INTERNATIONAL JOURNAL OF ECONOMICS AND FINANCE STUDIES
Vol: 17 **No:** 04 **Year:** 2025 **ISSN:** 1309-8055 (Online) (**pp.** 414-430) **Doi:** 10.34109/ijefs.202517419
Received: 11.09.2025 | **Accepted:** 20.11.2025 | **Published Online:** 30.12.2025

-RESEARCH ARTICLE-

THE IMPACT OF CORPORATE GOVERNANCE ON CYBERSECURITY RISKS: INTERNAL AUDITING AS A MEDIATING VARIABLE

Bushra Fadhil Khudhair Al-Taie

Associate Professor at Department of Accounting, College of Administration and Economics, University of Baghdad, Iraq
ORCID: https://orcid.org/0000-0002-3946-1045
Email: bushra@coadec.uobaghdad.edu.iq

Sallama Ibrahim Ali

Associate Professor at Department of Accounting, College of Administration and Economics, University of Baghdad, Iraq.
ORCID: https://orcid.org/0000-0003-0560-8528
Email: salama@coadec.uobaghdad.edu.iq

Hakeem Hammood Flayyih Al-Fandawi*

Department of Accounting Studies, Post-Graduate Institute for Accounting & Financial Studies, University of Baghdad, Iraq.
ORCID: https://orcid.org/0000-0003-0615-0854
Email: hakeem.hmood@coadec.uobaghdad.edu.iq

—Abstract—

The aim of the study was to examine the impact of Corporate Governance (CG) on Cybersecurity Risks (CRs), with special emphasis given to ascertaining the role of Internal Auditing (IA) as an intervening factor in the aforementioned relationship. To accomplish this, an analytical framework was developed and empirically tested via Partial Least Squares Structural Equation Modelling (PLS-SEM). The empirical study was carried out on 73 specialists working in the accounting, auditing, risk management, and information security departments of Iraqi banks. Primary data were collected via the electronic implementation of a structured questionnaire. The empirical findings of the study reveal that CG has a positive and statistically significant impact on IA. This reveals that an effective CG system can positively

Citation (APA): Al-Taie, B. F. K., Ali, S. I., Al-Fandawi, H. H. F. (2025). The Impact of Corporate Governance on Cybersecurity Risks: Internal Auditing As a Mediating Variable. *International Journal of Economics and Finance Studies*, 17(04), 414-430. doi: 10.34109/ijefs.202517419

Vol: 17 **No:** 04 **Year:** 2025 **ISSN:** 1309-8055 (Online) (**pp.** 414-430) **Doi:** 10.34109/ijefs.202517419

influence the strength of internal controls and, as a consequence, the effectiveness of the IA function. Furthermore, the findings reveal that IA is positively and statistically significantly correlated with CRs, thus underscoring its crucial role in evaluating the strength of technological controls and enhancing risk management practices in digitalised business environments. On the contrary, the link between CG and CRs is not statistically significant. However, the indirect link between CG and CRs via IA is statistically significant, thus affirming that IA is an absolute mediator between CG and CRs. The R-squared values indicate high values of determination of the structural model, especially with respect to the relationship between CG and CRs via IA, thus affirming the adequacy and empirical robustness of the proposed framework. The findings of the study thus underscore the strategic importance of integrating CG with IA to enhance the governance of CRs in digitalised business environments.

Keywords: Corporate Governance, Internal Auditing, Cybersecurity Risks, and Information Technology.

INTRODUCTION

Risks associated with cybersecurity within the context of enterprise information technology are normally defined as vulnerabilities of the system that are prone to being exploited, thus resulting in operational disruption or financial loss (Chowdhury, 2025). The importance of CRs as a form of communication within the board of organizations is undeniable, as it helps to articulate the risks, thus clearly illustrating the responsibilities of those in oversight or governance positions within the organization. Additionally, all members of staff within various hierarchical structures of organizations are able to recognize system-generated high-risk alerts and take necessary action to address the issue of cyber threats within their organizations to limit the negative impact of the threats (Aljumaiah et al., 2025). The digital aspects of social infrastructures are essential within the context of a globalized economy. The various essential infrastructures of modern societies include electricity networks, transportation systems, water facilities, and healthcare services, all of which are dependent on uninterrupted digital services. The uninterrupted nature of digital services is directly proportional to the welfare of nations, macroeconomic conditions, and security concerns of nations (Alzghoul, 2024; Flayyih et al., 2024).

The importance of addressing the issue of cybersecurity within the context of organizations has thus led to the international recognition of cybersecurity threats and risks as the most pressing strategic challenges facing organizations of the 21st century (Amani et al., 2025). The concern of organizations regarding cybersecurity has become a major issue within the past few years, mainly attributed to the increasing sophistication, flexibility, and financial implications of digital threats (Alahmari & Duncan, 2020). The various risk trends identified through past scholarly works (Alahmari & Duncan, 2020; Faraj & Wali, 2026; Kosub, 2015; Yaacob et al., 2023)

Vol: 17 No: 04 Year: 2025 ISSN: 1309-8055 (Online) (pp. 414-430) Doi: 10.34109/ijefs.202517419

indicate a strategic realignment of organizations towards cybersecurity threats, as indicated by the increase of cybersecurity expenditure within organizations. Organizations are spending more on cybersecurity to protect their digital infrastructures (Alzeban et al., 2026; Andrade et al., 2025).

