applied sciences

MDPI

Article

Internal Audit Strategies for Assessing Cybersecurity Controls in the Brazilian Financial Institutions

Lucas Vinicius Andrade Ferreira [1,†], Carlos André de Melo Alves [2], Laerte Peotta de Melo [1] and Rafael Rabelo Nunes [1,2,3,*,†]

[1] Electrical Engineering Department, University of Brasilia (UnB), Brasília 70910-900, DF, Brazil; lucas.vinicius@live.com (L.V.A.F.); peotta@gmail.com (L.P.d.M.)
[2] Business Administration Department, University of Brasilia (UnB), Brasília 70910-900, DF, Brazil; carlosandre@unb.br
[3] UniAtenas University Center, Paracatu 38602-002, MG, Brazil
* Correspondence: rafaelrabelo@unb.br
† These authors contributed equally to this work.

Abstract: The global financial sector's accelerating digitalization, propelled by the growing demand for rapid and tailored services, is increasingly vulnerable to complex cyber threats. This vulnerability underscores the critical need for comprehensive and coordinated cybersecurity efforts across all organizational levels. In this context, this study examines the role of internal audit as the third line of defense, investigating its potential to improve the effectiveness of cybersecurity controls within Brazilian financial institutions. The research aims to bridge existing gaps in cyber risk management by employing a qualitative methodology centered on semi-structured interviews with internal auditing, risk management, and information security experts across ten financial institutions. The data collected were analyzed using content analysis, enabling the categorization and interpretation of current practices and challenges in cyber risk management. The results indicated two perspectives on the depth of assessments conducted by internal audit and reinforced the fundamental role of internal audit in strengthening cybersecurity defenses: whether through high-level assessments of governance and management or penetration testing in specific scenarios, it can validate and increase the effectiveness of implemented controls. In addition, the study highlights the usefulness of data analytics for continuous auditing, identifying it as a proactive approach for the early detection of emerging cyber risks. These insights contribute significantly to the scholarly discourse on internal auditing's role in the improvement of a secure and resilient organizational environment. They also offer actionable strategies for financial institutions seeking to integrate effective cyber risk management practices, thus reinforcing the sector's preparedness against increasingly sophisticated cyber threats.

Keywords: cybersecurity; risk management; internal audit; financial institutions

Academic Editor: Young-Gab Kim

Received: 17 February 2025
Revised: 1 May 2025
Accepted: 6 May 2025
Published: 20 May 2025

Citation: Ferreira, L.V.A.; Alves, C.A.d.M.; Peotta de Melo, L.; Nunes, R.R. Internal Audit Strategies for Assessing Cybersecurity Controls in the Brazilian Financial Institutions. *Appl. Sci.* **2025**, *15*, 5715. https://doi.org/10.3390/app15105715

1. Introduction

Over the past decades, cybersecurity has become a central concern for organizations across all industries. This growing focus reflects the complexity and sophistication of digital threats and their potential impact on business. A review of recent literature reveals several trends and challenges that companies face in cybersecurity and risk management [1–3].

The first trend is the increase in budgets and investments in cybersecurity, a direct reflection of changes in corporate strategies. Companies recognize the need to allocate more resources to protect their digital assets [4]. Organizations often justify this increase in

investment by the need to address more sophisticated and frequent threats, as well as the pressure to comply with strict data protection regulations.

Despite the increase in investment, many challenges remain. One of these is ineffective or non-existent cyber risk management, as many organizations still need robust processes to identify, assess, and mitigate cyber risks [5]. This deficit is often due to a need for more internal expertise and senior management underestimating cyber threats.

Another worrying trend is the continued rise in the number of cyber attacks. Studies have documented a significant increase in cyber incidents, including ransomware attacks, phishing attacks, and data breaches. These attacks are more frequent and sophisticated, making it harder for organizations to defend themselves [1,6].

In parallel with the increase in attacks, there has been a rise in system vulnerabilities. McShane, Eling, and Nguyen [2] point out that the increasing complexity of IT systems and the rapid adoption of new technologies often result in unpatched vulnerabilities. These flaws provide attractive entry points for cybercriminals, exacerbating the risk of successful attacks.

The costs associated with data breaches and system outages are also rising. According to an IBM report [7], companies face increasing expenses to recover data, restore operations, and deal with legal and reputational repercussions of security incidents. These costs can be very significant, especially for small and medium-sized businesses that may not have the financial resources to bear such losses.

An organization's reputation can also suffer significant damage due to security breaches. Security incidents can seriously undermine consumer and partner trust, causing loss of business and opportunities. Rebuilding trust is a time-consuming process and can have a lasting impact on the viability and success of the organization [8].

Another challenge is the need for more cooperation and information sharing about threats and vulnerabilities. Collaboration between organizations can significantly improve the collective ability to respond to cyber threats. However, many companies are reluctant to share information due to privacy and competition concerns [5].

The study identified gaps in cyber risk management in the Brazilian context, particularly in the financial sector. Although financial institutions adopt international frameworks such as NIST CSF and ISO/IEC 27001 [9], challenges persist in adapting these standards to local regulations, such as the absence of strict deadlines for reporting incidents and the lack of requirements for offensive testing (red teaming) [10].

In addition, the integration between internal audit (third line) and IT and cybersecurity teams faces operational obstacles, such as divergences in terminology and objectives, limiting the effectiveness of collaborative approaches [11]. Another gap lies in the implementation of data-driven continuous auditing, where the lack of standardized metrics and the scarcity of technical resources hinder the real-time analysis of large volumes of information [12].

Therefore, this research is justified because, within financial institutions, internal audits play a central role in resolving several strategic issues. Due to the potential impact associated with cyber risks, it is urgent to identify tactics, techniques, and procedures so that the performance of internal audits as a third line can result in gains.

Finally, this study aims to identify the approaches through which Internal Audits can test, evaluate, and monitor the effectiveness of cybersecurity controls implemented in a financial institution to support the continuous improvement of these practices.

This work was organized into six sections to achieve this goal, starting with this introduction in Section 1. We will then explore related work in Section 2 and the context in Section 3. In Section 4, we will detail the research method. In Section 5, which focuses on the results of the research, we will present and categorize the findings based on the

interview themes and analyze them in light of the existing literature. Finally, in Section 6, the conclusion will briefly present the main findings, the study's limitations, and suggestions for future research.

2. Related Work

Cybersecurity is a critical component of modern business operations, particularly in the context of risk management. Within the risk management framework, a frequently used approach is the Three Lines model, where Internal Audit is the Third Line [13]. This paper will detail the model, functions and interactions between the lines in Section Three. In this section, we will present some relevant studies related to the role of internal audit in cybersecurity.

McShane, Eling, and Nguyen [2], in 2021, found that cyber risk is difficult to include in the overall enterprise risk management process and that a shift towards cyber resilience is necessary to address such a complex risk.

Eulerich and Eulerich [14], in 2020, identified that the added value of internal auditing lies in its ability to create value for stakeholders by providing them with the means to mitigate the potential effects of risks throughout the value chain. In addition, it contributes to savings by identifying optimization opportunities and strengthening corporate governance, reinforcing confidence in the organization's integrity.

Rosati, Gogolin, and Lynn [3], in their 2017 studies, revealed that auditors respond effectively to increased audit risk by intensifying testing and expanding their efforts. The evidence indicates that auditors have demonstrated greater awareness of audit risks and have adopted rigorous procedures to deal with the consequences of cybersecurity incidents.

Carcello et al. [15], in 2020, based on assessments of audited and non-audited units, found that managers of audited units perceive a more significant risk reduction, in addition to a more expressive increase in performance, compared to managers of non-audited units.

Lois et al. [16], in 2021, concluded that auditing remains a fundamental part of promoting efficiency and reliability in companies, highlighting the need for auditors to expand their knowledge of cybersecurity. This improvement is essential for the success and effectiveness of audits in the digital environment.

Kahyaoglu and Çalıyurt [17], in 2018, noted that internal auditors must comprehensively understand the impact of cyber threats on the organization and simultaneously incorporate it into their risk-based audit plan. In addition, they must be competent in proactively identifying emerging cybersecurity risks.

Georg et al. [18], in 2023, identified cyber attacks as one of the main challenges for institutions, exposing their vulnerabilities and putting their credibility at risk. With the increasing sophistication of these attacks, managers have emphasized the importance of mitigating such threats using the available tools, focusing on Advanced Persistent Threats (APTs).

Alves et al. [19], in 2023, related business risks to various operational risks, contributing to managing risks in the security of corporate processes, and defining controls that contribute to reducing the probability of occurrence or minimizing the consequences, should the risks materialize.

