points; RESOURCES IA resources is number of internal audit staff in the department; ACINDEP coded 1 if all AC members are independent, and zero otherwise; ACEXP is the proportion of AC members who possess financial expertise; READINESS is the extent of IA involvement in cybersecurity readiness using scale of 7 points; IAROLE is the average scores of two indicators: the extent of IA role to strengthen organisation security, and the extent of IA to aid in assuring the effectiveness of the organisational cybersecurity; PLAN is that cybersecurity is included in the IA annual plan; INDU is an industry dummy variable; YE is a year dummy variable.

Overall, these outcomes provide nuanced evidence that competencies (particularly, experienced in IT audit), and AC-CAE interactions interactively and substantially enhance the quality of cybersecurity. The economic effects of interaction terms are particularly large, indicating that the value of governance, readiness, and regulatory practices is magnified in contexts with stronger experience in IT audit or AC engagement. These findings extend the literature by empirically demonstrating key through which the quality of cybersecurity is elevated.

Moreover, results of Model (3) are presented in Table 5 (Panel B) showing that the effects of REGULATION, READINESS, and ITGOV on CYBER-SEC increased when it is combined with private meetings between AC and CAE (AC-CAE) (*Coef*. 1.106, 0.902, and 1.413 respectively), thus, leading to more effective security, and providing support to the results obtained in Table 4. These findings provide evidence of the importance of holding private meetings between AC and CAE to discuss high risk areas related to cybersecurity. Moreover, IAROLE remains strong direct predictors, affirming IA's pivotal role in cybersecurity assurance. The sustained significance of PLAN reinforces the strategic importance of explicitly incorporating cybersecurity in IA planning.

Secondly, alternative measure of cybersecurity (CYBER-SEC) is used as proxies of CYBER-SEC – coded 1 if company experience a cybersecurity incident in prior year, and 0 otherwise. Also, we also used alternative measure of the private meetings between AC and CAE (AC_CAE), using the proportion of private meetings (number of private meetings divided by the annual number of AC meetings). Model 1 is tested using these alternative indicators, and keeping the tested and control variables the same. The outcomes (untabulated for brevity) show no significant differences from those obtained and reported in Table 4, the significant levels of the independent and control variables remain the same – suggesting the findings are robust.

4.5. Discussion

The findings of this study provide important insights into the role of internal audit in enhancing cybersecurity quality. Specifically, the results highlight the significance of CAE competencies, audit committee interactions, IT governance, and internal audit's role in cybersecurity oversight.

The study's findings confirm that CAE IT competencies play a critical role in enhancing the effectiveness of organisational cybersecurity practices. Specifically, CAEs with robust IT audit experience and professional certifications (e.g., CISA) demonstrate a greater capacity to assess cybersecurity risks, detect system vulnerabilities, and recommend and implement resilient security controls. This aligns with prior literature, such as Steinbart et al. (2018) and Islam et

al. (2018), which underscores that IT-competent auditors contribute meaningfully to an organisation's ability to manage and mitigate cyber threats. Moreover, the results reinforce the growing view cybersecurity quality is crucially dependable in digital expertise; however, a combination of hard and soft skills is essential. As noted by Anderson et al. (2024) and Cyfert et al. (2025), cybersecurity effectiveness depends on technical skills such as IT audit and data security, but also alongside soft competencies, such as adaptability, critical thinking, and risk communication. These skills enable CAEs to work collaboratively across departments, align cybersecurity strategies with broader organisational goals, and respond dynamically to a rapidly evolving threat landscape.

An interesting dimension of the findings is the role of CAE tenure. While tenure showed a positive correlation with cybersecurity quality, its effect was statistically insignificant. This may suggest a diminishing marginal return of tenure on cybersecurity outcomes; potentially due to long-tenured CAEs becoming too accustomed to legacy systems or less responsive to emerging risks. As discussed by Wahhab et al. (2022) and Houlden et al. (2023), ongoing professional development is vital to maintaining cybersecurity competency, especially as emerging technologies like AI, blockchain, and cloud computing continue to reshape the digital threat environment. Therefore, tenure without active skill renewal may limit a CAE's effectiveness in addressing contemporary cybersecurity challenges. Practically, organisations should avoid equating long service with guaranteed effectiveness; instead, they should complement tenure with structured upskilling programs, periodic role rotation, and performance-based evaluations. Such measures can ensure that CAEs maintain both technical and adaptive competencies necessary for managing dynamic cyber risks

