Journal of Frontiers in Multidisciplinary Research

Cybersecurity Auditing in the Digital Age: A Review of Methodologies and Regulatory Implications

Oluwatosin Ilori [1*], Comfort Iyabode Lawal [2], Solomon Christopher Friday [3], Ngozi Joan Isibor [4], Ezinne C Chukwuma- Eke [5]
[1] Independent Researcher, Ontario, Canada
[2] Independent Researcher, Abuja Nigeria
[3] BDO Nigeria, Nigeria
[4] Deloitte & Touche LLP, Lagos, Nigeria
[5] Total Energies Nigeria Limited

* Corresponding Author: **Oluwatosin Ilori**

Article Info

E-ISSN: 3050-9726
P-ISSN: 3050-9718
Volume: 03
Issue: 01
January-June 2022
Received: 03-12-2021
Accepted: 02-01-2022
Published: 26-01-2022
Page No: 174-187

Abstract
In an increasingly digitized and interconnected global environment, cybersecurity auditing has become a critical pillar in safeguarding organizational assets and ensuring regulatory compliance. This review critically analyzes emerging methodologies for cybersecurity auditing, focusing on their alignment with key regulatory frameworks such as the Sarbanes-Oxley Act (SOX), the National Institute of Standards and Technology (NIST) Cybersecurity Framework, and the General Data Protection Regulation (GDPR). The study identifies a significant shift from traditional, reactive auditing approaches toward proactive, real-time, and risk-based methodologies supported by artificial intelligence, machine learning, and automation. These innovations enhance audit efficiency, enable continuous control monitoring, and support the identification of advanced persistent threats (APTs). The review evaluates leading cybersecurity audit frameworks, including Control Objectives for Information and Related Technologies (COBIT), ISO/IEC 27001, and NIST SP 800-53, and explores how they are being adapted to assess cloud environments, third-party risks, and remote work infrastructures. It further examines how emerging frameworks incorporate regulatory expectations, emphasizing transparency, accountability, and data minimization in line with GDPR, financial reporting integrity under SOX, and the five core functions of the NIST Framework—Identify, Protect, Detect, Respond, and Recover. The analysis reveals that while current methodologies offer improved standardization and scalability, they also present challenges, including audit fatigue, fragmented toolsets, and insufficient integration across enterprise risk management systems. Moreover, the paper underscores the growing need for auditor upskilling, the ethical handling of personal data, and continuous assurance mechanisms that go beyond periodic assessments. It proposes a holistic model that integrates technical assessments with governance, risk, and compliance (GRC) strategies to enhance cybersecurity audit effectiveness. Ultimately, this review highlights the urgency for organizations to adopt agile and adaptive auditing approaches that align with evolving digital threats and compliance mandates. It offers critical insights for regulators, auditors, and organizational leaders striving to build cyber-resilient ecosystems in an era marked by data proliferation, increasing regulatory scrutiny, and sophisticated cyberattacks.

DOI: https://doi.org/10.54660/.IJFMR.2022.3.1.174-187

Keywords: Cybersecurity Auditing, NIST Framework, SOX Compliance, GDPR, Audit Methodologies, Risk Management, Data Governance, Continuous Monitoring, ISO/IEC 27001, Regulatory Technology

1. Introduction

The rapid digitization of business operations, coupled with the burgeoning array of data-driven technologies and the widespread adoption of cloud computing and remote infrastructures, has substantially broadened the cybersecurity threat landscape. As organizations increasingly rely on digital platforms to store sensitive information and manage critical functions, they become

more exposed to sophisticated cyberattacks, data breaches, and regulatory non-compliance (Bristol-Alagbariya, Ayanponle & Ogedengbe, 2022). This evolving digital age, where cyber risks pose direct implications for financial stability, reputational integrity, and national security, underscores the urgent need for robust cybersecurity auditing practices (Santoso *et al*., 2021).

Cybersecurity auditing acts as a pivotal mechanism for assessing the effectiveness of an organization's information security controls, identifying vulnerabilities, and ensuring adherence to diverse regulatory mandates. The significance of audit practices in enhancing organizational resilience against cyber threats through compliance with frameworks such as the Sarbanes-Oxley Act (SOX), the National Institute of Standards and Technology (NIST) Cybersecurity Framework, and the General Data Protection Regulation (GDPR) cannot be overstated (Appelbaum, Kogan & Vasarhelyi, 2017). Evolving frameworks necessitate that cybersecurity audits adapt to reflect current risks and emerging technologies (Santoso *et al*., 2021; Rahman *et al*., 2021). For instance, as regulators impose stricter requirements, organizations are compelled to transition from conventional, checklist-driven audits to more dynamic, real-time, risk-based methodologies, ultimately reshaping the landscape of cybersecurity governance (Balios, *et al*., 2020, Rahman *et al*., 2021).

Recent innovations, including AI-driven monitoring, continuous auditing, and integrated risk management tools, are significantly influencing audit practices across various industries. These methodologies bolster compliance efforts and enhance the ability of auditors to respond efficiently to new cybersecurity challenges ("National Cybersecurity Strategies", 2021). An increasing emphasis on continuous assessment rather than periodic evaluation is evident, with auditors leveraging advanced technologies to analyze vulnerabilities and compliance statuses proactively (Buchheit, *et al*., 2020: Lewallen, 2020). Furthermore, regulatory compliance frameworks are being scrutinized regarding their effectiveness and the ability of organizations to meet stringent requirements, as studies indicate that businesses demonstrating higher compliance often achieve better security outcomes (Bristol-Alagbariya, Ayanponle & Ogedengbe, 2022).

Moreover, current literature stresses the necessity for organizations to continuously innovate their auditing approaches in light of emerging threats and regulations. The integration of artificial intelligence and advanced analytics into cybersecurity auditing practices has shown potential for significantly enhancing the quality and speed of audits, thus addressing complexities posed by the digital transformation of businesses (Sabillón, 2018). Furthermore, the establishment of comprehensive frameworks—such as the CyberSecurity Audit Model (CSAM)—offers organizations structured methodologies to enhance their cybersecurity assurance efforts (Sabillón *et al*., 2017).

In summary, the increasing reliance on digital operations across sectors has necessitated a paradigm shift in cybersecurity auditing, driving organizations toward more comprehensive, agile, and technology-centric audit methodologies (Ajiga, Ayanponle & Okatta, 2022, Francis Onotole, *et al*., 2022). Aligning auditing practices with evolving regulatory frameworks and emerging technologies is essential for compliance and critical in safeguarding against the sophisticated threats present in today's interconnected digital landscape (Chang & Luo, 2019).

2. Methodology

This study adopted a systematic literature review approach, guided by the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) framework, to examine cybersecurity auditing methodologies and their regulatory implications in the digital age. The objective was to identify prevailing frameworks, emerging audit techniques, and regulatory responses shaping the cybersecurity landscape. A comprehensive search strategy was implemented to identify relevant peer-reviewed articles, conceptual models, empirical studies, and regulatory discussions published in academic journals and conferences.

A total of 118 records were initially retrieved from online academic databases, including IEEE Xplore, ScienceDirect, Scopus, SpringerLink, and Google Scholar, using search terms such as "cybersecurity audit," "digital governance," "AI in auditing," "compliance frameworks," and "information security assurance." These were complemented by additional articles drawn from references in key papers to ensure coverage of recent developments and gray literature.

After removing 27 duplicates, 91 records proceeded to the screening phase. Each title and abstract was reviewed for relevance based on inclusion criteria such as a focus on digital auditing tools, frameworks integrating AI and machine learning, regulatory guidelines like NIST, ISO/IEC 27001, GDPR, and recent cybersecurity maturity assessment models. Studies that did not address either the audit methodology or regulatory aspect were excluded.