At the same time, businesses are functioning in a highly interconnected digital environment, characterised by a high level of technological innovation and a constant threat of cyber intrusions (Qudus, 2025; Safitra et al., 2023; Sendjaja et al., 2024). Cyber risk, therefore, must not be viewed as a mere technological failure, but a multidimensional governance risk, covering financial, operational, strategic, and reputational concerns (Elsayed et al., 2024; Kiesow Cortez & Dekker, 2022). Evidence of the threat of CRs can be found in the fact that the frequency and impact of cyberattacks have significantly increased in recent times. According to the Institute of Internal Auditors, cybersecurity and data protection have been rated as among the most critical technological risks facing businesses in the modern era. Data from the Heritage Foundation (2015) indicated that the average number of successful cyber intrusions stood at 160 incidents every week in 2014, a figure more than three times the average in 2010. Similarly, the financial impact of these attacks has been significant, with losses amounting to a mean of 15.4 million dollars for each U.S.-based company, a figure more than double the estimate in 2010, and data breach incidents continuing to grow in number. In addition, the total global cost of cybercrime was expected to reach 2 trillion dollars by 2019, a figure almost four times the estimate in 2015. Therefore, all these findings highlight the importance of managing CRs strategically, a fact that has been reinforced by the fact that boosting the ability to deal with cybersecurity threats is in line with the sustainability and protection of all relevant stakeholders.

The CR evaluation process comprises a broad range of organisational policies, preventive strategies, and internal control practices aimed at identifying, classifying, assessing, and communicating CRs to boards of directors (Al-Saudi & Flayyih, 2024; Oh et al., 2025). The overarching goal of CR evaluation is to maintain the confidentiality, integrity, and availability of information systems from any malicious internal or external attacks. Cybersecurity frameworks are put in place to mitigate threats to public and private critical infrastructures, including identity theft, malware distribution, ransomware deployment, and phishing attacks. These practices are aimed at averting, limiting, and monitoring CRs to ensure productivity and dependability in information systems. This need has become critical in modern times, as conventional internal control practices have been found wanting in protecting information systems in internationally operating financial institutions (Usman et al., 2024).

An organisation may use a variety of security practices aimed at averting, identifying, or remediating CRs, thus strengthening CR management architecture. Alternatively, CRs may be allowed to persist in alignment with the risk appetite of the organisation

Vol: 17 **No:** 04 **Year:** 2025 **ISSN:** 1309-8055 (Online) (**pp.** 414-430) **Doi:** 10.34109/ijefs.202517419

or in situations where the impact of CRs on operations is insignificant (Siyaya et al., 2025). As the scope and nature of CRs are increasing, boards of directors and audit committees are increasingly seeking IA to offer credible assurance on CRs (Al-Shaer et al., 2025). IA plays a critical role in the risk identification, evaluation, and mitigation of risks in organisations. By conducting a thorough evaluation of risk management practices, IA provides assurance on their sufficiency, effectiveness, and alignment with strategic objectives.

This process of risk identification entails a thorough comprehension of the organisational operational, financial, and strategic objectives, followed by the mapping of identified risks and external threat vectors. By conducting exhaustive risk analysis, IA ensures the development of mitigation strategies that aim to control the probability and impact of negative risks. In the case of internal auditors, the processes would include the analysis of credit risks, regulatory risks, and operational inefficiencies, with the aim of providing recommendations for addressing the risks identified. In the case of manufacturing organisations, the processes would include the analysis of the weaknesses in the supply chain and environmental risks with the aim of promoting sustainable business practices. By adopting risk management processes such as COSO and ISO 31000, IA ensures the alignment of risk control with organisational objectives (Udoh, 2024).

The evolutionary role of IA is further supported by theoretical foundations. Literature on corporate governance and financial control heavily cites Agency Theory, which explains agency conflicts based on divergent interest principles between the principal and the agent. Under this theory, IA assumes the role of corporate governance aimed at addressing information asymmetry and ensuring that managerial activities are aligned with the interest of stakeholders. As internal evaluators, internal auditors assess the integrity of financial reporting, identify control weaknesses, and detect fraud that might result from agency theory-related opportunism (Ogunsola et al., 2021). The ever-changing economic and technological environment further calls for the incorporation of IA within service-oriented and technology-intensive organisations. The increasing competitive environment forces organisations to adopt innovation-driven strategies to remain viable and successful. If stakeholders possess the required knowledge and expertise, they can contribute to strategic initiatives towards performance improvement strategies. Effective communication channels and information sharing promote collaboration towards this objective. Proactive responses to actualised risks are critical in a volatile environment, making IA's role strategically imperative. Cyber security assurance is currently one of the major risks identified in digital transformation and information systems implementation. As cyber breaches escalate in terms of financial implications and popularity, organisations must address this risk by developing strategies to innovate within the operational plan. As a response to this evolutionary environment, IA's role has moved from merely performing traditional compliance activities towards participating proactively in

Vol: 17 **No:** 04 **Year:** 2025 **ISSN:** 1309-8055 (Online) (**pp.** 414-430) **Doi:** 10.34109/ijefs.202517419

digital operations and online service security (Lois et al., 2021).

