INTEGRATING CYBERSECURITY INTO INTERNAL AUDIT THROUGH A SELF-ASSESSMENT TOOL BASED ON A SYSTEMATIC LITERATURE REVIEW

DOI: https://doi.org/10.36004/nier.es.2025.1-08
JEL Classification: M42, L86
UDC: 005.922.1+004.056.5

Cristina-Raluca CERNOVSCHI

PhD students, Ștefan cel Mare University of Suceava, Romania

https://orcid.org/0009-0001-6548-2608
cristina.cernovschi09@gmail.com

Marius-Sorin CIUBOTARIU

PhD in economics, Ștefan cel Mare University of Suceava, Romania

https://orcid.org/0000-0002-8560-9223
marius.ciubotariu@usm.ro

Svetlana MIHAILA

PhD in economics, Academy of Economic Studies of Moldova

https://orcid.org/0000-0001-5289-8885
svetlana.mihaila@ase.md

Received 01 March 2025

Accepted for publication 30 May 2025

SUMMARY

In an era where technological innovations are reshaping organisations' operational strategies and introducing new challenges related to data protection and privacy, internal auditing is compelled to expand its scope to address the risks associated with cybersecurity. In this context, we propose a systematic review of 16 studies indexed in the Web of Science database, covering the period from 2017 to 2025. These studies were selected based on clear inclusion and exclusion criteria, with the aim of capturing the interdependence between the internal audit function and an organisation's cybersecurity, in order to assess the contribution of internal auditors to mitigating cyber risks. The results are presented in two forms: first, a categorization of the reviewed studies according to the key ideas addressed by the authors; and second, a company-level selfassessment tool for integrating cybersecurity into the internal audit process. These results have dual relevance: firstly, they serve academics, who can more easily track the main interests in this area as well as the existing gaps in the literature; secondly, they help companies diagnose the maturity level of cybersecurity integration into internal audit processes. However, these results are limited by the analysis of a small number of studies, as restricted access to some articles prevented their inclusion in the analysis.

Keywords: *internal audit, cybersecurity, inovative technology, assurance, cyber risks*

INTRODUCTION

With the increasing assimilation of manual processes by intelligent technologies, cybersecurity is becoming an emerging topic among internal audit committees. The main risk factor of cyber-attacks is the misappropriation of a company's assets or the manipulation of data on a computer through the illegal use of hacking knowledge (Dutchak, R., et. al.,2021) and differs from other illegalities in that it takes place in cyberspace, not requiring the offender to move physically to the scene of the action. According to a report by IBM (2024) analyzing the financial impact of data breaches globally, in 2024 cyberattacks cost companies an estimated $4.88 million, up 10 percent from the previous year, and on top of that this was the highest since the pandemic. Cybercriminals operate with complicated and difficult to intercept schemes, and in these situations to which all entities that have included artificial intelligence in their business are involuntarily exposed, internal audit is seen as a savior, due to the assurance role and independence of this department within an organization. Our study focuses on the challenges faced by internal auditors while integrating cybersecurity into their assignments and their chances of success. Through a careful literature review, we tried to summarize the added value that the internal audit department brings to the organization in minimizing cyber risks. The results of our work materialized in a thematic framing of the research available to the general public so far in the Web of Science database, identifying three areas of interest: the role and updated competencies of internal auditors, risk minimization solutions developed following security breaches, and the factors leading to a quality cyber audit. This paper contributes to the literature, in addition to providing support to internal audit professionals, and aims to draw the attention of regulators to the lack of clear and up-to-date regulatory frameworks for the current context.

LITERATURE REVIEW

Currently, most organisations store their information on IT infrastructures, from business partner details to financial data, leading to a reliance on virtual environments and thus increasing the vulnerability of companies to cybersecurity threats. In addition, the latest technological innovations, while offering multiple benefits, expose organisations to the risk of compromise of sensitive information. All this means that internal audit has to reconsider its mode of action and proactively engage in minimizing cybersecurity risks. In this context, the literature tries to cover as broad a scope as possible on the relationship between internal audit and cybersecurity.