Following the screening process, 63 full-text articles were assessed in detail for eligibility. Articles were appraised on methodological rigor, practical relevance to modern auditing systems, and integration of regulatory mandates. The quality assessment also considered if the study proposed new frameworks, assessed existing tools, or provided comparative insights into traditional and modern audit practices.

Finally, 46 studies met the eligibility criteria and were included in the qualitative synthesis. These studies encompass a diverse range of contributions including the AI-Driven Predictive Analytics Model (Achumie *et al*., 2022), machine learning models for operational efficiency (Adekunle *et al*., 2021), cybersecurity maturity models (Aliyu *et al*., 2020; Sulistyowati *et al*., 2020), and regulatory-compliant auditing systems (Diamantopoulou *et al*., 2020; Antunes *et al*., 2022). Methodologies extracted ranged from automated audit engines and AI-enhanced detection systems to visualization frameworks for audit clarity. These studies collectively informed the synthesis of themes in the results and discussion sections of this paper.

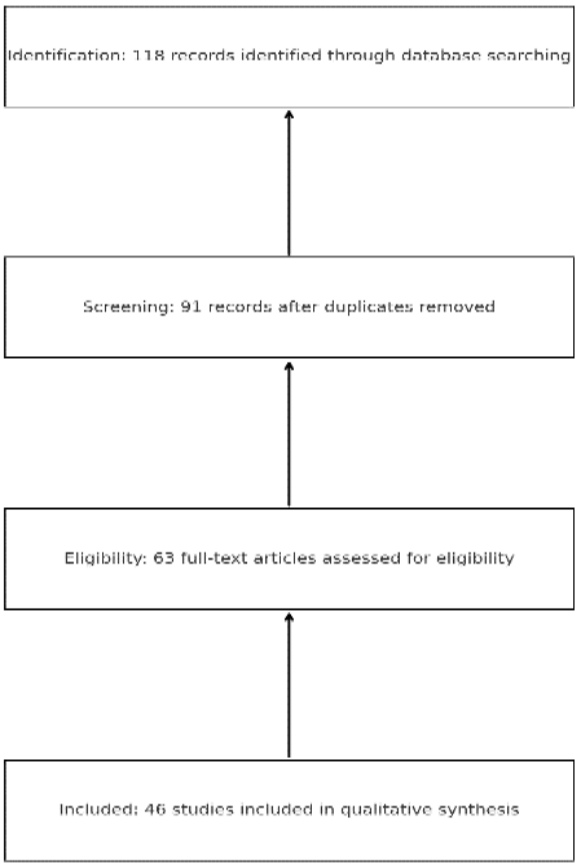

Fig 1: PRISMA Flow chart of the study methodology

2.1 The evolution of cybersecurity auditing

The early stages of information technology adoption saw cybersecurity auditing emerge primarily as a reactive, manual, and compliance-driven process. Auditors focused on verifying the presence and sufficiency of technical controls, which included essential measures such as firewalls, antivirus software, and password policies. The practice typically involved conducting periodic assessments, usually on an annual or semi-annual basis (Dagilienė & Klovienė, 2019). These assessments were aimed at ensuring organizations complied with regulatory requirements and internal security protocols, relying mostly on documentation reviews, physical inspections of IT infrastructure, and interviews with staff (DiGabriele, 2016: Sulistyowati *et al*., 2020).

However, these traditional audit methods had significant limitations. They often took the form of checklist-style audits that evaluated compliance with predetermined standards like ISO 27001, COBIT, or sector-specific regulations, including HIPAA and PCI DSS. Such structures especially focused on access controls, incident response procedures, and backup mechanisms; nonetheless, the periodicity of these audits led to a gap in detecting real-time vulnerabilities or anticipating intricate cyber threats (Gepp, *et al*., 2018: Sardi *et al*., 2020). Consequently, risks could potentially remain undetected between audit cycles, enhancing organizational vulnerability to breaches and regulatory penalties. The constraints of this static auditing model became increasingly critical as organizations navigated a rapidly evolving digital landscape marked by more sophisticated and frequent cyberattacks (Bristol-Alagbariya, Ayanponle & Ogedengbe, 2022). Figure 2 shows Cybersecurity Maturity Assessment Framework (HCYMAF) presented by Almomani, Ahmed & Maglaras, 2021.

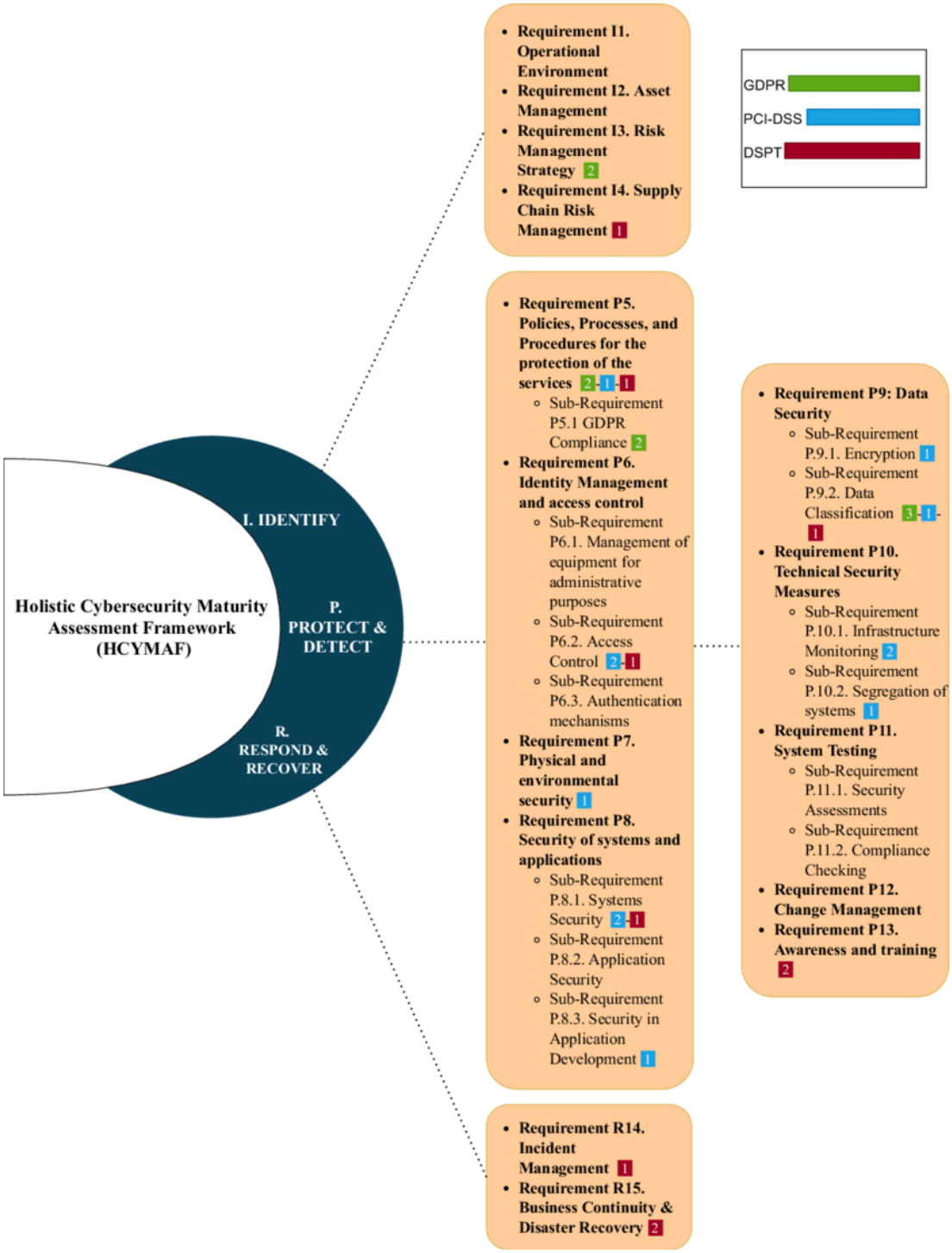

Fig 2: Cybersecurity Maturity Assessment Framework (HCYMAF) (Almomani, Ahmed & Maglaras, 2021).