This progression, therefore, reflects a significant change in the conceptualisation of IA, from a traditional control-oriented concept towards a more strategic contributor in the governance of cyber resilience in organisations. The major streams for managing ever-rising CRs, as identified by the scholarly discourse, comprise governance and institutional dimensions, auditor-specific professional and behavioural attributes, and technological capabilities, including AI and data analytics. However, integrative models that bring together these dimensions into a coherent framework for understanding the value creation process through IA in high-risk digital environments remain underdeveloped. The research gap, therefore, becomes evident. While CRs have gained more attention in the realm of scholarly research, and IA has gained a more prominent place in the value creation process through ER, the lack of empirical research remains a problem, particularly with regard to the systematic incorporation of CR assessment into IA processes, as expected by CG. Further, the relationship between CR management maturity and the cybersecurity assurance levels delivered by IA for the board has not been adequately explored. This, therefore, reflects the need for further research, particularly with regard to contemporary digitally transformed business environments.

LITERATURE REVIEW AND HYPOTHESES DEVELOPMENT

The current research highlights the significance of a strategic role for IA in the cybersecurity domain, particularly with regard to digital transformation and the proliferation of AI and advanced data analytics technologies. The research conducted by Usman et al. (2024) revealed that the effectiveness of internal auditors in assessing CRs is dependent upon a combination of professional and behavioral characteristics, which include integrity, objectivity, proficiency, competence, expertise, incentives, and advisory proficiency. These characteristics have a positive influence on the effectiveness and robustness of risk evaluation processes and the development of supervisory and mitigation processes in financial institutions.

In tandem with the rising digitalisation, there has been an increased body of research on the technological enhancement of IA practices. Udoh (2024) found that the incorporation of artificial intelligence, data analytics, and automation technologies into the IA processes transforms the IA function from a periodic exercise for ensuring regulatory compliance into a continuous process for ensuring organisational assurance with real-time risk detection capabilities. In another study, Ogunsola et al. (2021) suggested an advanced governance-oriented IA risk assessment framework for enhancing financial integrity, reducing the risk of fraud, regulatory non-compliance, and unethical practices in financial institutions. Their findings revealed that the incorporation of artificial intelligence, data analytics, and predictive modeling methodologies improves risk identification in the early stages while enhancing

transparency and accountability. Their findings also revealed that a comprehensive governance framework improves regulatory compliance, consolidates internal control environments, and improves the overall financial systems' resilience to financial instabilities. This was further supported by Andrade et al. (2025), who found that the incorporation of data analytics methodologies and penetration testing procedures improves the accuracy and effectiveness of cybersecurity control evaluation methodologies in financial organisations. Maisyarah (2025) also found that the incorporation of cybersecurity audit frameworks, along with transparent disclosures regarding previous cyber-related incidents, improves the overall credibility and quality of risk-related disclosures for financial organisations. In another study, Mahmood et al. (2026) found that the overall level of cybersecurity maturity is a foundational requirement for optimising the overall effectiveness of IA practices with the incorporation of artificial intelligence. Their findings revealed that the benefits of IA incorporation into the IA processes are more significant after the achievement of a predetermined maturity threshold.

In their systematic literature review, Siyaya et al. (2025) sought to identify the contribution of IA in the management of CRs. The literature characterised IA as the third line of defence, which is critical in coordinating the efforts of the organisation, alongside the information technology function, which is the first line of defence, and the risk management function, which is the second line of defence. The literature underscored the need for functional alignment and collaborative integration of these different levels of governance towards strengthening the overall internal control environment, oversight quality, and organisational preparedness in managing CRs. From the analysis in the foregoing paragraphs, the following hypotheses are proposed.

H1: *There is a statistically significant effect of Corporate Governance on Cybersecurity Risks.*
H2: *There is a statistically significant effect of Corporate Governance on Internal Audit effectiveness.*
H3: *There is a statistically significant effect of Internal Audit effectiveness on Cybersecurity Risks.*
H4: *Internal Audit plays a mediating role in the relationship between Corporate Governance and Cybersecurity Risks.*

METHODOLOGY

Sample

Table 1 indicates the demographic and occupational characteristics of the study participants, who were composed of 73 employees recruited from Iraqi banks. These statistical values were provided to create a general overview of the profile of the

Vol: 17 **No:** 04 **Year:** 2025 **ISSN:** 1309-8055 (Online) (**pp.** 414-430) **Doi:** 10.34109/ijefs.202517419

respondents based on the distribution of gender, educational level, professional experience, and job designation.

Table 1: Sample Characteristics

Variable	Category	Frequency	Percentage
Six	Male	41	56.2%
	Female	32	43.8%
Educational Qualification	Bachelor's	68	93.2%
	Master's	4	5.5%
	PhD	1	1.4%
Years of Experience	Less than 5 Years	12	16.4%
	5–10 Years	26	35.6%
	11–15 Years	20	27.4%
	More than 15 Years	15	20.5%
Current Position	Accounting Department	34	46.6%
	Audit Department	27	37.0%
	Information Technology Department	9	12.3%
	Risk Management Department	3	4.1%

Measurement of Variables

As far as the evolution of the concept of IA is concerned, previous research suggests the existence of an important change in its conceptualization, moving from its traditional role as an oversight mechanism towards its new status as an important participant in the strategic governance of cyber resilience. The relevant literature suggests the existence of three main pillars of the evolution of the concept of IA. These pillars are the governance and the associated architecture in which the process of IA is exercised, the professional skills and the associated behavioural characteristics of the members of the internal audit team, and the technological environment of modern internal auditing, particularly with regard to the application of artificial intelligence and data analytics in dealing with CRs. Despite the evident evolution in the relevant literature with regard to the concept of IA, the absence of an overall framework integrating these different elements towards the development of an overall model capable of illuminating the manner in which IA can contribute to the creation of value is evident.