Professionals in the field provide us with studies that trace the ways in which internal auditing can help prevent data breaches; internal auditing should consider in its activity what cyber threats the company is facing, then it should propose the implementation of special programs for monitoring the company's digital behavior and develop a set of procedures for the use of cyberspace (Dutchak, et. al., 2021). Moreover, some authors (Usman, et. Al., 2023) attempt to characterize internal auditors and assess their risk awareness, citing professional ethics, personality traits and rewards as influential factors in detecting cybersecurity issues. Similarly, (Jiang, 2024). statistically demonstrates that auditors' rewards grow directly proportional to the company's exposure to attacks.

Also, to support internal auditors, researchers analyze the level of vulnerability of business sectors to risks associated with IT infrastructure, according to (Arcuri, et. al., 2018), the financial sector is considered the most prone to cyber-attacks because banks are additionally tasked with defending their financial assets. Analogously, (Gulyas & Kiss. 2023), manage to identify the most common attack methods that cybercriminals use on financial institutions (social engineering and phishing, ransomware attacks) and propose customized solutions for this industry (blockchain technology implementation) which in their opinion should be treated differently from the others for the direct impact it has on the economy. Furthermore, (Kelton, & Yang, 2025) find that if a company operating in a particular industry suffers a cyber attack, the whole industry is affected and the effects are usually reflected on reputation (Fotis, 2024). In addition to reputation, the directly affected company faces costs related to IT repairs, legal expenses or business continuity disruptions. We can even find in the literature a guide proposed by Sánchez-García which he calls CRAG, and which contains 7 steps and 28 activities, accompanied by practical applications and implementation examples, as well as aspects to be taken into account when writing the audit report. Ferreira et al. (2025) based on risk management theory, presents processes and tools used in internal audit to assess and continuously improve cyber controls. such as interdepartmental cooperation, continuous audit or real-time monitoring. Consistent with the other context of smart technology development, Chin et al. (2025) built a cybersecurity auditing model based on an autonomous agent using Large Language Model, which can identify breaches of security policies such as password violations.

After reviewing the scientific sources dealing with cybersecurity and internal audit, we can conclude that although the main issues are touched upon, the dynamics of the subject mean that they cannot cover all aspects in depth. This conclusion stems from the fact that cybersecurity is a constantly evolving field, influenced by technological innovations, and the speed with which cyber attackers act. Therefore, in the following, we will give a complete overview of all the topics discussed at the moment to see in which areas there is still work to be done and where the literature has reached saturation point.

METHODOLOGY

An important step in achieving the proposed goal is the choice of an appropriate research method, so in order to be able to present an overview of the involvement of internal auditors in reducing the threat of cybersecurity breaches, we considered it appropriate to use the SLR (systematic literature review) method, which consists of an analysis of all existing studies in a database on a given topic. In our case, we chose Web of Science as the documentation space and the search expression was „cybersecurity in internal audit". As to how the relevant studies were selected, we have included all the details in Table 1.

Table 1.
Selection criteria for studies included in the analysis

Database	Web of science
Query	Cybersecurity in Internal Audit
Time period	2017-2025
Initial result	37 studies
Exclusion criteria:	
• - Language	English=> 37 studies
• - Document type	Article => 30 studies
• - Availability	OpenAccess => 16 studies available
Final result	16 studies analysed

Source: *own processing*

As can be seen in the table above, the studies included in the analysis were conducted over a period of 9 years, we also preferred to focus only on articles, 4 proceeding papers, 3 review articles and 2 early access were excluded. Our search was limited by open access to papers, 14 studies dealing with the topic of adopting cybersecurity risks in annual internal audit plans, conducted in the years 2024 and 2025, were eliminated. Limiting open access influences the results as more recent studies that certainly contain novel approaches could not be included because they could not be fully analyzed. Refinement of the database resulted in 16 available studies that met all criteria, each study was subjected to critical interpretation and thematically categorized. Specifically, we read all articles in their entirety, identified the purpose and outcomes, first extracted them all into a table, then based on keywords identified common purposes, and then created three thematic categories:

the role of internal auditors in ensuring cybersecurity, determinants of effective cyber auditing, and practical examples of breach or audit. Each individual study has been classified into one of the three categories and discussed, so that in the end we can synthesize the current knowledge on integrating cyber risks into internal audit activities. The thematic coding process may include an inherent degree of subjectivity as it was done manually and not with the help of any computerized system. Based on the main findings of the 16 thoroughly analyzed studies, we constructed a self-assessment sheet on the need for integrating cybersecurity into internal audit processes addressed to the board of directors. The sheet is divided into 4 points of 5 questions each, the answer to which can be yes or no, in case those who fill in the form feel the need to explain the answer, we have also created an explanation box. The structure and interpretation are drawn from the risk-based audit theory according to which the audit should correspond to the organisation's exposure and the effectiveness of control measures. The first item looks at the degree of exposure, the more yes answers, the more exposed the company is, criterion number 2 looks at the measures a company takes to protect itself from cyber risks, and the last two criteria look at the positioning of the internal audit function and the qualities that the internal auditor should possess. A majority of yes answers in these last three sections means that the entity has understood the current context and has adapted to the new requirements, and a negative answer means that the internal audit function urgently needs to be reconfigured. Briefly, after analyzing the 16 studies, based on the scopes, we managed a thematic grouping of the trends in the field, and based on the extracted results we developed a self-assessment sheet on the understanding of the need to adapt internal audit processes in the context of cybersecurity.

RESULTS AND DISCUSSION

The omnipresence of cyber risk and the major financial losses created by data privacy breaches have led to the expansion of the work of internal auditors who are charged with providing independent assurance on the quality of information systems, procedures and strategy to mitigate cyber threats. In addition, the increasing pressures generated by the contagion of damage to other organisations operating in the same environment are driving the audit department to mobilize to prevent threats. In order to gain a clearer understanding of the trends in research on this topic, we conducted a literature review and then grouped the relevant studies according to thematic areas, to be able to make comparisons between findings, but also proposals.Table 1 below lists studies that focus on the roles that internal auditors play in maintaining strong cybersecurity, the changes that have occurred in the work of auditors, and how three-dimensional internal auditing models have evolved from compliance to proactive engagement.

Table 2.

Studies based on identifiying the role of internal audit in cybersecurity

Author	Title	Aim, Objectives	Results
Bozkus Kahyaoglu, S., & Caliyurt, K. (2018)	Cyber security assurance process from the internal audit perspective	The study examines the issues, vulnerabilities and limitations of the internal audit function in ensuring cybersecurity	The authors note that the role of auditors should be expanded from support to strategic advice, they should provide assurance not only on compliance but also on the methods adopted to manage cybersecurity risks, and cybersecurity should be included in annual audit plans
Stafford, T., Deitz, G., & Li, Y. (2018)	The role of internal audit and user training in information security policy compliance	The study focuses on the role of internal auditors in identifying non-compliance with information security policies, focused on the organisation's human resources.	Research has shown that improving a company's cybersecurity depends on internal audits that identify both non-compliance in the application of procedures and the underlying reasons for breaches.

Author	Title	Aim, Objectives	Results
Betti, N., & Sarens, G. (2021)	Understanding the internal audit function in a digitalised business environment	The study investigates the changes that have occurred in the internal audit function with the digitization of business	The researchers emphasize the need for increased attention to cybersecurity risks on the part of internal auditors and the need to hone digital literacy. They also emphasize the advisory role and changing the way internal auditors work.
Elmaasrawy, H. E., & Tawfik, O. I. (2025)	Impact of the assertive and advisory role of internal auditing on proactive measures to enhance cybersecurity: evidence from GCC	This paper aims to determine the impact that the internal auditor's assurance and advisory role has on improving cybersecurity	The results of the study show that the proactive organisational, human and technical measures taken to improve cybersecurity are positively influenced by the assurance and advisory role of internal audit, while the traditional role influences only technical measures.
Guohong, Z., Zhongwei, X., Feng, H., & Zhongyi, X. (2025)	The audit committee's IT expertise and its impact on the disclosure of cybersecurity risk	The research aims to assess how the internal auditor's IT skills influence the extent to which internal auditors identify and report cybersecurity risks	The findings of the study state that internal audit with IT skills report cybersecurity risks more often, and for entities with weak corporate governance and weak internal controls, the influence of internal auditors with IT skills is greater