Alves, Queiroz, and Nunes [20], in 2024, identified the need to modernize the information security structure of the judiciary to prevent system unavailability and the loss or leakage of data from citizens and entities. Furthermore, they highlighted that adopting the Three Lines Model in the cybersecurity structure strengthens security policies and helps prevent cyber risks.

Based on the reviewed literature, studies highlight organizations' challenges in managing cyber risks and the essential role internal audit plays in this context. However,

financial institutions must maintain clearly defined and adequately dimensioned processes to identify threats and mitigate associated risks. In addition, there is a demand for effective techniques to test the effectiveness of implemented cybersecurity controls, which aim to reduce exposure to cyber risks. In this scenario, our study highlights how internal audits can assess the effectiveness of cybersecurity controls and ensure continuous improvement of these processes.

3. Background

3.1. Cyber Risk Managment

Cyber Risk Management (CRM) refers to identifying, assessing, and responding to cyber risks associated with an organization's information systems [1]. It aligns with broader enterprise risk management by embedding security measures into organizational processes to ensure operational continuity and protection against malicious cyber activity [21].

Scholars have noted the importance of a systematic approach to CRM. Such an approach begins with clearly understanding an organization's assets and potential vulnerabilities [22]. The organization must then assess the threats to these assets, ranging from internal, such as employee negligence, to external, such as APTs [23]. The next step involves determining the potential impacts of these threats and the organization's risk tolerance [24]. Based on these findings, risk mitigation strategies are then formulated and implemented.

The effectiveness of CRM can be improved by continuously updating risk assessment methodologies to keep pace with evolving threats [2]. While no one-size-fits-all approach to cyber risk management exists, standards such as COBIT 2019 [25], NIST in Special Publication 800-39, CIS Controls and ISO 27005 [26] provide guidelines for managing cyber risks.

However, the complexity and dynamic nature of cyber threats require organizations to consider more sophisticated methods. Applying artificial intelligence (AI) and machine learning in cyber risk management can help in cyber threat real-time detection, mitigation, and response [24]. Despite their potential, applying these technologies needs scrutiny due to the risks associated with false positives and unintentional algorithmic biases.

3.2. Three Lines Model

The Three Lines Model, originally known as the Three Lines of Defense Model, provides a comprehensive framework for managing risk and establishing effective governance in organizations [27]. Its most recent revision, conducted by the Institute of Internal Auditors (IIA) in 2020, revamped the model to improve its adaptability, scalability, and ease of implementation across various organizational structures [11].

The 2020 revisions, while maintaining the essence of the model, attempted to increase its versatility and eliminate some of its inherent limitations. One significant change is removing the term "defense", suggesting a shift from rigid, siloed functions to a more fluid, collaborative approach to risk management [11]. The updated model also emphasizes the oversight and strategic roles of the board of directors and that all parts of an organization contribute to its governance and risk management [27].

The Three Lines Model provides a structured approach to risk management that aligns organizational objectives with risk identification, assessment, and mitigation strategies [28].

The first line includes operational management, which identifies, assesses, and manages risks in their respective areas. The second line consists of specialized risk management and compliance functions, which oversee risk monitoring, policy development, and implementation of internal controls. The third line comprises the internal audit function, which provides independent assurance and evaluation of risk management practices. The governing body is responsible for establishing strategic direction and ensuring the effectiveness of

the organization's governance system. The external assurance providers give additional assurance to satisfy legislative and regulatory expectations that protect the interests of stakeholders and requests by management and the governing body to complement internal sources of assurance [27].

The model emphasizes the distinct but complementary roles of the first line (operations), the second line (risk and compliance functions), and the third line (internal audit) while emphasizing that responsibility for risk management and internal controls ultimately rests with management [11].

The model further redefines organizational management, risk management, governance, external assurance providers and internal audit roles, viewing them as interconnected but distinct components of an over-arching governance framework [27]. This shift represents a move from the original model's defense perspective to a 'lines of sight' viewpoint, focusing on organizational accountability and risk management rather than solely on risk control [29].

3.3. Financial Regulation

Prudential Regulation (CMN Resolution No. 4,553/2017) is a form of financial regulation that imposes standards on financial institutions, focusing on risk management to cover the risks associated with their operations. These minimum capital and risk management measures help prevent a failure in the financial sector from triggering a chain reaction known as systemic risk, which could ultimately result in losses for society as a whole [30].

The regulatory framework divides the institutions of the National Financial System (SFN) into five segments based on their size, international activity, and risk profile. This segmentation creates a regulatory environment that is more appropriate for the application of prudential standards, particularly for smaller institutions, which tend to be more innovative and dynamic [30].

With this division, smaller institutions follow more straightforward rules than those imposed on large banks. Prudential standards are proportional to each institution's activities and risk profile, increasing the efficiency of financial intermediaries, reducing costs, and stimulating competitiveness in the financial market [30].

According to the prudential regulation of the Central Bank of Brazil, in September 2023, Brazil had 1,291 financial institutions distributed in five segments following the rules detailed in Table 1.

Table 1. Segments of Brazilian financial institutions.

Segment	Composition	Size	Number of Institutions
S1	Banks	Greater than or equal to 10% of GDP (Gross Domestic Product) or relevant international activity	6
S2	Banks smaller than 10% of GDP and other institutions larger than 1% of GDP	From 1% to 10% of GDP	6
S3	Banks and non-banking institutions	From 0.1% to 1% of GDP	58
S4	Banks and non-banking institutions	Less than 0.1%	366
S5	Non-banking institutions with simplified risk profile	Less than 0.1%	855

The allocation of institutions in each segment presented in Table 1 was the most recent, carried out in September 2023. According to the data released, it is possible to infer that

there is an intense concentration of assets in segment one, making it more representative of the national economic scenario.

3.4. International Regulations

Globally, frameworks include the NIST Cybersecurity Framework (USA) [31], which offers voluntary guidelines focused on identifying, protecting, detecting, responding to, and recovering from threats; the NIS2 Directive (EU, 2023) [32], which mandates annual penetration tests and 24-h incident reporting for critical situations; and PCI DSS [33], the international standard for payment data security, requiring encryption, continuous monitoring, and regular testing. Furthermore, DORA (EU, 2025) [34] emerges as a pivotal regulation, concentrating on operational resilience and IT risk management, while Singapore's MAS Guidelines [35] necessitate independent audits and offensive testing (red teaming).

In Brazil, the Central Bank has issued specific regulations to strengthen cybersecurity in the financial system. CMN Resolution No. 4,968/2021 [10] requires financial institutions to conduct periodic security tests on their IT systems, partially aligning with PCI DSS but without specifying a minimum frequency. CMN Resolution No. 4,879/2020 [36] mandates internal audits to assess system reliability and integrity, resembling NIS2 but lacking requirements for rapid failure reporting. Meanwhile, CMN Resolution No. 4,893/2021 [37] establishes continuous control mechanisms and periodic testing, reflecting aspects of DORA but without mandating crisis simulations. Finally, BCB Normative Instruction No. 305/2022 [38] introduces mandatory annual penetration testing for Open Finance, aligning with NIS2 and PCI DSS, although its scope is limited compared to global standards that cover the entire financial sector.

Despite progress, gaps persist in Brazilian regulations. There are no strict deadlines for incident reporting (unlike NIS2's 24-h requirement), no obligation for offensive testing (red teaming), and regulatory coverage remains fragmented, with Open Finance-specific rules instead of a unified approach for the entire financial system. To enhance resilience, Brazil could benefit from adopting clear timelines for incident reporting, expanding penetration testing beyond Open Finance, and better integrating policies across the Central Bank, CVM (Securities Commission), and ANPD (Data Protection Authority), following models like those of the EU.

3.5. Cyber Resilience in the Financial Sector

Cybersecurity in the financial sector has evolved from a focus on technical controls to a model that integrates human and organizational aspects. As emphasized by [31,34], an organization's capacity to prevent, detect, and respond to security incidents relies as much on its processes as on the culture developed among its employees.

Recent regulations, including the European [32] and Brazil's Central Bank resolutions [10,37], acknowledge this interdependence. They establish technical requirements and require financial institutions to create governance structures that foster security as a collective responsibility.

In this context, three factors are particularly relevant:

Leadership engagement: Institutional leadership must show commitment to security practices by allocating sufficient resources and actively participating in decisions related to cyber risk [35].

Ongoing training: Awareness programs should be conducted regularly and customized for different organizational levels, surpassing simple regulatory compliance [33].