The findings also indicate that private meetings between the CAE and the audit committee are positively associated with improved cybersecurity quality. This reinforces the theoretical premise advanced by Bissell (2013) and KPMG (2015), who emphasize the strategic importance of private and confidential dialogue in addressing sensitive and complex cybersecurity issues. Such private interactions enable the CAE to communicate candidly, without the constraints of broader boardroom dynamics, leading to a more transparent and accurate portrayal of the organisation's cybersecurity posture. As highlighted by the IIA (2024), informal and frequent exchanges enhance trust, foster independence, and improve the quality of oversight; particularly crucial in managing rapidly surfacing cyber threats. Moreover, the results support the view that these meetings empower the CAE to elevate cyber risks directly to governance bodies, thereby increasing the strategic salience of cybersecurity within board-level discussions (Al-Shaer, 2025; Vuko et al., 2025). When the CAE has the autonomy to raise concerns and present nuanced risk assessments in a private setting, audit committees are better equipped to allocate resources effectively and guide long-term cybersecurity strategies. This alignment promotes proactive rather than reactive cybersecurity governance. Additionally, private meetings strengthen coordination between the audit function and the organisation's risk management ecosystem. As noted by Vuko et al. (2025), these sessions serve as a critical bridge between the first and second lines of defence and the board, facilitating early detection and a more integrated approach to cyber risk mitigation.

Furthermore, the findings establish a significant positive association between strong IT corporate governance and the quality of cybersecurity. This result emphasises the theoretical arguments made by Sabillon et al. (2017), Kamiya et al. (2021), and Rothrock et al. (2018), who assert that effective IT governance mechanisms, such as board oversight, strategic policies, and integrated risk management, serve as foundational pillars for cybersecurity resilience. When cybersecurity is embedded within broader governance structures, it facilitates proactive threat mitigation, ensures resource allocation, and aligns cybersecurity initiatives with organisational strategy. The findings also align with the emerging view that board involvement,

particularly when directors possess cybersecurity expertise, enhances oversight quality and strengthens disclosure practices (Cortez & Dekker, 2022). Likewise, the findings is in alignment with Al-Shaer et al. (2025) who found that cybersecurity as both a strategic and ethical concern allows CEOs and audit committees to strengthen oversight of cyber risks, reinforcing the governance dimension of resilience. As noted by Tan et al. (2025), such governance enhances investor confidence and long-term value creation, suggesting that cybersecurity governance has both operational and strategic implications. Furthermore, the study affirms the importance of board diversity and engagement, which Radu and Smaili (2022) link to improved cybersecurity transparency and readiness.

Moreover, the study highlights the multifaceted and strategic role of IA in enhancing cybersecurity quality through governance policy reviews, regulatory compliance assurance, and readiness evaluations. The significant positive impact of IA on cybersecurity outcomes aligns strongly with the emerging academic consensus that effective IA involvement serves as a cornerstone in organisational cyber resilience (Vuko et al., 2025; Elmaasrawy & Tawfik, 2025; Adesokan-Imran, 2025; Alhawtmeh, 2025). The findings lend strong support to the hypothesis that when IA actively reviews cybersecurity governance policies, organisations benefit from more structured risk ownership, clearer escalation protocols, and better-defined strategies. This is consistent with Al-Shaer (2025), who highlights that internal audit reviews ensure that cybersecurity governance is embedded within the broader enterprise risk framework and that it evolves in line with emerging threats. Alhawtmeh (2025) also reinforces this point by showing that proactive IA review activities contribute to improved governance maturity and lower vulnerability to cyber threats.

The results additionally demonstrate that IA plays a vital role in ensuring compliance with increasingly complex cybersecurity regulations. This consistent with Adesokan-Imran (2025), who noted that internal audit-led assessments help ensure comprehensive compliance across internal operations and third-party relationships. This study affirms that audit-driven regulatory reviews do more than reduce legal exposure, but they also enhance the overall maturity of cybersecurity systems by institutionalizing best practices and reducing inconsistencies in security enforcement across departments. The findings also confirm that IA's involvement in assessing cybersecurity readiness and resilience is crucial for organisational preparedness. The study supports the view of Elmaasrawy and Tawfik (2024), who assert that the assurance and advisory functions of internal audit significantly enhance human, technical, and organisational preparedness. Regular testing of business continuity and incident response plans by IA leads to faster recovery, better coordination during crises, and more effective threat containment. Alhawtmeh (2025) further argues that such organisations tend to experience fewer severe cyber incidents and are even recognised externally via reduced cyber insurance premiums; a proxy indicator of lower residual cyber risk.

