Journal of Digital Innovation in Financial and Administrative Studies, 2025, Vol.1 No.0, (11-16)
ISSN: 3080-1907, **DOI**: https://doi.org/10.69513/jdifas.v1.i0.a2

Journal of Digital Innovation in Financial and Administrative Studies

https://jdifas.alnoor.edu.iq/

The Role of Internal Auditing in Cybersecurity: A Theoretical and Analytical Study

A S Ali[1] **N H Rashid** [1]

[1]Department of Accounting Techniques, College of Administrative Technologies, Alnoor University, Mosul, 41012, Iraq

Article information

Article history:
Received: 25 May 2025
Revised: 8 June 2025
Accepted: 2 July 2025

Keywords:
Cybersecurity
Cybersecurity Auditing
Cybersecurity Topical Requirements

Correspondence:
Nadhim Hassan Rashid
Nadhim.hassan@alnoor.edu.iq

Abstract

The research aims to understand the concept of cybersecurity auditing, the most important future skills required for internal auditors in the field of cybersecurity auditing, the main roles of internal auditing in this field, the most important steps taken by internal auditors to conduct a cybersecurity audit, the main areas on which internal cybersecurity auditing should focus, and an explanation of the role of internal auditing in cybersecurity governance.

To achieve the research objectives, the researchers used a deductive approach to study and analyze, utilizing periodicals, books, and websites that address the research topic, particularly in relation to the following areas: cybersecurity auditing, the main roles of internal auditing in the field of cybersecurity, future skill requirements, the Institute of Internal Auditors' (IIA) cybersecurity Topical requirements, and the use of these three lines of defense against cybersecurity risks.

The research reached a set of conclusions, the most important of which are:

1. Integrating cybersecurity risks into audit plans, rather than isolating them from other audit activities. This ensures the continued effectiveness of audit operations in the face of rapidly evolving threats.
2. It is important for internal audit units to understand the purpose of the objective requirements for cybersecurity and their relationship to the International Professional Practices Framework and global internal auditing standards. A comprehensive and accurate understanding of these requirements will help internal audit units adhere to the Institute of Internal Auditors (IIA) standards while ensuring cybersecurity practices.

Based on the research findings, proposals were made that are consistent with these findings, the most important of which are:

1. Entities involved in the internal audit profession should hold specialized seminars and workshops to introduce the concept and dimensions of cybersecurity auditing, the steps internal auditors take to conduct cybersecurity audits, the key areas of focus for cybersecurity audits, and the role of internal auditing in cybersecurity governance.
2. Support internal auditors in improving the future technical and non-technical skill requirements for internal auditors in the field of cybersecurity auditing through continuous learning and professional development, to provide the skills and knowledge necessary to conduct effective cybersecurity audits.

ISSN: 3080-1907, **DOI**: https://doi.org/10.69513/jdifas.v1.i0.a2

Introduction

Cyber threats represent a pressing issue faced by any organization anywhere in the world, due to the increasing reliance on computer systems, infrastructure, the Internet, social media, and technological innovation. The global cybersecurity ecosystem has evolved radically, and its protection has become a complex matter, largely because cybercriminals' attacks are developing at a faster pace than security solutions.

In our interconnected world, cybersecurity is a primary responsibility shared by the board of directors and all organizational employees, including administrators and staff. The changes and improvements that accompany new technologies and innovations—and their adoption by organizations—have become more complex than the development of auditing and oversight, limiting their ability to provide cybersecurity assurances. Therefore, the increasing complexity of cybersecurity and its technologies is a major concern for organizations, as many have not significantly changed their oversight approaches.

Internal auditors play a vital role in raising cybersecurity awareness within organizations by leveraging their expertise in risk assessment, governance frameworks, and regulatory compliance. They can support organizations in making improvements and work alongside certified cybersecurity consulting firms to reduce cyber threats and protect critical assets. By adhering to key risk and governance standards and collaborating among themselves, they can help ensure organizations adopt effective cybersecurity practices amid an ever-evolving threat environment.

