Accounting and Management Information Systems
Vol. 24, No. 4, pp. 673-691, 2025
DOI: http://dx.doi.org/10.24818/jamis.2025.04006

The contribution of a good relationship between internal audit and information systems to information protection outcomes: The case of banks in Greece

Dimitrios Mitskinis[1, a], Nikolaos Antonakis[b], George Drogalas[b] and Maria Koumoundourou[c]

[a]*University of West Macedonia, Greece*
[b]*University of Macedonia, Greece*
[c]*Hellenic Open University, Greece*

Abstract

Research Question: How is the impact of the relationship between internal control and information systems on information protection outcomes moderated by the characteristics of the internal auditor, the characteristics of quality information systems audits and the relationship between internal audit and information security management?
Motivation: We draw on the lack of prior research on how a strong relationship between internal control and information systems affects information security outcomes, drawing on data from staff of Greek banks.
Idea: This paper examines the impact of a strong relationship between internal audit and information systems on information protection outcomes in Greek Banks.
Data: We analyse a sample of 114 respondents, personnel within banking institutions in Greece.
Tools: We survey personnel within banking institutions in Greece, who answered a questionnaire with closed-ended questions. The data was analyzed using the Structural Equation Modeling (SEM) approach.
Findings: Findings indicate that the quality control characteristics of information systems, along with the collaboration between internal audit and information security management,

[1] *Corresponding author:* Department of Economics, University of West Macedonia, Fourka area, Kastoria, GR 52100, Greece, email: mitskd@gmail.com
Funding: there is no funding for this research.

Article History: Received 2 June 2025; Accepted 6 December 2025.
Accepted by: Sînziana-Maria Rîndașu

significantly and positively influence the relationship between internal audit and information systems in enhancing information protection outcomes.
Contribution: This study adds the case of Greek banks to the existing literature on the contribution of a good relationship between internal audit and information systems to information protection outcomes. The originality of this research lies in two main aspects: first, the absence of previous studies focusing on Greek banking institutions with a similar scope; and second, the methodological approach employed for data analysis.

Keywords*:* Internal audit, information systems, information protection, Information Security Directorate, Structural Equation Modeling (SEM)

JEL codes: M42

1. Introduction

The role of internal audit evolves and adapts in response to the organization's needs, technological advancements, regulatory changes, and legislation to ensure and safeguard the quality of information (Drogalas *et al*., 2024).The stages of its evolution began in the early 20th century with supportive services to mid-level accounting staff for combating fraud (Chambers & Odar, 2015; Ramamoorti, 2003), followed by its development in the 1940s towards providing assurance regarding the control mechanisms related to organizations' accounting systems (Hazaea *et al.*, 2023; Chambres & Odar, 2015), and its redefinition in the 1980s to provide assurance concerning business processes that mitigate organizational risks (Chambres & Odar, 2015). Today, in the 21st century, the role of internal audit has been readjusted to follow the advancement of technology and information systems (Rîndașu, 2017), contributing with its multidimensional function and advisory capacity to strategy implementation, adding value in developing future plans, and avoiding risks arising from the use of technology for organizations (Nordin, 2023; Drogalas *et al.*, 2020; Hazaea *et al.*, 2020).

Information systems are an integral part of organizations, determining their success through smooth operation (Kim, 2022) but also their failure due to the risks inherent in their use. The adoption and implementation of an information system that does not align with the strategic direction of the organization or the needs of its users can lead to outcomes contrary to expectations (Rezvani *et al.*, 2017; Malaurent & Avison, 2015). Risks related to information systems include data leakage during processing, breaches of associated control mechanisms (Shiau *et al.*, 2023), as well as potential cyber threats or hacker attacks aimed at damaging the organization.

Addressing the risks and challenges faced by organizations from the use of information systems is managed through audits of these systems by internal audit,

for which this constitutes a top priority (Khando *et al.*, 2021). Therefore, internal audit, besides its advisory role in selecting the appropriate information system for an organization, is called upon to continuously monitor the impacts of such systems to protect the organization from undesirable outcomes (Christ *et al.*, 2021; Betti & Sarens, 2021; Otero, 2019).

Previous literature (Usman *et al.*, 2023; Hepworth *et al.*, 2022; Lois *et al.*, 2021; Islam *et al.*, 2018; Yeghaneh *et al.*, 2015; Stoel *et al.*, 2012) shows that the features of internal auditors, the quality characteristics of information system audits, and the relationship between internal audit and information security management play an important role in the connection between internal audit and information security management. Moreover, Steinbart *et al.* (2018) emphasize the positive effect of the relationship between internal audit and information security functions on reducing internal audit weaknesses and incidents of non-compliance. Likewise, Salihu and Hoti (2019) demonstrated that implementing recommendations from information system audits resulted in fewer security incidents.

The purpose of this research is to investigate the beneficial relationship between internal audit and information systems on the outcomes of information protection. The research objectives focus on ensuring that information derived from information systems leads to accurate and reliable representation of organizational metrics, rational decision-making by management, and compliance with applicable laws and regulations for information protection. This study makes a significant contribution to expanding research on this topic, as there is no extensive and specialized literature regarding Greek banks. Through empirical research, results and conclusions are drawn about the contribution of a good relationship between internal audit and information systems to the outcomes of information protection in the banking sector, which should be considered by decision-makers and stakeholders.