As digital transformation reshaped business operations, the necessity for real-time and continuous cybersecurity auditing became apparent. This shift was fueled by the advent of emerging technologies such as machine learning, artificial intelligence, and advanced data analytics. Unlike traditional methods, real-time auditing not only continuously monitors systems and user behavior but also empowers auditors to detect anomalies and trigger immediate interventions (Honigsberg, 2020: Lois, *et al*., 2020). The integration of automated auditing tools has significantly minimized reliance on manual processes, enabling organizations to analyze vast data volumes efficiently and provide instantaneous insights through rule-based logic and comprehensive dashboards (Adewoyin, 2022, Chukwuma-Eke, Ogunsola & Isibor, 2022).

Moreover, real-time auditing systems facilitate continuous compliance, allowing organizations to maintain ongoing adherence to regulatory frameworks, particularly the NIST Cybersecurity Framework, which stresses iterative risk management across its core functions: Identify, Protect, Detect, Respond, and Recover (Bristol-Alagbariya, Ayanponle & Ogedengbe, 2022). This dynamic approach enables entities to perform regular self-assessments, modify their risk scores, and adjust controls in response to emerging threats and vulnerabilities (Lowe, *et al*., 2017: Salek *et al*., 2022). Technologies such as Security Information and Event Management (SIEM) systems and Security Orchestration Automation and Response (SOAR) platforms have become

integral in modern auditing methodologies, enhancing not only detection and response capabilities but also documentation and audit trails necessary for compliance (Malatji *et al*., 2021). Reference architecture for next-generation cyber-security frameworks for digital value chains presented by Repetto, *et al*., 2021, is shown in figure 3.

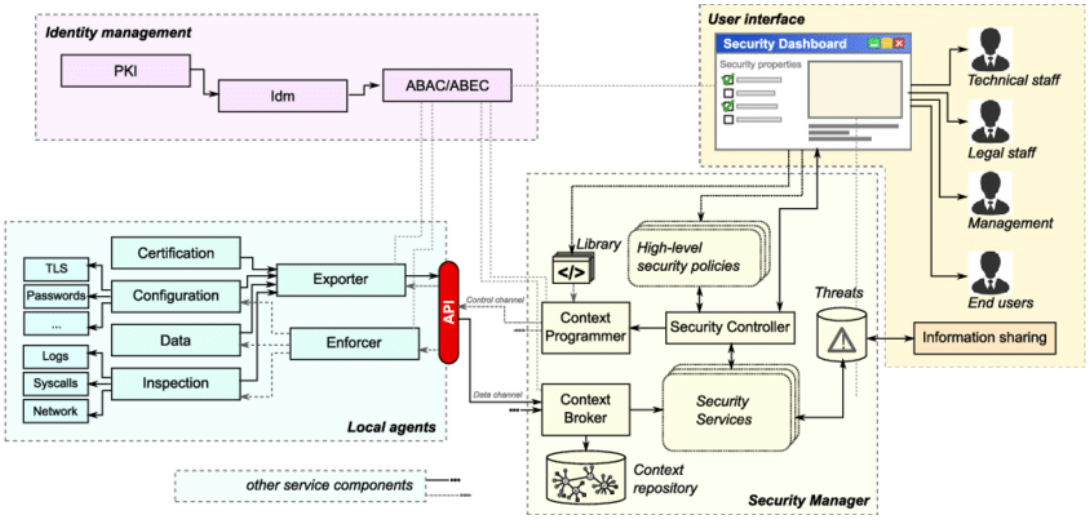

Fig 3: Reference architecture for next-generation cyber-security frameworks for digital value chains (Repetto, *et al*., 2021).

The broader scope of regulatory frameworks has also transformed the landscape of cybersecurity auditing. Regulations like the Sarbanes-Oxley Act have pushed organizations to establish rigorous internal controls for protecting financial data, identifying the need for cybersecurity audits to address technical safeguards (Mamahit & Urumsah, 2018: Sulistyowati *et al*., 2020). In tandem, the NIST Cybersecurity Framework offers a flexible and comprehensive structure for managing cybersecurity risks. GDPR has further broadened audit scopes, compelling organizations to include data governance and privacy assessments in their auditing practices, thereby emphasizing personal data collection and processing (Ajayi, *et al*., 2022, Chukwuma-Eke, Ogunsola & Isibor, 2022). The requirements for accountability and transparency imposed by GDPR necessitate that organizations ensure robust mechanisms for incident detection and response along with timely breach notifications, thus introducing a more holistic dimension to cybersecurity audits (Oluoha, 2021: Perdana, Rob & Rohde, 2018).

Additionally, as organizations embrace Agile methodologies and DevOps practices, the rigid nature of traditional audits is increasingly challenged. The emergence of DevSecOps reflects a paradigm shift where security considerations are integrated throughout the software development lifecycle, promoting continuous validation of the integrity of digital assets (Rahman, 2020: Sow & Gehrke, 2019). Consequently, cybersecurity auditing has transitioned toward being an enterprise-wide responsibility rather than a standalone department's task. This evolution has underscored the critical role of cybersecurity audits in enterprise risk management, aligning security metrics with overarching business strategies to foster resilience and innovation (Agho, *et al*., 2022, Egbuhuzor, *et al*., 2022). Ohki, *et al*., 2009, proposed Framework of Information Security Governance shown in figure 4.

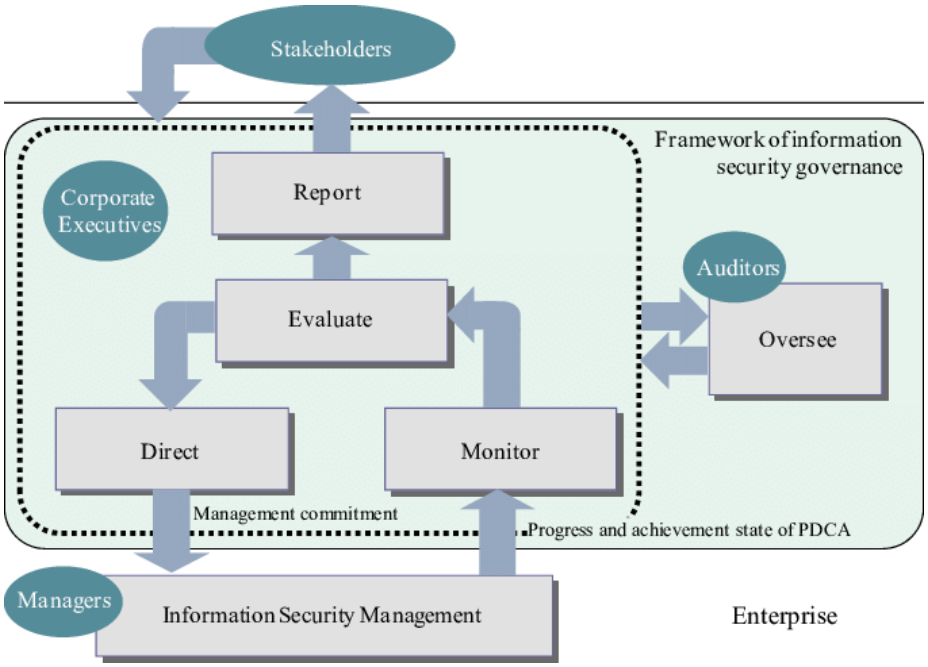

Fig 4: Proposed Framework of Information Security Governance (Ohki, *et al*., 2009).