Source: own processing based on literature

The following table summarizes 6 studies indexed in the Web of Science database that emphasize the importance of internal auditing in maintaining cybersecurity in an organisation. The authors of these papers use mixed research methods, both conceptual analysis, interviews and surveys or questionnaires. All results have at their center the role of the internal auditor and the idea that traditional duties have become insufficient for today's user requirements. The common themes show that it is not enough for internal auditors to focus only on compliance with entity, state or other internationally mandated policies and procedures, but that they need to be actively involved in evaluating the organisation's strategies and to acquire technical skills. This means assessing password generation policies, how passwords are managed, whether antivirus applications are up to date and working, and if signs of a cyber-attack occur, how employees respond. In addition, they need to conduct cyber-attack simulations to assess the resilience of prevention plans and come up with recommendations. In short, today's internal auditors need to do more than just check what's already been done; they need to help prevent problems before they occur. If we were to look at when the first studies on the role of the internal auditor in preventing cyber risks originated, the first year of publication is 2018. Coupled with the fact that in the same year the General Data Protection Regulation was also implemented and interpreted through or say that this research emerged as a response to coercive pressures that forced organisations to comply with these rules. With the implementation of this regulation, a number of new responsibilities have been placed on internal auditors, given that the subject of personal data is a sensitive topic that needs to be dealt with at the moment, the role of auditors is starting to tend towards strategic partner.

After having identified all the research that is only on the role of internal auditors in maintaining cybersecurity, the next aspect addressed by specialists in the field is related to practical examples, which present with the help of case studies both audit models tested in organisations and data breaches. These papers have been grouped in Table 3 for easier visualization.

Table 3.
Studies based on organisational measures and response models

Author	Title	Aim, Objectives	Results
Sabillon, R. (2018)	A Practical Model to Perform Comprehensive Cybersecurity Audits	This paper presents a cybersecurity audit model that can be used by internal auditors regardless of the type or size of the organisation.	The results materialize in the development of a Cybersecurity Security Audit Model (CSAM). This CSAM has 18 domains; domain 1 is specific to national cybersecurity and domains 2-18 can be implemented in any organisation.
Bakarich, K. M., & Baranek, D. (2020)	Something Phish-y is Going On Here: A Teaching Case on Business Email Compromise	This study aims to draw attention to the need to include cybersecurity risks in the audit plan by illustrating a real case	The authors draw attention to the large financial losses that a cyber-attack has caused due to the lack in implementing internal controls and correlate this problem with the deficiencies discovered in company financial reporting
Le, T. D., Le-Dinh, T., & Uwizeyemungu, S. (2024)	Search engine optimization poisoning: A cybersecurity threat analysis and mitigation strategies for SMEs	The research addresses the vulnerability of SMEs to cyber attacks and proposes solutions to mitigate the risks in relation to the resources available to them.	The results of the study emphasize the need to adopt an organisational culture based on cyber-risk awareness and the need for cybersecurity audits to combat cyber-attacks.

Source: own processing based on literature

Examining the papers summarized above, we note the focus on situations that already exist in practice, ranging from evaluating cybersecurity audit models, to calculating financial losses from cyberattacks, to presenting methods of operating small and medium-sized businesses. Given that only three studies were included in this category, there is less emphasis on what already exists in practice. This disproportion indicates that the literature provides an overview but fails to identify implementation methods for varied operational environments. While the focus is on sophisticated cybersecurity auditing methods, it does not take into account the limited resources of SMEs and the fact that these methods can only be implemented by large enterprises. In addition, as regulations are not clear enough and internal auditors are new to cybersecurity auditing, there are few examples of models and none are customized to business sectors. We therefore see a need for studies targeted at real areas of application and believe that we need to pay more attention to already known incidences in order to learn from them.

The third and broadest category comprises 8 papers that share the common goal of identifying factors that influence the quality of an internal cybersecurity audit. The details have been summarized in Table 4, and in the following we aim to extract from the table the elements that add value to the cyber audit.

Table 4.

Factors Influencing the Effectiveness of Internal Audit in Ensuring Cybersecurity