The research is structured as follows. The next section includes theoretical background, followed by a literature review, and the development of hypotheses. Then, the research methodology and questionnaire analysis are presented. The following section contains descriptive statistics and reliability verification of the scale using Cronbach's alpha and Exploratory Factor Analysis (EFA). The final part of the results analysis includes Structural Equation Modeling (SEM). Finally, the study concludes with a summary of findings, limitations of the research, and suggestions for future research.

2. Literature review and hypothesis development

The information held by an organization is among its most valuable assets and ensuring its protection is an integral part of its smooth operation and future growth. This information is used to carry out the organization's activities and to support

managerial decisions (Thomson & von Solms, 2005; Flowerday & von Solms, 2005). The significant development of information technology has greatly influenced how organizations collect, use, and process the information they rely on for their daily operations and activities (Kohli & Melville, 2019). At the same time, technology has notably shaped how control is exercised over organization's systems and has a direct impact on the field of internal audit.

Internal audit is expected to oversee the multiple aspects of an organization, focusing on the adoption and implementation of new technologies, and subsequently, evaluating the potential impacts these technologies may entail. Therefore, internal auditors need to enhance their technological and technical expertise in order to effectively assess information systems (Christ *et al*., 2021; Betti & Sarens, 2021; Otero, 2019). The use of new technologies (cloud computing, blockchain, artificial intelligence), besides offering excellent development opportunities for organizations, is accompanied by significant risks (Butler *et al.*, 2023; Yang *et al.*, 2021). These risks relate to information leakages and security breaches, which can cause substantial financial damage and harm an organization's reputation (Shiau *et al.*, 2023). Therefore, data security and privacy have become top priorities for internal audit, aiming to provide real value to an organization (Khando *et al.*, 2021). Thus, the role of internal audit has been redefined and follows a risk-based approach to offer assurance services regarding business processes that mitigate the risks faced by an organization (Chambers & Odar, 2015).

Steinbart *et al.* (2018) examined the quality of the relationship between internal audit and information security functions and found a positive impact of this relationship on the number of internal audit weaknesses and non-compliance incidents, as well as on the number of security incidents detected both before and after causing significant damage to the organization. Similarly, Havelka and Merhout (2013) argue that good working relationships between the internal audit function and other organizational departments improve both the effectiveness and efficiency of the audit, as they enhance the auditor's access to evidence and increase the honesty and openness of the business unit in communicating with the internal audit function. Additionally, Salihu and Hoti (2019) found that implementing the recommendations of information systems audits resulted in a reduction of security incidents.

2.1 Characteristics of an internal auditor

Internal auditors play a critical role in the internal control processes of information systems, particularly in mitigating breaches in security controls (Lois *et al.*, 2021). It is essential for internal audit personnel to possess technical expertise related to information technology, exemplified by certifications such as CISA or CISSP (Usman *et al.*, 2023). Additionally, the evolving responsibilities of internal auditors concerning information protection require continuous professional development and

up-to-date training in information systems (Hepworth *et al.*, 2022). Moreover, the competencies of internal auditors, including communication skills and a strong sense of teamwork, enhance their auditing effectiveness and facilitate collaboration with organizational information systems stakeholders (Usman *et al.*, 2023). The ethical standards upheld by internal auditors constitute a pivotal attribute that shapes their professional identity and can be instrumental in evaluating and identifying various risk facets related to IT systems, as well as cybersecurity threats within organizations (Czerniawska & Szydło, 2021).

The integrity and objectivity exhibited by internal auditors further reinforce their authority in assessing risks associated with information systems (Usman *et al.*, 2023). Nonetheless, such integrity and objectivity may be influenced by the prevailing cultural, socio-economic, and religious contexts within business entities (Pasculli, 2020).

The interplay between internal auditors' characteristics, their IT-related education, and their collaboration with specialized information systems personnel collectively ensures the cybersecurity posture of an organization and mitigates occurrences of information system breaches (Lois *et al.*, 2021). Concurrently, internal auditors' personal attributes, communication proficiency, and professional ethics exert a positive influence on cybersecurity risk assessment (Usman *et al.*, 2023). Drawing upon the extant literature on internal auditors' characteristics, the following hypothesis is posited:

H_1: *The impact of the relationship between internal audit and information systems on information protection outcomes is positively moderated by the characteristics of the internal auditor.*

2.2 Quality control characteristics of information systems

Information systems are subject to scrutiny by both external and internal auditors. The internal audit function within an organization plays a pivotal role in the examination of its information systems, providing assurance regarding their operational effectiveness, efficiency, and security (Stoel *et al.*, 2012). Moreover, the rigorous quality audit of information systems conducted by internal auditors can serve as a safeguard for the organization against risks inherent in their utilization (Merhout & Havelka, 2008).