Despite these advancements, challenges persist, particularly regarding the integration of automated tools necessitating investments in technology and training (Wang *et al*., 2021). Organizations also face the pressing need to ensure that human judgment remains central to auditing practices and that they navigate the complexities of overlapping compliance obligations in a global environment (Sun, 2019). In summary, the evolution of cybersecurity auditing reflects significant changes in technology, threat landscapes, and regulatory environments. From traditional, static strategies to modern approaches that embrace real-time monitoring and automation, the function of auditing has matured into a critical element for maintaining compliance, managing risk, and supporting strategic organizational objectives in an era marked by digital transformation (Sun & Vasarhelyi, 2018).

2.2 Emerging methodologies in cybersecurity auditing

In the evolving landscape of cybersecurity, auditing practices have undergone significant transformations driven by the complexities of digital environments and emerging threats. This shift has catalyzed the move from traditional compliance-driven approaches to a more dynamic, risk-focused methodology. Organizations are now compelled not only to comply with basic regulatory standards but also to anticipate and respond to emerging risks while aligning their cybersecurity strategies with overarching business objectives (Egbuhuzor, *et al*., 2021, Ogunnowo, *et al*., 2021). This transformation is necessitated by the need for continuous oversight and the integration of innovative technologies into the auditing process, leading to the emergence of several key methodologies in cybersecurity auditing (Tiwari & Debnath, 2017: Yuara, Ibrahim & Diantimala, 2019).

Risk-based auditing has become a central tenet of modern audit practices. Unlike traditional methods that impose uniform scrutiny across all assets, risk-based auditing allows organizations to focus resources on areas with the highest potential exposures and business impacts (Chukwuma-Eke, Ogunsola & Isibor, 2022). This methodology begins with a thorough risk assessment, identifying critical assets, evaluating vulnerabilities, and mapping potential threat vectors (Antunes *et al*., 2022). By targeting audits towards high-risk areas, organizations can optimize their resource allocation and align their cybersecurity efforts with their strategic goals (Aliyu, *et al*., 2020: Sabillón, 2022). This approach not only enhances the relevance of audits but also supports compliance with frameworks such as the NIST Cybersecurity Framework and regulations like the GDPR, which emphasize risk management and protective measures against privacy breaches (Adiloğlu & Güngör, 2019: Diamantopoulou, Tsohou & Karyda, 2020).

Complementing this risk-focused approach, continuous auditing and monitoring systems have gained traction. In a landscape where cyber threats can emerge rapidly, traditional audit cycles are no longer sufficient. Continuous auditing incorporates real-time data analysis and monitoring, allowing organizations to detect anomalies and policy violations instantly (Drivas, *et al*., 2020: Rahman *et al*., 2021). Leveraging advanced technologies, organizations can maintain a current snapshot of their compliance status and control effectiveness, enhancing their ability to respond swiftly to threatening events "National Cybersecurity Strategies", 2021). This constant vigilance is particularly crucial in sectors such as finance and healthcare, where compliance failures can lead to significant financial and reputational harm (Islam, Farah & Stafford, 2018: Rahman *et al*., 2021).

Moreover, the integration of artificial intelligence (AI) and machine learning (ML) into cybersecurity auditing represents a revolutionary development. These technologies empower auditors to process vast datasets, unveil hidden patterns, and automate repetitive tasks that have traditionally burdened human auditors. For instance, AI can analyze extensive logs to identify threats and flag high-risk activities, and ML can improve detection capabilities over time by learning from historical data (Bristol-Alagbariya, Ayanponle & Ogedengbe, 2022). The combination of AI and automation not only enhances the efficiency and accuracy of auditing processes but also makes them scalable across complex digital environments characterized by remote work and multi-vendor ecosystems (Joshi, Elluri & Nagar, 2020).

Additionally, organizations are increasingly adopting robust cybersecurity control frameworks to streamline audit processes. The ISO/IEC 27001 standard, for example, offers a structured methodology for managing sensitive data through clearly defined policies and controls. This framework assists auditors in evaluating the effectiveness of security measures and ensures alignment with regulatory requirements like the GDPR and corporate governance mandates (Diamantopoulou *et al*., 2020: Kahyaoğlu & Çalıyurt, 2018). COBIT, another essential framework, addresses broader governance aspects, allowing auditors to assess whether cybersecurity measures align with organizational goals and risk management strategies (Lankton, Price & Karim, 2020). Meanwhile, the CIS Controls provide actionable best practices that are immediately applicable and measurable, helping organizations prioritize their cybersecurity efforts (Sabillón, 2022).

Despite these advancements, the full implementation of these innovative methodologies faces challenges. Organizations contend with limited budgets, integration complexity of new technologies, and skill shortages in cybersecurity (Lewallen, 2020: Rahman *et al*., 2021). Moreover, as the reliance on automated systems increases, concerns surrounding data privacy, algorithmic transparency, and ethical audit practices become paramount (Chukwuma-Eke, Ogunsola & Isibor, 2021, Paul, *et al*., 2021). Nonetheless, as the digital landscape continues to evolve, organizations must adapt their auditing practices to these new realities. Embracing these emerging methodologies in cybersecurity auditing is no longer an option; it is a strategic necessity for safeguarding assets, ensuring compliance, and fostering trust in an interconnected world (Antunes *et al*., 2022; "National Cybersecurity Strategies", 2021).

In summary, the transformation in cybersecurity auditing, characterized by risk-based approaches, continuous monitoring, the application of AI and ML, and adherence to frameworks like ISO/IEC 27001, reflects a broad shift towards adaptive and intelligent audit practices. These innovations enable organizations to navigate the complex threats of the digital age and align their cybersecurity strategies with business objectives, thereby ensuring a robust defense against an ever-evolving array of cyber risks (Sabillón, *et al*., 2017).

2.3 Comparative analysis: alignment with SOX, NIST, and GDPR

A comprehensive understanding of cybersecurity auditing in the digital age indeed requires deep exploration into emerging methodologies, along with a critical comparative analysis vis-à-vis major regulatory frameworks such as the Sarbanes-Oxley Act (SOX), the National Institute of Standards and Technology (NIST) Cybersecurity Framework, and the General Data Protection Regulation (GDPR). The convergence of these elements informs the current landscape of cybersecurity audit practices, which increasingly adapt to the complexities of digital operations across jurisdictions (Sardi, *et al*., 2020).

The Sarbanes-Oxley Act (SOX) emphasizes internal controls related to financial reporting, mandating stringent protocols to ensure data integrity and accountability. Cybersecurity audit methodologies that focus on access control, audit trails, and segregation of duties are crucial in fulfilling SOX's requirements, particularly under Section 404, which covers management's assessment of internal controls (Adiloğlu & GÜNGÖR, 2019). These practices help to secure sensitive financial information from unauthorized access and ensure compliance with legal standards, thus fostering trust among stakeholders. Cybersecurity audits that focus on these areas create an environment where financial data is traceable and verifiable, thereby adhering to SOX expectations (Antunes *et al*., 2021: Sulistyowati, Handayani & Suryanto, 2020).

Conversely, the NIST Cybersecurity Framework provides a more adaptive and strategic approach by encapsulating five core functions: Identify, Protect, Detect, Respond, and Recover. The alignment of methodologies with NIST typically involves continuous risk assessments and the validation of security controls, which are critical for comprehensive audits (Akhigbe, *et al*., 2021, Odio, *et al*., 2021). This framework's flexibility allows organizations to adapt their cybersecurity practices to evolving threats while maintaining compliance across various regulatory spectra (Joshi *et al*., 2020; Sulistyowati *et al*., 2020). NIST's focus on systematic risk management fosters organizational resilience and promotes a pragmatic audit framework that balances regulatory compliance with operational flexibility (AlKetbi, *et al*., 2014: "National Cybersecurity Strategies", 2021).

