Magna Scientia Advanced Research and Reviews

eISSN: 2582-9394

Cross Ref DOI: 10.30574/msarr

Journal homepage: https://magnascientiapub.com/journals/msarr/

(REVIEW ARTICLE)

Check for updates

Risk-Based IT Auditing and Cybersecurity Assurance in Regulated U.S. Organizations: A Review of Governance, Methods, and Outcomes

William Asare Yirenkyi [1,*], Apaflo Godson Teye [2], Matilda Konotey [1] and Yeboah Mary Magdalene [3]

[1] *Temple University, Fox School of Business, Philadelphia, PA.*
[2] *University of Energy and Natural Resources.*
[3] *University of Ghana.*

Magna Scientia Advanced Research and Reviews, 2026, 17(02), 316–322

Publication history: Received on 13 June 2026; revised on 21 July 2026; accepted on 23 July 2026

Article DOI: https://doi.org/10.30574/msarr.2026.17.2.0142

Abstract

Risk-based IT auditing and cybersecurity assurance have become central mechanisms for protecting regulated organizations amid evolving digital threats. This review synthesizes peer-reviewed literature on governance structures, auditing methods, and resulting outcomes across key sectors including financial services, capital markets, healthcare, and critical infrastructure. Drawing from a broad body of literature, it examines how regulatory frameworks shape risk identification and control deployment while highlighting assurance practices that contribute to measurable improvements in threat mitigation and compliance. The analysis reveals consistent emphasis on integrated governance approaches alongside persistent implementation tensions, such as mismatches between risk-based ideals and practical application. Key insights underscore the role of adaptive controls, outcome-focused assurance, and sector-specific adaptations in enhancing overall cybersecurity posture. The review also identifies areas where current practices fall short, offering grounded directions for advancing both theory and practice in regulated environments.

Keywords: Risk-based IT auditing; Cybersecurity assurance; Regulatory governance; Control mechanisms; Audit effectiveness

1. Introduction

In regulated organizations, the convergence of information technology risks and cybersecurity threats has elevated the importance of structured auditing and assurance practices (Walton et al., 2020; Taherdoost, 2022). Organizations face increasing pressure to safeguard sensitive data, maintain operational continuity, and meet stringent compliance obligations. Risk-based IT auditing offers a systematic way to prioritize resources toward the most significant vulnerabilities, while cybersecurity assurance provides independent verification that controls function as intended. These practices have grown essential as digital transformation accelerates across sectors. Governance structures play a pivotal role in guiding these efforts (Wu et al., 2024; Slapničar et al., 2022). Regulatory expectations establish accountability mechanisms that extend from board oversight to operational controls. In this environment, IT auditing moves beyond traditional compliance checklists to incorporate proactive risk assessment and adaptive methodologies (Frank et al., 2023). Assurance activities further support organizational resilience by linking audit findings to broader performance outcomes. The interplay between governance, risk identification, control deployment, and outcome evaluation creates a multifaceted landscape that demands careful examination. The topic holds substantial importance for several reasons. Regulatory non-compliance can result in significant financial penalties and reputational damage (Christensen et al., 2024). Effective cybersecurity assurance helps protect critical infrastructure and sensitive information that underpins public trust (Onyekwuluje et al., 2025). As artificial intelligence and other emerging technologies introduce new risk dimensions, auditing practices must evolve to maintain relevance (Agbadamasi et al.,

* Corresponding author: Apaflo Godson Teye

2025; Li & Goel, 2025). Understanding current governance approaches, methodological developments, and resulting outcomes therefore contributes to both academic knowledge and practical application. The scope of this review centers on regulated U.S. organizations and contexts where findings transfer directly to similar regulatory environments. Emphasis falls on how governance frameworks influence auditing methods and how those methods produce observable outcomes in risk mitigation and assurance effectiveness (Amoako et al., 2025; Osifowokan & Adukpo, 2024). The discussion integrates perspectives from capital markets, financial services, healthcare, pharmaceutical, and critical infrastructure settings, recognizing that sector contexts shape practice without diminishing shared regulatory principles. This synthesis reveals patterns in how organizations approach risk-based auditing and cybersecurity assurance. It highlights the role of controls and assurance mechanisms in addressing threats while noting where limitations and implementation challenges remain evident. By examining these elements together, the review provides a comprehensive view of the current state of the field. Beyond individual organizations, these practices contribute to the stability of broader economic and societal systems that depend on secure digital operations.