The efficacy of quality audits in information systems is contingent upon several critical factors, including the audit methodology employed, the adequacy of time allocated to the audit process, and the existence of robust collaboration and support among auditors, auditees, and senior management. Additionally, sufficient time must be dedicated during periods of organizational change to enable the internal audit function to comprehend modifications in processes engendered by such changes.

Finally, a clear delineation of audit objectives and scope is essential (Merhout & Havelka, 2008).

Findings from Stoel *et al.* (2012) underscore the audit methodology as a fundamental determinant of the quality of information systems audits. In consonance, Yeghaneh *et al.* (2015) assert that alongside an appropriate audit methodology, a well-defined scope and the application of suitable frameworks are imperative. Furthermore, Merhout and Havelka (2008) emphasize the significance of both the time devoted to conducting the audit and the time required for the internal audit department to adjust to organizational transformations. Concurrently, the prevailing cooperative climate and the accessibility granted to internal auditors to organizational resources are recognized as pivotal factors influencing audit quality (Stoel *et al.*, 2012; Merhout & Havelka, 2008). In summary, a high-quality internal audit of an organization's information systems is instrumental in mitigating risks associated with the use of these systems (Merhout & Havelka, 2008). Accordingly, based on extant literature concerning the characteristics of quality information systems audits, the following hypothesis is posited:

H_2: *The contribution of the relationship between internal audit and information systems to information protection outcomes is positively moderated by the characteristics of quality information systems audits.*

2.3 Relationship between internal audit and information security management

Modern organizations are required to establish an information security department to safeguard themselves against contemporary risks and threats. According to the findings of Singleton and Singleton (2008), the internal audit department must maintain a relationship with information security management, as their collaboration yields benefits not only to both parties but also to the organization as a whole. The effectiveness of the relationship between internal audit and information security management is contingent upon the internal auditors' level of information technology knowledge, their attitude towards cooperation with information security personnel, top management's support for such collaboration, as well as organizational characteristics such as regulatory compliance requirements and formal communication channels (Steinbart *et al.*, 2012).

The findings derived from internal audits can provide essential measures to address vulnerabilities or gaps that may exist within the organization's security controls, which are monitored and overseen by information security management (Steinbart *et al.*, 2012). Additionally, these findings help ensure the quality and reliability of the information utilized by the organization, upon which internal audit missions largely depend on. Islam *et al.* (2018) concluded that the degree to which internal

audit is involved in security audits is determined by the auditors' competencies in governance, risk management, and regulatory compliance. Furthermore, the relationship between internal audit and information security management depends on the extent to which the organization's board of directors supports conducting relevant audits within the framework of best corporate governance practices (Islam *et al.*, 2018), as well as the presence of formal communication channels between internal audit and information security management (Steinbart *et al.*, 2012). Moreover, collaboration between members of both departments plays an equally critical role in maintaining an effective relationship between the two parties. Consequently, based on the extant literature concerning the relationship between internal audit and information security management, the following hypothesis is proposed:

H_3*: The contribution of the relationship between internal audit and information systems to information protection outcomes is positively influenced by the relationship between internal audit and information security management.*

3. Research methodology

3.1 Data collection, sample, and questionnaire

The purpose of this research is to examine the contribution of a strong relationship between internal audit and information systems to the effectiveness of information protection. The aim is to determine whether the information provided by information systems ensures an accurate and reliable representation of the organization's data, supports rational decision-making by management, and facilitates compliance with institutional regulations and legislation related to information protection.

The questionnaire (see Appendix 1), as one of the most important tools in most qualitative research studies (Rasamanie & Kanapathy, 2011; Arvaiova *et al.*, 2009; Prickett & Rapley, 2001) was developed based on a review of the relevant literature and investigates the effective contribution of internal audit to the protection of organizational information. Prior to distribution, the questionnaire was reviewed and refined through discussions with three internal auditors. It consists of closed-ended questions to avoid ambiguous interpretations, enabling easier response coding, and facilitating statistical analysis. Specifically, the questionnaire includes five closed-ended questions and 17 multiple-choice questions, using a five-point Likert scale where respondents indicate their level of agreement or disagreement, ranging from "Not at all" to "Very much." The questionnaire is divided into five sections. The first section contains five questions related to participants' demographic data. The second section includes four questions addressing the characteristics of the internal auditor. The third section contains five questions on the characteristics of the information systems quality control. The fourth section includes three questions concerning the

relationship between internal audit and information security management and the fifth section comprises four questions focused on the effective contribution of internal audit to the protection of information systems, which serves as the dependent variable of the study.

The questionnaire was distributed to banks institutions in Greece, specifically targeting internal auditors, information systems specialists, professionals in the field of information security, and employees of large organizations who are more likely to be involved in the implementation of relevant procedures and policies. A total of 152 emails were sent, and 131 responses were received. Of these, 17 were excluded due to missing essential data, resulting in 114 valid responses, corresponding to a response rate of 75%. According to the literature (Hair *et al.*, 2017), a minimum of 10–20 observations per predictor variable is required. Since this study includes three independent variables, at least 60 observations are necessary, making the sample size sufficient. Furthermore, Bollen (1989) recommends a sample size-to-parameter ratio of at least 5:1 for metric analysis. Thus, for the 17 questionnaire items, a minimum of 85 observations is required, a criterion that is also met.