Cybersecurity auditing plays a multifaceted and critical role. By bridging the gap between auditing and cybersecurity, assessing cyber risks, ensuring compliance, facilitating effective communication, promoting a culture of continuous improvement, embracing technological advances, strengthening cybersecurity training, and preparing comprehensive incident response plans, internal cybersecurity auditing can significantly enhance an organization's cybersecurity posture.

Cybersecurity audits enable organizations to take a proactive approach to improve their security posture and remain protected against cyber threats.

Internal auditing plays a vital role in promoting institutional innovation and developing a change-oriented mindset. To effectively fulfill this role, the internal audit function must shift from its traditional focus on retrospective analysis and control testing to a more consultative, forward-looking approach supported by professional and academic research, benchmarking, advanced data analytics, and business process analysis methodologies.

The objective requirements of cybersecurity provide a foundational approach for internal audit functions when assessing cybersecurity as an audit subject or identifying it as a risk within other audit processes. Among the other key requirements are the clear definition of roles and responsibilities within the organization concerning strategic cybersecurity goals, ensuring a robust and up-to-date risk management approach to address recurring cyber risks, and confirming that management establishes an effective internal control environment.

Research Problem

The primary research problem is encapsulated in the following main question:

Can internal auditing conduct cybersecurity audits?

This question branches into the following sub-questions:

1.How can internal auditing support effective management of cybersecurity risks?

2.What future skills are required for internal auditors in the field of cybersecurity auditing?

3.What are the main roles of internal auditing in the field of cybersecurity?

4.What steps does the internal auditor take to conduct a cybersecurity audit?

5.What are the key areas internal cybersecurity auditing should focus on?

6.As a third line of defense, what steps can internal auditing take against cybersecurity risks?

Research Significance

The significance of the research stems from the critical role of cybersecurity in protecting organizational assets and information from cyber threats. Managing and assessing cybersecurity risks has become increasingly important as organizations become more dependent on technology. To mitigate or entirely avoid potential attacks, cybersecurity risks must be identified, assessed, and prioritized.

Organizations operate in a dynamic and ever-changing environment and are exposed to a variety of risks, most notably cybersecurity. Internal auditors, through their diverse roles, can contribute to reducing breaches in information systems.

This research serves as a call to boards of directors, internal audit, and risk management to recognize cybersecurity threats and the importance of auditing them as organizational threats. It also emphasizes the necessity for collaboration among them as partners in managing the organization's risks and challenges. However, available studies addressing the relationship between internal auditing and cybersecurity around the world are limited. Therefore, this study is a novel effort that has not been sufficiently addressed previously. Hence, this research aims to enrich the body of knowledge regarding internal auditing of cybersecurity.

ISSN: 3080-1907, **DOI**: https://doi.org/10.69513/jdifas.v1.i0.a2

Research Objectives

This study aims to achieve the following objectives:

Define the concept of cybersecurity auditing and its dimensions.

Identify the most important future skills required for internal auditors in the field of cybersecurity auditing.

Identify the main roles of internal auditing in the field of cybersecurity.

Define the key steps an internal auditor takes to conduct a cybersecurity audit and the core areas that internal cybersecurity auditing should focus on.

Explain the role of internal auditing in cybersecurity governance.

As a third line of defense, identify the primary steps internal auditing can take against cybersecurity risks.

Research Hypotheses

Internal auditing can effectively support cybersecurity risk management.

Internal audit units work on providing the future skills required for internal auditors in the field of cybersecurity auditing.

An internal audit work program can be developed that includes the steps taken by internal auditors to conduct cybersecurity audits and the key areas they should focus on.

The three lines of defense can be used against cybersecurity risks as a fundamental means to establish and organize roles, responsibilities, accountability, decision-making, risk management, and control to achieve effective governance risk management and assurance.