2. Regulatory Governance Structures Shaping IT Auditing Practices

Regulatory oversight forms a foundational layer for IT auditing and cybersecurity assurance in regulated organizations. Governance structures, including frameworks aligned with SOX, NIST, and sector-specific rules such as NYDFS Part 500 and HIPAA, establish the boundaries within which risk-based auditing operates. These governance frameworks influence audit effectiveness by formalizing accountability structures, standardizing control evaluation criteria, and enabling traceability between identified risks and implemented controls. These structures also emphasize compliance mechanisms and oversight systems that guide how organizations approach cybersecurity controls. Studies illustrate how board-level and regulatory expectations drive internal audit functions to evaluate IT governance effectiveness (Wu et al., 2024; Tadesse et al., 2024). In financial contexts, governance references frequently highlight the integration of cybersecurity risk management into broader regulatory reporting requirements (McCoy, 2025; Frank et al., 2023). Regulatory governance provides the scaffolding for assurance activities. Onyekwuluje et al. (2025) and Agbadamasi et al. (2025) demonstrate how legal and ethical compliance expectations in capital markets and corporate settings influence the design of AI governance protocols. Osifowokan and Adukpo (2024) link regulatory compliance in pharmaceutical clinical trials to quality assurance processes that mirror broader IT control expectations. These examples show that governance structures are not static but actively shape audit priorities. Variations appear in how different sectors operate these structures. Banking environments often integrate FFIEC guidelines more explicitly than healthcare settings, which prioritize HIPAA security controls (Amoako et al., 2025; El Rob, 2023). Additional studies on multi-framework alignment further illustrate how organizations combine overlapping regulatory demands into cohesive governance strategies that support consistent audit execution across departments (Taherdoost, 2022; El Rob, 2023). Emerging regulations continue to add layers of complexity to this governance landscape. Recent developments, such as updates to data privacy rules, artificial intelligence oversight proposals, and evolving cybersecurity reporting mandates, are increasingly influencing how organizations design their audit and assurance programs. While the core frameworks remain foundational, these newer requirements demand greater adaptability and forward-looking compliance strategies from both auditors and regulated entities (El Rob, 2023).

Oversight can sometimes constrain adaptive responses when rules lag behind technological change (Slapničar et al., 2025; Christensen et al., 2024). Effective risk-based IT auditing begins with strong governance alignment, yet such structures require ongoing refinement to remain relevant. The evidence consistently positions governance as the enabling foundation that allows risk-based approaches to function effectively while still revealing the need for periodic updates to address emerging gaps in regulatory coverage. In practice, organizations that maintain close alignment between governance expectations and operational realities tend to achieve more stable assurance outcomes over time. Many compliance teams discover that periodic governance reviews help bridge the gap between regulatory intent and day-to-day audit execution, creating a more responsive framework for handling emerging cyber risks.

3. Comparative Analysis of Key Regulatory Frameworks

Several key regulatory frameworks form the foundation of risk-based IT auditing and cybersecurity assurance in regulated U.S. organizations. The Sarbanes-Oxley Act (SOX) primarily addresses internal controls over financial reporting and IT general controls to ensure the accuracy and reliability of financial statements. The National Institute of Standards and Technology (NIST) Cybersecurity Framework offers a flexible, risk-based approach to managing cybersecurity risk through its core functions of identify, protect, detect, respond, and recover. New York Department of Financial Services (NYDFS) Part 500 imposes mandatory cybersecurity program requirements on financial institutions, including risk assessments, multi-factor authentication, and timely incident reporting. HIPAA establishes security and privacy standards specifically for protected health information in the healthcare sector. These frameworks overlap

significantly in areas such as risk assessment, control implementation, continuous monitoring, and incident response, yet each has distinct emphases that organizations must integrate when designing unified assurance programs. For instance, SOX and NIST share a strong focus on risk-based control evaluation and governance, while the New York Department of Financial Services (NYDFS) and Health Insurance Portability and Accountability Act (HIPAA) add sector-specific obligations for data protection and reporting. Organizations that successfully harmonize these frameworks achieve more robust governance and assurance outcomes than those treating them in isolation (Taherdoost, 2022; El Rob, 2023). The comparative perspective underscores the practical need for organizations to map overlapping requirements and address unique gaps when developing comprehensive risk-based IT auditing strategies.