3.2 Methodology analysis

The researchers examined the model using the SPSS 20 software in combination with AMOS 20. First, scale verification was performed. The scales were verified usingthe Cronbach's alpha estimate of credibility and the Exploratory Factor Analysis (EFA) method. The research hypotheses were verified by structural equation modeling (SEM) using the AMOS 20 software. For the purposes of the research, three independent variables and one dependent variable were identified. The dependent variable refers to the "effective contribution of internal audit to information protection" while the three independent variables represent the corresponding hypotheses refer to the "characteristics of the internal auditor", the "characteristics of information systems quality control", and the "relationship between internal audit and information security management".

4. Results

4.1. Descriptive Statistics

The descriptive statistics are provided below.

Table 1. Sample's descriptive statistics

		Frequency	Percent
Age group	18 - 30	23	20.2
	31 - 40	37	32.5
	41 – 50	43	37.7
	51 <	11	9.6
	Secondary Education	2	1.8

		Frequency	Percent
Education level	Bachelor's Degree	24	21.0
	Master's Degree	86	75.4
	Doctoral Degree	2	1.8
Employee Position	Internal Audit Department Employee	51	44.7
	Information Security Department Employee	26	22.8
	Accounting Department Employee	10	8.8
	Administration member	18	15.8
	Other	9	7.9
Experience	0-5 years	30	26.3
	6-10 years	27	23.7
	11-15 years	19	16.7
	16-20 years	22	19.3
	21years or more	16	14.0
Organization size (staff)	1 – 50	24	21.1
	51 – 100	21	18.4
	101 – 200	18	15.8
	201 <	51	44.7

Source: authors' survey, 2025

According to Table 1, of the 114 respondents, 44.7% work in the Internal Audit Department, and 75.4% hold a master's degree. Additionally, 37.7% are aged 41–50, while 26.3% have up to five years of work experience.

4.2 Testing of Cronbach's alpha coefficient

Results of testing of Cronbach's Alpha coefficient are shown in Table 2.

Table 2. Results of testing of Cronbach's Alpha coefficient of scales

No	Scales	Symbol	Number of obs. variables	Cronbach's Alpha
	Independent variables			
1	Characteristics of an Internal Auditor	CIA	4	0.748
2	Quality Control Characteristics of Information Systems	QCCIS	5	0.878
3	Relationship between internal audit and information security management	IAISM	4	0.725

No	Scales	Symbol	Number of obs. variables	Cronbach's Alpha
	Dependent variables			
4	The contribution of internal audit to information protection	IAIP	4	0.761

(source: authors' survey, 2025)

The results of the Cronbach's alpha tests for the ranges described in Table 2 above showed that these scales had the Cronbach coefficient of > 0.6.

4.3 Exploratory factor analysis (EFA)

The data that was obtained from the results was analyzed with the use of EFA and the SPSS 20 software support. The final results of the analysis are presented in Table 3.

Table 3. Results of testing of EFA of scales

Symbol	KMO	Sig	Cumulative of Variance	Eigen Value	Harman Value	VIF
CIA	0.697	0.000	0.57545	2.302	0.45475	2.602
QCCIS	0.805	0.000	0.61408	3.370	0.49471	2.622
IAISM	0.688	0.000	0.57464	2.299	0.45447	1.019
IAIP	0.658	0.000	0.58740	2.350	0.46141	

(source: authors' survey, 2025)

The suitability of the variables was verified by measuring the Kaiser-Meyer-Olkin sampling adequacy (Kaiser, 1974, 1970), following the rule that the value for KMO should be greater than 0.5 for any factor analysis to yield accurate results. The results of the above analyses showed that the KMO factor was above 0.5, the Bartlett test had a p-value p = 0.000 <0.05, the cumulative of variance was above 50%, according to Hair *et al.* (2010) the factor loadings were greater than 0.5 and the Eigen Value was greater than 1. Therefore, the criteria for the use of EFA suggested that the factors were consistent with the data set research.

4.4 Testing of model and results

Researchers use the Structural Equation Modeling (SEM) model to attest existing models and research hypotheses (Hai & Tu, 2019). The credibility of the measurement model's adaptation was evaluated using the CFI, the Standardized Root Mean Square Residual (SRMR) and the Root Mean Square Error of Approximation (RMSEA) (Kline, 2015; Zu *et al.*, 2010;). The criteria for evaluating the adjustment model recommended by the literature (Byrne, 2013; Hu

& Bentler, 1999) match all the statistics falling within the suggested range for appropriate model adaptation to data: CFI = 0.911 where the values ranged from 0 to 1, with values close to 0.90 or greater representing an agreeable adaptation to the data (Bentler, 1992) while a value of 1.0 indicates a perfect fit. RMSEA = 0.080 is exactly at the limit, since according to Hu and Bentler (1999), values below 0.080 indicate a suitable adjustment of the model. SRMR = 0.045 has a value of less than 0.080 and is acceptable according to Hu and Bentler (1999) while when index values are close to 0.00, they indicate a perfect fit. In addition, the model has 111 degrees of freedom and p = 0.000 <0.05 (Hair *et al.*, 2006) while Chi-square/df = 1.785 <5 (Lomax, 2004). According to the regression weights (Table 4), quality control characteristics of information systems and relationship between internal audit and information security management have the same significant impact on the contribution of the relationship between internal audit and information systems to information protection outcomes.