Research Methodology

The research adopts a deductive methodology in study and analysis by utilizing journals, books, and websites that discuss the research topic, particularly in the following areas:

The concept and dimensions of cybersecurity

Cybersecurity auditing

Future skill requirements for internal auditors in cybersecurity auditing

The main roles of internal auditing in cybersecurity

Key areas internal auditing should focus on in cybersecurity

The role of internal auditing in cybersecurity governance

Accordingly, the study is divided as follows:

Chapter One: Cybersecurity Auditing and Its Dimensions

Chapter Two: Future Skill Requirements for Internal Auditors in Cybersecurity Auditing

Chapter Three: Cybersecurity and the Role of Internal Auditing

Chapter One: Cybersecurity Auditing and Its Dimensions

Cybersecurity is the process of protecting computer systems and networks from unauthorized access, use, disclosure, disruption, modification, or destruction. It involves a set of technologies, policies, and procedures aimed at securing data and systems from cyber threats. Cybersecurity is essential for maintaining the confidentiality, integrity, and availability of information, especially in a time when organizations rely heavily on digital technology. This means that cybersecurity is the strategy, processes, and controls used to protect systems, networks, programs, devices, and data from cyberattacks.

1. The Importance of Cybersecurity

Cybersecurity has become a vital necessity in the contemporary digital age. With the widespread adoption of digital technologies in all aspects of life, cybersecurity has become indispensable. Organizations and individuals depend on digital systems for communication, work, and personal matters. Consequently, any threat to these systems can have serious consequences, including financial losses, damage to reputation, and threats to national security. Therefore, cybersecurity aims to ensure the safety and security of information and systems against cyber threats.

2. Cybersecurity Objectives

Cybersecurity seeks to achieve several goals to ensure the protection of digital systems and data. These goals include:

Protecting data from unauthorized access or manipulation.

Ensuring the availability of systems and services at all times.

Maintaining the confidentiality and integrity of sensitive information.

Protecting against cyberattacks and identifying them quickly.

Minimizing the damage resulting from cyberattacks.

Ensuring compliance with laws and regulations related to data protection.

3. Types of Cybersecurity

Cybersecurity encompasses various types that cover different aspects of information and system protection, including:

Network Security: Protects communication networks from unauthorized access or attacks.

Information Security: Focuses on protecting data and ensuring its confidentiality, integrity, and availability.

Application Security: Secures software applications from vulnerabilities and attacks.

Operational Security: Involves managing and protecting the processes and procedures that control data and systems.

Disaster Recovery and Business Continuity: Ensures the continuity of operations in the event of a cyberattack or data loss.

User Security: Emphasizes educating users on how to deal safely with digital systems and avoid risks.

ISSN: 3080-1907, **DOI**: https://doi.org/10.69513/jdifas.v1.i0.a2

Cloud Security: Protects data stored in cloud computing systems.

4. The Concept of Cybersecurity Auditing

Cybersecurity auditing is a systematic and comprehensive process aimed at evaluating and verifying the organization's security practices and policies to ensure they align with recognized standards and best practices. This audit involves reviewing and analyzing security systems, policies, and procedures, in addition to conducting penetration tests and security reviews. The goal of cybersecurity auditing is to identify potential vulnerabilities and risks and provide recommendations to enhance the organization's security.

5. The Importance of Cybersecurity Auditing

Cybersecurity auditing is essential for ensuring the safety of digital systems and maintaining trust among stakeholders. The importance of cybersecurity auditing lies in the following:

Identifying Security Gaps: Helps discover weaknesses in current security systems.

Ensuring Compliance: Ensures compliance with cybersecurity laws and standards.

Improving Security: Provides recommendations to strengthen protection and enhance security practices.

Reducing Risks: Helps reduce exposure to cyberattacks and minimize damage.

Raising Awareness: Increases awareness among employees about cybersecurity risks and how to avoid them.

6. Cybersecurity Auditing Stages

Cybersecurity auditing goes through several main stages, including:

Planning: Determining the scope of the audit, identifying objectives, and selecting the appropriate tools and methods.

Data Collection: Gathering information about systems, applications, and existing security policies.

Analysis and Evaluation: Evaluating the current security situation, identifying weaknesses and potential risks.

Reporting: Preparing a detailed report that includes findings and recommendations.

Follow-Up: Ensuring that the recommended improvements are implemented and verifying their effectiveness.

7. The Role of Internal Audit in Cybersecurity

Internal audit plays a vital role in supporting cybersecurity within organizations. Its role includes:

Assessing Risk: Evaluating cyber risks and identifying the organization's exposure to them.

Evaluating Controls: Reviewing the effectiveness of technical and administrative security controls.

