Available on: https://jmrr.ep-journals.org/ E-ISSN: 3051-3588, P-ISSN: 3051-357X

Journal of Management Research and Review

Volume: 02 Issue: 07 July-2026

# A Critical Integrative Review of Technology Assurance for Operational Resilience in U.S. Regulated Organizations

**Matilda Konotey**
Temple University, Fox School of Business, Philadelphia, PA, USA

**Daniel Akoto-Bamfo**
Temple University, Fox School of Business, Philadelphia, PA, USA

**Godson Teye Apaflo**
Independent Researcher, Texas, USA

**Published Date: July 20, 2026** **Article DOI: 10.65150/EP-jmrr/V2E7/2026-06**

**ABSTRACT:** Technology assurance practices have become central to efforts aimed at strengthening operational resilience across U.S. regulated sectors, including finance, healthcare, and critical infrastructure. This integrative review examines how audits, compliance mechanisms, governance frameworks, and emerging-technology controls are discussed in the recent peer-reviewed literature. Drawing on a synthesis of recent peer-reviewed studies, the analysis reveals recurring attention to traditional compliance-oriented approaches alongside growing interest in adaptive practices and data-protection balances. Studies consistently identify resource constraints, static checklists, and dynamic threats as barriers that limit the translation of assurance activities into sustained resilience. In financial and healthcare contexts, audits and regulatory implementation show promise for risk mitigation but frequently lack integration with broader operational strategies. Similar patterns appear in utility-sector discussions of cyber-physical threats and in examinations of AI governance, where qualitative reviews emphasize ethical and compliance balances without extensive empirical outcome data. Disclosure quality and framework application are linked to market or organizational responses, yet long-term quantitative evaluation remains underdeveloped. Overall, the literature suggests alignment around the identification of barriers and the need for adaptive cultures, while remaining fragmented on consistent linkages to resilience outcomes and silent on cross-sector empirical validation. These insights point to practical implications for regulated organizations seeking to move beyond compliance checklists toward more responsive assurance systems. The review contributes a grounded perspective on current evidence and highlights targeted areas for future inquiry.

**KEYWORDS:** Operational Resilience, Technology Assurance, Cybersecurity Governance, Regulatory Compliance, AI Governance

## INTRODUCTION

In U.S. regulated organizations, technology assurance encompasses the processes, controls, and oversight mechanisms designed to safeguard information systems, ensure regulatory adherence, and support continued operations amid disruption. Operational resilience, by contrast, refers to an organization's capacity to anticipate, withstand, and recover from adverse events while maintaining critical functions. Both concepts have gained prominence as digital dependencies deepen across sectors such as financial services, healthcare delivery, and utility infrastructure. Regulators increasingly expect entities to demonstrate not only technical compliance but also the ability to adapt to evolving threats ranging from sophisticated cyberattacks to systemic disruptions (Taiwo et al. 2025; Tetteh-Kpakpah et al., 2025). Several lines of inquiry have emerged in response. In financial markets attention has focused on the role of cybersecurity audits in protecting capital-market integrity and supporting stakeholder confidence (Wu et al., 2024). Healthcare organizations grapple with longstanding data-compliance obligations under frameworks such as HIPAA, now complicated by cloud adoption, interconnected devices, and artificial-intelligence applications (Osifowokan et al., 2025; Barbaria et al., 2025). Utility providers confront cyber-physical risks to supervisory control and data acquisition systems where breaches can have immediate safety implications (Panful et al., 2025). Across these domains governance frameworks and risk-disclosure practices are examined for their influence on market reactions and internal readiness (Harel & Carmeli, 2025). Despite this activity questions persist about whether prevailing assurance practices effectively translate into measurable resilience. Traditional approaches often rely on periodic audits and checklist-based controls which may not keep pace with rapid technological change or sophisticated adversaries (Mojtahedi & Zhou, 2024). Resource limitations, particularly in smaller or public-sector entities, further complicate implementation (Bhat, 2023). At the same time emerging technologies introduce new layers of complexity: data-protection rules must accommodate AI development while organizational culture appears to mediate the shift from mere compliance to adaptive risk management (Papagiannidis et al., 2025; Hassan et al., 2025). This integrative review synthesizes recent peer-