Table 4. Results of test for discriminant validity of research concepts and the results of hypotheses testing

Relationship			Estimate	S.E.	C.R.	P	Label
CIA	<--	IAIP	0.087	0.062	1.402	0.161	H_1 Rejected
QCCIS	<--	IAIP	0.986	0.106	9.332	0.000***	H_2 Accepted
IAISM	<--	IAIP	0.858	0.100	8.546	0.000***	H_3 Accepted

(source: authors' survey, 2025)

The presence of a significant positive correlation (t=9.332, p<0.01) between the independent variable—namely, the characteristics of information systems quality control—and the dependent variable, which reflects the relationship between internal audit and information systems in achieving information protection outcomes, is consistent with the findings of previous studies (Yeghaneh *et al.*, 2015; Stoel *et al.*, 2012; Merhout & Halveka, 2008). Specifically, these studies emphasize the pivotal role of quality control mechanisms in enhancing the efficiency and reliability of information systems, which, in turn, strengthens internal audit processes. These findings affirm that well-integrated quality control procedures facilitate more effective collaboration between information systems and internal audit functions, ultimately contributing to the safeguarding of information confidentiality, integrity, and availability. Moreover, the findings corroborate the results of Stoel *et al*. (2012) and Yeghaneh *et al*. (2015), highlighting audit methodology as a pivotal determinant of information systems audit quality, while simultaneously extending the international literature with empirical evidence from the banking sector. Finally, to achieve high-quality information systems audits within the banking sector, internal auditors need to devote a substantial portion of their time to the auditing process.

Similarly, the significant positive correlation (t=8.546, P<0.01) identified between the third independent variable—pertaining to the relationship between internal audit and information security management—and the dependent variable is also in alignment with the results of prior relevant research (Islam *et al.*, 2018; Steinbart *et al.*, 2012; Singleton & Singleton, 2008). These surveys identify a close and strategic relationship between internal auditors and information security teams strengthening organizational resilience against information-related risks. Integrating security controls into internal audit activities improves the organization's ability to detect, assess, and mitigate cybersecurity threats, thereby reinforcing the overall information protection framework.

In contrast to prior studies (Usman *et al.*, 2023; Hepworth *et al.*, 2022; Lois *et al.*, 2021), internal audit characteristics are not significantly correlated (t = 1,402, p > 0.01) with the internal audit's contribution to information protection. This result diverges from the conclusions drawn in prior studies which argue that factors such as auditor independence, professional competence, and operational objectivity are crucial in enhancing the audit function's capacity to contribute meaningfully to information security outcomes.

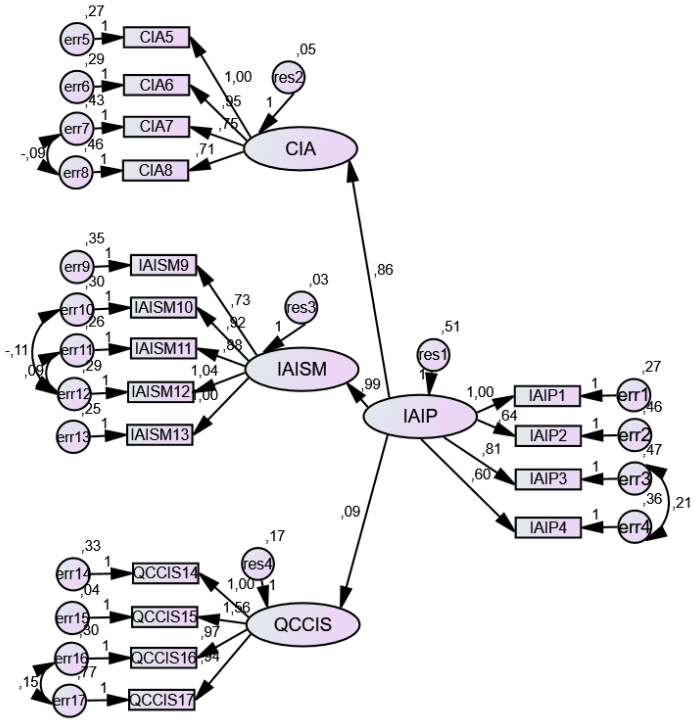

Figure 1. Results of the model testing
Source: authors' survey, 2025

The discrepancy of these findings compared to previous studies (Usman *et al.*, 2023; Hepworth *et al.*, 2022; Lois *et al.*, 2021) may stem from sector-specific contexts, organizational culture, or differences in auditors' access to technical resources and training, suggesting that the impact of traditional audit characteristics on information protection may not be as universal as previously assumed. Additionally, this divergence may be attributed to specific attributes of the respondents, such as limited communication skills or the ethical codes prevailing in the respective banking institutions concerning professional standards. Finally, it is worth noting that these findings highlight the importance of investigating additional mediating factors, such as organizational support, contextual constraints, and evolving information technology risks, which may shape the internal audit function's capacity to contribute effectively to information security outcomes.