Author	Title	Aim, Objectives	Results
Islam, M.S., Farah, N. and Stafford, T.F(2018)	Factors associated with security/ cybersecurity audit by internal audit function	This study aims to see whether certain characteristics of the audit committee and firm management are positively associated with cybersecurity risk reduction.	The authors found that the degree of involvement of internal auditors determines an effective security audit, the active presence of the Board of Directors helps internal audit in identifying cybersecurity risks, and additional certifications do not increase the effectiveness of cybersecurity audit.
Slapničar, S., Vuko, T., Čular, M., & Draščček, M. (2022).	Effectiveness of cybersecurity audit	The purpose of this paper is to measure the effectiveness of internal cybersecurity auditing in terms of several determinants.	The results of the research materialize in a Cybersecurity Audit Index composed of three dimensions: planning, conducting the audit activity, and reporting; the index scores vary between companies, is positively associated with the quality of risk management, and does not significantly correlate with reducing the likelihood of a cyber attack.
Masoud, N., & Al-Utaibi, G. (2022)	The determinants of cybersecurity risk disclosure in firms' financial reporting: Empirical evidence	The research aims to analyze the relationship between reporting deficiencies and the degree of disclosure of cybersecurity risks	The study results show that organisations that have suffered cyber-attacks increase the quality of their financial reporting, and auditors intensify the audit process by focusing on information breach risks
Slapničar, S., Axelsen, M., Bongiovanni, I., & Stockdale, D. (2023)	A pathway model to five lines of accountability in cybersecurity governance	This paper examines the influence of the relationship between the management and internal audit in ensuring a cybersecurity.	The study argues that the role of internal auditors is under-emphasized in ensuring cybersecurity in organisations. Furthermore, the researchers believe that managers and employees should be more involved and communicate with the internal audit department so that the latter can include a cybersecurity audit in its plan.
Zhou, F., & Huang, J. (2024)	Cybersecurity data breaches and internal control	The purpose of the research is to analyze how organisations that have experienced cybersecurity incidents respond through the lens of internal control.	The researchers find that management change is positively correlated with improved internal controls based on preventing cyber-attacks, and usually after an organisation faces such a problem it tends to improve its policies to avoid a recurrence.

Author	Title	Aim, Objectives	Results
Héroux, S., & Fortin, A. (2024)	How the three lines of defense can contribute to public firms' cybersecurity effectiveness	The paper focuses on how public entities manage cybersecurity issues with an emphasis on the three lines of defense	The results of the study emphasize the need for collaboration between internal audit and IT departments to strengthen the data security system as well as the fact that effective internal audit alone does not eliminate problems, but that each line of defense must be actively involved.
Calvin, C., Eulerich, M., & Holt, M. (2025)	Characteristics of cybersecurity and IT involvement by the IA activity	The study tracks the level of involvement of internal audit in cybersecurity assurance activities	The study argues that the role of internal auditors is under-emphasized in ensuring cybersecurity in organizations. Furthermore, the researchers are of the opinion that managers and employees should be more involved and communicate with the internal audit department so that the latter can include a cybersecurity audit in its plan.
Vuko, T., Slapničar, S., Čular, M., & Drašček, M. (2025)	Key drivers of cybersecurity audit effectiveness: A neo-institutional perspective	The research analyzes how coercive forces, normative forces and mimetic forces contribute to cybersecurity assurance	The authors emphasize that cybersecurity is ensured by the training of internal auditors and the support of the board of directors, and is not influenced by international regulations and the outsourcing of IT audit services.

Source: own processing based on literature

Upon further analysis of the information summarized in the table above, we conclude that several research studies highlight a gap between senior management's awareness of cyber risks and the actual level of integration of these risks into audit processes. Although boards of directors state that cybersecurity is a priority, they are not sufficiently engaged and there is a lack of adequate communication between management and the audit department. Also, another factor influencing the integration of cybersecurity into audit is the lack of technical skills of auditors, which contrary to expectations, is not given by certifications, as internal auditors who hold these certifications are not trained to assess IT systems, encryption, firewalls or responses to attacks. At the same time, we see that companies that have had at least one cyber-crime are more attentive and more open to accepting the idea that internal auditors should also take on the issue of cybersecurity. These companies are also willing to offer more to internal audit professionals to be more vigilant in their work. Therefore, the determinants of effective internal cyber internal audit mentioned in the studies are: the level of involvement of senior management, the existence of communication between internal audit and IT departments, the level of rewards given to internal auditors and the skills of internal auditors.

In order for our study to have practical, not just theoretical, applicability, starting from the three thematic categories discussed by experts in the field: the role of the internal auditor in cybersecurity, organisational measures and response models as well as the determinants of an effective cybersecurity audit, we thought it would be relevant to develop a self-assessment tool to evaluate the degree of integration of cybersecurity in the internal audit process, a checklist type, with binary answers: yes or no, which we considered relevant to divide into 4 dimensions. The first dimension concerns how exposed the company is to risk, and the next three are themes identified in the literature. The questions were formulated by analysing the results and recommendations from each study, considering the challenges faced by companies, the construction of integration models, the elements breached during cyber attacks, and translating theoretical findings into practical applications.This self-assessment sheet will help organisations to see where they stand in relation to the guidelines, advices and models found in the literature.