Providing Recommendations: Offering advice and recommendations to enhance security.

Monitoring Compliance: Ensuring the organization complies with cybersecurity policies and laws.

Training and Awareness: Contributing to increasing employees' awareness of cybersecurity risks.

8. Challenges Facing Cybersecurity Auditing

Despite its importance, cybersecurity auditing faces several challenges, including:

Rapid Technological Development: Constant evolution of technologies makes it difficult to keep up with threats.

Shortage of Specialized Skills: Lack of experienced professionals in cybersecurity auditing.

Complexity of Systems: Increasing complexity of systems and networks complicates the audit process.

Resistance to Change: Organizations' reluctance to implement necessary improvements.

Cost: High cost of implementing cybersecurity audit recommendations.

9. Cybersecurity Auditing Standards

Several international standards are used to guide cybersecurity auditing, including:

ISO/IEC 27001: Specifies requirements for information security management systems.

NIST Cybersecurity Framework: Provides a comprehensive framework for managing cybersecurity risks.

COBIT Framework: Helps manage IT risks and ensures alignment between IT and business goals.

PCI DSS Standard: Ensures secure handling of credit card information.

Conclusions and Recommendations

Conclusions

Internal auditing for cybersecurity is an in-depth review of an organization's security procedures and is a key element in a comprehensive risk management strategy. When properly conducted, cybersecurity audits should reveal all cybersecurity risks within the organization and detail the policies, procedures, and controls implemented to effectively manage those risks.

The importance of managing and assessing cybersecurity risks is growing as companies become more reliant on technology. To mitigate or avoid the impact of potential attacks and protect the company's assets and information, cybersecurity risks must be identified, assessed, and prioritized. Internal auditing can play a significant role in this process.

Cybersecurity risks should be integrated into audit plans rather than isolated from other auditing activities. This ensures the continued effectiveness of audit operations in the face of rapidly evolving threats.

Internal auditors are encouraged to work closely with their counterparts in the information security field to achieve objectives, share knowledge, and conduct a comprehensive assessment of cybersecurity controls.

Internal audit units understand the objective requirements of cybersecurity and their relationship to

the International Professional Practices Framework and global internal audit standards. A comprehensive and accurate understanding of these requirements will help internal audit units comply with the standards of the Institute of Internal Auditors (IIA) while ensuring cybersecurity practices.

Internal auditors should apply a consistent methodology in cybersecurity audit processes. This highlights the need for auditors to develop a comprehensive understanding of the cybersecurity environment, including potential threats, vulnerabilities, and the impact of cyber incidents on organizational operations. This will serve as the foundation for cybersecurity audit processes.

As the audit landscape evolves due to technological advancements, changing regulatory environments, and cybersecurity risks, the skills and competencies required of the next generation of auditors are undergoing a fundamental transformation. Future auditors will possess a combination of traditional auditing expertise and advanced technical knowledge to handle the complexities of modern auditing practices. The core skills and competencies identified will enable auditors to meet the demands of the future auditing environment, including cybersecurity auditing, and add value to their organizations.

Recommendations

Entities concerned with the internal audit profession should hold specialized seminars and workshops to introduce the concept and dimensions of cybersecurity auditing, guide stakeholders on the key roles of internal auditing in cybersecurity, outline the steps internal auditors take in conducting cybersecurity audits, and identify the main areas of focus and the role of internal auditing in cybersecurity governance.

Entities involved in internal auditing should assign internal audit units to develop a work program for evaluation and auditing that addresses aspects related to cybersecurity auditing within the organization, defines key objectives, scope of work, and the necessary procedures to achieve those objectives.

Support internal auditors in improving the future technical and non-technical skill requirements for cybersecurity auditing through continuous learning and professional development, in order to provide the necessary skills and knowledge for effective cybersecurity audits.

Organizations and professional institutes specializing in internal auditing should develop and update their training and academic curricula by issuing new guidelines and standards to enable internal auditors to perform the new tasks required by technologies such as cybersecurity and emphasize the importance of auditing it.

Internal auditing is an independent service responsible for providing independent reports and opinions. Accordingly, top management is responsible for ensuring the integrity and independence of the internal auditor within the organization (32).