5. Conclusion

5.1 Findings

In the modern era, the increasing reliance of organizations on their information systems makes the protection of information a top priority. The rapid advancement of technology, while bringing new opportunities, also introduces new risks, making the safeguarding of data against malicious threats an urgent necessity. The growing frequency of cybersecurity incidents, along with their significant financial and reputational consequences, is prompting organizations to place greater emphasis on managing cybersecurity risks (Steibart *et al.*, 2018). Monitoring is a key element of effective internal audit (COSO, 2004). Therefore, it makes sense that consistently monitoring information security controls can enhance the overall performance of an organization's information security program (Ransbotham & Mitra 2009).

This study examined the relationship between internal audit and information systems in achieving information protection outcomes within Greek banks. Specifically, the research investigated whether characteristics of internal auditors, the quality control features of information systems, and the relationship between internal audit and the information security management department contribute to the link between internal audit and information systems in supporting information protection outcomes.

The findings of this study indicate that both the quality control characteristics of information systems and the level of collaboration between internal audit and information security management play a significant and positive role in enhancing the internal audit function's contribution to safeguarding organizational information assets. These results align with prior research that underscores the importance of strong system controls and cross-functional coordination in ensuring effective information protection (Islam *et al.*, 2018; Yeghaneh *et al.*, 2015). For instance, Stoel

et al. (2012) and Steinbart *et al.* (2012) emphasized that effective internal audit involvement, particularly when integrated with robust information system frameworks and continuous oversight, leads to improved security outcomes and risk mitigation. Similarly, Merhout and Halveka (2008), as well as Singleton and Singleton (2008), argued that internal auditors can add substantial value to information security initiatives, especially when internal controls are well-defined and when auditors possess a strong understanding of information technology governance principles.

Interestingly, contrary to what has been suggested in more recent studies (Usman *et al.*, 2023; Hepworth *et al.*, 2022; Lois *et al.*, 2021;), this study found no significant relationship between the intrinsic characteristics of the internal audit function—such as independence, objectivity, or technical expertise—and its actual contribution to information protection. This divergence may suggest that structural and procedural integration with information security functions could outweigh traditional audit attributes in determining audit effectiveness in this domain. As such, the evolving complexity of cybersecurity environments might necessitate a shift in focus from internal audit's formal characteristics to more dynamic factors such as collaboration, adaptability, and system-level controls.

5.2 Theoretical – practical implications

This study contribute to the limited related literature using a sample of banking organizations and to support the effectiveness of an organization’s information security efforts by developing and maintaining a positive, collaborative relationship with the information security function.Furthermore, this study shows that the internal audit can contribute to the efficacy of a bank's information security efforts by developing and supporting a positive collaborative relationship with the information protection function. Our results can be used by audit managers to identify risks and opportunities associated with the information systems in banks. Audit managers may wish to self-evaluate each factor to determine their ability to improve their information technology audits. Audit managers can also use the findings to identify and prioritize training and development opportunities, focusing on the factors considered most critical for audit success. In conclusion, the study bears substantial practical significance for banking institution boards, cybersecurity and information management officers, regulatory authorities, bank clients, and other relevant stakeholders, including financial analysts and the academic community, by informing policy development and guiding future scholarly inquiries in the domain of cybersecurity risk management.

5.3 Limitations – future research

The research also has limitations related to the structure of the questionnaire, such as the use of closed-ended questions, which restrict the ability to collect more

detailed information. This constraint may have restricted the depth of the data collected, particularly regarding the influence of cultural and psychological factors that often shape employees' attitudes and behaviors. Additionally, the small sample size leads to limited conclusions but also provides motivation for future research focused on a larger sample and a broader range of targeted questions that would further contribute to the topic under examination. The relatively small sample size, as well as the position held by each respondent, may limit the generalizability of the study's results. Employees in the information security department may be more knowledgeable about information technology audits and might possess a broader range of experience with information systems. Finally, future research could focus on further exploring this specific topic using a sample of individuals working in bank subsidiaries in the rest of Europe.

References

Arvaiova, M., Aspinwall, E. M., & Walker, D. S. (2009) "An initial survey on the use of costs of quality programmes in telecommunications", *The TQM Journal,* vol. 21, no. 1: 59-71

Bentler, P. M. (1992) "On the fit of models to covariances and methodology to the Bulletin", *Psychological bulletin,* vol. 112, no. 3: 400-404

Betti, N., & Sarens, G. (2021) "Understanding the internal audit function in a digitalised business environment", *Journal of Accounting & Organizational Change,* vol. 17, no. 2: 197-216

Bollen, K. A. (1989) "A new incremental fit index for general structural equation models", *Sociological methods & research,* vol. 17, no. 3: 303-316

Butler, T., Gozman, D., & Lyytinen, K. (2023), "The regulation of and through information technology: Towards a conceptual ontology for IS research", *Journal of Information Technology,* vol. 38, no. 2: 86-107

Byrne, B. M. (2013) *Structural equation modeling with LISREL, PRELIS, and SIMPLIS: Basic concepts, applications, and programming*, New York: Psychology Press