Improvement mechanisms: Security incident experiences should be systematically documented and analyzed to improve existing controls [38].

In the Brazilian case, although the regulatory framework has advanced with norms like [36,38], there is still room for better integration between technical and organizational aspects of cybersecurity. Adopting established international practices while considering the national financial market's specificities could help develop a more effective security culture.

3.6. Techniques for Auditing Cybersecurity

Continuous auditing transforms traditional audit practices into a real-time, technology-driven assurance process. Unlike periodic reviews, this approach involves the ongoing monitoring of controls and transactions [39]. Eulerich et al. [40], 2024, observed that many internal audit functions have been slow to adopt such technologies, as the benefits, such as improved risk detection, take time to materialize. This suggests that organizations need patience and clear objectives when implementing these tools.

Continuous monitoring has stood out as an effective resource for mitigating risks by enabling the early identification of control failures and allowing agile responses to cybersecurity issues [41]. Modern solutions capable of real-time control, monitoring, and automated anomaly detection in financial environments promote constant vigilance over critical operations, making it possible to immediately detect suspicious behavior or non-standard activities [42]. This format transforms the audit function into a proactive risk management tool, aligning internal auditing with the dynamic and growing pace of cyber threats. Anand, Chirputkar, and Ashok [43], 2023, proposed an analytics-based solution that describes threats, predicts future malicious behavior, and suggests protections in real time, reinforcing the efficient integration between technology and risk governance.

In this context, it is worth noting that the evolution of continuous auditing aligns with advances brought by artificial intelligence (AI), especially in enhancing the ability of financial organizations to anticipate and respond to cyber threats [44]. The application of AI has revolutionized cybersecurity risk management, particularly in the financial sector, by automating both incident detection and responses [42].

Recent research and industry guidance highlight that AI and machine learning techniques allow for the automation of the analysis of large volumes of data, making processes more efficient and accurate [45]. The systematic review conducted by Jada and Mayayise [41], 2023, corroborates that using machine learning models for threat detection significantly improves organizational cyber risk management. However, it introduces governance challenges, such as model bias.

In practice, AI assists internal auditors and risk managers by performing rapid log analysis, prioritizing alerts, and predicting attack patterns [46]. Additionally, solutions such as AI-assisted risk scoring expand traditional assessment methods, while intelligent tools support continuous control testing, including automated vulnerability scanning and compliance checks [47].

The growing complexity of the digital environment requires increasingly comprehensive and adaptive approaches to cybersecurity auditing. New models, such as the one proposed by Sabillon et al. [48], 2024, exemplify advances in this regard by offering an empirically validated framework to assess the effectiveness of cyber controls in real-world scenarios, focusing not only on compliance but also on the maturity and readiness of security controls. Furthermore, Saravanan et al. [49], 2023, discuss the need to adapt audit practices to the adoption of emerging technologies, such as cloud computing and artificial intelligence, highlighting that auditors must continually improve their methods as the technological landscape evolves.

However, challenges persist in consolidating universal guidelines and consistent practices for comprehensive cybersecurity audits, as Sabillon and Bermejo Higuera [50], 2023, determined in their review of global best practices. Even with consolidated frameworks,

such as ISO 27001 and NIST CSF, internal auditors still encounter obstacles in ensuring complete and consistent assessments of cyber controls, especially when considering sector-specific details, such as local regulations and the particular threat profile of the Brazilian banking sector.

4. Methodology

To achieve the central objective of identifying ways in which internal audit could contribute to processes related to Cyber Risk Management within financial institutions, the defined mechanism involved conducting semi-structured interviews with professionals from financial institutions and consulting companies that operate in Brazil and abroad, using a qualitative approach of an exploratory nature, which culminated in this descriptive study.

4.1. Sample of Interviewees

Due to the specificity determined for the profile of the professionals, the sample of interviewees for this study was carried out in a non-probabilistic manner, taking into account the experiences and performances in activities of internal controls, risk management, internal or external auditing, and consulting, in institutions in the financial sector. In addition, the interviewees performed these activities and obtained experiences in information technology and cybersecurity processes.

The choice of institutions in the financial sector was due to the complex environment and the significant dependence of the financial sector on technology, making it the sector with the second-highest average data breach cost, as demonstrated in [7]. It is also susceptible to elaborate cyber attacks.

In addition, financial institutions' connections with other areas of the economy can generate systemic impacts if attacked, since they make up the critical infrastructure of several countries, especially those with international financial operations. An example is the growing trend of attacks targeting international financial communication networks, such as the Society for Worldwide Interbank Financial Telecommunications (SWIFT), responsible for international transfers between banks, often involving large sums and in solid currencies, such as the dollar or the pound sterling [51].

Furthermore, to better represent Brazilian financial institutions, the distribution of interviewees was carried out to reflect the size and international activity of the financial institution, according to the prudential regulations of the Central Bank of Brazil (BACEN).

According to Bacen, in April 2024 [52], although it is decreasing, 68% of the credit collections carried out in 2023 are still concentrated in banks in segment S1, so we decided to maintain a higher percentage of professionals from this segment among the interviewees. Thus, Table 2 shows the number of interviewees and the final distribution between the segments.

Table 2. Interviewees by segments of Brazilian financial institutions.

Segment	Number of Interviewees	(%)
S1	8	50%
S2	2	12.5%
S3	2	12.5%
S4	1	6.25%
S5	1	6.25%
External Audit	2	12.5%
Total	16	100%

It is worth noting that the research team interviewed two professionals who work for External Audit companies. These companies are part of what the market calls the 'Big Four', a group of the largest international audit firms. The target market of these companies mainly includes large institutions operating in various sectors of the global economy and regions of the world. Over the years, the 'Big Four' have led the global market for audit services [53].

The External Auditors interviewed were selected based on their extensive experience and roles in structuring and independently assessing the maturity of Cybersecurity and Information Technology Audit frameworks in S1 segment banks in recent years.

4.2. Interviews and Script

In order to protect the identity of the participants and ensure the confidentiality of information about critical processes of the institutions involved, the interviewees were disguised and each participant was identified with a unique identifier starting with INT01 to INT16. This action does not harm the achievement of the objectives proposed in this study and was important to instill confidence and allow the interviewee to express their ideas and perceptions about the topics studied as freely as possible.

The script defined to guide the interview was developed based on the information in the bibliographies mapped during this work's theoretical framework survey stage, addressed in sections two, three, four and five. The script was divided into seven blocks, or indexes, containing two questions each, totaling fourteen, as detailed in Table 3.

Table 3. Interview script.

Id.	Question	References
Q01	Tell us a little about your academic background and professional experiences.	
Q02	How would you describe your current role in relation to cybersecurity and/or Internal Audit?	
Q03	How do you believe the organizational structure should work, in terms of lines, in relation to cybersecurity?	[14,28,29,54]
Q04	How can an organization include cyber risk management in its corporate strategy?	[22,55–57]
Q05	How do you see the role of internal audit in cyber risk management?	[17,55,58,59]
Q06	How can internal audit work and collaborate with other areas of the company to identify and mitigate cyber risks?	[13,60,61]
Q07	How can auditing help an organization monitor and assess potential cyber threats?	[22–24]
Q08	What practices or frameworks do you consider essential to help auditing assess how the organization manages and mitigates cyber risks?	[9,25,31]
Q09	How does internal auditing assess the effectiveness of the cybersecurity controls implemented by the organization?	[3,16,17]
Q10	What metrics or indicators can be used by internal audit to measure the effectiveness of cybersecurity controls?	[12,62]
Q11	How can internal audit contribute to ensuring compliance with standards and regulations related to cybersecurity?	[12,63,64]
Q12	How can nonconformities identified by audit be addressed and communicated within the organization?	[17,55,58,65]
Q13	Based on your experiences, what are the main lessons learned about internal audit and/or cyber risk?	[56]
Q14	What trends and innovations in the area of cybersecurity and/or audit do you consider most relevant for the coming years?	[56]

At the end of the interview, we allocated time to ensure the interviewee could provide all necessary contributions and share any additional ideas, opinions, and perceptions related to the topics discussed. If the interviewee had any relevant input, we introduced new topics to address those contributions.

4.3. Data Collection

The interviews were conducted via videoconference using Microsoft Teams to gather the interviewees' perceptions and information.

The interviews were conducted individually with each interviewee between 14 March 2024, and 2 May 2024, with durations ranging from 46 min to 1 h and 20 min.