GDPR introduces an additional layer of complexity by centering data protection rights and ethical considerations. It mandates that organizations conduct Data Protection Impact Assessments (DPIAs) and implement strong cybersecurity measures to safeguard personal data through transparent data processing practices (Drivas *et al*., 2020). Auditors ensuring compliance with GDPR must assess not just technical and procedural controls but also the alignment of data-handling practices with individual rights, such as those concerning access and erasure of personal data (Adekunle, *et al*., 2021, Oyedokun, 2019). This necessitates an in-depth understanding of both legal stipulations and practical implications of data management strategies.

While there are distinct priorities and methodologies associated with SOX, NIST, and GDPR, there are also converging themes, particularly in their emphasis on risk management strategies. For instance, risk-based auditing methodologies provide an adaptable approach applicable across all three frameworks, allowing auditors to prioritize high-risk areas and ensure compliance consistently (Joshi *et al*., 2020; Sulistyowati *et al*., 2020). This adaptability is enhanced by automation and integrated governance, risk management, and compliance (GRC) systems, which streamline compliance efforts across various regulatory landscapes while maintaining a solid audit trail.

Despite advancements in aligning audit methodologies to meet regulatory demands, notable challenges persist. Differences in the scope and enforcement of frameworks can create compliance gaps. SOX's focus on financial controls, for instance, may lead to oversight in broader risks outlined by NIST or GDPR's nuances surrounding personal data protection Schmidt *et al*., 2021). Furthermore, organizational capacity can significantly influence the effectiveness of audit frameworks; smaller organizations may struggle to implement comprehensive cybersecurity measures amid resource constraints (Antunes *et al*., 2021).

To overcome these obstacles, integrating audit models that harmonize various regulatory compliance efforts presents a promising direction. By aligning controls across frameworks, organizations can reduce duplication of efforts and streamline audit processes to enhance overall cybersecurity compliance and effectiveness (Kahyaoğlu & Çalıyurt, 2018; Schmidt *et al*., 2021). Initiatives such as the Cloud Controls Matrix and cybersecurity maturity assessments offer frameworks that support comparative compliance adherence and facilitate cooperative auditing practices on a global scale, addressing multi-regulatory alignment in today's integrated digital environments (Joshi *et al*., 2020; Drivas *et al*., 2020).

In summary, the intersection of cybersecurity auditing methodologies with SOX, NIST, and GDPR exemplifies a multidimensional challenge that necessitates a strategic and integrated approach. Organizations are called upon to foster a culture of proactive compliance while evolving their auditing methodologies to not only meet existing regulatory demands but also anticipate emerging threats in a rapidly changing digital landscape (Agbede, *et al*., 2021, Oyegbade, *et al*., 2021).

2.4 Sector-specific applications and case studies

In the realm of cybersecurity auditing, it is increasingly clear that a one-size-fits-all approach is ineffective due to the varying regulatory landscapes, operational structures, and threat environments across different sectors. These variances underscore a profound need for tailored audit strategies that align with the unique characteristics of each industry. The nature and complexity of threats faced by organizations, alongside regulatory requirements, intricately influence the cybersecurity audit process (Achumie, *et al*., 2022, Oyeniyi, *et al*., 2022).

For financial institutions, the Sarbanes-Oxley Act (SOX) significantly shapes the cybersecurity audit landscape. SOX's stringent requirements for accurate financial reporting necessitate a focus on safeguarding the integrity, confidentiality, and availability of financial data. The reliance on sophisticated IT systems in this sector means that cybersecurity audits often prioritize access control validation, transaction log immutability, and change management protocols (Islam *et al*., 2018). Within this context, the adoption of integrated frameworks like COSO emphasizes the critical intersection between financial controls and cybersecurity measures, ensuring a robust defense against fraud and operational missteps (Akhigbe, *et al*., 2022, Oyegbade, *et al*., 2022). Recent studies illustrate how U.S. banks have evolved their audit practices in response to digitalization and fintech innovations, employing continuous auditing techniques that promote real-time monitoring of

compliance with SOX mandates (Antunes *et al*., 2022).

The cloud computing sector, governed primarily by the National Institute of Standards and Technology (NIST) Cybersecurity Framework, presents a complex auditing environment. This sector demands agility due to the dynamic nature of cloud services and the shared responsibility model, where both providers and clients play essential roles in cybersecurity. Auditors in this domain focus on assessing controls related to identity management, data protection, and incident response readiness (Agho, *et al*., 2021, Otokiti, *et al*., 2021). Prominent cloud service providers, such as AWS and Microsoft Azure, illustrate the effective implementation of NIST-aligned controls through extensive compliance frameworks, enhancing customer assurance (Taherdoost, 2022). Case studies of SaaS companies adopting zero-trust architectures highlight the importance of adapting NIST principles to ensure robust security and facilitate smoother compliance audits.

The healthcare and consumer services sectors are uniquely impacted by the General Data Protection Regulation (GDPR), which imposes stringent data protection requirements. In this context, cybersecurity audits must evaluate not only technical controls but also compliance with legal and ethical data processing standards (Ogunnowo, *et al*., 2022, Sobowale, *et al*., 2022). For instance, audits conducted after data breaches in healthcare organizations have revealed critical gaps in access control and data encryption practices, underscoring the necessity for comprehensive audit strategies that align with GDPR principles (Drivas *et al*., 2020). Additionally, the proactive identification of potential breaches through rigorous testing and simulation ensures organizations can quickly respond to incidents while maintaining compliance with GDPR timelines regarding breach notifications.

Across all these industries, there is a clear shift toward customized auditing approaches that reflect each sector's specific regulatory frameworks and operational realities. Throughout finance, cloud services, and healthcare, the evolution of cybersecurity auditing is marked by the increasing sophistication of threat landscapes and the demand for stringent compliance measures (Ogunyankinnu, *et al*., 2022, Oyeniyi, *et al*., 2022). Audit methodologies are becoming more varied, reflecting sector-specific requirements while increasingly leveraging technology and real-time monitoring tools to enhance efficiency and effectiveness. As organizations continue to navigate this complex landscape, aligning audit practices with sector-specific needs will be essential for achieving both compliance and trust in a digitally transforming environment (Akintobi, Okeke & Ajani, 2022, Oyegbade, *et al*., 2022).

In conclusion, the landscape of cybersecurity auditing is marked by significant complexity and necessitates a differentiated approach based on the unique characteristics of each sector. As cyber threats grow more sophisticated, the ongoing refinement of audit practices that integrate sector-specific regulations, operational challenges, and supporting technologies will be critical for fostering robust security and compliance (Adewoyin, 2021, Tula, *et al*., 2004).

2.5 Challenges and Gaps

Despite significant advancements in methodologies and frameworks, cybersecurity auditing remains beset by persistent challenges and systemic gaps that undermine its effectiveness. These deficiencies not only pose risks to corporate governance but also have broader implications for organizational resilience in an increasingly complex regulatory landscape. Key challenges identified in the literature include fragmentation in audit tools, a shortage of skilled auditors, audit fatigue due to compliance burdens, and ethical dilemmas regarding data access and usage (Akintobi, Okeke & Ajani, 2022, Otokiti, *et al*., 2022).

Fragmentation in audit tools and practices is a primary barrier disrupting cohesive cybersecurity auditing. Current audit environments are characterized by diverse technologies and software solutions, leading to a reliance on various tools for essential functions such as vulnerability assessment, log analysis, and compliance tracking (Achumie, *et al*., 2022, Ozobu, *et al*., 2022). Many of these tools are derived from multiple vendors and lack integration, necessitating significant effort to reconcile findings across formats and control frameworks (Antunes *et al*., 2022). This fragmentation leads to inefficiencies and increases the risk of leaving security gaps in assessments. The absence of universally accepted audit protocols exacerbates this issue, as organizations must navigate a labyrinth of differing regulatory requirements. This reality is underscored by studies revealing that organizations often have to adapt their audit practices to align with multiple sets of standards (e.g., ISO 27001, NIST SP 800-53) from various jurisdictions, complicating the audit process (Antunes *et al*., 2022; Antunes *et al*., 2021).