Chambers, A. D., & Odar, M. (2015) "A new vision for internal audit", *Managerial Auditing Journal,* vol. 30, no. 1: 34-55

Christ, M. H., Eulerich, M., Krane, R., & Wood, D. A. (2021) "New frontiers for internal audit research", *Accounting Perspectives,* vol. 20, no. 4: 449-475

COSO (2004) "Enterprise risk management — integrated framework: executive summary", available on-line at https://www.coso.org/_files/ugd/3059fc_61ea5985b03c4293960642fdce408eaa.pdf

Czerniawska, M., & Szydło, J. (2021) "Do values relate to personality traits and if so, in what way? – Analysis of relationships", *Psychology Research and Behavior Management*, 511-527

Drogalas, G., Pazarskis, M., Mitskinis, D., & Koulikas, A. (2024) "The contribution of internal audit to fraud audit: evidence from Greece", *International Journal of Critical Accounting*, vol. 14, no. 1: 50-67

Drogalas, G., Petridis, K., Petridis, N. E., & Zografidou, E. (2020) "Valuation of the internal audit mechanisms in the decision support department of the local government organizations using mathematical programming", *Annals of Operations Research,* vol. 294: 267-280

Flowerday, S., & von Solms, R. (2005) "Continuous auditing: Verifying information integrity and providing assurances for financial reports", *Computer Fraud & Security,* vol. 2005, no. 7: 12-16

Hai, P. T., & Tu, C. A. (2019) "Research on factors affecting organizational structure, operating mechanism and audit quality: An empirical study in Vietnam", *Journal of Business Economics and Management,* vol. 20, no. 3: 526-545

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2010) *Multivariate Data Analysis*, New Jersey: Pearson Prentice Hall

Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., & Tatham, R. L. (2006) *Multivariate data analysis*, 6th edition, New Jersey: Pearson Prentice Hall

Hair, J., Hollingsworth, C. L., Randolph, A. B., & Chong, A. Y. L. (2017) "An updated and expanded assessment of PLS-SEM in information systems research", *Industrial Management & Data Systems,* vol. 117, no. 3: 442-458

Havelka, D., & Merhout, J. W. (2013) "Internal information technology audit process quality: Theory development using structured group processes", *International Journal of Accounting Information Systems*, vol. 14, no. 3: 165-192

Hazaea, S. A., Tabash, M. I., Khatib, S. F. A., Zhu, J., & Al-Kuhali, A. A. (2020) "The impact of internal audit quality on the financial performance of Yemeni commercial banks: An empirical investigation*", Journal of Asian Finance, Economics and Business,* vol.7, no. 11: 867-875

Hazaea, S. A., Zhu, J., Khatib, S. F. A., & Elamer, A. A. (2023) "Mapping the literature of internal auditing in Europe: A systematic review and agenda for future research", *Meditari Accountancy Research,* vol. 31, no. 6: 1675-1706

Hepworth, R. L., Greenman, C., Esplin, D., & Johnston, R. (2022) "Cybersecurity and data privacy: The rising expectations within internal audit", *Journal of Forensic and Investigative Accounting,* vol. 14, no. 3: 454-465

Hu, L. T., & Bentler, P. M. (1999) "Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives", *Structural Equation Modeling: A Multidisciplinary Journal,* vol. 6, no. 1: 1-55

Islam, M. S., Farah, N., & Stafford, T. F. (2018) "Factors associated with security/cybersecurity audit by internal audit function: An international study", *Managerial Auditing Journal,* vol. 33, no. 4: 377-409

Kaiser, H. F. (1970) "A second generation little jiffy", *Psychometrika,* vol. 35, no. 4: 401-415

Kaiser, H. F. (1974) "An index of factorial simplicity", *Psychometrika,* vol. 39, no. 1: 31-36

Khando, K., Gao, S., Islam, S. M., & Salman, A. (2021) "Enhancing employees information security awareness in private and public organisations: A systematic literature review", *Computers & security,* vol. 106: 102267

Kim, S. (2022) "Critical success factors evaluation by multi-criteria decision-making: a strategic information system planning and strategy-as-practice perspective", *Information,* vol. 13, no. 6: 1-26

Kline, R. B. (2015) *Principles and practice of structural equation modelling*, New York: Guilford publications

Kohli, R., & Melville, N. P. (2019) "Digital innovation: a review and synthesis", *Information Systems Journal*, vol. 29, no. 1: 200-223

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,* vol. 13, no. 1: 25-47

Lomax, R. G. (2004) *A beginner's guide to structural equation modeling*, New York: Psychology Press

Malaurent, J., & Avison, D. (2015) "From an apparent failure to a success story: ERP in China-Post implementation", *International Journal of Information Management*, vol. 35, no. 5: 643-664

Merhout, J. W., & Havelka, D. (2008) "Information Technology Auditing: A value-added IT Governance Partnership between IT management and audit", *Communications of the Association for Information Systems*, vol. 23: 463-482

Nordin, I. G. (2023) "Narratives of internal audit: The Sisyphean work of becoming "independent", *Critical Perspectives on Accounting,* vol. 94: 102448