Of the total number of interviewees, 15 of them, or 93.7% hold managerial or coordination roles, meaning they are responsible for decision-making, directing assessments, and managing teams or audit processes related to Cybersecurity, Security, and Information Technology. One interviewee (6.25%) works as a risk specialist. Additionally, the average years the interviewees have spent performing first, second, and third line functions is 10.25, 3.7, and 8.31 years, respectively. 88% of the interviewees were working in second or third-line roles at the time of the interview and 12% are External Auditors. These data highlight the significant level of responsibility and extensive experience the professionals possess in the topics covered by this study.

4.4. Data Analysis

Data analysis was applied following methodology to analyze the data collected through the instruments defined in this research [66]. This approach aims to systematically and objectively extract knowledge and meaning from the narrated texts based on the messages conveyed in the verbalized responses

The technique consists of applying three well-defined steps to perform content analysis methodically as follows: (I) pre-analysis, (II) exploration of the material, and (III) treatment of results, inference, and interpretation.

This study adopted the categorical analysis technique, segmenting the text into units and categorizing them through analogical regroupings. This technique is highly effective in qualitative research, as it allows for insightful interpretations grounded in systematic inferences, enhancing the depth and clarity of the analysis [66].

5. Results

The main objective of this paper is to map and understand how internal audits can assess the effectiveness of cybersecurity controls implemented in institutions. This section explores the methods and practices used to ensure these controls function as expected, identifying possible failures and suggesting improvements. In addition, it aims to provide insight into the ability of these controls to protect institutions against cyber threats, ensuring the integrity, confidentiality, and availability of information. In this way, internal audits can play a fundamental role in maintaining cybersecurity and strengthening organizational resilience in the face of digital risks.

5.1. Depth of Assessments Carried out by Internal Audit

This was a topic that raised different opinions and reflections. On the one hand, seven interviewees argue that internal audit should focus on the most general aspects of process management and governance, avoiding a granular approach to the execution of activities. This view proposes that, by focusing on high-level and strategic assessments, internal audit can provide a more comprehensive and lasting vision, capable of promoting systemic adjustments that benefit the entire organization.

In this context, internal audits should direct their efforts toward the broader process management and governance aspects. Proponents of this approach believe that internal audit should prioritize evaluating policies, control structures, and governance practices that oversee the organization. The rationale is that by concentrating on these broader areas, internal audit can ensure that sound management and governance principles are followed, thereby providing a solid foundation for the organization's operations.

Interviewee INT02 provided the following comment in their recording unit regarding the topic: "*Assuming that the first and second lines actively engage in risk management, the audit can complement their work by leveraging the analyses conducted by the first and second lines. In this way, assessing how management carries out these activities is important, ensuring that the identified risks are the most relevant and that the implemented controls effectively mitigate them*".

On the other hand, six interviewees reinforced that the independence of the third line also allows it to focus its assessments on operational aspects, including re-performing tests and procedures already performed by the second line, if applicable.

In this context, internal audit should also focus on detailed assessments of operational aspects. This perspective suggests that internal audit should review high-level management and, if necessary, conduct tests and examine operational procedures already performed by the second line. This approach would involve reassessing operational controls, reviewing daily procedures, and identifying gaps or areas for improvement that require immediate attention. By doing so, an internal audit can ensure that all levels of the organization, from governance to daily operations, function efficiently and effectively.

Regarding this context unit, interviewee INT09 made the following comment: "*Internal audit should delve deeper into first-line operational activities where there are signs that controls are not functioning effectively or where significant risks require further assessment*".

Additionally, interviewee INT03 made the following observation on the subject: '*Replication of tests by internal audit also serves as a mechanism for verifying and validating processes. It assures that processes function as expected and that teams manage risks effectively. Such an approach is critical in susceptible areas like cybersecurity, where risks can lead to incalculable consequences for any organization*'.

Refs. [27,67] discuss the scope of assessments conducted by internal audit, yet they do not restrict its role. Refs. [59,68] emphasize the contribution of internal audit to cyber risk management, providing independent assurance that organizational processes and controls are effective. In support of this goal, the third line can test the controls implemented by the first and second lines, assessing and reporting on their effectiveness.

5.2. Penetration Tests (Internal or External)

Among those advocating for deeper audit testing in operational activities, some suggested Penetration Tests (PenTests) as a viable option. Auditors or specialized external companies could conduct these tests to evaluate the effectiveness of vulnerability analysis, security patch management, and incident response. In this case, it is crucial to develop strong technical capabilities to validate first-line processes and identify opportunities for improvement effectively.

Regarding this context unit, interviewee INT03 made the following contribution: "*The hiring of specialized companies can be done with a forecast curve and knowledge transfer, where they would initially perform the tests and, over time, would transfer the knowledge and responsibility to the audit, until the point where the latter assumes full responsibility for the tests on an ongoing basis, making the notes to the first line in a more timely manner. At this point, some may argue that the independence of the third line could be affected; however, by making clear and documenting all the methods, tools, and criteria used in the tests, this strategy can contribute greatly to increasingly relevant and in-depth assessments of the audit on the subject*".

5.3. Process Management

In contrast, supporters of the thesis that auditing should focus on the management of the process itself, the tools used, the established stages, documentation generated, and rules defined and applied argue that by acting in this way, the changes would be more structural and lasting, in addition to highlighting challenges related to human and financial resources.

Interviewee INT04 added the following information to their record unit on the subject: '*Although theoretically appealing, the absorption or adoption of Red Team practices by the third line—such as executing penetration tests to challenge the model and identify weaknesses in controls—becomes impractical in reality. This impracticality arises from the significant labor assigned to audit activities and the numerous duties and responsibilities these professionals carry. At a certain point, professionals abandon the idea because of the lack of technical, human, and financial resources. In such cases, focusing the audit on managing the process, tools used, established procedures, generated documentation, and defined and applied rules would result in more structural and lasting changes. Moreover, institutions and technical teams already possess expensive tools and highly specialized professionals in this field; therefore, it may not be operationally efficient to allocate additional resources to hire other companies and tools that would likely impact network performance and other IT resources in order to challenge and stress the systems*'.

5.4. Joint Assessments and Testing

Furthermore, internal audits can work closely with IT and cybersecurity teams to understand current security policies, established processes, implemented technologies, and applied controls. Conducting security assessments and testing together can help identify more complex vulnerabilities and threats before attackers exploit them. Internal audits can bring an external, independent, and impartial perspective to these assessments, helping identify risks and ensuring that teams meticulously test all security aspects.

Regarding this context unit, interviewee INT05 recorded the following observation: "*The third line can work together with the cybersecurity and IT areas, understanding the established processes, implemented controls, current security policies, tools and technologies employed, to perform more technical and in-depth assessments and, when necessary, issue more assertive recommendations for improvements*".

5.5. Continuous Auditing Based on Advanced Data Analytics

To assist in executing audit activities, interviewees reinforced the continuous auditing strategy based on data, representing an innovative and proactive approach to protecting digital assets and sensitive information. Unlike traditional audits performed periodically, continuous auditing uses data analysis, which can even be in real-time, to monitor and evaluate security controls and processes continuously.

Regarding this context unit, interviewee INT12 made the following comment: "*Decisions based on concrete data make cyber risk management more reliable. Using analytical tools for auditing and monitoring cyber risks can significantly increase the ability to detect and respond to emerging risks. Using data and metrics to support recommendations and actions improves the credibility and effectiveness of security initiatives*".

At this point, the interviewees expressed another point of disagreement. One side highlighted the high degree of precision and the complete and detailed view of the statistical analyses on the population universe. In this context, the INT03 registration unit on the subject stands out: '*In the existence of a thousand critical assets, if auditors test nine hundred assets, I cannot say with any degree of certainty, although statistically correct, that the organization is safe since only one vulnerable asset needs to trigger a chain of catastrophic events*'.

As a counterpoint, the other side highlighted the speed and efficiency in statistical analyses performed on samples, as long as they correctly represent the entire universe

with quality and representativeness. Regarding this context unit, interviewee INT06 made the following contribution: '*In a context of resource scarcity, it may be interesting to select a representative sample to represent the whole or even prioritize what may be most exposed or most critical for the organization*'.

The data-driven continuous audit strategy was also highlighted in the works of [1,5,12,62]. In a complementary manner, ref. [12,69] pointed out that by leveraging data analysis, the third line can identify trends and anomalies indicative of a cyber threat, thus enabling a proactive response and decision-making that makes cyber risk management more reliable.