Research Model

In consideration of the aforementioned theoretical underpinning and body of empirical evidence, a conceptual model has been developed to inform understanding of the relationship between CG and CRs, including a consideration of IA as a mediating variable in this relationship. The model is predicated upon the understanding of CG as the structure and system of rules by which organisational policies are set and risk governance is managed. However, the model does not posit a direct relationship

Vol: 17 No: 04 Year: 2025 ISSN: 1309-8055 (Online) (pp. 414-430) Doi: 10.34109/ijefs.202517419

between CG and CRs. Rather, the impact of CG is conceived as being mediated through internal managerial and control systems, of which IA is conceived as being the primary medium of influence. In this context, the model suggests that CG influences the effectiveness and nature of IA, which in turn impacts upon CRs. A consideration of the direct relationship between CG and CRs is included in the model to examine the nature of the structural relationship between the variables of the study constructs. Figure 1 presents the suggested analytical framework, including the hypothesised interrelationships between variables.

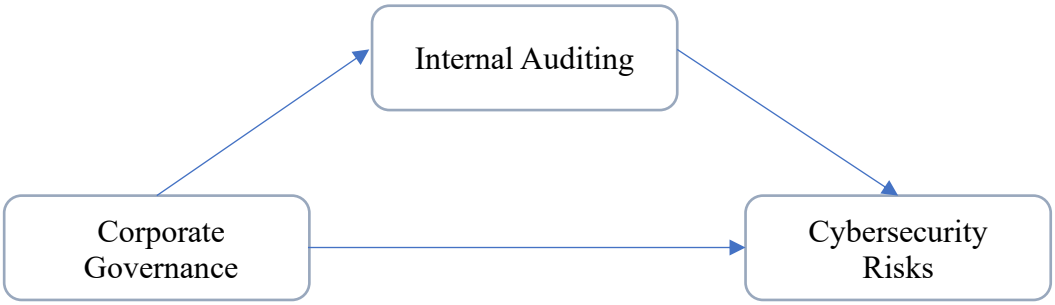

Figure 1: Research Model

The proposed framework for analysis would identify the hypothesised structural relationships between CG, IA, and CRs. Specifically, the model suggests that CG can have an impact on CRs through two different routes: one direct and one indirect via the mediating construct of IA.

RESULTS

Measurement Model Assessment

The measurement model was assessed with the aid of the PLS-SEM method, and the procedural guidelines for the same were followed as suggested by Hair et al. (2021). In this evaluation, the focus was on the internal consistency reliability and the convergent validity of the latent variables. This evaluation is a primary step before the estimation of the structural model for the purpose of hypothesis evaluation. In order to assess the internal consistency reliability, the Composite Reliability and Cronbach's Alpha coefficients were calculated. On the other hand, the convergent validity was assessed based on the loadings along with the Average Variance Extracted (AVE) results. In order to assess the quality of the results, the following benchmark criteria were used: the loadings had to be > 0.70, Composite Reliability > 0.70, Cronbach's Alpha > 0.70, and the AVE > 0.50. Table 2 shows the results obtained for the evaluation of the measurement model along with the reliability and validity results obtained for the constructs.

Vol: 17 **No:** 04 **Year:** 2025 **ISSN:** 1309-8055 (Online) (**pp.** 414-430) **Doi:** 10.34109/ijefs.202517419

Table 2: Model Quality Test

Variables	Outer Lodgings		Cronbach's Alpha	rho_A	Composite Reliability	Average Variance Extracted (AVE)
Corporate Governance	x1	0.697	0.898	0.902	0.916	0.522
	x2	0.766				
	x3	0.676				
	x4	0.721				
	x5	0.604				
	x6	0.773				
	x7	0.755				
	x8	0.712				
	x9	0.757				
	x10	0.747				
Internal Auditing	M1	0.905	0.908	0.928	0.925	0.56
	M2	0.557				
	M3	0.761				
	M4	0.762				
	M5	0.63				
	M6	0.722				
	M7	0.468				
	M8	0.845				
	M9	0.862				
	M10	0.849				
Cybersecurity Risks	Y1	0.834	0.941	0.946	0.95	0.68
	Y2	0.866				
	Y3	0.805				
	Y4	0.837				
	Y5	0.839				
	Y6	0.878				
	Y8	0.804				
	Y9	0.741				
	Y10	0.808				

In terms of internal consistency reliability, the CG construct has been found to be consistent, with Cronbach's Alpha value equal to 0.898, rho_A equal to 0.902, and Composite Reliability equal to 0.916. All the values are much higher than the minimum threshold value of 0.70 (Hair et al., 2021). In the same vein, the IA construct has also been found consistent, with Cronbach's Alpha value equal to 0.908, rho_A equal to 0.928, and Composite Reliability equal to 0.925. In the case of the CRs construct, the highest reliability value has been obtained, with Cronbach's Alpha equal to 0.941, rho_A equal to 0.946, and Composite Reliability equal to 0.950. While the obtained results are close to the value of 0.95, it can be stated that the results are within the acceptable limits (Hair et al., 2021).