Internal auditing plays a critical role in enhancing the organization's ability to serve the public interest. While the core function of internal auditing is to strengthen governance, risk management, and control processes, its impact extends beyond the organization. Internal auditing contributes to the overall stability and sustainability of the organization by providing assurance on operational efficiency, reliability of reporting, compliance with laws and regulations, asset protection, and ethical culture. This, in turn, enhances public confidence in the organization and the broader systems to which it belongs (12).

Internal auditing is conducted by professionals with a deep understanding of the organization's culture, systems, and processes. It ensures the efficiency of the organization’s controls to mitigate its risks, the effectiveness of governance operations, and the achievement of organizational objectives. This includes evaluating emerging technologies, analyzing opportunities, assessing risks, controls, ethics, quality, economy, and efficiency, ensuring adequate controls to reduce risks, and clearly and accurately communicating information and conclusions. These diverse responsibilities give internal auditors a broad perspective of the organization and make the internal audit function a valuable resource for boards and senior management (25).

This means that internal auditing enhances the organization’s ability to create, protect, and sustain value by providing the board and management with independent, risk-based, and objective assurance, advice, insight, and foresight.

In the digital age, the role of internal auditing is rapidly evolving, with cybersecurity being one of the main drivers of this transformation. As organizations increasingly rely on digital infrastructure and data, the risks associated with cyber threats have become a major concern. Cybersecurity has been placed at the forefront of internal audit functions, prompting a restructuring of its strategies, methodologies, and skill requirements.

Cyber threats are no longer a distant possibility but a real and growing danger. From ransomware attacks that can disrupt organizational operations to data breaches that can cause severe financial and reputational damage, the impact of cyber threats is far-reaching. This evolving risk landscape has necessitated a fundamental shift in the internal audit function. Auditors are now expected to ensure the effectiveness of cybersecurity controls and risk management strategies within the organization (33).

As cybersecurity threats continue to evolve, the role of internal auditors has undergone a profound transformation. While they previously focused on

financial and operational risks, they now must navigate the complex world of cybersecurity. Protecting sensitive data, evaluating IT infrastructure, and ensuring compliance with ever-changing regulations are now fundamental elements of the modern internal audit function (19).

In just a few years, cybersecurity has become one of the most critical risk management challenges facing almost every type of organization. The key question now is: Is the internal audit function keeping pace with this rapidly changing risk landscape? (24)