Ref. [39] highlights that continuous auditing transforms traditional practices by enabling real-time monitoring through digital technologies. According to [40], adoption remains slow because benefits, such as improved risk detection, take time to manifest. This necessitates that organizations be patient and have clear objectives when implementing these tools.

5.6. Continuous Security Monitoring Strategy and Integration of Advanced Technologies

Internal audits can assess how cybersecurity and IT areas implement continuous real-time monitoring tools that detect abnormal or suspicious activities. These tools include intrusion detection and prevention systems (IDS/IPS), network traffic monitoring, user and entity behavior analysis (UEBA), and SIEM (Security Information and Event Management), which aggregates and analyzes security data in real-time to identify potential threats. If the institution's strategy fails to integrate these technologies or present consistent results effectively, the audit may recommend a feasibility study and create an action plan to adjust the processes.

Interviewee INT14 made the following comment in his context unit regarding the topic: "*Investing in cutting-edge technology for threat monitoring, detection, and response can mean the difference between a minor breach and a catastrophe. Advanced tools such as AI for anomaly detection and automation for incident response enable a more dynamic and adaptive approach to addressing cyber risks and significantly increase an organization's ability to respond to threats*".

Modern tools for continuous monitoring and automated anomaly detection enable real-time oversight of financial operations and rapid identification of suspicious activities [42]. This shifts auditing toward proactive risk management, keeping pace with evolving cyber threats. Ref. [43] presents an analytics-driven tool that detects, predicts, and mitigates threats in real time, enhancing the integration between technology and risk governance.

The evolution of continuous security monitoring is closely linked to advances in AI, which enhances financial organizations' ability to anticipate and address cyber threats [44]. AI automates incident detection and response, improving cybersecurity risk management [42]. AI and machine learning also streamline the analysis of large data volumes, boosting efficiency and accuracy [45], though challenges like model bias remain [41].

5.7. Threat Intelligence and Trend Analysis

Auditors may compile and analyze data on past security breaches and incidents, as well as current trends in cybersecurity, to anticipate emerging risk areas. Such efforts may include partnering with other organizations, government agencies, or industry groups to share threat intelligence.

Regarding this context unit, interviewee INT10 made the following comment: "*Intelligence insights can advise management on areas that need immediate attention or enhanced security. Compiling and reporting on cyber threat trends and security incidents can provide important information to guide the work of the third line of business and assist senior management in making strategic decisions and investing in cybersecurity*".

Ref. [49] discusses the necessity of adapting audit practices to the adoption of emerging technologies and highlights that auditors must continuously enhance their methods as

the technological landscape evolves. AI helps auditors and risk managers by analyzing logs quickly, prioritizing alerts, and predicting attacks [46]. It also enables AI-based risk scoring and supports continuous control testing through automated vulnerability scans and compliance checks [47].

5.8. Security Reports and Dashboards

Security reports and dashboards should be developed to provide an overview of the organization's cybersecurity status. These reports can highlight vulnerabilities, security incidents, and the progress of mitigation initiatives. To support the creation and monitoring of these dashboards, the audit team can work continuously with the help of analytical tools to visualize the data. This approach can be beneficial in scenarios where the first and second lines already maintain databases and data lakes with extensive information about the processes.

Interviewee INT01 made the following note in their registration unit on the subject: '*With the volatility seen today in the corporate, IT, and cybersecurity world, audits with periodic assessment cycles may not be sufficient to identify emerging risks promptly. These risks can lead to financial and brand losses and undermine the audit area's contribution to the organization's value generation. Any change in the technological environment may alter the institution's risk exposure, and producing continuous information through a security dashboard may offer a more effective way to propose structural improvements*'.

Refs. [12,17,62] highlighted that the data obtained should support the construction of security reports with information on risk quantification and control panels that present a view of the organization's cybersecurity status. Similarly, interviewees emphasized that auditors can create trend analysis and monitor threat intelligence reports to define risk analysis and quantification strategies within institutions, building their own performance and risk indicators or in conjunction with the areas and a joint effort.

5.9. Metrics and Use of Indicators

Metrics and indicators provide a clear and objective view of the current state of cybersecurity in the organization. By using these metrics, internal audits can identify areas for improvement, offer accurate and measurable recommendations, and ensure that security controls align with the company's strategic objectives.

In conjunction with the cybersecurity and IT areas, the audit can establish key risk indicators (KRIs) and key performance indicators (KPIs) to monitor the institution's cybersecurity environment continuously. These indicators provide a comprehensive and real-time view of potential threats and vulnerabilities.

Interviewees recognize that metrics and indicators to audit and monitor cybersecurity processes continuously contribute significantly to identifying weaknesses and opportunities for improvement. Regarding this context unit, interviewee INT05 said the following: '*Changes in KRIs, such as a sudden increase in intrusion attempts or the frequency of detected vulnerabilities, may indicate the need for a more detailed review of current defenses or immediate actions to mitigate emerging risks. Similarly, organizations can use KPIs to assess the effectiveness of implemented security policies, such as incident response time, the success rate in mitigating threats, and compliance with established security standards*'.

Refs. [12,62,70] highlighted the importance of organizations defining and monitoring performance indicators in their work.

Among the indicators indicated by the interviewees, the following stand out as essential for any financial institution:

- Security Incident Rate in a specific period.

- Mean Time to Detect (MTTD) and Mean Time to Respond or Recover (MTTR) of security incidents.
- Percentage of vulnerability fixes on and off schedule.
- False Positive and Negative Rate generated by solutions.
- Level of awareness and participation rate in security training.
- Effectiveness of Business Continuity Plans and Attack Simulation Response Plans.

5.10. Frameworks and Good Practices

Interviewees highlighted the importance of adopting frameworks that offer standardized structures for process management, risk assessment, and security controls. Good practices and frameworks ensure that internal audits can assess cyber risk management entirely, accurately, and efficiently, promoting greater organizational security and resilience.

Interviewee INT07 made the following observation in his registration unit on the topic: "*Frameworks and best practices are generally products that are tested, approved and constantly improved by the community and offer an opportunity to "talk" to the "rest of the world" at events, forums, and organizations*".

Interviewees indicated the NIST CSF [31], ISO/IEC 27001 [9], COBIT 2019 [25] and CIS Controls as essential frameworks to help both the organization and internal audit to manage and assess cyber risks. The literature search also indicated that the Cybersecurity Capability Maturity Model (C2M2) [71] can help verify and monitor the company's cyber maturity and [48] propose a validated framework that assesses not just compliance but also the maturity and readiness of security controls in real-world scenarios.

Ref. [50] concluded that even with the existence of consolidated frameworks, such as ISO 27001 [9] and NIST CSF [31], internal auditors still face obstacles in ensuring the complete and consistent assessments of cyber controls, particularly when considering industry-specific factors, such as local regulations and the specific threat profile of the Brazilian banking sector.

Table 4 summarizes the approaches that Internal Audit can adopt to evaluate the effectiveness of cybersecurity controls.

According to the interviewees, implementing the techniques and strategies presented in this research can achieve the following **benefits**:

- **Strategic Decision-Making and Resource Allocation**—The visibility provided by clear reports and dashboards enables managers to assess the cybersecurity landscape, facilitating data-driven decision-making accurately. The availability of strategic intelligence supports efficient resource allocation, directing investments to high-risk areas while avoiding waste. Additionally, identifying improvement areas through objective metrics allows for continuous adjustments, aligning security measures with organizational goals.
- **Proactive Risk and Vulnerability Management**—The ability to identify vulnerabilities and prioritize mitigation actions is essential for an effective defensive posture. Combined with trend analysis, which anticipates emerging threats, organizations can take preventive measures before risks materialize. Rapid response to indicators ensures that changes in the security environment are addressed swiftly, reducing potential impacts. Comprehensive risk mapping guarantees that no critical threats are overlooked.
- **Continuous Monitoring and Evaluation**—Real-time KPIs and KRIs enable ongoing monitoring of security postures, facilitating early detection of anomalies. Periodic evaluation of implemented policies and controls helps measure their effectiveness, ensuring they fulfill their intended purposes. Furthermore, performance analysis of security controls verifies their alignment with organizational needs.