Interestingly, the interaction effects tested in the study reveal that the impact of regulation compliance, cybersecurity readiness, and IT governance on cybersecurity quality is further strengthened when IA staff possess IT expertise. This finding underscores the importance of IT knowledge among internal auditors, as it enhances their ability to interpret, assess, and implement cybersecurity controls effectively. Similarly, the study finds that private meetings between the CAE and AC amplify the impact of IT governance and cybersecurity regulations, suggesting that effective communication between governance bodies leads to stronger cybersecurity outcomes.

5. Conclusion, practical implications, limitations and future research

5.1 Conclusion

This study supports the growing importance of internal audit in cybersecurity governance and highlights the need for strong CAE competencies, governance structures, and proactive cybersecurity oversight. The findings demonstrate that a well-integrated IA function, supported by IT expertise, strategic governance, and AC engagement, can significantly enhances cybersecurity effectiveness. As cyber threats continue to evolve, organisations must adopt a more dynamic, technology-driven approach to internal auditing to safeguard digital assets and maintain regulatory compliance. The study contributes to the growing literature on internal audit and cybersecurity by integrating multiple dimensions, including CAE competencies, IT governance, IA oversight, and AC-CAE interactions, into a comprehensive cybersecurity framework. Unlike previous research that examines these factors in isolation, this study demonstrates how their interactions collectively enhance cybersecurity quality. The findings extend corporate governance and IT governance theories by highlighting the synergistic effect of IA and governance structures in managing cybersecurity risks.

Overall, the findings highlight that CAEs must balance digital competences such as expertise and certification with continuous learning to remain effective. Organisations should therefore invest not only in hiring IT-competent audit leaders but also in fostering a culture of lifelong learning and interdisciplinary collaboration. Such efforts will ensure that internal audit functions remain agile and proactive in securing the organisation's digital infrastructure. Furthermore, the structured, confidential engagement between the CAE and AC is a cornerstone of effective cybersecurity governance and contributes significantly to an organisation’s cyber resilience. Moreover, a balanced approach where strong IT governance forms the strategic backbone of cybersecurity management, but technical competence and dynamic risk responses serve as essential complements. Organisations that integrate governance with operational cyber capabilities are more likely to achieve sustained resilience and maintain trust in an increasingly digital and threat-prone environment. Collectively, these results reinforce the assertion that internal audit must not be limited to a compliance monitoring role. Instead, it should be empowered as a strategic partner in cybersecurity governance. The integration of IA across governance, regulatory, and operational domains fosters a culture of cyber resilience, proactive threat management, and continuous improvement in cybersecurity quality. This expanded role enhances not only security outcomes but also organisational reputation, stakeholder trust, and regulatory alignment in a dynamic risk landscape.

5.2 Practical Implications:

The findings of this study provide several important implications for organisations, regulators, and society at large. At the organisational level, the results underscore the need to prioritise IT competencies within internal audit functions. Recruitment, certification, and continuous training of CAEs and internal auditors in IT and cybersecurity should be viewed as strategic investments, ensuring that audit teams possess the technical and adaptive skills required to address rapidly evolving cyber risks. In addition, audit committees should institutionalise private meetings with CAEs, as these strengthen communication, enhance trust, and ensure that cybersecurity issues are given appropriate strategic importance at the board level. Similarly, embedding cybersecurity oversight within broader IT governance frameworks promotes alignment with enterprise-wide strategies, improves resource allocation, and strengthens risk ownership across departments. Internal auditors should also play a greater role in cybersecurity readiness assessments, ensuring compliance with regulations and strengthening incident response strategies. By enhancing audit expertise, governance structures, and proactive oversight, organisations can significantly improve their cybersecurity resilience and risk management frameworks.

The finding that CAE tenure was not a significant predictor of cybersecurity quality further suggests that stability in leadership alone is insufficient. Organisations must therefore

complement tenure with structured upskilling, adaptability, and performance evaluations that reward ongoing competency development rather than longevity. Internal audit's critical role in regulatory compliance and readiness also highlights the importance of positioning IA as a strategic partner in enhancing resilience, not only by ensuring adherence to existing frameworks but also by advising on emerging risks and preparedness testing.