4. Sector-Specific Contexts Influencing Cybersecurity Assurance

Regulated U.S. sectors create distinct environments that influence how cybersecurity assurance is practiced. Capital markets, banking, healthcare, and critical infrastructure each impose unique contextual pressures on audit activities. In capital markets, assurance efforts focus on protecting investor confidence through cybersecurity audits (Onyekwuluje et al., 2025). Financial institutions emphasize adaptive defense strategies in response to high-stakes transaction environments (Tetteh-Kpakpah et al., 2025). Pharmaceutical and healthcare contexts highlight data integrity concerns in clinical trials and patient information systems (Osifowokan & Adukpo, 2024). Contextual factors shape assurance priorities. Critical infrastructure studies stress accounting-linked cybersecurity frameworks (Chowdhury & Pub, 2022), while SME-transferable frameworks adapt broader regulatory expectations to smaller-scale operations (El-Hajj & Mirza, 2024). Hepworth et al. (2022) illustrate how financial institutions tailor internal audit strategies to sector-specific privacy and cyber expectations. Sector contexts actively modulate the application of risk-based approaches. Banking studies integrate AI/ML fraud detection more prominently than capital market analyses (Amoako et al., 2025). All sectors emphasize regulatory compliance, but healthcare contexts place heavier weight on data integrity outcomes (Osifowokan & Adukpo, 2024), whereas capital market research focuses on market protection (Onyekwuluje et al., 2025). Cybersecurity assurance cannot be understood in isolation from the regulated environments in which it unfolds. Additional evidence from integrative reviews shows that sector-specific adaptations also influence the speed with which organizations adopt new assurance tools. Larger financial entities often lead in implementation while healthcare and critical infrastructure follow with more cautious, compliance-first adjustments (Walton et al., 2020; Taherdoost, 2022). These contextual differences underscore the practical need for tailored yet harmonized assurance strategies across regulated industries. In many cases, the unique pressures of each sector drive organizations to develop specialized internal processes that still remain grounded in shared regulatory principles. Sector leaders frequently note that ignoring these contextual nuances leads to assurance programs that feel misaligned with operational realities on the ground. Across sectors, cybersecurity assurance effectiveness appears to depend less on regulatory intensity and more on how well sector-specific risks are operationalized into audit procedures.

5. Risk Identification and Assessment Approaches in IT Audit Practices

Risk identification and assessment processes sit at the core of risk-based IT auditing. Organizations identify threats through cybersecurity audits, fraud risk evaluations, and digital-age methodologies (Tetteh-Kpakpah et al., 2025; Amoako et al., 2025; Ilori et al., 2022). Framework-driven assessment appears frequently, with references to outcome-focused models guiding how risks are evaluated (Muhammad, 2025). AI-related risks receive particular attention in corporate governance contexts (Agbadamasi et al., 2025; Li & Goel, 2025). Risk orientation signals vary considerably across studies, reflecting notable differences in how organizations identify, assess, and manage cybersecurity risks. Some studies emphasize threat mitigation and regulatory risk identification in financial sectors (McCoy, 2025; Huang & Murthy, 2024), while others highlight breach-related assessment within COSO frameworks (Tadesse et al., 2024). Specialized risk assessment frameworks for transferable contexts further illustrate the adaptability of these processes (El-Hajj et al., 2024). Nartey et al. (2026) extend risk identification into forensic auditing using AI and blockchain tools.