The convergent validity for the research model was checked via outer loadings and AVE values. For the CG construct, the AVE value achieved 0.522, which is above

Vol: 17 **No:** 04 **Year:** 2025 **ISSN:** 1309-8055 (Online) (**pp.** 414-430) **Doi:** 10.34109/ijefs.202517419

0.50, indicating that more than half of the variance for the indicators is explained by the latent construct. However, some outer loading values were slightly below 0.70, but according to (Hair et al., 2021), it is recommended that indicators with loadings between 0.40 and 0.70 be retained when their removal does not significantly improve the quality of the measures, which is applicable in this case. The IA construct had an AVE value of 0.56, which meets the convergent validity criterion. However, some indicators had lower loadings, indicating that they contribute minimally to the latent construct, although the AVE and Composite Reliability values were still acceptable, and there is theoretical support for retaining the indicators. For the CR construct, the AVE value was 0.68, and all the outer loading values were above 0.70, indicating that it has good convergent validity and that the latent construct is well represented. The result of the convergent validity and internal consistency reliability for the research model confirms that all the research constructs have met the necessary conditions for internal consistency reliability and convergent validity, as recommended for a PLS-SEM research model (Hair et al., 2021). The result therefore shows that the research model is statistically sound, and it is now possible to move forward with the analysis and hypothesis testing with methodological confidence. Figure 2 shows the structural model for the analysis.

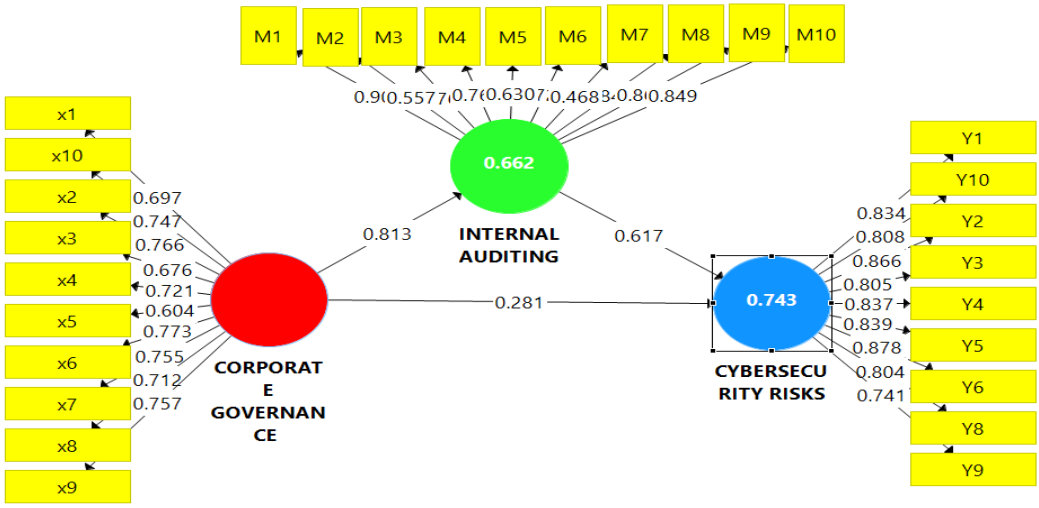

Figure 2: Structural Model for Measurement Quality Assessment

As indicated by the analysis of the proposed structural model as presented in Figure 2, it is evident that the IA construct has a value of 0.662 for the R^2 measure, implying that the CG construct accounts for 66.2% of the variability of the IA construct. This is a substantial value of explanatory power, thus suggesting that CG is a key determinant of the effectiveness of IA as presented within the proposed structural model. Additionally, the proposed structural model indicates that the CRs construct has a value of 0.743 for the R^2 measure, implying that the CG and IA constructs combined account for 74.3% of the variability of the CRs construct. As indicated by the

Vol: 17 **No:** 04 **Year:** 2025 **ISSN:** 1309-8055 (Online) (**pp.** 414-430) **Doi:** 10.34109/ijefs.202517419

established PLS-SEM constructs, this is a substantial value of predictive power, thus suggesting that the proposed structural relationships are adequate for analysis purposes.

Hypothesis Testing

Direct Effects Testing

Table 3 presents the outcomes of the direct path analysis, which was conducted to evaluate the first, second, and third hypotheses regarding the relationships among the study constructs.

Table 3: Direct Effects among Study Variables

Paths	Original Sample	T Statistics	P Values
GC -> CRs	0.282	1.579	0.115
GC -> IA	0.821	17.541	0.000
IA -> CRs	0.589	3.674	0.000

The analysis indicates that the direct effect from CG to CRs revealed a path coefficient of 0.282, a T-value of 1.579, and a p-value of 0.115. It should be noted that the p-value is greater than the significance level of 0.05, whereas the T-value is less than the critical value of 1.96 at a 95% confidence level. As a result, the direct effect of CG on CRs is deemed statistically insignificant. It should therefore be concluded that there is a lack of empirical evidence to prove the direct effect of CG on CRs. As a result, Hypothesis H1 is rejected. On the contrary, the direct effect from CG to IA revealed a strong positive effect, as the path coefficient was 0.821, the T-value was 17.541, and the p-value was 0.000. It should therefore be concluded that the direct effect of CG on IA is highly statistically significant. As a result, Hypothesis H2 is supported. In the same vein, the direct effect from IA to CRs revealed a positive effect, as the path coefficient was 0.589, the T-value was 3.674, and the p-value was 0.000. It should therefore be concluded that the direct effect of IA on CRs is statistically significant. As a result, Hypothesis H3 is supported. It should therefore be concluded that the direct effect of CG on CRs is completely mediated by IA.