At the societal and regulatory level, the implications extend beyond organisational boundaries. Improved cybersecurity audit quality strengthens consumer protection by reducing risks of data breaches that can compromise sensitive personal and financial information. In industries such as healthcare, banking, and government services, strong internal audit oversight directly supports public trust by safeguarding critical digital infrastructures. Furthermore, these findings align closely with global regulatory frameworks such as the General Data Protection Regulation (GDPR) and cybersecurity standards like the National Institute of Standards and Technology (NIST) Cybersecurity Framework, which stress accountability, privacy, and resilience. Organisations that embed internal audit more deeply into their cybersecurity strategy not only comply with such frameworks but also contribute to building societal trust in digital systems. Ultimately, the operationalisation of these findings allows firms to move beyond compliance-driven approaches and embrace audit quality as a driver of both organisational resilience and societal benefit.

5.3 Limitations and future research

Despite its contributions, this study has some limitations. While this study focuses on UK-listed companies, cybersecurity challenges vary across industries and regions. Future research should explore how IA's role in cybersecurity differs across global contexts, particularly in emerging markets where cybersecurity regulations may be less developed. Future research also could incorporate longitudinal data and case studies to provide richer insights into the evolving role of internal audit in cybersecurity. Lastly, future studies could investigate the role of artificial intelligence (AI) and machine learning in supporting internal auditors in cybersecurity assessments, an area that remains underexplored. Further limitation of this study is that certain theoretically important variables, namely CAE tenure and internal audit (IA) resources, did not exhibit statistically significant relationships with cybersecurity quality. This may be due in part to measurement constraints. For example, IA resources were measured in terms of size and budget, but not the efficiency, specialization, or strategic use of those resources. Future research could explore interaction effects, or develop more nuanced indicators such as resource utilization ratios, training intensity, or functional integration with cybersecurity teams.

AI Declaration: During the preparation of this work the author used ChatGPT in order to improve readability and language of the work. After using this tool, the author reviewed and edited the content as needed and take full responsibility for the content of the publication.

References

Abdelrahim, A., & Al-Malkawi, H.-A. N. (2022). The Influential Factors of Internal Audit Effectiveness: A Conceptual Model. *International Journal of Financial Studies*, *10*(3), 71. https://doi.org/10.3390/ijfs10030071

Adesokan-Imran, T. O. (2025). The Impact of Cybersecurity Governance on National Security by Strengthening Critical Infrastructure through IT Auditing and Risk Management. *Asian Journal of Research in Computer Science*, *18*(4), 301-322.

Adiloglu, B., & Gungor, N. (2019). The impact of digitalization on the audit profession: A review of Turkish independent audit firms. *Journal of Business Economics and Finance, 8*(4), 209–214.

Anderson, A., Ahmad, A., & Chang, S. (2024). Case-based learning for cybersecurity leaders: A systematic review and research agenda. *Information & Management, 61*, 104015. https://doi.org/10.1016/j.im.2024.104015

Anderson, R. J. (2015). Why information security is hard—An economic perspective. *Proceedings of the 17th Annual Computer Security Applications Conference*.

Alhawtmeh, O. M. (2025). The role of internal audit as a tool for enhancing cybersecurity effectiveness in Jordanian government agencies. Vol. 7, No. 1, 2025, pp.319-330.

Al-Shaer, H., Albitar, K., Derouiche, I., & Hussainey, K. (2025). The role of CEO power and audit committees in cybersecurity risk management. The International Journal of Accounting. Advance online publication. https://doi.org/10.1142/S1094406025420041

Ashraf, M. (2019). Cybersecurity and quality management: An integrated approach. *Journal of Information Security, 10*(3), 115–130.

Bissell, K. (2013). Cybersecurity: It's about strategy, not compliance. *Journal of Strategic Security, 6*(2), 56–67.

Brenner, L. (2020). Internal audit's role in cybersecurity: Ensuring robust protection. *Cybersecurity Journal, 14*(2), 87–102.

Chammaa, H., Ed-Daoudi, R., & Benazzi, K. (2025). Large language models for academic internal auditing. *International Journal of Advanced Computer Science and Applications, 16*(1). https://doi.org/10.14569/IJACSA.2025.0160166.

Computer Crime Research Center. (2024). *Cost of cybercrime to reach over $12 trillion globally by 2025 – Report*. Nairametrics. Retrieved from https://nairametrics.com/2024/01/25/cost-of-cybercrime-to-reach-over-12-trillion-globally-by-2025-report [Accessed: 20 September 2025]

Cortez, E. K., & Dekker, M. (2022). A corporate governance approach to cybersecurity risk disclosure. *European Journal of Risk Regulation*, *13*(3), 443-463.

Coulson-Thomas, C. (2012). Transforming corporate governance and enhancing sustainability. *Management Services, 56*(2), 26–30.