- **Resilience and Process Validation**—Organizations enhance their ability to withstand and recover from cyber incidents, strengthening overall resilience. Penetration testing and other process validation methods verify the efficiency of vulnerability assessments, patch management, and incident response, ensuring readiness for real-world scenarios.
- **Operational Efficiency and Standardization**—Optimized security processes lead to productivity gains and reduced rework, fostering lasting structural improvements. Standardized methodologies ensure consistent risk assessments, while streamlined audits improve execution efficiency. Clearly defined security controls eliminate ambiguity and promote best practices.
- **Technical Capability Development and Independence**—Knowledge transfer between specialists and internal teams enhances technical skills, empowering organizations to address security challenges. Audit independence ensures unbiased risk assessments, which are free from internal biases and contribute to a more objective perspective.
- **Transparency and Communication**—Transparent reporting and relevant metrics improve communication with stakeholders, both internal and external. This builds trust in security management and ensures alignment on risks and protective measures.

Table 4. Summary of context units.

Evaluating the Effectiveness of Cybersecurity Controls	
How internal audit can evaluate the effectiveness of cybersecurity controls implemented in institutions.	
A.	Verify aspects of management and governance of processes, performing high-level and strategic evaluations.
B.	Perform or hire specialized companies to perform Invasion or Penetration Tests (PenTest).
C.	Evaluate the vulnerability management process using tools, established steps, documentation generated, and rules defined and applied.
D.	Conduct security assessments and testing jointly with IT and Cybersecurity teams.
E.	Utilize continuous auditing based on data and information to monitor and evaluate security controls and processes continually.
F.	Assess how cybersecurity and IT areas implement continuous real-time monitoring tools that detect abnormal or suspicious activity.
G.	Compile and analyze data on past security breaches and incidents and current trends in cybersecurity to identify areas of emerging risk.
H.	Develop security reports and dashboards that provide a view of the organization's cybersecurity status.
I.	Establish metrics and indicators that provide a clear and objective view of the organization's current cybersecurity state.
J.	Adopt frameworks that offer standardized structures for process management, risk assessment, and security controls.

Likewise, according to interviewees, when implementing the techniques and strategies presented in this research, auditors may face the following **challenges**:

- **Governance and Independence**—Challenges in this category are directly tied to organizational structure and the preservation of audit impartiality. The absence or ineffectiveness of the second line of defense (risk management and compliance) overburdens internal audit, exposing it to pressure from the first line (operations). Additionally, consulting activities performed by internal audit may compromise its independence if the team becomes too involved in the processes it is meant to evaluate. Another critical issue is cross-departmental alignment, as teams like IT, cybersecurity, and audit often have differing objectives and terminology, hindering effective collabo-

ration. Finally, having the audit team conduct penetration tests can create conflicts of interest, requiring rigorous documentation of methods to preserve objectivity.

- **Technical and Operational Capability**—Technical complexity is one of the biggest hurdles for modern auditing. Integrating data from disparate sources is time-consuming and resource-intensive, while managing large volumes of information demands specialized tools and skills. Data quality is another concern, as unreliable or inconsistent sources can lead to flawed analyses. Furthermore, maintaining dashboards and reports requires significant effort, especially in environments with legacy systems or fragmented infrastructure.
- **Metrics and Indicators**—Defining and interpreting relevant metrics remains a persistent challenge. Many organizations struggle to identify key performance indicators (KPIs) aligned with their strategic risks and objectives, often collecting data that fails to yield actionable insights. Even when metrics are well-defined, their interpretation requires specialized expertise, and superficial analysis can lead to incorrect conclusions, impacting decision-making.
- **Human Resources and Skills Development**—The shortage of qualified talent and the need for continuous upskilling present critical challenges. Relying on external specialists for security testing and other technical tasks not only increases costs but also creates knowledge gaps. Furthermore, the lack of professionals skilled in cybersecurity, data analysis, and governance hinders the audit function's capacity to adopt advanced practices such as Red Team exercises. The ongoing demand for training further strains budgets and necessitates a structured career development plan.
- **Financial and Infrastructure Constraints**—Limited budgets directly affect audit effectiveness. Implementing continuous monitoring tools and security frameworks requires significant licenses, infrastructure, and training investments. Many organizations struggle to justify these costs, especially when tangible returns are not immediate. Moreover, hiring specialized services, such as penetration testing and framework consulting, may become unfeasible under financial constraints.
- **Framework Implementation and Maintenance**—Adopting frameworks like NIST, ISO 27001, or COBIT is essential but fraught with obstacles. Customizing them to the organization's context demands time and expertise, while implementation complexity requires experienced teams. The high upfront deployment costs and the need for ongoing training to maintain updated frameworks pose additional barriers. Without a clear strategy, these initiatives risk becoming never-ending projects that fail to deliver the expected value.

6. Conclusions

The study identified ways internal audits could contribute to ensuring the effectiveness and improvement of cybersecurity controls within Brazilian financial institutions.

Two opposing perspectives emerged regarding the depth of the assessments conducted by Internal Audit. The first suggests that internal audits should focus on high-level management and governance aspects. In contrast, the second argues that internal audits should also conduct detailed assessments of operational activities.

Some proposed conducting penetration tests (PenTests) to assess the effectiveness of cybersecurity processes, either by the third-line team or by companies contracted to validate and improve operational processes. However, the idea may be unfeasible in practice due to technical and budgetary limitations, and it may also be operationally inefficient, given that the first line already employs specialized tools and professionals to perform these activities. Some suggested that the lines work together as an alternative solution, where each could contribute within their specific attributions.

Continuous data-driven auditing was helpful in continually monitoring and evaluating security controls and processes, improving cyber risk management. Analytical tools increase the ability to detect and respond to emerging risks, making recommendations and actions more effective. However, some disagreement existed regarding the accuracy of statistical analyses in large populations versus the efficiency and representativeness of samples in contexts with limited resources. In this sense, the construction of metrics, key risk indicators (KRIs), and performance indicators (KPIs) for continuous monitoring of processes emerged as essential resources for cyber risk management. These metrics help identify weaknesses and opportunities for improvement, with KRIs highlighting potential threats and KPIs evaluating the effectiveness of security policies, such as incident response and compliance with established standards. Financial institutions can directly benefit from the conclusions obtained, especially regarding the performance of internal audits and the use of emerging technologies to evaluate and improve the effectiveness of cybersecurity controls.

Identifying and addressing emerging risks requires a dynamic and systematic approach that combines continuous assessment with concrete mitigation actions. Structured processes must be implemented to prioritize vulnerabilities, adjust controls, and execute specific remediation plans. Collaboration between audit, risk management, and technical areas provides a comprehensive view of threats, facilitating agile and informed decision-making. Utilizing objective metrics and recognized frameworks supports the definition of appropriate measures, while strategic reporting ensures the monitoring of implemented actions. In this manner, organizations can respond effectively to constantly changing risks while maintaining their operational resilience.

Theoretically, this study contributes to the existing literature by analyzing the role of the third line in cyber risk management using the Three Lines Model. Despite the results obtained, this study has some limitations. The sample was composed of a limited number of interviewees, which may not cover all perspectives and experiences within the universe of Brazilian financial institutions, in addition to biasing the results. Although the qualitative nature of the research allows for an in-depth understanding of the phenomena studied, it is difficult to generalize the results to other organizations or contexts. The subjectivity inherent in content analysis can influence the interpretation of the data, even with efforts to maintain objectivity and systematization in the analytical process.

Based on the findings of this study, opportunities for future research emerge. One possibility is to replicate the study with a larger and more diverse sample, including different institutions, countries, and sectors relevant to society. For example, how do the results vary between public and private organizations across different geographic regions? Another possibility would be to explore the topic of continuous auditing, comparing the effectiveness of this approach with traditional auditing in terms of early threat detection, incident response, and prevention of security breaches. This could also involve developing specific risk models that integrate continuous auditing as a critical variable in assessing cyber risk exposure. Does continuous auditing significantly reduce the time it takes to detect vulnerabilities compared to traditional methods? Regarding the integration of threat modeling into internal audit processes, researchers could explore methods to incorporate it at all stages- from the planning phase to execution and reporting- or develop and validate specific tools that internal auditors can use to conduct threat modeling efficiently and effectively. What would be the impact of automating threat modeling on the accuracy and efficiency of audit processes? Finally, studies could investigate how internal audits can systematically integrate penetration testing into their security assessments or explore the effectiveness of third-party penetration testing. For example, are penetration tests conducted by internal teams as effective as those carried out by external experts? Addi-

tionally, it would be relevant to include a cost-benefit analysis of how implementing the proposed assessment methods can help institutions understand the potential return on investment and make informed decisions. What is the optimal balance between investing in continuous auditing, threat modeling, and penetration testing to maximize cybersecurity without compromising the financial viability of organizations?