Indirect Effects Testing

Table 4 presents the findings of the indirect effects analysis, which was conducted to evaluate the fourth hypothesis regarding the mediating role of IA in the relationship between CG and CRs.

Table 4: Results of Indirect Effects Testing

Paths	Original Sample	T Statistics	P Values
GC -> IA -> CRs	0.484	3.864	0.000

Vol: 17 **No:** 04 **Year:** 2025 **ISSN:** 1309-8055 (Online) (**pp.** 414-430) **Doi:** 10.34109/ijefs.202517419

As indicated by the analysis, the indirect effect of CG on CRs via IA has a coefficient of 0.484, implying a positive mediation effect. The T-value is 3.864, which is well above the minimum threshold of 1.96 at a 95% confidence level. The p-value of 0.000 is far below the minimum requirement of 0.05 to establish a significant relationship. As established earlier, the direct effect of CG on CRs was not significant; thus, the positive effect of IA on CRs implies a full mediation role of IA as a mediator between CG and CRs. This suggests that CG has a significant impact on CRs via IA, which in turn has a significant impact on cybersecurity risk levels. The strategic role of IA as a mediator between CG and CRs is further emphasized by the fact that it serves as a mechanism of execution of various governance practices on the improvement of CR management. The structural model is presented in Figure 3 below:

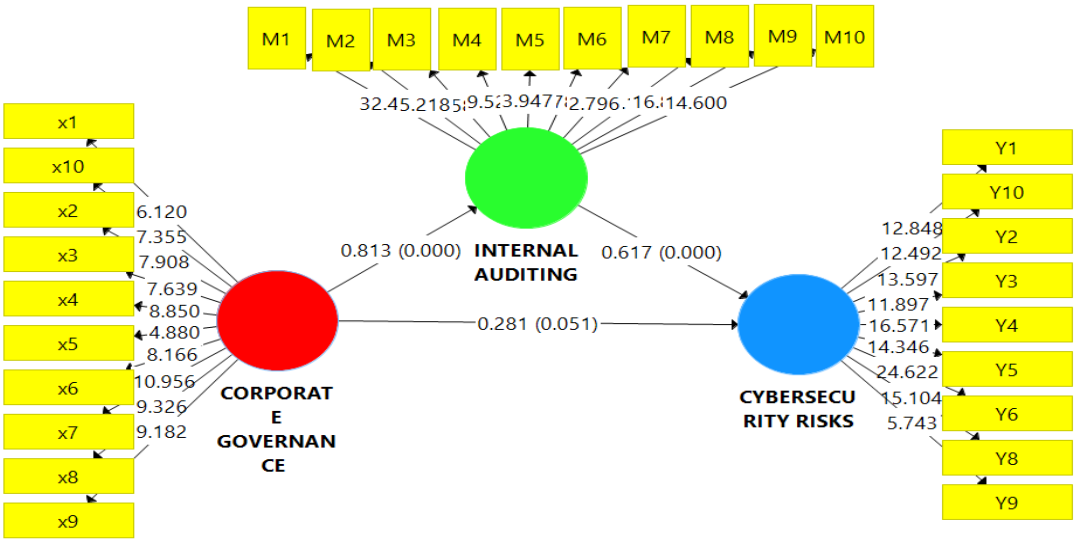

Figure 3: Structural Model

The findings indicate that the path between CG and IA has a coefficient of 0.813 with a significance level of 0.000. This further affirms that sound CG practices have a direct and significant influence on the IA system of the organisation. The path between IA and CRs reveals a coefficient of 0.617 with a significance level of 0.000. This reveals that IA has a positive and statistically significant influence on the system of CRs. The path between CG and CRs reveals a coefficient of 0.281 with a significance level of 0.051. The p-value is slightly higher than 0.05, and hence it is not statistically significant. Therefore, it is evident that there is no direct influence of CG on CRs. Regarding the measurement model, it is found that nearly all the outer loadings have T-values higher than 1.96, thereby affirming that the measurement model is reliable and valid. The findings reveal that IA mediates between CG and CRs. The influence of CG on CRs is not direct but is realised via the enhancement of IA practices. Therefore, Hypothesis H4 is supported.

Vol: 17 **No:** 04 **Year:** 2025 **ISSN:** 1309-8055 (Online) (**pp.** 414-430) **Doi:** 10.34109/ijefs.202517419

DISCUSSION OF RESULTS

The results obtained from the research indicate that CG has a positive and statistically significant impact on IA, which, in its turn, has a positive and statistically significant impact on CRs. On the other hand, the direct impact of CG on CRs is not statistically significant, while the indirect effect is confirmed. The results indicate that IA plays a key role in the process of converting governance into effective cybersecurity risk management. This result is consistent with the findings of (Flayyih et al., 2024), which showed that the effectiveness of IA is significantly related to governance support and board engagement. The result is also consistent with (Omolere, 2025), which showed that the influence of the board is critical in the process of defining the priority of risks and supporting IA activities. The result is also consistent with Usman et al. (2024), which showed that IA plays a critical role in assessing CRs, internal control, and cybersecurity risks. The result obtained from the mediation analysis is consistent with (Siyaya et al., 2025), which showed that IA acts as a third line of defines that connects governance with technical risk management processes. The above arguments and findings from the existing literature indicate that the enhancement of auditing tools and the use of data analytics significantly improve the effectiveness of IA in managing cybersecurity risks, which is consistent with the findings of the current research and provides support for the interpretation that IA plays a key role in the governance-risk nexus. The result obtained from the research confirms that CG has no direct influence on CRs, while its influence is realised through the activation and reinforcement of the IA function, which plays a key role in ensuring effective cybersecurity risk management in a digitally driven organisational environment.