References

1. Babiker, I. (2025). *The role of internal audit in enhancing cyber security from the auditors' point of view*. Journal of Business and Environmental Sciences, 4(1).
2. Gassama, S., & Sudaryati, E. (2022). The role of internal audit quality to the sustainability and success of microfinance program. *Manajemen Bisnis*, *12*(1), 45–51.
3. The Institute of Internal Auditors. (2017a). *Measuring internal audit effectiveness and efficiency*.
4. PricewaterhouseCoopers. (2017). *COSO internal control framework*.
5. Alih, U., Elaigwu, M., & Salau, R. K. (2021). Cybersecurity risk assessment and the role of internal audit function among the listed financial companies in Nigeria: A global empirical perspective. *Creative Journal of Business Research*, *1*(1).
6. Eling, M., & Wirfs, J. H. (2016). Cyber risk: Too big to insure? Risk transfer options for a mercurial risk class. *Institute of Insurance Economics, University of St. Gallen*, 23–57.
7. Badawy, H. A. (2021). The impact of assurance quality and level on cybersecurity risk management program on non-professional Egyptian investors' decisions: An experimental study. *Alexandria Journal of Accounting Research*, *5*(3), 1–56.
8. EC-Council. (2023). *What is cyber security? Definition, meaning, and purpose*. https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/what-is-
9. Hartmann, C. C., & Carmenate, J. (2021). Academic research on the role of corporate governance and IT expertise in addressing cybersecurity breaches: Implications for practice, policy, and research. *American Accounting Association*, *15*(2), A9–423.
10. KnowledgeLeader. (2017). *What is internal audit's role in cyber security?* https://info.knowledgeleader.com/what-is-internal-audits-role-in-cyber-security
11. AuditBoard. (2023). *NIST cybersecurity framework (NIST CSF) overview & guide*. https://auditboard.com/blog/nist-cybersecurity-framework
12. The Institute of Internal Auditors. (2024b). *The three lines of defense: An update*.
13. Shea, S. (2024). *What is cybersecurity?* https://www.techtarget.com/searchsecurity/definition/cybersecurity
14. Navarro, A. (2024). *Internal audit's role in cybersecurity: A strategic imperative*. https://www.linkedin.com/pulse/internal-audits-role-cybersecurity-strategic-arturo-navarro-cpa-ncrtc
15. Ennia, C. (2025). *Cybersecurity audit essentials: Roles & responsibilities, steps, and best practices*. https://auditboard.com/blog/cybersecurity-audit-essentials
16. Sweny, G. (2024). *What is a cybersecurity audit & why is it important?* https://agileblue.com/what-is-a-cybersecurity-audit
17. Emily, B. (2024). *The critical role of cybersecurity audits and how to conduct one*. https://secureframe.com/blog/cybersecurity-audit
18. CyberTalents. (2023). *Cybersecurity audit: Everything you need to know*. https://cybertalents.com/blog/cyber-security-audit
19. ACI Learning. (2024). *The impact of cybersecurity on internal auditing: What auditors need to know*. https://www.acilearning.com/blog/the-impact-of-cybersecurity-on-internal-auditing-what-auditors-need-to-know
20. Wolden, M., Valvere, R., & Talla, M. (2015). The effectiveness of COBIT 5 information security framework for reducing cyber attacks on supply chain management system. *IFAC PapersOnLine*, *85*(2), 1846–48.
21. Sweny, G. (2023). *What is a cybersecurity audit & why is it important?* https://agileblue.com/what-is-a-cybersecurity-audit
22. Hunton, J., et al. (2021). Business and audit risks associated with ERP systems: Knowledge differences between information systems audit specialists and financial auditors.
23. Thangaraja, R. (2024). *The role of internal audit in cybersecurity risk management.* https://www.bdo.com.mt/en-gb/insights/internal-audit-insights-articles/internal-audit-in-cybersecurity-risk-management
24. Jamison, J., Morris, L., & Wilkinson, C. (2019). *The future of cybersecurity in internal audit*. Internal Audit Foundation and Crowe. https://www.crowe.com/-/media/Crowe/LLP/folio-pdf/The-Future-of-Cybersecurity-in-IA-RISK-18000-002A-update.pdf
25. The Institute of Internal Auditors. (2025). *The cybersecurity topical requirements*. https://www.theiia.org
26. SPI Undip. (2022). *Internal audit on cybersecurity*. https://spi.undip.ac.id/en/internal-audit-cybersecurity
27. Smith, S. (2023). *How to become a cybersecurity auditor*. https://www.devry.edu/blog/how-to-become-a-cyber-security-auditor.html
28. ACI Learning. (2025). *5 skills every internal auditor should focus on in 2025*. https://www.acilearning.com/blog/5-skills-every-internal-auditor-should-focus-on-in-
29. Charandura, K., & Pretorius, M. (2024). *Strengthening cyber security: The crucial role of internal audit*. https://www.mondaq.com/southafrica/security/1475592/strengthening-cyber-security-the-crucial-role-of-internal-audit
30. The Institute of Internal Auditors. (2025). *What is internal auditing?* https://www.theiia.org/en/about-us/about-internal-audit/
31. Elbeheri, A. (2020). *Internal audit and cybersecurity*. https://www.linkedin.com/pulse/internal-audit-cybersecurity-ala-a-elbeheri
32. Anojan, V. (2022). Factors affecting internal audit reporting on public sector in Sri Lanka.
33. Kwaku, D. (2023). *The impact of cybersecurity on the future of internal audit*. https://www.linkedin.com/pulse/impact-cybersecurity-future-internal-audit-daniel
34. Moore, M. (2025). *How to become a security auditor: Career & salary guide*. https://onlinedegrees.sandiego.edu/cyber-security-auditor-career-guide
35. SailPoint. (2023). *What is a cybersecurity audit and why is it important?* https://www.sailpoint.com/identity-library/benefits-of-a-cybersecurity-audit