Table 5.
Self-Assessment sheet on the need to integrate cybersecurity into internal audit processes

Nr.	Assessment criteria	YES	NO	EXPLAIN
	THE COMPANY'S EXPOSURE TO CYBERSECURITY RISK			
1.	Is the organisation dependent on information systems to run its day-to-day business?			
2.	Does the company's business requires the processing and storage of personal data?			
3.	Does the company allow employees or collaborators to remotely access the organisation's systems?			
4.	Does the organisational culture encourage reporting security issues?			
5.	Have data leaks or IT incidents been identified in recent years?			
	CYBERSECURITY MEASURES IMPLEMENTED BY THE COMPANY			
1.	Does the company have guidelines for the use of information systems and the protection of sensitive data?			
2.	Is access to sensitive data restricted to certain individuals who are trained annually on cyber risks, and is employee access regularly reviewed?			
3.	Are IT systems regularly updated and monitored for signs of attack or unusual activity?			
4.	Are anti-virus applications and multi-factor authentication installed?			
5.	Is there a tested cyber attack response plan?			
	THE POSITIONING OF THE INTERNAL AUDIT FUNCTION			
1.	Does the internal auditor have access to all company IT systems?			
2.	Is the internal auditor familiar with global regulations for assessing cybersecurity (COBIT, NIST, ISO27001)?			
3.	Does the internal auditor have ongoing discussions with the IT team or person responsible for security?			
4.	Are cybersecurity audits included in the annual audit plan?			
5.	Have there been concrete proposals from internal audit related to the company's cybersecurity?			
	LEVEL OF TRAINING OF INTERNAL AUDITORS			
1.	Is the internal auditor IT literate and qualified?			
2.	Is the internal auditor able to assess whether the technical controls implemented are relevant to the risks to which the company is exposed?			
3.	Does the internal auditor have the ability to prioritize cyber risks based on the amount of damage to the organisation?			
4.	Is the internal auditor involved in assessing risk control systems as they are being developed, not retrospectively?			
5.	Does the auditor in turn use smart technologies for continuous monitoring?			

Source: own processing

In setting the scores, we propose three appropriate levels for each dimension: low, medium, high, which are set according to the number of affirmative answers. We consider a low level when negative answers predominate, a medium level when the number of yes answers is 3, and a high level is equivalent to 4 or 5 yes answers. . To interpret the per-set table, we will correlate the answers given for the first dimension with those for the other dimensions. According to these levels of each dimension, we logically interpreted the results, deriving 6 organisational profiles described in the following paragraphs:

Unexposed and unprepared organisation (0 positive answers at first dimension) Although their field of activity does not force them to protect themselves from cyber-attacks and they have not suffered any incidents, the lack of current exposure creates a false security, and in the current context, this profile is the most vulnerable to becoming the target of attackers if they do not invest in prevention measures and internal audit training.

Unexposed and Prepared Organisation (0 positive answers at first dimension) These companies are the most secure, although the risk is low, they have still chosen to protect themselves and involve internal audit in cybersecurity.

Exposed and unprepared organisation.(0-6 positive answers) - This type of entity is susceptible to cyber risks, lacking technical measures and internal audit involvement. In this case urgent decisions should be taken to integrate cybersecurity into the audit processes; the internal auditor should actively participate in the development of procedures and rules, should strengthen the relationship with the IT department in the shortest possible time and invest heavily in technical knowledge training.

Protected organisation but without governance: (7-11 positive answers). Entities that fall into this category are exposed to cybersecurity risks, have integrated measures, but internal audit is not actively involved. Therefore, organisations at this stage need to consider integration internal audit into cybersecurity, as the existence of measures does not guarantee their effectiveness. Although the fact that the IT department is in charge of risk prevention, they do not provide independent assurance but are subjective. Auditors may point out that risks are not properly assessed Although not as urgent as in the first case, the reorganisation of the internal audit function needs to be done.

Exposed but aware organisation: (12-16 positive answers) For these organisations, a relationship between cybersecurity and internal audit is already starting to take shape, but it is still developing, it does not meet all the requirements and there is space for improvement. Internal auditors need to take their role more seriously, consolidate relations with the IT department, improve their security knowledge and continuously evolve a training plan.