AI-specific auditing challenges represent a growing area of concern. Auditing AI systems directly involves assessing model risk, algorithmic decision-making, and the transparency of complex machine learning models. These challenges require new auditor competencies and governance frameworks to ensure accountability and reliability in algorithmic systems (Li & Goel, 2025; Agbadamasi et al., 2025).

Risk processes contain contradictions. Slapničar et al. (2025) critique the illusion of purely risk-based approaches, noting qualitative-quantitative mismatches, while implementation challenges in banking highlight gaps between assessment and execution (Amoako et al., 2025). Risk processes, though central, are not uniformly effective across contexts. Further analysis in the literature reveals that these contradictions often stem from differences in organizational maturity. More established entities achieve smoother integration of risk signals while newer or resource-

constrained ones face persistent hurdles in translating assessment findings into actionable audit plans (Vuko et al., 2025; Ballou et al., 2021). This variation emphasizes the importance of context-aware risk methodologies that account for both technical and organizational realities. Organizations that successfully navigate these differences tend to build more resilient assurance programs over the long term. The practical reality is that risk assessment maturity often determines whether an organization can move beyond reactive compliance toward truly proactive threat management.

6. Design and Deployment of Control Mechanisms

Control mechanisms represent the operational backbone of cybersecurity assurance. IT, security, and compliance controls are frequently discussed in relation to audit evaluation and risk management (Slapničar et al., 2022; Wu et al., 2024). Adaptive security controls, AI and blockchain mechanisms, and framework-specific tools appear across the literature (Tetteh-Kpakpah et al., 2025; Nartey et al., 2026). Reporting and assurance controls further link governance to practical deployment (Frank et al., 2023; Zhang et al., 2024). Deployment varies by context. In financial institutions, AI/ML fraud detection controls receive emphasis (Amoako et al., 2025), while critical infrastructure studies focus on cybersecurity accounting controls (Chowdhury & Pub, 2022). Bharathan (2025) and Vuko et al. (2025) address technology audit quality assurance as a means of strengthening control evaluation. Controls are responsive to identified risks, yet their effectiveness depends on integration with broader audit activities. Legal and ethical constraints in AI governance (Agbadamasi et al., 2025) and outsourcing issues (Vuko et al., 2025) illustrate limits to deployment. Controls are essential yet require careful alignment with regulatory and risk contexts. Evidence from multiple studies further demonstrates that successful deployment often hinges on continuous monitoring and iterative refinement. Organizations report higher control maturity when audit teams collaborate closely with compliance and IT functions rather than operating in silos (Hepworth et al., 2022; Li & Goel, 2025). This collaborative dimension adds another layer of complexity to control design that the literature consistently acknowledges as critical for long-term effectiveness. In many regulated settings, the interplay between technical deployment and organizational buy-in ultimately determines how well controls perform under real-world conditions. Control teams that prioritize cross-functional dialogue consistently report fewer implementation setbacks and stronger overall resilience against evolving threats.

7. Operational Practices in Cybersecurity Auditing and Assurance

Cybersecurity auditing practices encompass a range of activities from internal IT control evaluation to forensic and risk-based methodologies. Cybersecurity audits serve as key tools for threat mitigation and compliance (Onyekwuluje et al., 2025; Slapničar et al., 2022). Internal audit strategies for assessing controls in financial institutions highlight operational integration (Hepworth et al., 2022). Forensic auditing with AI and blockchain tools extends these practices into investigative domains (Nartey et al., 2026). Operational descriptions vary widely in literature, showing a range of practices in cybersecurity auditing and assurance. Digital-age methodologies review regulatory implications (Ilori et al., 2022), while SOC assurance practices focus on regulated entities (Perols & Murthy, 2025). Quality assurance in technology audits and clinical trials provides additional operational layers (Bharathan, 2025; Osifowokan & Adukpo, 2024). These practices respond to both governance expectations and sector contexts. Audit activities serve as the practical expression of risk and control elements. Organizations move from planning to execution in assurance work. The literature additionally notes that operational maturity in these practices improves when organizations adopt standardized audit templates that incorporate real-time data analytics. Auditors shift from periodic reviews to more continuous assurance models that better match the pace of cyber threats (Ahmad & Al-Shayed, 2025; Perols & Murthy, 2025). This evolution in operational practice reflects a broader trend toward proactive rather than reactive auditing across regulated settings. Many organizations find that these refined operational approaches lead to greater consistency in assurance outcomes even when facing rapidly changing threat landscapes. The literature suggests that the transition toward continuous auditing models has significantly reshaped interactions between audit teams and operational units.