License: This is an open access article under the CC BY 4.0 license: https://creativecommons.org/licenses/by/4.0/

reviewed scholarship to illuminate how technology assurance is conceptualized and applied in support of operational resilience. Rather than offering a comprehensive inventory of every study the analysis centers on recurring patterns evident across financial, healthcare, and utility contexts. It highlights areas of agreement such as the persistence of implementation barriers as well as variations in emphasis and noted limitations in the evidence base. The purpose is to provide a clear evidence-grounded account of what the literature currently shows, where it converges, and where important gaps remain. By focusing on these patterns, the review provides regulated organizations and assurance professionals with a consolidated, evidence-grounded perspective on current patterns and persistent gaps (Taherdoost, 2022; Wang et al., 2024)

**Cybersecurity Audits in Financial Institutions**

Cybersecurity audits continue to serve as a foundational mechanism for technology assurance inside U.S. financial institutions. Taiwo et al. (2025) show that moving beyond traditional compliance checks toward proactive, AI-supported practices has become necessary if audits are to address today's evolving threats. Most capital-market firms, they note, still face resource constraints and legal burdens that slow comprehensive adoption, while the absence of standard procedures makes it difficult to compare effectiveness across institutions. In their case study of financial institutions, Tetteh-Kpakpah et al. (2025) reach a similar conclusion: robust and dynamic practices can foster system resilience and protect stakeholder confidence, yet audits are typically performed at fixed intervals rather than continuously and often rely on checklists that do not integrate well with broader strategies, especially for smaller organizations. External work on internal controls echoes these concerns. Wu et al. (2024) argue that an internal-auditing lens is essential when examining IT governance because it helps surface material weaknesses in financial reporting under SOX requirements. Mojtahedi & Zhou (2024) document persistent deficiencies in information-technology controls despite years of regulatory pressure. Bhat (2023) adds that although technical capabilities exist, organizational realities frequently limit the benefits organizations actually realize. Harel and Carmeli (2025) broaden the view by treating board-level strategic oversight as an imperative that can embed cybersecurity more firmly into governance frameworks. Luidold & Jungbauer. (2024) observe that policy requirements in the financial sector regularly encounter implementation inconsistencies, particularly among smaller entities. What becomes evident when these accounts are placed side by side is a shared recognition that proactive elements improve risk identification, yet practical barriers remain formidable. Financial-market studies stress legal burdens and investor-confidence implications, while internal-control analyses point more directly to segregation-of-duties conflicts and ineffective risk assessment. Resource constraints surface repeatedly as a limiting factor, and interval-based monitoring rather than continuous oversight consistently reduces effectiveness. Taiwo et al. (2025) and Tetteh-Kpakpah et al. (2025) both highlight the lack of standard procedures that would allow meaningful outcome comparisons. Wu et al. (2024) and Mojtahedi and Zhou (2024) note that quantitative long-term metrics for control effectiveness are still scarce. Taken together, the studies indicate that audits hold clear value as assurance tools, but their contribution to genuine operational resilience depends on integration and resource support that many organizations have yet to secure (Wang et al. 2024). For entities operating under strict capital-market oversight, this gap matters because investor confidence ultimately rests on demonstrable audit effectiveness rather than formal compliance alone.

## 2. DATA COMPLIANCE AND HIPAA IMPLEMENTATION IN HEALTHCARE

Data compliance under HIPAA and HITECH forms a core assurance obligation for U.S. healthcare providers. Osifowokan et al. (2025) explain that while these regulations created a solid foundation for protecting personal health information, they now struggle to keep up with cloud computing, IoT integration, and contemporary cybersecurity threats. Their qualitative review of case studies, industry reports, and literature concludes that meaningful progress will require revised regulatory frameworks, greater interdisciplinary collaboration, and a workforce better equipped for healthcare-specific cybersecurity. Barbaria et al. (2025) examine how HIPAA intersects with GDPR in healthcare settings and underscore the persistent difficulties surrounding data management and sharing for research purposes. Subramanian et al. (2024) find through mixed-methods analysis that federal and state rules have not meaningfully lowered either the frequency or the impact of data breaches. Supporting studies fill in the picture. Anderson et al. (2023) describe how privacy regulations are translated into practice through guardrails in health information exchange and note that compliance structures alone do not guarantee resilient outcomes. Conduah et al. (2025) highlight U.S. HIPAA and NIST alignments while pointing out that smaller providers face amplified resource limitations. Olorunlana (2024) focuses on cloud security and documents how legacy systems, high installation costs, and human error continue to undermine protection despite regulatory requirements. When these findings are compared, a clear tension appears. Foundational protection exists, yet modern threats outpace the rules. Resource constraints and the lack of continuous monitoring emerge as recurring obstacles across Osifowokan et al. (2025), Anderson et al. (2023), and Conduah et al. (2025). Hospital-centered analyses, such as Subramanian et al. (2024), emphasize the persistence of breaches, whereas cloud-focused work, such as Olorunlana (2024), draws attention to interoperability problems. Osifowokan et al. (2025) acknowledge that HIPAA and HITECH fall short in IoT and cloud environments. Subramanian et al. (2024) report that regulations have failed to reduce breach impacts. Anderson et al. (2023) and Conduah et al. (2025) observe that empirical linkages between compliance and patient-safety outcomes remain underdeveloped. In short, compliance mechanisms are widely applied, but their conversion into adaptive, threat-responsive operations remains uneven (Barbaria et al., 2025; Olorunlana, 2024). Smaller providers feel this mismatch most acutely when legacy systems must somehow satisfy current regulatory expectations, and the pattern that runs through the literature is therefore one of foundational rules that require continuous adaptation if they are to support genuine resilience in environments where patient data protection is non-negotiable.