Mature integrated organisation: (17-20 positive answers) The companies that are in this category have already integrated cybersecurity into their internal audit, trained auditors, well-developed measures and a high level of exposure. Internal auditors must continue to improve; procedures and controls require regular review and optimisation.

CONCLUSIONS

The present study aimed to analyze the integration of cybersecurity into the internal audit process through a systematic review of the literature. The first finding is related to the novelty of the topic; the relevant studies were published after 2017, and there are enough aspects not yet discussed. Starting from the 16 identified studies, in our research, we managed to compile the topics into three thematic categories, as we wanted to provide a more structured view of what it means to integrate cybersecurity into the internal audit process. Following this categorization, we could clearly see that the researchers' interests are focused on the reorganisation of the audit function, the skills needed by future professionals, and the financial impact that cyber criminals can cause to companies that neglect cybersecurity risk.

Based on the rankings we have developed a checklist with 20 questions to assess the level of integration of cybersecurity in the internal audit process. For its interpretation we resorted to the creation of 6 organisational profiles that help to self-assess the current status and to identify weaknesses that require intervention to strengthen the relationship between internal audit and cybersecurity.

This study contributes to the literature by thematically structuring the research on internal audit and cybersecurity in three directions: role, measures, determinants that can be starting points for future analysis. On the application side, the self-assessment sheet and the 6 organisational profiles support organizations in understanding their own positioning and in implementing improvements in the relationship between internal audit and cybersecurity. In contrast to a simple checklist, the proposed tool has a comparative function as the questions are drawn from international literature reviews and organizations can benefit from an assessment against existing global trends and recommendations.

This research was constrained by open access to scholarly materials on the Web of Science platform, and since this study was conducted on the basis of critical thinking, we consider the risk of arbitrary categorization, as some research included in the analysis was on the borderline between one category and another.

After examining the existing topics, we found that the issue of cybersecurity in underdeveloped or developing countries is treated superficially, for example in Romania, such a topic has not yet been addressed, therefore we propose as future research directions to investigate the challenges faced by Eastern European countries. The factors that determine the effectiveness of a cyber audit should be studied individually and, last but not least, the need to update the regulatory frameworks should be emphasized. Also, in order to refine the proposed tool, future studies could focus on the practical application of the checklist and the comparison of profiles by business sectors.

AUTHORS' CONTRIBUTIONS

- Conceptualization: Cristina-Raluca Cernovschi, Marius-Sorin Ciubotariu, Svetlana Mihaila
- Methodology: Cristina-Raluca Cernovschi
- Formal analysis: Marius-Sorin Ciubotariu
- Investigation: Cristina-Raluca Cernovschi
- Writing – original draft: Cristina-Raluca Cernovschi, Marius-Sorin Ciubotariu, Svetlana Mihaila
- Writing – Cristina-Raluca Cernovschi, Marius-Sorin Ciubotariu, Svetlana Mihaila
- Supervision: Svetlana Mihaila

REFERENCES

Arcuri, M. C., Brogi, M., & Gandolfi, G. (2018). The effect of cyber-attacks on stock returns. *Corporate Ownership & Control*, *15*(2), 70-83. https://doi.org/10.22495/cocv15i2art6

Bakarich, K. M., & Baranek, D. (2020). Something phish-y is going on here: A teaching case on business email compromise.*Current Issues in Auditing*, *14*(1), https://doi.org/10.2308/ciia-52706

Betti, N., & Sarens, G. (2021). Understanding the internal audit function in a digitalised business environment. *Journal of Accounting & Organizational Change*, *17*(2), 197-216. https://doi.org/10.1108/JAOC-11-2019-0114

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

Calvin, C., Eulerich, M., & Holt, M. (2025). Characteristics of cybersecurity and IT involvement by the IA activity. *International Journal of Accounting Information Systems*, *56*, https://doi.org/10.1016/j.accinf.2025.100726

Chin, J. H., Zhang, P., Cheong, Y. X., & Pan, J. (2025). *Automating Security Audit Using Large Language Model based Agent: An Exploration Experiment*. ArXiv.org. https://arxiv.org/abs/2505.10732