8. Measurement of Audit Effectiveness and Assurance Outcomes

Outcomes and effectiveness measures provide evidence of value delivered by risk-based IT auditing. Studies report improvements in market protection, cyber threat reduction, fraud detection effectiveness, and data integrity (Onyekwuluje et al., 2025; Tetteh-Kpakpah et al., 2025; Amoako et al., 2025; Osifowokan & Adukpo, 2024). These improvements, however, are largely based on correlational evidence rather than causal measurement. Enhanced reporting and independent assurance yield benefits for investors and regulated entities (Frank et al., 2023; Muhammad, 2025). Audit effectiveness drivers and SOC assurance contribute to positive outcomes in governance and risk management (Vuko et al., 2025; Perols & Murthy, 2025). Variations in outcome reporting reflect sector differences. Financial contexts emphasize threat reduction and compliance (Tetteh-Kpakpah et al., 2025), while healthcare highlights data integrity (Osifowokan & Adukpo, 2024). COSO adoption links to breach reduction (Tadesse et al., 2024),

and auditor focus correlates with improved client reporting (Zhang et al., 2024). Outcome-based assurance approaches advance measurement practices (Muhammad, 2025). Literature documents tangible results while acknowledging that outcomes depend on effective integration of prior elements. Further examination shows that organizations achieving higher outcome metrics often combine strong governance with robust control deployment. These combinations create measurable gains in both compliance rates and incident response times that extend beyond initial audit findings (Christensen et al., 2024; Ballou et al., 2021). Integrated successes reinforce the interconnected nature of the assurance ecosystem described throughout the reviewed evidence. In practice, the most compelling outcome stories emerge when organizations maintain clear visibility into how governance, risk, and control elements interact over time. Outcome tracking teams frequently observe that sustained visibility leads to faster course corrections and more reliable long-term performance metrics.

9. Persistent Limitations and Implementation Challenges

Limitations and constraints temper the optimism found in outcome reports. Implementation challenges in banking, legal and ethical constraints in AI governance, non-significant drivers such as regulation and outsourcing, and critiques of risk-based illusions appear across studies (Amoako et al., 2025; Agbadamasi et al., 2025; Vuko et al., 2025; Slapničar et al., 2025). These limitations coexist with otherwise positive findings, highlighting inherent tensions between theoretical risk-based models and practical implementation realities. Literature presents these tensions as inherent to current practice. Risk-based approaches sometimes create illusions when qualitative realities clash with quantitative expectations (Slapničar et al., 2025). Ethical constraints in AI systems and regulatory lags further complicate deployment (Agbadamasi et al., 2025). Governance, methods, and outcomes show progress, yet acknowledged limitations remain a consistent feature of the evidence base. Additional insights from the literature indicate that these challenges are particularly pronounced in organizations undergoing rapid digital transformation. Legacy systems and skill gaps compound the difficulties of aligning controls with evolving regulatory demands (Walton et al., 2020; Ilori et al., 2022). Addressing such persistent limitations requires sustained attention to both technical and human factors within the assurance process. Organizations that confront these realities directly often develop more robust strategies for long-term resilience. Implementation teams that openly acknowledge these constraints tend to build more realistic roadmaps and achieve steadier progress despite ongoing hurdles.