## 3. INTERNAL CONTROLS AND IT GOVERNANCE PRACTICES

Internal controls and IT governance constitute another essential pillar of technology assurance. Wu et al. (2024) examine IT controls through an internal-auditing lens and conclude that effective general controls are indispensable for financial-reporting integrity under the Sarbanes-Oxley Act (SOX). Mojtahedi and Zhou (2024) track material weaknesses in information technology controls and show that deficiencies persist even after prolonged regulatory attention. Bhat (2023) evaluates control effectiveness more broadly and finds that technical capabilities are present, yet organizational realities often prevent organizations from realizing the full benefit. Internal auditing emerges as a common thread in these accounts.

License: This is an open access article under the CC BY 4.0 license: https://creativecommons.org/licenses/by/4.0/

Wu et al. (2024) and Mojtahedi and Zhou (2024) both stress its role in surfacing weaknesses. Differences in emphasis are nonetheless noticeable: governance-structure discussions dominate one set of findings, while segregation-of-duties conflicts receive more attention in another. Quantitative long-term metrics for control effectiveness remain scarce across the board (Mojtahedi & Zhou, 2024). The studies collectively suggest that internal controls can strengthen assurance, but stronger integration with day-to-day operational strategies is needed before resilience improves in any sustained way (Wu et al., 2024; Mojtahedi & Zhou, 2024; Bhat, 2023). Material weaknesses continue to appear in financial reporting even when controls are formally documented, a reminder that documentation alone is rarely sufficient and that organizations appear to gain most when they treat controls not as isolated technical requirements but as elements embedded within wider governance practices where resource and organizational factors repeatedly moderate performance.

## 4. RISK DISCLOSURE AND GOVERNANCE FRAMEWORKS

Risk disclosure practices attract attention because they can shape how markets and organizations respond to threats. Analyses show that higher disclosure quality tends to reduce adverse market reactions by lowering uncertainty (Harel & Carmeli, 2025; Luidold & Jungbauer, 2024). Governance-framework reviews treat structured oversight as a practical aid to compliance while survey-based examinations confirm their relevance to U.S. regulated settings and note sector-specific adaptations (Taherdoost 2022; Wang et al., 2024). Smaller companies nonetheless encounter resource-related inconsistencies that undermine consistent application (Luidold & Jungbauer, 2024). Long-term effectiveness metrics are rarely presented, which leaves the actual contribution of frameworks to sustained resilience difficult to quantify (Harel & Carmeli, 2025; Wang et al. 2024). Disclosure quality can influence responses, yet the linkage is not always backed by extensive quantitative data (Harel & Carmeli, 2025). Board-level strategic cybersecurity oversight is described as an imperative that regulated entities cannot ignore (Harel & Carmeli, 2025). Policy requirements in various sectors routinely encounter implementation challenges that limit their reach (Luidold & Jungbauer, 2024). The literature agrees on the value of structured governance but shows variation in how that value is realized; empirical support for actual resilience outcomes remains fragmented (Taherdoost, 2022; Wang et al., 2024). Frameworks can guide assurance activities, yet the step from guidance to measurable resilience gains still needs closer examination. This observation fits the wider literature's pattern of useful structures tempered by implementation realities in regulated public-company environments.