Dutchak, R., Kondratiuk, O., Rudenko, O., Shaikan, A., & Shubenko, E. (2021). Internal Audit of Cybercrimes in Information Technologies of Enterprises Accounting. In *SHS Web of Conferences*. Vol. 100, https://doi.org/10.1051/shsconf/202110001006

Ferreira, L. V. A., Alves, C. A. de M., Peotta de Melo, L., & Nunes, R. R. (2025b). Internal Audit Strategies for Assessing Cybersecurity Controls in the Brazilian Financial Institutions. *Applied Sciences*, *15*(10). https://doi.org/10.3390/app15105715

Fotis, F. (2024). Economic Impact of Cyber Attacks and Effective Cyber Risk Management Strategies: A light literature review and case study analysis. *Procedia Computer Science*, *251*, 471-478. https://easychair.org/publications/preprint/vfks

Gulyas, O., & Kiss, G. (2023). Impact of cyber-attacks on the financial institutions. *Procedia Computer Science*, *219*, 84-90. https://doi.org/10.1016/j.procs.2023.01.267

Guohong, Z., Zhongwei, X., Feng, H., & Zhongyi, X. (2025). The audit committee's IT expertise and its impact on the disclosure of cybersecurity risk. *Research in International Business and Finance*, *73*, 102542. https://doi.org/10.1016/j.ribaf.2024.102542

Héroux, S., & Fortin, A. (2024). How the three lines of defense can contribute to public firms' cybersecurity effectiveness. *International Journal of Disclosure and Governance*, 1-20. https://doi.org/10.1057/s41310-024-00226-7

IBM. (2024). *Cost of a data breach report 2024*. IBM. https://www.ibm.com/reports/data-breach

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

Jiang, W. (2024). Cybersecurity risk and audit pricing—A machine learning-Based Analysis. *Journal of Information Systems*, *38*(1), 91-117. https://doi.org/10.2308/ISYS-2023-019

Kelton, A. S., & Yang, Y. W. (2025). The Role of Internal Controls in Reducing Cybersecurity Contagion Effects. *Current Issues in Auditing*, 1-9. https://doi.org/10.2308/CIIA-2024-036

Le, T. D., Le-Dinh, T., & Uwizeyemungu, S. (2024). Search engine optimization poisoning: A cybersecurity threat analysis and mitigation strategies for small and medium-sized enterprises. *Technology in Society*, *76*, https://doi.org/10.1016/j.techsoc.2024.102470

Masoud, N., & Al-Utaibi, G. (2022). The determinants of cybersecurity risk disclosure in firms' financial reporting: Empirical evidence. *Research in Economics*, *76*(2), 131-140. https://doi.org/10.1016/j.rie.2022.07.001

Sabillon, R. (2018). A practical model to perform comprehensive cybersecurity audits. *Enfoque UTE*, *9*(1), 127-137. https://doi.org/10.29019/enfoqueute.v9n1.214

Sánchez-García, I. D., Gilabert, T. S. F., & Calvo-Manzano, J. A. (2023, November). CRAG: A Guideline to Perform a Cybersecurity Risk Audits. In *International Congress of Telematics and Computing*. pp. 517-532. Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-45316-8_33

Slapničar, S., Axelsen, M., Bongiovanni, I., & Stockdale, D. (2023). A pathway model to five lines of accountability in cybersecurity governance. *International journal of accounting information systems*, *51*, https://doi.org/10.1016/j.accinf.2023.100642

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

Stafford, T., Deitz, G., & Li, Y. (2018). The role of internal audit and user training in information security policy compliance. *Managerial Auditing Journal*, *33*(4), 410-424. https://doi.org/10.1108/MAJ-07-2017-1596

Usman, A., Ahmad, A. C., & Abdulmalik, S. O. (2023). The role of internal auditors characteristics in cybersecurity risk assessment in financial-based business organisations: A conceptual review. *International Journal of Professional Business Review: Int. J. Prof. Bus. Rev.*, *8*(8), 32. https://doi.org/10.24857/rgsa.v18n6-008

Vuko, T., Slapničar, S., Čular, M., & Drašček, M. (2025). Key drivers of cybersecurity audit effectiveness: A neoinstitutional perspective. *International journal of auditing*, *29*(1), 188-206. https://doi.org/10.1111/ijau.12365

Zhou, F., & Huang, J. (2024). Cybersecurity data breaches and internal control. *International Review of Financial Analysis*, *93*, https://doi.org/10.1016/j.irfa.2024.103174