10. Future Research Directions

Among these directions, developing hybrid risk assessment models that integrate quantitative and qualitative approaches appears to be the most critical priority. The literature reveals several evidence-grounded opportunities for advancing risk-based IT auditing and cybersecurity assurance. Tensions between reported outcomes and observed implementation challenges point to the need for more longitudinal studies examining how controls evolve over time in response to regulatory updates. Sector-specific variations suggest comparative research across additional regulated industries to identify transferable best practices beyond current financial and healthcare emphases. The presence of risk-assessment critiques, such as illusions in purely risk-based models, indicates value in developing hybrid quantitative-qualitative assessment tools that better align with real-world applications. Limitations around AI governance and ethical constraints highlight the importance of research into auditor readiness for emerging technologies, including auditability frameworks that address both technical and regulatory dimensions. Outcome measurement studies could be extended to include cost-benefit analyses of assurance practices in smaller regulated entities, where resource constraints amplify existing implementation gaps. Future work might also explore how independent assurance mechanisms influence stakeholder perceptions in ways not fully captured by current reporting-focused evidence. These directions remain anchored in the identified gaps. Researchers need to bridge governance structures with operational realities, to refine risk and control processes amid technological change, and to better understand the conditions under which positive outcomes materialize despite persistent limitations. Such research would strengthen the foundation for more resilient cybersecurity assurance in regulated organizations.

11. Conclusion

Risk-based IT auditing and cybersecurity assurance in regulated organizations reflect a dynamic interplay of governance structures, contextual influences, risk and control processes, operational practices, outcome measurement, and acknowledged limitations. The evidence shows that regulatory frameworks provide essential direction while sector environments shape practical application. Auditing activities and assurance approaches deliver measurable improvements in threat mitigation, compliance, and stakeholder confidence, yet implementation challenges and tensions around risk-based ideals persist. These insights collectively portray a field in active development, where governance and methods continue to evolve in response to both regulatory demands and technological realities. The

review contributes a synthesized understanding that highlights both achievements and areas requiring attention, reinforcing the ongoing importance of integrated approaches to cybersecurity in regulated settings. Future advancements will likely depend on the integration of adaptive, data-driven auditing models capable of aligning real-time risk signals with evolving regulatory expectations.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Agbadamasi, T., Opoku, L. K., Adukpo, T. K., & Mensah, N. (2025). Artificial Intelligence Governance in U.S. Corporations: Legal and Ethical Implications for Business Intelligence and Regulatory Compliance. *International Journal of Research Publication and Reviews.*

[2] Ahmad, H. M. & Al-Shayed, A-S. (2025). The impact of cybersecurity assurance on the quality of internal audit at the Financial Technology Companies in Jordan: The Moderating Role of COBIT 2019. *International Journal of Applied Economics, Finance, and Accounting.*

[3] Amoako, D., Boboye, C. O., Boateng, V., & Laryea, J. E. N. (2025). Artificial Intelligence and Machine Learning for Fraud Detection in the U.S. Banking Industry: Regulatory Frameworks, Implementation, and Challenges. *EPRA International Journal of Economics, Business, and Management Studies.*

[4] Ballou, B., Grenier, J. H., & Reffett, A. (2021). Stakeholder Perceptions of Data and Analytics-Based Auditing Techniques (cyber risk context). *Accounting Horizons.*

[5] Bharathan, R. (2025). Mastering Technology Audit Quality Assurance: A Framework for Auditors. *Technical Disclosure Commons.*

[6] Chowdhury, R. H. & Pub, A. (2022). Cybersecurity Accounting Frameworks for Critical Infrastructure: Integrating Advanced Accounting Systems and Cybersecurity Protocols to Safeguard National Financial Data. *International Journal of Management and Organizational Research.*

[7] Christensen, B. E., Newton, N. J., & Wilkins, M. S. (2024). Costs and Benefits of a Risk-Based PCAOB Inspection Regime. *Accounting, Organizations and Society*.

[8] El-Hajj, M., & Mirza, Z. A. (2024). Protecting Small and Medium Enterprises: A Specialized Cybersecurity Risk Assessment Framework and Tool. *Electronics, 13(19), 3910.*

[9] El Rob, M. F. A. (2023). A Narrative Review of Advantageous Cybersecurity Frameworks and Regulations in the United States Healthcare System. *Issues in Information Systems*.