LIMITATIONS, SOCIAL IMPLICATIONS, AND SCIENTIFIC CONTRIBUTION OF THE STUDY

The study is subject to certain limitations, which should be taken into consideration. Firstly, the empirical research was carried out on a specific sample group within a specific contextual environment. This could be considered to limit the generalisation of the results to other sectors and organisational environments, especially if they have different structural characteristics and levels of digitalisation. Secondly, the study is subject to certain limitations, as it is based on cross-sectional data collected via a questionnaire, which could be subject to certain response and self-reporting biases. Additionally, it does not capture the changes in the relationships between variables across different periods of time. Furthermore, it should be noted that the proposed model included a small number of variables, which suggests that there could be certain variables in the organisational and technological environment that could affect CRs but were not included in the model.

Vol: 17 **No:** 04 **Year:** 2025 **ISSN:** 1309-8055 (Online) (**pp.** 414-430) **Doi:** 10.34109/ijefs.202517419

Despite the limitations of the study, it should be noted that it contributes to the body of knowledge to a great extent. The study presents an integrative framework of analysis between CG, IA, and CRs, as well as testing the mediating effect of IA via PLS-SEM. The findings of the study provide empirical evidence of IA as an essential tool of governance that can effectively implement governance principles in the form of effective CR management, which is an issue of great interest in the current literature. From a more general point of view, it should be noted that the study is of great social and organisational importance, as it reveals the crucial role of IA in improving CR management. The findings of the study suggest that it is essential to strengthen governance and auditing to protect digital assets and safeguard the interests of stakeholders, especially in digitalised environments. Furthermore, the study contributes to the literature by explaining the indirect link between governance and CRs, thus forming a robust basis for further research to expand and deepen the subject.

CONCLUSION

The study aimed to examine the impact of CG on CRs, with a focus on the mediating effect of IA in the relationship between CG and CRs. To achieve this purpose, a structural model was conceptualized and empirically tested to examine the causal relationships between the study variables. The results of the study revealed a positive and statistically significant impact of CG on IA, supporting the effectiveness of internal control systems in organizations and the importance of IA in achieving a strong internal control environment. On the other hand, the study found a positive and statistically significant impact of IA on CRs, underscoring the importance of IA in the evaluation of technical controls, risk management practices, and organizational readiness to address potential cyber threats. Conversely, the direct impact of CG on CRs was found to be insignificant, although the indirect effect was significant, indicating a fully mediated relationship between CG and CRs through IA. This finding supports the importance of internal executive and control mechanisms in managing cybersecurity risk, as a function of the broader governance function, mediated by the critical operational conduit of IA. Therefore, the study concludes by recommending the integration of CG and the IA function, supporting the independence of the IA function, and developing the technical and analytical skills of the function to improve the effectiveness of cybersecurity risk management in organizations. Future research can expand the study model to other sectors or industries to examine the external validity of the study results in other contexts, including cross-cultural environments. Future studies can also consider incorporating additional variables, including the impact of cybersecurity maturity, the use of AI and data analytics in the IA function, to examine their impact on CR management in organizations. Future studies can also consider a longitudinal design to examine the

evolution of the relationship between governance, IA, and CRs, particularly in the context of rapidly changing digital transformation in organizations.

REFERENCES

Al-Saudi, N. H., & Flayyih, H. H. (2024). The impact of digital transformation on office management efficiency. Journal of Economics and Administrative Sciences, 30(142), 645-661. https://doi.org/10.33095/fqfn7h48

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, 2542004. https://doi.org/10.1142/S1094406025420041

Alahmari, A., & Duncan, B. (2020). Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence. 2020 international conference on cyber situational awareness, data analytics and assessment (CyberSA), https://doi.org/10.1109/CyberSA49311.2020.9139638

Aljumaiah, O., Jiang, W., Addula, S. R., & Almaiah, M. A. (2025). Analyzing cybersecurity risks and threats in IT infrastructure based on NIST framework. J. Cyber Secur. Risk Audit, 2025(2), 12-26. https://doi.org/10.63180/jcsra.thestap.2025.2.2

Alzeban, A., Al-Hajaya, K., Sawan, N., Chammaa, H., & Foster, S. (2026). The quality of cybersecurity audits: do synergies among the chief audit executive, IT governance and internal audit functions matter? Managerial Auditing Journal, 41(2), 322-349. https://doi.org/10.1108/MAJ-05-2025-4825

Alzghoul, M. S. (2024). The Mediating Role of Internal Audit Quality in the Relationship between Cyber Security Governance and Reducing the Risks of Cloud Accounting. Pakistan Journal of Life & Social Sciences, 22(2). https://doi.org/10.57239/PJLSS-2024-22.2.00937

Amani, F., Magnan, M., & Moldovan, R. (2025). Cybersecurity risks and incidents disclosure: a literature review. Accounting Perspectives, 24(3), 605-667. https://doi.org/10.1111/1911-3838.12411

Andrade, F. L. V., de Melo, A. C. A., de Melo Laerte, P., & Nunes, R. R. (2025). Internal Audit Strategies for Assessing Cybersecurity Controls in the Brazilian Financial Institutions. Applied Sciences, 15(10), 5715. https://doi.org/10.3390/app15105715