Cyfert, S., Dyduch, W., Szumowski, W., & Prause, G. (2025). Are we ready for digital transformation? *Central European Management Journal, 33*(2). https://doi.org/10.1108/CEMJ-11-2024-0346

Elmaasrawy, H. E., & Tawfik, O. I. (2025). Impact of the assertive and advisory role of internal auditing on proactive measures to enhance cybersecurity: Evidence from GCC. *Journal of Science and Technology Policy Management*, *16*(1), 68-93.

Flora, P., & Rai, A. (2015). Cybersecurity risk: Insights from the CBOK 2015 Global Internal Audit Practitioner Survey. *The IIA*.

Gatzert, N., & Schmit, J. (2016). Supporting and opposing internal audit functions in cybersecurity. *Risk Management Journal, 22*(1), 45–63.

Haislip, J., Pinsker, R., & Young, M. (2017). The role of corporate governance in cybersecurity. *Journal of Information Systems, 31*(1), 57–81.

Houlden, N., Jackson, V., & Youssef, M. H. (2023). The perception of cybersecurity education and its implications. *ITNOW, 65*(1), 46–47.

Institute of Internal Auditors (IIA). (2016). *Assessing cybersecurity risks: The internal auditor's role*. The IIA.

Islam, M. S., Farah, N., & Stafford, T. F. (2018). Factors associated with security/cybersecurity audit by internal audit function. *Managerial Auditing Journal, 33*(4), 377–409.

Jamison, J. D., Morris, L. J., & Wilkinson, C. R. (2018). *The future of cybersecurity in internal audit*. Internal Audit Foundation and Crowe.

KPMG. (2015). *Global audit committee survey*. KPMG International.
Lanz, J. (2014). The audit committee's role in cybersecurity oversight. *Journal of Accountancy, 218*(4), 52–55.
Pate, K., & Chudasam, D. (2021). National security threats in cyberspace. *National Journal of Cyber Security Law, 4*(1), 12–29.
Popescu, C. R. G., & Popescu, G. N. (2018). Risks of cyber-attacks on financial audit activity. *The Audit Financiar Journal, 16*(149), 140–140.
Rosati, P., Gogolin, F., & Lynn, T. (2019). Cyber-security incidents and audit quality. *European Accounting Review*, 1–28.
Rosati, P., Gogolin, F., & Lynn, T. (2020). Cyber-security incidents and audit quality. *European Accounting Review*, 1–28.
Rothrock, R. A., Kaplan, J., & Van Der Oord, F. (2018). The board's role in managing cybersecurity risks. *MIT Sloan Management Review, 59*(2), 12–15.
Sabillon, R., Cavaller, V., Serra-Ruiz, J., & Cano, J. (2017). A comprehensive cybersecurity audit model to improve cybersecurity assurance. *International Conference on Information Systems and Computer Science*, 253–259.
Soh, D. S. B., & Martinov-Bennie, N. (2011). The internal audit function, perceptions of internal audit roles, effectiveness and evaluation. *Managerial Auditing Journal, 26*(7), 605–622.
Slapničar, S., Vuko, T., Čular, M., & Drašček, M. (2022). Effectiveness of cybersecurity audit. *International Journal of Accounting Information Systems*, *44*, 100548.
Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2014). The influence of a good relationship between the internal audit and information security functions on information security outcomes. *Accounting, Organizations and Society, 39*(7), 546–570.
Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2018). The influence of a good relationship between the internal audit and information security functions on information security outcomes. *Accounting, Organizations and Society, 71*, 15–29.
The IIA Research Foundation (IIARF). (2015). *Cybersecurity: What the board of directors needs to ask*. The Institute of Internal Auditors.
Turetken, O., Jethefer, S. and Ozkan, B. (2020) Internal Audit Effectiveness: Operationalization and Influencing Factors. Managerial Auditing Journal, 35, 238-271. https://doi.org/10.1108/MAJ-08-2018-1980
Vuko, T., Slapničar, S., Čular, M., & Drašček, M. (2025). Key drivers of cybersecurity audit effectiveness: A neo-institutional perspective. *International journal of auditing*, *29*(1), 188-206.
Wahhab, A. M. A., Jawad, B. H., & Alajeli, E. H. (2022). Auditing cybersecurity risks considering the information renaissance and its impact on the continuity of companies. *Technium Social Sciences Journal, 35*, 18–28.
Young, R. R., & Wang, W. (2014). The role of the audit committee in cybersecurity. *The CPA Journal, 84*(9), 28–33.