Furthermore, the field faces a grave shortage of qualified cybersecurity auditors. As cyber threats evolve, the demand for auditors possessing a blend of technical skill sets and regulatory knowledge has surged, outpacing supply (Aliyu *et al*., 2020). The shortage is particularly acute in small and medium-sized enterprises (SMEs) and in developing regions where cybersecurity training is limited (Chukwuma, *et al*., 2022, Onukwulu, *et al*., 2022). The literature emphasizes that effective auditing requires expertise beyond mere IT proficiency, necessitating a comprehensive understanding of cryptographic principles, data governance laws, and structured audit methodologies (Antunes *et al*., 2021). This skills gap hinders organizations from undertaking robust audits, leaving them vulnerable to emerging threats and compliance issues.

Compounding these challenges is the growing phenomenon of audit fatigue, exacerbated by the increasing regulatory complexity that organizations face. As companies are subjected to overlapping audits from internal and external bodies, auditors and their teams may experience burnout, leading to diminished engagement and oversight quality (Lankton *et al*., 2020). The pressures of compliance can reduce the essence of auditing from a strategic function to a mere exercise in checkbox compliance, undermining the overarching goal of improving security postures (Lankton *et al*., 2020). Moreover, organizations that grapple with multiple regulatory frameworks often experience significant resource strain as they attempt to meet the demands of diverse compliance requirements (Adekunle, *et al*., 2021, Sobowale, *et al*., 2021).

Ethical concerns also loom large in the realm of cybersecurity auditing, particularly regarding data access and usage. Auditors typically require access to sensitive information to conduct thorough assessments, raising questions about privacy and potential conflicts of interest (Tronnier *et al*., 2022). In jurisdictions governed by stringent data protection regulations, such as the GDPR, there is an imperative to

navigate ethical boundaries carefully to prevent violations that could arise from unauthorized data disclosure or misuse (Tronnier *et al*., 2022). The integration of automated tools in audits introduces further ethical considerations, as these technologies often operate opaquely, possibly leading to biases or misinterpretations of data (Ajayi, *et al*., 2021, Sobowale, *et al*., 2021). Therefore, auditing frameworks must evolve to incorporate ethical guidelines that ensure responsible data handling while maintaining the integrity of the audit process (Tronnier *et al*., 2022).

In conclusion, cybersecurity auditing has advanced significantly; however, persistent challenges remain. Fragmentation in audit tools and practices undeniably hampers effectiveness, while the shortage of skilled auditors and the burden of regulatory compliance continue to strain audit functions. Ethical concerns surrounding data access must also be addressed to safeguard the integrity of audits. To mitigate these issues, cross-sector collaboration is essential, involving industry stakeholders, regulatory bodies, and academic institutions to create a more unified and ethically sound approach to cybersecurity auditing.

2.6 Proposed integrated cybersecurity audit model

The present discourse emphasizes the increasing necessity for a holistic and integrated cybersecurity audit model, motivated by the complexities prevalent in the realm of cybersecurity auditing. Professionals, regulatory bodies, and researchers alike acknowledge that existing frameworks are inadequate, particularly in fostering resilience against cyber threats. Current auditing practices often lean toward fragmented compliance checklists rather than a unified approach that encapsulates regulatory mandates, risk management, and governance structures into a singular, cohesive framework (Sabillón, 2022). Scholars argue that this integrated model not only fulfills compliance requirements but also enhances organizational resilience and promotes efficient strategic decision-making (Sabillón, 2022).

The integrated cybersecurity audit model fundamentally relies on three pillars: compliance, risk management, and governance. Compliance ensures adherence to legal standards such as the General Data Protection Regulation (GDPR) and guidelines from the National Institute of Standards and Technology (NIST) (Sabillón, 2022). It acts as the foundational layer upon which risk management builds by facilitating the identification, assessment, and prioritization of cybersecurity threats based on potential impacts and likelihoods of occurrences. The governance pillar integrates these two dimensions through a strategic lens that incorporates cybersecurity audit functions into broader corporate management practices, invoking the need for executive oversight and stakeholder accountability (Коваленко *et al*., 2021).

This model fosters a layered auditing methodology where compliance evaluations form the foundation, while risk assessments direct the audit priorities. This allows organizations to create a unified control matrix that aligns auditing criteria across various regulatory frameworks and risk domains, significantly reducing overall redundancies and enhancing audit comprehensiveness. For example, a unified control addressing access management might simultaneously satisfy the internal control requirements of SOX, the protective measures of NIST, and the confidentiality standards imposed by GDPR. This systematic mapping of controls streamlines audit processes and optimizes resource allocation within organizations, addressing the inefficiencies exhibited in fragmented approaches.

Technological advancements play a crucial role in this integrative framework. Automation tools for audits can significantly enhance efficiency by centralizing evidence collection, control testing, and reporting across several compliance requirements (Sabillón, 2022). Emerging technologies such as artificial intelligence (AI) and machine learning can be employed to analyze historical data, identify anomalies, and suggest enhancements, thus empowering audit functions with continuous assurance capabilities—vital features in an era characterized by rapid digital transformation and evolving cyber threats (Sabillón, 2022). The automation of these processes not only supports scalability but also provides real-time oversight into compliance status and risk exposure, facilitating timely decision-making by stakeholders (Sabillón, 2022; Sabillón, 2022).

To shepherd the adoption of this integrated audit model, several recommendations are posited for policymakers that include the establishment of harmonized audit standards adaptable across various sectors. Policy frameworks should converge around clear audit mandates and encourage interoperability among prominent models such as ISO/IEC 27001, NIST SP 800-53, and GDPR guidelines (Sabillón, 2022). Concurrently, policymakers must invest in fostering audit capacity through educational initiatives and incentivize the development of AI-enhanced auditing tools, particularly for small to medium enterprises (SMEs), thereby enhancing overall cybersecurity readiness at both organizational and national levels (Pace & Cornish, 2021).

Moreover, practitioners must embrace a holistic view of cybersecurity auditing that integrates these functions within their existing operational frameworks. Cybersecurity audits need to transition from a reactive to a proactive posture, underlining the importance of leadership buy-in for integrating cybersecurity into organizational culture (Sabillón, 2022). Creating centralized audit offices responsible for oversight of the integrated audit model can significantly streamline processes and enhance efficacy.

In conclusion, the proposed integrated cybersecurity audit model responds adeptly to the modern demands of digital risk and compliance, weaving together compliance, risk management, and governance into a single strategic framework. In recognizing the critical role of technology in enabling this model, it underlines an urgent necessity for a collaborative approach among policymakers, practitioners, and regulators to uphold the integrity of information systems across the globe. The establishment of globally standardized auditing practices is a vital imperative, one that serves to bolster trust and enhance resilience in our increasingly interconnected digital landscape (Sabillón, 2022).

3. Conclusion

Cybersecurity auditing in the digital age has undergone a significant transformation, evolving from traditional, periodic compliance checks to dynamic, integrated frameworks that align with the multifaceted demands of regulatory compliance, risk management, and organizational governance. This review has examined the development of audit methodologies in response to escalating cyber threats and complex digital infrastructures, highlighting how frameworks like SOX, NIST, and GDPR shape the scope and execution of cybersecurity audits across various sectors.