## 5. AI GOVERNANCE AND DATA PROTECTION IN HEALTH AND CORPORATE CONTEXTS

Discussions of AI governance center on the need to balance technological advancement with compliance and ethical safeguards. Qualitative reviews repeatedly stress privacy-by-design principles and the cultivation of accountable organizational cultures (Papagiannidis et al., 2025; Hassan et al., 2025). Maturity models and tailored frameworks are proposed for healthcare AI applications (Freeman et al., 2025; Bodnari & Travis., 2025). Ethical considerations and transparency appear as recurring concerns (Batool et al. 2025). Patient-safety data that would allow firmer conclusions about real-world impact remain limited (Papagiannidis et al., 2025). Governance discussions are clearly maturing, but the practical connections between these frameworks and operational resilience are still underdeveloped (Hassan et al., 2025), though the evidence base remains largely review-driven. The works underscore the importance of ethical and compliance balances in AI deployment while acknowledging that qualitative approaches currently dominate over outcome-focused measurement.

## 6. CYBER-PHYSICAL THREATS AND SCADA VULNERABILITIES IN UTILITIES

Cyber-physical threats strike directly at operational technology in the utility sector. Case-study reviews of recent SCADA attacks conclude that prioritized controls such as network segmentation and credential hygiene can measurably lower risk probability (Panful et al. 2025). Efforts to advance digitalization are associated with resilience improvements in critical infrastructure (Chen et al. 2025; Tabansky & Lichterman, 2025). Public reporting of incidents remains uneven and attribution is often opaque, which restricts collective learning (Panful et al., 2025). Technical solutions exist, yet the practical obstacles to scaling them across utilities persist (Chen et al., 2025). The reviewed cases therefore illustrate both the vulnerabilities utilities face and the controls that appear capable of mitigating them, while simultaneously calling for better mechanisms to share lessons learned (Panful et al., 2025; Chen et al., 2025).

## 7. ORGANIZATIONAL CULTURE AND OPERATIONAL READINESS IN CRITICAL INFRASTRUCTURE

Organizational culture makes a noticeable difference in how well utilities translate compliance into readiness. Public utilities tend to emphasize required controls and reporting, whereas private utilities more often adopt adaptive, learning-oriented approaches (Panful et al., 2026). Leadership accountability and culture metrics appear to influence how effectively controls become embedded in daily operations (Iyer & Babu, 2025; Pilosof et al., 2025). Technical controls remain necessary, yet organizational factors consistently mediate their impact (Iyer & Babu, 2025). Standardized ways to measure cultural contributions are still scarce (Pilosof et al. 2025). Culture therefore functions as a mediating element in the compliance-to-readiness pathway, although the literature has yet to offer widely accepted tools for assessing its contribution (Panful et al., 2026; Iyer & Babu, 2025)

### Future Research Directions

Several avenues for future research emerge directly from the patterns and limitations repeatedly noted across the reviewed literature. Longitudinal studies that follow assurance practices and their outcomes over extended periods would help clarify whether the prioritized controls and adaptive mechanisms identified in financial, healthcare, and utility settings actually produce lasting resilience gains rather than short-term compliance improvements. Such work could address the current scarcity of long-term quantitative metrics that several studies highlighted as a persistent gap and would allow researchers to track how audit methodologies, data-compliance efforts, and governance frameworks perform under sustained operational stress. Greater use of quantitative metrics, particularly in the domains of AI governance and utility readiness, could strengthen claims about effectiveness beyond the qualitative descriptions that currently dominate the evidence base. Researchers might develop standardized

License: This is an open access article under the CC BY 4.0 license: https://creativecommons.org/licenses/by/4.0/

indicators for culture-to-readiness translation or for measuring the real-world impact of privacy-by-design principles in AI deployment, thereby filling the empirical voids noted in multiple healthcare and corporate AI-focused examinations and providing clearer benchmarks for regulated organizations. Cross-sector comparisons, especially those that move beyond the current healthcare dominance in the literature, would illuminate whether lessons learned in one regulated domain transfer reliably to others. For example, comparing how disclosure quality influences market responses in finance with how SCADA controls affect operational continuity in utilities could reveal transferable assurance strategies or sector-specific barriers that remain underexplored, helping to reduce the fragmentation that currently limits broader applicability of findings. Finally, research that specifically examines the integration of continuous monitoring technologies with existing compliance structures could directly tackle the recurring gap between interval-based audits and real-time threat response that appears across financial audits, HIPAA implementation studies, and utility case reviews. This line of inquiry might test hybrid models that combine traditional regulatory frameworks with adaptive, data-driven oversight, offering regulated organizations clearer pathways from checklist compliance to genuine operational resilience while addressing the resource and integration challenges documented throughout the literature.