Chowdhury, T. K. (2025). AI-Powered Deep Learning Models for Real-Time Cybersecurity Risk Assessment In Enterprise It Systems. ASRC Procedia: Global Perspectives in Science and Scholarship, 1(01), 675-704. https://doi.org/10.63125/137k6y79

Elsayed, D. H., Ismail, T. H., & Ahmed, E. A. (2024). The impact of cybersecurity disclosure on banks' performance: the moderating role of corporate governance in the MENA region. Future Business Journal, 10(1), 115. https://doi.org/10.1186/s43093-024-00402-9

Faraj, M. K., & Wali, A. H. (2026). Multiple Perspectives for Evaluating of Eco-Efficiency Using Environmental Management Accounting Information. In R. El Khoury (Ed.), Empowering Business Through Technology: Innovations Shaping Our Future (pp. 287-298). Springer Nature Switzerland. https://doi.org/10.1007/978-3-032-02056-7_23

Flayyih, H. H., Shamukh, S. A., Jabbar, H. A., & Abbood, H. Q. (2024). Artificial Intelligence and Trends Using in Sustainability Audit: A Bibliometric Analysis. Explainable Artificial Intelligence in the Digital Sustainability Administration, Cham. https://doi.org/10.1007/978-3-031-63717-9_19

Hair, J. F., Hult, G. T. M., Ringle, C. M., Sarstedt, M., Danks, N. P., & Ray, S. (2021). Partial least squares structural equation modeling (PLS-SEM) using R: A workbook. Springer. https://doi.org/10.1007/978-3-030-80519-7

Kiesow Cortez, E., & Dekker, M. (2022). A Corporate Governance Approach to Cybersecurity Risk Disclosure. European Journal of Risk Regulation, 13(3), 443-463. https://doi.org/10.1017/err.2022.10

Kosub, T. (2015). Components and challenges of integrated cyber risk management. Zeitschrift für die gesamte Versicherungswissenschaft, 104(5), 615-634. https://doi.org/10.1007/s12297-015-0316-8

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

Mahmood, M. R., Naseem, S., & Ullah, K. I. (2026). Evaluating How Cybersecurity Threat Intelligence Enhances AI-Driven Risk Assessment in Internal Auditing. Policy Journal of Social Science Review, 4(1), 134-158. https://doi.org/10.5281/zenodo.18336904

Maisyarah, R. (2025). Cybersecurity Audit and IT Risk Management. Proceedings of International Conference on Islamic Community Studies, https://proceeding.pancabudi.ac.id/index.php/ICIE/article/view/543

Ogunsola, K. O., Balogun, E. D., & Ogunmokun, A. S. (2021). Enhancing financial integrity through an advanced internal audit risk assessment and governance model. International Journal of Multidisciplinary Research and Growth Evaluation, 2(1), 781-790. https://doi.org/10.54660/.IJMRGE.2021.2.1.781-790

Oh, K. B., Hoang, G., Sturdy, J., & Guo, S. S. (2025). Cybersecurity and Governance. In K. B. Oh, G. Hoang, J. Sturdy, & S. S. Guo (Eds.), Cybersecurity Governance: An Enterprise Risk Management Strategy for Cyber Risk Control (pp. 19-63). Springer Nature Singapore. https://doi.org/10.1007/978-981-95-3865-2_2

Omolere, O. (2025). Cybersecurity Governance and Board Oversight: Implications for Internal Audit Investigating How Board-Level Cyber Governance Influences Audit Planning and Risk Prioritization. https://doi.org/10.2139/ssrn.5999794

Qudus, L. (2025). Advancing cybersecurity: strategies for mitigating threats in evolving digital and IoT ecosystems. Int Res J Mod Eng Technol Sci, 7(1), 3185. https://doi.org/10.56726/IRJMETS66504

Safitra, M. F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking cyber threats: A framework for the future of cybersecurity. Sustainability, 15(18), 13369. https://doi.org/10.3390/su151813369

Sendjaja, T., Irwandi, Prastiawan, E., Suryani, Y., & Fatmawati, E. (2024). Cybersecurity In The Digital Age: Developing Robust Strategies To Protect Against Evolving Global Digital Threats And Cyber Attacks. International Journal of Science and Society, 6(1), 1008-1019. https://doi.org/10.54783/ijsoc.v6i1.1098

Siyaya, M. C., Dubihlela, J., & Sibanda, M. (2025). A literature review of internal auditing involvement in cybersecurity risk management of the organisation. Journal of Contemporary Management, 22(si1), 89-115. https://doi.org/10.35683/jcm24.030.293

Udoh, O. R. (2024). Enhancing Internal Audit Efficiency for Effective Risk Management and Corporate Governance Frameworks. International Journal of Research Publication and Reviews, 5(12), 3646-3659. https://doi.org/10.55248/gengpi.5.1224.250122

Usman, A., Che-Ahmad, A., & Abdulmalik, S. O. (2024). The Role of Internal Auditors Characteristics in Cybersecurity Risk Assessment in Financial-Based Business Organisations: a Conceptual Review. Revista de Gestão Social e Ambiental, 18(6), 1-33. https://doi.org/10.24857/rgsa.v18n6-008

Yaacob, M. N., Idrus, S. Z. S., & Idris, M. (2023). Managing cybersecurity risks in emerging technologies. International Journal of Business and Technopreneurship (IJBT), 13(3), 253-270. https://doi.org/10.58915/ijbt.v13i3.297