[10] Frank, M. L., Grenier, J. H., Pyzoha, J. S., & Zielinski, N. B. (2023). Implications of Enhanced Cybersecurity Risk Management Reporting and Independent Assurance. *Current Issues in Auditing.*

[11] Hepworth, L. R., Greenman, C., Esplin, D., & Johnston, R. (2022). Cybersecurity and Data Privacy: Rising Expectations Within Internal Audit. *Journal of Forensic and Investigative Accounting.*

[12] Huang, J. A. & Murthy, U. S. (2024). The Impact of Cybersecurity Risk Management Strategy Disclosure on Investors' Judgement and Decision. *International Journal of Accounting Information Systems* 54(2):100696.

[13] Ilori, O., Friday, S. C., Isibor, N. J., & Chukwuma-Eke, E. C. (2022). Cybersecurity Auditing in the Digital Age: A Review of Methodologies and Regulatory Implications. *Journal of Frontiers in Multidisciplinary Research.*

[14] Li, Y., & Goel, S. (2025). Artificial Intelligence Auditability and Auditor Readiness for Auditing Artificial Intelligence Systems. *International Journal of Accounting Information Systems. Elsevier, vol. (56) (C)*

[15] McCoy, E. (2025). Cybersecurity Regulations and Risk Management in the Financial Sector: A Comparative Analysis. *Law, Economics, and Society*. *1. 10.30560/les.v1n1p115.*

[16] Muhammad, Y. M. (2025). Advancing Cybersecurity Assurance: A novel outcome-based Approach for Evaluating Cybersecurity Controls.

[17] Nartey, O. L., Agyei, E., Anim, B., & Yeboah, M. M. (2026). AI and Blockchain in Forensic Auditing: A Review of Tools for Investigating Financial Crimes in the U.S. *International Journal for Multidisciplinary Research.*

[18] Onyekwuluje, T. P., Akoto-Bamfo, D., Tetteh-Kpakpa, C., & Panful, B. (2025). Evaluating the Role of Cybersecurity Audits in Protecting the U.S. Capital Market. *World Journal of Advanced Research and Reviews 25(2):974-980*

[19] Osifowokan, A. S., & Adukpo, T. K. (2024). The importance of quality assurance in clinical trials: Ensuring data integrity and regulatory compliance in the U.S. pharmaceutical industry. *World Journal of Advanced Research and Reviews.*

[20] Perols, J. & Murthy, U. S. (2025). System and Organizational Controls (SOC) for Cybersecurity as a Non-Audit Service. *Current Issues in Auditing.*

[21] Slapničar, S., Vuko, T., Čular, M., & Drašček, M. (2022). Effectiveness of Cybersecurity Audit. *International Journal of Accounting Information Systems.*

[22] Slapničar, S., Axelsen, M., & Eulerich, M. (2025). Cyber Risk Management: The Illusion of the Risk-Based Approach. *Journal of Management Control.*

[23] Tadesse, A., Walton, S., & Zhang, Y. (2024). COSO Framework Adoption and Cybersecurity Breaches. *Journal of Information Systems.*

[24] Taherdoost, H. (2022). Understanding Cybersecurity Frameworks and Information Security Standards: A Review and Comprehensive Overview. *Electronics*

[25] Tetteh-Kpakpah, C., Adjaottor, S., & Donkor, A. A. (2025). Mitigating Cyber Threats Through Cybersecurity Audits and Adaptive Defense: A Case Study on Financial Institutions. *International Journal of Economic and Business Review (JEBR).*

[26] Vuko, T., Slapničar, S., Čular, M., & Drašček, M. (2025). Key Drivers of Cybersecurity Audit Effectiveness: A Neo-Institutional Perspective. *International Journal of Auditing.*

[27] Walton, S., Wheeler, P., Zhang, Y., & Zhao, (R.) X. (2020). An Integrative Review and Analysis of Cybersecurity Research: Current State and Future Directions. *Journal of Information Systems.*

[28] Wu, T-H, Huang, S. Y., Chiu, A-A, & Yen, D. C. (2024). IT Governance and IT Controls: Analysis from an Internal Auditing Perspective. *International Journal of Accounting Information Systems.*

[29] Zhang, Y., Walton, S., Liu, M., Tang, J., & Zhao, X. (2024). Auditor Cybersecurity Focus and Client Cybersecurity Reporting.