These directions remain firmly grounded in the evidence and limitations documented in the current body of work. Pursuing them would move the field from identifying barriers and proposing frameworks toward demonstrating sustained, measurable improvements in resilience across U.S. regulated sectors. Such efforts would not only address the fragmentation currently evident in the literature but also provide practitioners with more actionable guidance for translating assurance mechanisms into robust operational capabilities that can withstand evolving threats.

## CONCLUSION

The literature on technology assurance for operational resilience in U.S. regulated organizations reveals repeated emphasis on audits, compliance mechanisms, governance frameworks, and adaptive practices across financial, healthcare, and utility sectors. Studies converge in identifying resource constraints, static approaches, and dynamic threats as persistent barriers that hinder full translation of assurance activities into resilient outcomes. At the same time variations surface in how organizations, public versus private or traditional versus technology-forward, attempt to bridge these gaps. AI-related discussions add another layer, stressing the importance of ethical and data-protection balances, yet they largely remain qualitative in nature. Disclosure quality and framework application appear linked to responses but quantitative, long-term evidence is limited. Collectively the scholarship suggests that assurance practices provide essential structure while falling short of consistently delivering adaptive resilience. The evidence base is strongest when documenting challenges and proposing targeted controls; it is more fragmented when demonstrating sustained operational impact. These patterns underscore the need for regulated entities to look beyond checklist compliance toward integrated, culturally supported systems. The review therefore offers a measured account of current knowledge and its boundaries, highlighting both practical insights and the areas where further evidence is required.

## REFERENCES


1) Anderson, C., Baskerville, R., & Kaul, M. (2023). Managing compliance with privacy regulations through translation guardrails: A health information exchange case study. Information and Organization, 33(1), Article 100455. https://doi.org/10.1016/j.infoandorg.2023.100455
2) Barbaria, S., Jemai, A., Ceylan, H. İ., Muntean, R. I., Dergaa, I., & Boussi Rahmouni, H. (2025). Advancing compliance with HIPAA and GDPR in healthcare: A blockchain-based strategy for secure data exchange in clinical research involving private health information. Healthcare, 13(20), 2594. https://doi.org/10.3390/healthcare13202594
3) Batool, A., Zowghi, D., & Bano, M. (2025). AI governance: A systematic literature review. AI and Ethics, 5, 3265–3279. https://doi.org/10.1007/s43681-024-00653-w
4) Bhat, S. (2023). The effectiveness of internal controls in preventing fraud and financial misconduct. Journal of Law and Sustainable Development, 11(5), e1178. https://doi.org/10.55908/sdgs.v11i5.1178
5) Bodnari, A., & Travis, J. (2025). Scaling enterprise AI in healthcare: The role of governance in risk mitigation frameworks. npj Digital Medicine, 8(1), Article 272. https://doi.org/10.1038/s41746-025-01700-4
6) Chen, Y., Li, B., & Huo, B. (2025). Building operational resilience through digitalization: The roles of supply chain network position. Technological Forecasting and Social Change, 211, Article 123918. https://doi.org/10.1016/j.techfore.2024.123918
7) Conduah, A. K., Ofoe, S. H., & Siaw-Marfo, D. (2025). Data privacy in healthcare: Global challenges and solutions. Digital Health, 11, Article 20552076251343959. https://doi.org/10.1177/20552076251343959
8) Freeman, S., Wang, A., Saraf, S., Potts, E., McKimm, A., Coiera, E., & Magrabi, F. (2025). Developing an AI governance framework for safe and responsible AI in health care organizations: Protocol for a multimethod study. JMIR Research Protocols, 14(1), Article e75702. https://doi.org/10.2196/75702
9) Harel, Y., & Carmeli, A. (2025). A strategic cybersecurity oversight framework: A board's imperative. Journal of Cybersecurity, 11(1), tyaf021. https://doi.org/10.1093/cybsec/tyaf021
10) Hassan, M., Borycki, E. M., & Kushniruk, A. W. (2025). Artificial intelligence governance framework for healthcare. Healthcare Management Forum, 38(2), 125–130. https://doi.org/10.1177/08404704241291226
11) Iyer, V. R., & Babu, K. (2025). Resilience at the core: Enhancing cyber-resilience and cybersecurity practices in healthcare sector. Journal of Contingencies and Crisis Management, 33(3), e70061. https://doi.org/10.1111/1468-5973.70061
12) Luidold, C., & Jungbauer, C. (2024). Cybersecurity policy framework requirements for the establishment of highly interoperable and interconnected health data spaces. Frontiers in Medicine, 11, 1379852. https://doi.org/10.3389/fmed.2024.1379852
13) Mojtahedi, A., & Zhou, L. (2024). Information technology internal control material weaknesses in financial reporting: Categories, trends, associations, and industry effects. International Journal of Accounting Information Systems, 53, Article 100679. https://doi.org/10.1016/j.accinf.2024.100679