Author Contributions: Conceptualization, L.V.A.F.; methodology, L.V.A.F. and R.R.N.; validation, L.V.A.F., C.A.d.M.A., L.P.d.M. and R.R.N. All authors contributed equally to writing and revising the document. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the University of Brasilia (UnB).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data and information presented in this study are available upon request to the authors.

Acknowledgments: The authors acknowledge the University of Brasília (UnB) for the financial support provided by the Grant nº 001/2025 DPI/BCE/UnB.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

AI	Artificial Intelligence
BACEN	Banco Central do Brasil
C2M2	Cybersecurity Capability Maturity Model
CIS	Center for Internet Security
CMN	National Monetary Council
COBIT	Control Objectives for Information and Related Technologies
CRM	Cyber Risk Management
CSF	Cybersecurity Framework
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IIA	The Institute of Internal Auditors
IPS	Intrusion Prevention System
ISO	International Organization for Standardization
IT	Information Technology
KPI	Key Performance Indicator
KRI	Key Risk Indicator
MTTD	Mean Time to Detect
MTTR	Mean Time to Repair
NIST	National Institute of Standards and Technology
Pentest	Penetration Testing
SFN	National Financial System
SIEM	Security Information and Event Management
SWIFT	Society for Worldwide Interbank Financial Telecommunication
UEBA	User and Entity Behavior Analytics

References

1. Cremer, F.; Sheehan, B.; Fortmann, M.; Kia, A.; Mullins, M.; Murphy, F.; Materne, S. Cyber risk and cybersecurity: A systematic review of data availability. *Geneva Pap. Risk Insur. Issues Pract.* **2022**, *47*, 698–736. [CrossRef] [PubMed]
2. McShane, M.; Eling, M.; Nguyen, T. Cyber risk management: History and future research directions. *Risk Manag. Insur. Rev.* **2021**, *31*, 701–728.

3. Rosati, P.; Gogolin, F.; Lynn, T. Cyber-Security Incidents and Audit Quality. *Eur. Account. Rev.* **2017**, *31*, 701–728. [CrossRef]
4. PWC PriceWaterhouseCoopers. *Global Digital Trust Insights 2023, A C-Suite United On Cyber-Ready Futures*; PWC PriceWaterhouse-Coopers: Adelaide, Australia, 2024.
5. Benz, M.; Chatterjee, D. Calculated risk? A cybersecurity evaluation tool for SMEs. *Bus. Horizons* **2020**, *63*, 531–540. [CrossRef]
6. VERIZON Verizon Business. *2021 Data Breach Investigations Report*; VERIZON Verizon Business: Basking Ridge, NJ, USA, 2021.
7. IBM International Business Machines. *Cost of A Data Breach Report 2023*; IBM International Business Machines: Armonk, NY, USA, 2023.
8. Tripathi, M.; Mukhopadhyay, A. Does privacy breach affect firm performance? An analysis incorporating event-induced changes and event clustering. *Inf. Manag.* **2022**, *59*, 24. [CrossRef]
9. *ISO/IEC 27001:2022*; Information Technology—Security Techniques—Information Security Management Systems—Requirements. ISO/IEC International Organization for Standardization/International Electrotechnical Commission: Geneva, Switzerland, 2022.
10. *Resolution CMN No. 4,968*; On Internal Control Systems of Financial Institutions. Brazilian National Monetary Council: Brasília, Brazil, 2021
11. Bantleon, U.; D'Arcy, A.; Eulerich, M.; Hucke, A.; Pedell, B.; Ratzinger-Sakel, N. Coordination Challenges in Implementing the Three Lines of Defense Model. *Corp. Governance Intern. Gov.* **2021**, *25*, 59–74. [CrossRef]
12. Afrifah, W.; Epiphaniou, G.; Ersotelos, N.; Maple, C. Barriers and Opportunities In Cyber Risk And Compliance Management For Data-Driven Supply Chains. In Proceedings of the 55th Hawaii International Conference on System Sciences (HICSS 2022), Virtual Event, 4–7 January 2022; ScholarSpace, University of Hawai'i at Mānoa: Honolulu, HI, USA, 2022.
13. Chen, Y.; Galletta, D.; Lowry, P.; Luo, X.; Moody, G.; Willison, R. Understanding Inconsistent Employee Compliance with Information Security Policies Through the Lens of the Extended Parallel Process Model. *Inf. Syst. Res.* **2021**, *32*, 1043–1065. [CrossRef]
14. Eulerich, A.; Eulerich, M. What Is the Value of Internal Auditing?—A Literature Review on Qualitative and Quantitative Perspectives. *Corp. Governance Actors Play. J.* **2020**, *94*, 83–92. [CrossRef]
15. Carcello, J.; Eulerich, M.; Masli, A.; Wood, D. Are Internal Audits Associated with Reductions in Perceived Risk? *Audit. J. Pract. Theory* **2020**, *39*, 55–73. [CrossRef]
16. Lois, P.; Drogalas, G.; Karagiorgos, A.; Thrassou, A.; Vrontis, D. Internal auditing and cyber security: Audit role and procedural contribution. *Int. J. Manag. Financ. Account.* **2021**, *13*, 25–47. [CrossRef]
17. Kahyaoglu, S.; Çalıyurt, K. Cyber security assurance process from the internal audit perspective. *Manag. Audit. J.* **2018**, *33*, 360–376. [CrossRef]
18. Georg, M.A.C.; Rodrigues, W.M.S.; Alves, C.A.D.M.; Silveira Júnior, A.; Nunes, R.R. Os desafios da Segurança Cibernética no setor público federal do Brasil: Estudo sob a ótica de gestores de tecnologia da informação. *RISTI* **2023**, *E54*, 602–616.
19. Alves, R.S.; Georg, M.A.C.; de Sousa, R.T.; Nunes, R.R. Judiciário sob ataque hacker: Riscos de negócio para segurança cibernética em tribunais brasileiros. *RISTI* **2023**, *E56*, 344–357.
20. Alves, R.S.; Queiroz, C.E.M.; Nunes, R.R. Os Tribunais têm Estrutura Para Gerenciar Riscos de Segurança da Informação? Um estudo à luz das Três Linhas. *Revista CEJ* **2024**, *27*, 145–160.
21. Walker, P.; Shenkir, W. Enterprise Risk Management: Frameworks, Elements, and Integration. *Risk Manag. J.* **2018**, *33*, 36–42.
22. Chong, W.; Feng, R.; Hu, H.; Zhang, L. Cyber Risk Assessment for Capital Management. *arXiv* **2022**, arXiv:2205.08435. [CrossRef]
23. Alahmari, A.; Duncan, B. Cybersecurity Risk Management in Small and Medium-Sized Enterprises: A Systematic Review of Recent Evidence. In Proceedings of the 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), Dublin, Ireland, 15–19 June 2020; pp. 1–5.
24. Deebak, B.; Al-turjman, F. Privacy-preserving in smart contracts using blockchain and artificial intelligence for cyber risk measurements. *J. Inf. Secur. Appl.* **2021**, *58*, 102749. [CrossRef]
25. ISACA Information Systems Audit and Control Association. *COBIT® 2019 Framework: Governance and Management of Enterprise IT*; ISACA Information Systems Audit and Control Association: Schaumburg, IL, USA, 2019.
26. *ISO/IEC 27005*; Information Technology—Security Techniques—Information Security, Cybersecurity and Privacy Protection—Guidance on Managing Information Security Risks. ISO/IEC International Organization for Standardization/International Electrotechnical Commission: Geneva, Switzerland, 2022.
27. IIA Institute of Internal Auditors. *The IIA's Three Lines Model: An Update of the Three Lines of Defense*; IIA Institute of Internal Auditors: Lake Mary, FL, USA, 2022.
28. Deloitte Deloitte Touche Tohmatsu Limited. *Modernizing the Three Lines of Defense Model*; Deloitte Deloitte Touche Tohmatsu Limited: London, UK, 2020.
29. Eulerich, M. The New Three Lines Model for Structuring Corporate Governance—A Critical Discussion of Similarities and Differences. *Entrep. Soc. Sci. J.* **2021**, *18*, 180–187.
30. BRASIL Banco Central do Brasil. *Regulação Prudencial—Resolução CMN N° 4.553 De 30/1/2017*; BRASIL Banco Central do Brasil: Brasília, Brazil, 2017.