Otero, A. R. (2019) *Information technology control and audit*, USA: CRC Press, Taylor & Francis Group

Pasculli, L. (2020) "The global causes of cybercrime and state responsibilities: Towards an integrated interdisciplinary theory", *Journal of Ethics and Legal Technologies,* vol. 2, no.1 :48-74

Prickett, T. W., & Rapley, C. W. (2001) "Quality costing: A study of manufacturing organizations. Part 2: Main survey", *Total Quality Management,* vol. 12, no. 2: 211-222

Ramamoorti, S. (2003) *Internal auditing: History, evolution, and prospects*, Altamonte Springs: The Institute of Internal Auditors Research Foundation

Ransbotham, S. & Mitra, S. (2009) "Choice and chance: A conceptual model of paths to information security compromise", *Information Systems Research*, vol. 20, no. 1: 121-139

Rasamanie, M., & Kanapathy, K. (2011) "The implementation of cost of quality (COQ) reporting system in Malaysian manufacturing companies: Difficulties encountered and benefits acquired", *International Journal of Business and Social Science,* vol. 2, no. 6: 243-247

Rezvani, A., Dong, L., & Khosravi, P. (2017) "Promoting the continuing usage of strategic information systems: The role of supervisory leadership in the successful implementation of enterprise systems", *International Journal of Information Management*, vol. 37, no. 5: 417-430

Rîndaşu, S. M. (2017) "Emerging information technologies in accounting and related security risks–what is the impact on the Romanian accounting profession", *Journal of Accounting and Management Information Systems*, vol. 16, no. 4: 581-609

Salihu, A., & Hoti, X. B. (2019) "The effect of IT audit on security incidents", *International Journal of Scientific & Technology Research*, vol. 8, no. 8: 1342-1347

Shiau, W. L., Wang, X., & Zheng, F. (2023) "What are the trend and core knowledge of information security? A citation and co-citation analysis", *Information and Management*, vol. 60, no. 3: 103774

Singleton, T. W., & Singleton, A. J. (2008) "The potential for a synergistic relationship between information security and a financial audit", *Information Security Journal: A Global Perspective*, vol. 17, no. 2: 80-86

Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2012) "The relationship between internal audit and information security: An exploratory investigation", *International Journal of Accounting Information Systems*, vol. 13, no. 3: 228-243

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*, vol. 71: 15-29

Stoel, D., Havelka, D., & Merhout, J. W. (2012) "An analysis of attributes that impact information technology audit quality: A study of IT and financial audit practitioners", *International Journal of Accounting Information Systems,* vol.13: 60-79

Thomson, K. L., & von Solms, R. (2005) "Information security obedience: A definition", *Computers & Security*, vol. 24, no. 1: 69-75

Usman, A., Che-Ahmad, A., & Abdulmalik, S. O. (2023) "The role of internal auditors characteristics in cybersecurity risk assessment in financial-based business organizations: A conceptual review", *International Journal of Professional Business Review*, vol. 8, no. 8: 1-31

Yang, Y., Ying, H., Jin, Y., Cheng, H. K., & Liang, T. P. (2021) "Special issue editorial: Information systems research in the age of smart services", *Journal of the Association for Information Systems*, vol. 22, no. 3: 579- 590

Yeghaneh, Y. H., Zangiabadi, M., & Firozabadi, S. M. D. (2015) "Factors Affecting Information Technology Audit Quality", *Journal of Investment and Management*, vol. 4, no. 5: 196-203

Zu, X., Robbins, T. L., & Fredendall, L. D. (2010) "Mapping the critical links between organizational culture and TQM/Six Sigma practices", *International Journal of Production Economics,* vol. 123, no. 1: 86-106

Appendix 1: Questionnaire

Kindly, evaluate the subsequent variable items using the criterion shown below:

- Strongly disagree
- Disagree
- Neither disagree / nor agree.
- Agree
- Strongly agree

Characteristics of an Internal Auditor

- Do internal auditors possess technical knowledge related to information technology (e.g., CISA/CISSP certification)?
- Do internal auditors possess communication skills?
- Do internal auditors demonstrate professional ethics and integrity?

Quality Control Characteristics of Information Systems

- Does internal auditing follow a specific methodology across different audits?
- Is the time allocated for conducting an internal audit sufficient?
- Is there good cooperation and support between the auditor, the auditee, and senior management during the conduct of an audit?
- In the event of organizational changes, is sufficient time given to the internal audit employees to understand the changes in the procedures that these changes entail
- Are the objectives and scope of an audit clearly defined?

Relationship between internal audit and information security management

- Do internal audit employees clearly communicate the scope and purpose of an audit?
- Do internal audit employees approach the information security staff with a collaborative attitude during an audit?
- Does senior management encourage collaboration between internal audit and information security?
- Are there official communication channels within your organization between internal audit and information security?

The contribution of internal audit to information protection

- Does the internal audit function perform regular evaluations related to confidentiality and security?
- Does internal control assist in identifying problems concerning information security?
- Internal control contributes to the detection of security breach incidents both before and after they cause damage.
- Does internal audit contribute to the reduction of security incidents?