License: This is an open access article under the CC BY 4.0 license: https://creativecommons.org/licenses/by/4.0/

14) Olorunlana, T. J. (2024, June). Securing healthcare data in the cloud under HIPAA and NIST frameworks. International Journal of Science, Architecture, Technology and Environment, 1(3), 61–80. https://doi.org/10.63680/ijsate032528.07
15) Osifowokan, A. S., Ahmed, Z., Adukpo, T. K., & Mensah, N. (2025). Enhancing data compliance in the United States healthcare system: Addressing challenges in HIPAA and HITECH Act implementation. EPRA International Journal of Multidisciplinary Research, 11(4). https://doi.org/10.36713/epra21263
16) Panful, B., Apaflo, B., & Hutchful, N. (2025). Cyber-physical systems under threat: A case-study review of recent SCADA attacks in the U.S. utility sector. Sarcouncil Journal of Engineering and Computer Sciences, 4(12), 104–117. https://sarcouncil.com/download-article/SJECS-613-2025-104-117.pdf
17) Panful, B., Apaflo, B., & Hutchful, N. (2026). From compliance to culture: Assessing organizational cybersecurity readiness in public vs. private U.S. utility companies. EPRA International Journal of Research and Development, 11(1), Article 18669. https://doi.org/10.36713/epra25731
18) Papagiannidis, E., Mikalef, P., & Conboy, K. (2025). Responsible artificial intelligence governance: A review and research framework. The Journal of Strategic Information Systems, 34(2), Article 101885. https://doi.org/10.1016/j.jsis.2024.101885
19) Pilosof, N. P., Welcman, Y., Barrett, M., Oborn, E., & Barrett, S. (2025). Building digital resilience: Leading healthcare transformation through an online community. Frontiers in Digital Health, 7, 1656804. https://doi.org/10.3389/fdgth.2025.1656804
20) Subramanian, H., Sengupta, A., & Xu, Y. (2024). Patient health record protection beyond the health insurance portability and accountability act: Mixed methods study. Journal of Medical Internet Research, 26, Article e59674. https://doi.org/10.2196/59674
21) Tabansky, L., & Lichterman, E. (2025). PROGRESS: the sectoral approach to cyber resilience. International Journal of Information Security, 24, Article 18. https://doi.org/10.1007/s10207-024-00910-3
22) Taiwo, P. O., Akoto-Bamfo, D., Tetteh-Kpakpah, C., Panful, B., & Oware, D. (2025). Evaluating the role of cybersecurity audits in protecting the US capital market. World Journal of Advanced Research and Reviews, 25(2), 974–980. https://doi.org/10.30574/wjarr.2025.25.2.0183
23) Taherdoost, H. (2022). Understanding cybersecurity frameworks and information security standards—A review and comprehensive overview. Electronics, 11(14), Article 2181. https://doi.org/10.3390/electronics11142181
24) Tetteh-Kpakpah, C., Adjaottor, S., & Donkor, A. A. (2025). Mitigating cyber threats through cybersecurity audits and adaptive defense: A case study on financial institutions. EPRA International Journal of Economic and Business Review, 13(7). https://doi.org/10.36713/epra23002
25) Wang, W., Sadjadi, S. M., & Rishe, N. (2024, May). A survey of major cybersecurity compliance frameworks. In 2024 IEEE 10th Conference on Big Data Security on Cloud (BigDataSecurity) (pp. 23–34). IEEE. https://doi.org/10.1109/BigDataSecurity62737.2024.00013
26) 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, 52(Suppl. C), Article 100663. https://doi.org/10.1016/j.accinf.2023.100663

License: This is an open access article under the CC BY 4.0 license: https://creativecommons.org/licenses/by/4.0/