Emerging practices such as risk-based auditing, continuous monitoring, and the integration of AI and automation are reshaping audit capabilities, while sector-specific applications underscore the critical role of contextual awareness in designing and implementing effective audits. Despite these advancements, considerable challenges persist, including fragmented tools and standards, workforce limitations, audit fatigue, and ethical dilemmas surrounding data use and access. These gaps underscore the urgency of adopting a more unified and strategic approach to cybersecurity auditing.

The findings of this review make clear that the traditional audit paradigm is no longer sufficient in a rapidly changing digital and regulatory landscape. Organizations must evolve their audit strategies to become more proactive, intelligent, and continuous. This requires embedding audit functions into core business and IT processes, investing in skill development and audit technologies, and embracing integrated frameworks that holistically address compliance, risk, and governance. Regulatory bodies must also take the lead in fostering global audit standardization, offering clear, adaptable guidance, and supporting organizations of all sizes in building audit capacity. Cybersecurity audits should be leveraged not merely as tools for regulatory verification but as essential components of digital resilience and strategic decision-making.

Future research should explore the practical implementation of integrated audit models in diverse organizational contexts, the role of AI explainability in automated auditing systems, and the development of universally accepted cybersecurity audit standards. Further investigation is also needed into balancing audit transparency with data privacy, and into the effectiveness of cross-sectoral audit collaboration models. As digital threats and technologies continue to evolve, cybersecurity auditing must remain agile, ethical, and forward-looking—anchored in accountability, driven by innovation, and dedicated to safeguarding the integrity of our increasingly digital world.

4. References

1. Achumie GO, Oyegbade IK, Igwe AN, Ofodile OC, Azubuike C. A conceptual model for reducing occupational exposure risks in high-risk manufacturing and petrochemical industries through industrial hygiene practices. 2022.
2. Achumie GO, Oyegbade IK, Igwe AN, Ofodile OC, Azubuike C. AI-driven predictive analytics model for strategic business development and market growth in competitive industries. International Journal of Social Science Exceptional Research. 2022;1(1):13-25.
3. Adekunle BI, Chukwuma-Eke EC, Balogun ED, Ogunsola KO. A predictive modeling approach to optimizing business operations: A case study on reducing operational inefficiencies through machine learning. International Journal of Multidisciplinary Research and Growth Evaluation. 2021;2(1):791-799. https://doi.org/10.54660/.IJMRGE.2021.2.1.791-799
4. Adekunle BI, Chukwuma-Eke EC, Balogun ED, Ogunsola KO. Machine learning for automation: Developing data-driven solutions for process optimization and accuracy improvement. International Journal of Multidisciplinary Research and Growth Evaluation. 2021;2(1):800-808. https://doi.org/10.54660/.IJMRGE.2021.2.1.800-808
5. Adewoyin MA. Developing frameworks for managing low-carbon energy transitions: overcoming barriers to implementation in the oil and gas industry. 2021.
6. Adewoyin MA. Advances in risk-based inspection technologies: Mitigating asset integrity challenges in aging oil and gas infrastructure. 2022.
7. Adiloğlu B, Güngör N. Investigation of increasing technology use and digitalization in auditing. Pressacademia. 2019;9(9):20-23. https://doi.org/10.17261/pressacademia.2019.1058
8. Adiloğlu B, Güngör N. Investigation of increasing technology use and digitalization in auditing. Pressacademia. 2019;9(9):20-23. https://doi.org/10.17261/pressacademia.2019.1058
9. Agbede OO, Akhigbe EE, Ajayi AJ, Egbuhuzor NS. Assessing economic risks and returns of energy transitions with quantitative financial approaches. International Journal of Multidisciplinary Research and Growth Evaluation. 2021;2(1):552-566. https://doi.org/10.54660/.IJMRGE.2021.2.1.552-566
10. Agho G, Aigbaifie K, Ezeh MO, Isong D, Oluseyi. Advancements in green drilling technologies: Integrating carbon capture and storage (CCS) for sustainable energy production. World Journal of Advanced Research and Reviews. 2022;13(2):995-1011. https://doi.org/10.30574/ijsra.2023.8.1.0074
11. Agho G, Ezeh MO, Isong M, Iwe D, Oluseyi KA. Sustainable pore pressure prediction and its impact on geo-mechanical modelling for enhanced drilling operations. World Journal of Advanced Research and Reviews. 2021;12(1):540-557. https://doi.org/10.30574/wjarr.2021.12.1.0536
12. Ajayi AJ, Akhigbe EE, Egbuhuzor NS, Agbede OO. Economic analysis of transitioning from fossil fuels to renewable energy using econometrics. International Journal of Social Science Exceptional Research. 2022;1(1):96-110. https://doi.org/10.54660/IJSSER.2022.1.1.96-110
13. Ajayi AJ, Akhigbe EE, Egbuhuzor NS, Agbede OO. Bridging data and decision-making: AI-enabled analytics for project management in oil and gas infrastructure. International Journal of Multidisciplinary Research and Growth Evaluation. 2021;2(1):567-580. https://doi.org/10.54660/.IJMRGE.2021.2.1.567-580
14. Ajiga D, Ayanponle L, Okatta CG. AI-powered HR analytics: Transforming workforce optimization and decision-making. International Journal of Science and Research Archive. 2022;5(2):338-346.
15. Akhigbe EE, Egbuhuzor NS, Ajayi AJ, Agbede OO. Optimization of investment portfolios in renewable energy using advanced financial modeling techniques. International Journal of Multidisciplinary Research Updates. 2022;3(2):40-58. https://doi.org/10.53430/ijmru.2022.3.2.0054
16. Akhigbe EE, Egbuhuzor NS, Ajayi AJ, Agbede OO. Financial valuation of green bonds for sustainability-focused energy investment portfolios and projects. Magna Scientia Advanced Research and Reviews. 2021;2(1):109-128. https://doi.org/10.30574/msarr.2021.2.1.0033
17. Akintobi AO, Okeke IC, Ajani OB. Advancing economic growth through enhanced tax compliance and revenue generation: Leveraging data analytics and strategic policy reforms. International Journal of