31. NIST National Institute of Standards and Technology. *The NIST Cybersecurity Framework (CSF) 2.0*; NIST National Institute of Standards and Technology: Gaithersburg, MD, USA, 2024.
32. European Union. *Directive (EU) 2022/2555 (NIS2) on Measures for a High Common Level of Cybersecurity Across the Union*; European Union: Brussels, Belgium, 2023.
33. PCI Security Standards Council. *PCI DSS v4.0—Payment Card Industry Data Security Standard*; PCI Security Standards Council: Wakefield, MA, USA, 2022
34. European Union. *Digital Operational Resilience Act (DORA)—Regulation (EU) 2022/2554*; European Union: Brussels, Belgium, 2025.
35. Monetary Authority of Singapore. *Technology Risk Management Guidelines*; Monetary Authority of Singapore: Singapore, 2021.
36. Brazilian National Monetary Council. *Resolution CMN No. 4,879—On Internal Audit Activities in Financial Institutions*; Brazilian National Monetary Council: Brasília, Brazil, 2020.
37. Brazilian National Monetary Council. *Resolution CMN No. 4,893—On Security Policy Implementation and Effectiveness Monitoring Mechanisms*; Brazilian National Monetary Council: Brasília, Brazil, 2021.
38. Central Bank of Brazil. *Normative Instruction BCB No. 305—Open Finance Security Manual Version 4.0*; Central Bank of Brazil: Brasília, Brazil, 2022.
39. Cai, T. Continuous Auditing and Risk Monitoring: Implementation with Automation. *ISACA J.* **2024**, *5*.
40. Eulerich, M.; Fligge, B.; Lopez-Kasper, V.I.; Wood, D.A. Patience Is Key: The Time It Takes to See Benefits from Continuous Auditing. *Account. Horizons* **2024**, *39*, 69–86. [CrossRef]
41. Jada, I.; Mayayise, T.O. The impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review. *Data Inf. Manag.* **2023**, *8*, 100063. [CrossRef]
42. Taiwo, P.; Akoto-Bamfo, D.; Kpakpa, C.T.; Panful, B.; Oware, D. Evaluating the role of cybersecurity audits in protecting the US capital market. *World J. Adv. Res. Rev.* **2025**, *25*, 974–980. [CrossRef]
43. Anand, A.; Chirputkar, A.; Ashok, P. Mitigating Cyber-Security Risks using Cyber-Analytics. In Proceedings of the 7th International Conference on Trends in Electronics and Informatics (ICOEI 2023), Tirunelveli, India, 11–13 April 2023.
44. Schreiber, A.; Schreiber, I. AI for cyber-security risk: Harnessing AI for automatic generation of company-specific cybersecurity risk profiles. *Inf. Comput. Secur.* 2025, *ahead-of-print*.
45. Ali, S.M.; Razzaque, A.; Yousaf, M.; Shan, R.U. An Automated Compliance Framework for Critical Infrastructure Security Through Artificial Intelligence. *IEEE Access* **2025**, *13*, 4436–4459. [CrossRef]
46. Almaqtari, F.A. The Role of IT Governance in the Integration of AI in Accounting and Auditing Operations. *Economies* **2024**, *12*, 199. [CrossRef]
47. Jiang, W. Cybersecurity Risk and Audit Pricing—A Machine Learning-Based Analysis. *J. Inf. Syst.* **2024**, *38*, 91–117. [CrossRef]
48. Sabillon, R.; Higuera, J.R.B.; Cano, J.; Higuera, J.B.; Montalvo, J.A.S. Assessing the Effectiveness of Cyber Domain Controls When Conducting Cybersecurity Audits: Insights from Higher Education Institutions in Canada. *Electronics* **2024**, *13*, 3257. [CrossRef]
49. Saravanan, S.; Menon, A.K.; Saravanan, K.; Gopalakrishnan, J. Cybersecurity Audits for Emerging and Existing Cutting Edge Technologies. In Proceedings of the 2023 IEEE International Symposium (ISED 2023), Dehradun, India, 15–17 December 2023.
50. Sabillon, R.; Bermejo Higuera, J.R. New Validation of a CyberSecurity Audit Model to Audit the Cybersecurity Program in a Canadian Higher Education Institution. In Proceedings of the 2023 Conference on Information Communications Technology and Society (ICTAS), Durban, South Africa, 8–9 March 2023; pp. 1–6.
51. Shalabi, K.; Al-Fayoumi, M.; Al-Haija, Q. Enhancing Financial System Resilience Against Cyber Threats via SWIFT Customer Security Framework. In Proceedings of the 2023 International Conference On Information Technology (ICIT), Kyoto, Japan, 14–17 December 2023; pp. 260–265.
52. BRASIL Banco Central do Brasil. *Relatório de Estabilidade Financeira N° 26*; BRASIL Banco Central do Brasil: Brasília, Brazil, 2024.
53. Gordieieva, T.; Tsaturian, A. Analysis of trends and determinants of the 'Big 4' companies in the global audit market. *Technol. Audit. Prod. Reserv.* **2023**, *4*, 6–11. [CrossRef]
54. Staveren, M. What can controllers and internal auditors do to support risk ownership. *Maandbl. Voor Account. Bedrijfsecon.* **2021**, *95*, 261–268. [CrossRef]
55. Eling, M.; Elvedi, M.; Falco, G. The Economic Impact of Extreme Cyber Risk Scenarios. *North Am. Actuar. J.* **2022**, *27*, 429–443. [CrossRef]
56. Kikuchi, M.; Okubo, T. Cyber Governance Complex in Firms. In Proceedings of the 2nd International Conference on Control and Computer Vision, Jeju Island, Republic of Korea, 15–18 June 2019.
57. Brunner, M.; Sauerwein, C.; Felderer, M.; Breu, R. Risk Management Practices in Information Security: Exploring the Status Quo in the DACH Region. *Comput. Secur.* **2020**, *92*, 101776. [CrossRef]
58. ISACA Information Systems Audit and Control Association. *Risk IT Framework for IT Risk Management—A Practical Application for the Risk IT Framework*; ISACA Information Systems Audit and Control Association: Schaumburg, IL, USA, 2020.
59. Bank for International Settlements (BIS). *Cyber-resilience: Range Of Practices*; BCBS Basel Committee on Banking Supervision—Bank for International Settlements (BIS): Basel, Switzerland, 2018.

60. Setyaningrum, D.; Kuntadi, C. The effects of competence, independence, audit work, and communication on the effectiveness of internal audit. *J. Econ. Bus. Account. Ventur.* **2019**, *22*, 39–47. [CrossRef]
61. Johari, R.; Razali, F.; Hashim, A. Enterprise Risk Management: Internal Auditor's Role Perspective. *Int. J. Acad. Res. Account. Financ. Manag. Sci.* **2022**, *12*, 1–14. [CrossRef] [PubMed]
62. Hubbard, D.; Seiersen, R. *How to Measure Anything in Cybersecurity Risk*; John Wiley & Sons, Inc.: Hoboken, NJ, USA, 2016.
63. Zaidirina, L.; Bangsawan, S. Implementation of corporate governance and mandatory disclosure in the Indonesian banking sector: Good news or bad news. *Int. J. Monet. Econ. Financ.* **2017**, *10*, 281–294. [CrossRef]
64. Dacorogna, M.; Debbabi, N.; Kratz, M. Building up Cyber Resilience by Better Grasping Cyber Risk Via a New Algorithm for Modelling Heavy-Tailed Data. *Eur. J. Oper. Res.* **2022**, *311*, 708–729. [CrossRef]
65. IBM International Business Machines. *Cost of a Data Breach Report 2020*; IBM International Business Machines: Armonk, NY, USA, 2020.
66. Bardin, L. *Análise de Conteúdo*; Edições 70—Almedina Brasil: São Paulo, Brazil, 2016.
67. Deloitte Deloitte Touche Tohmatsu Limited. *Risk Management in the Digital Age—Bitcoin Futures and Hedge Accounting*; Deloitte Deloitte Touche Tohmatsu Limited: London, UK, 2019.
68. IIA Institute of Internal Auditors. *Global Perspectives & Insights: Cybersecurity*; IIA Institute of Internal Auditors: Lake Mary, FL, USA, 2023.
69. Muhsyaf, S.; Cahyaningtyas, S.; Sasanti, E. Three Line of Defense: An Effective Risk Management. In Proceedings of the 18th International Symposium On Management (INSYMA 2021), Online, 27–28 May 2021.
70. BCI Business Continuity Institute. *Good Practice Guidelines*; BCI Business Continuity Institute: Reading, UK, 2018.
71. USA Office of Cybersecurity, Energy Security, and Emergency Response. *Cybersecurity Capability Maturity Model (C2M2)—Version 2.1*; USA Office of Cybersecurity, Energy Security, and Emergency Response: Washington, DC, USA, 2022.