Frontline Research in Multidisciplinary Studies. 2022;1(2):085-093.
18. Akintobi AO, Okeke IC, Ajani OB. Transformative tax policy reforms to attract foreign direct investment: Building sustainable economic frameworks in emerging economies. International Journal of Multidisciplinary Research Updates. 2022;4(1):008-015.
19. Aliyu A, Μαγλαράς Λ, He Y, Yevseyeva I, Boiten E, Cook A, *et al*. A holistic cybersecurity maturity assessment framework for higher education institutions in the United Kingdom. Applied Sciences. 2020;10(10):3660. https://doi.org/10.3390/app10103660
20. Aliyu A, Μαγλαράς Λ, He Y, Yevseyeva I, Boiten E, Cook A, *et al*. A holistic cybersecurity maturity assessment framework for higher education institutions in the United Kingdom. Applied Sciences. 2020;10(10):3660. https://doi.org/10.3390/app10103660
21. AlKetbi L, Neglekerke N, Ali H, ZeinAlDeen S, Ameri T. Audit of healthy lifestyle behaviors among patients with diabetes and hypertension attending ambulatory health care services in the United Arab Emirates. Global Health Promotion. 2014;21(4):44-51. https://doi.org/10.1177/1757975914528248
22. Almomani I, Ahmed M, Maglaras L. Cybersecurity maturity assessment framework for higher education institutions in Saudi Arabia. PeerJ Computer Science. 2021;7:e703.
23. Antunes M, Maximiano M, Gomes R. A client-centered information security and cybersecurity auditing framework. Applied Sciences. 2022;12(9):4102. https://doi.org/10.3390/app12094102
24. Antunes M, Maximiano M, Gomes R. A client-centered information security and cybersecurity auditing framework. Applied Sciences. 2022;12(9):4102. https://doi.org/10.3390/app12094102
25. Antunes M, Maximiano M, Gomes R. A client-centered information security and cybersecurity auditing framework. Applied Sciences. 2022;12(9):4102. https://doi.org/10.3390/app12094102
26. Antunes M, Maximiano M, Gomes R, Pinto D. Information security and cybersecurity management: A case study with SMEs in Portugal. Journal of Cybersecurity and Privacy. 2021;1(2):219-238. https://doi.org/10.3390/jcp1020012
27. Antunes M, Maximiano M, Gomes R, Pinto D. Information security and cybersecurity management: A case study with SMEs in Portugal. Journal of Cybersecurity and Privacy. 2021;1(2):219-238. https://doi.org/10.3390/jcp1020012
28. Appelbaum D, Kogan A, Vasarhelyi M. Big data and analytics in the modern audit engagement: Research needs. Auditing: A Journal of Practice & Theory. 2017;36(4):1-27. https://doi.org/10.2308/ajpt-51684
29. Balios D, Kotsilaras P, Eriotis N, Vasiliou D. Big data, data analytics and external auditing. Journal of Modern Accounting and Auditing. 2020;16(5). https://doi.org/10.17265/1548-6583/2020.05.002
30. Bristol-Alagbariya B, Ayanponle LO, Ogedengbe DE. Developing and implementing advanced performance management systems for enhanced organizational productivity. World Journal of Advanced Science and Technology. 2022;2(1):39-46.
31. Bristol-Alagbariya B, Ayanponle LO, Ogedengbe DE. Integrative HR approaches in mergers and acquisitions ensuring seamless organizational synergies. Magna Scientia Advanced Research and Reviews. 2022;6(1):78-85.
32. Bristol-Alagbariya B, Ayanponle LO, Ogedengbe DE. Strategic frameworks for contract management excellence in global energy HR operations. GSC Advanced Research and Reviews. 2022;11(3):150-157.
33. Bristol-Alagbariya B, Ayanponle OL, Ogedengbe DE. Strategic frameworks for contract management excellence in global energy HR operations. GSC Advanced Research and Reviews. 2022;11(3):150-157.
34. Bristol-Alagbariya B, Ayanponle OL, Ogedengbe DE. Developing and implementing advanced performance management systems for enhanced organizational productivity. World Journal of Advanced Science and Technology. 2022;2(1):039-046.
35. Buchheit S, Dzuranin A, Hux C, Riley M. Data visualization in local accounting firms: Is slow technology adoption rational? Current Issues in Auditing. 2020;14(2):A15-A24. https://doi.org/10.2308/ciia-2019-501
36. Chang C, Luo Y. Data visualization and cognitive biases in audits. Managerial Auditing Journal. 2019;36(1):1-16. https://doi.org/10.1108/maj-08-2017-1637
37. Chukwuma CC, Nwobodo EO, Eyeghre OA, Obianyo CM, Chukwuma CG, Tobechukwu UF, *et al*. Evaluation of noise pollution on audio-acuity among sawmill workers in Nnewi Metropolis, Anambra State, Nigeria. Changes. 2022;6:8.
38. Chukwuma-Eke EC, Ogunsola OY, Isibor NJ. Designing a robust cost allocation framework for energy corporations using SAP for improved financial performance. International Journal of Multidisciplinary Research and Growth Evaluation. 2021;2(1):809-822. https://doi.org/10.54660/.IJMRGE.2021.2.1.809-822
39. Chukwuma-Eke EC, Ogunsola OY, Isibor NJ. A conceptual approach to cost forecasting and financial planning in complex oil and gas projects. International Journal of Multidisciplinary Research and Growth Evaluation. 2022;3(1):819-833. https://doi.org/10.54660/.IJMRGE.2022.3.1.819-833
40. Chukwuma-Eke EC, Ogunsola OY, Isibor NJ. A conceptual framework for financial optimization and budget management in large-scale energy projects. International Journal of Multidisciplinary Research and Growth Evaluation. 2022;2(1):823-834. https://doi.org/10.54660/.IJMRGE.2021.2.1.823-834
41. Chukwuma-Eke EC, Ogunsola OY, Isibor NJ. Developing an integrated framework for SAP-based cost control and financial reporting in energy companies. International Journal of Multidisciplinary Research and Growth Evaluation. 2022;3(1):805-818. https://doi.org/10.54660/.IJMRGE.2022.3.1.805-818
42. Dagilienė L, Klovienė L. Motivation to use big data and big data analytics in external auditing. Managerial Auditing Journal. 2019;34(7):750-782. https://doi.org/10.1108/maj-01-2018-1773
43. Diamantopoulou V, Tsohou A, Karyda M. From ISO/IEC 27001:2013 and ISO/IEC 27002:2013 to GDPR compliance controls. Information and Computer Security. 2020;28(4):645-662. https://doi.org/10.1108/ics-01-2020-0004

44. Diamantopoulou V, Tsohou A, Karyda M. From ISO/IEC 27001:2013 and ISO/IEC 27002:2013 to GDPR compliance controls. Information and Computer Security. 2020;28(4):645-662. https://doi.org/10.1108/ics-01-2020-0004
45. DiGabriele J. The expectation differences among stakeholders in the financial valuation fitness of auditors. Journal of Applied Accounting Research. 2016;17(1):43-60. https://doi.org/10.1108/jaar-06-2013-0043
46. Drivas G, Chatzopoulou A, Μαγλαράς Λ, Lambrinoudakis C, Cook A, Janicke H. A NIS directive compliant cybersecurity maturity assessment framework. 2020. https://doi.org/10.1109/compsac48688.2020.00-20
47. Drivas G, Chatzopoulou A, Μαγλαράς Λ, Lambrinoudakis C, Cook A, Janicke H. A NIS directive compliant cybersecurity maturity assessment framework. 2020. https://doi.org/10.1109/compsac48688.2020.00-20
48. Egbuhuzor NS, Ajayi AJ, Akhigbe EE, Agbede OO. AI in enterprise resource planning: Strategies for seamless SaaS implementation in high-stakes industries. International Journal of Social Science Exceptional Research. 2022;1(1):81-95. https://doi.org/10.54660/IJSSER.2022.1.1.81-95
49. Egbuhuzor NS, Ajayi AJ, Akhigbe EE, Agbede OO, Ewim CP-M, Ajiga DI. Cloud-based CRM systems: Revolutionizing customer engagement in the financial sector with artificial intelligence. International Journal of Science and Research Archive. 2021;3(1):215-234. https://doi.org/10.30574/ijsra.2021.3.1.0111
50. Francis Onotole E, Ogunyankinnu T, Adeoye Y, Osunkanmibi AA, Aipoh G, Egbemhenghe J. The role of generative AI in developing new supply chain strategies-future trends and innovations. 2022.
51. Gepp A, Linnenluecke M, O'Neill T, Smith T. Big data techniques in auditing research and practice: Current trends and future opportunities. Journal of Accounting Literature. 2018;40(1):102-115. https://doi.org/10.1016/j.acclit.2017.05.003
52. Honigsberg C. Forensic accounting. Annual Review of Law and Social Science. 2020;16(1):147-164. https://doi.org/10.1146/annurev-lawsocsci-020320-022159
53. Isibor NJ, Ewim CPM, Ibeh AI, Adaga EM, Sam-Bulya NJ, Achumie GO. A generalizable social media utilization framework for entrepreneurs: Enhancing digital branding, customer engagement, and growth. 2021.
54. Isibor NJ, Ibeh AI, Ewim CPM, Sam-Bulya NJ, Martha E. A financial control and performance management framework for SMEs: Strengthening budgeting, risk mitigation, and profitability. 2022.
55. Islam M, Farah N, Stafford T. Factors associated with security/cybersecurity audit by internal audit function. Managerial Auditing Journal. 2018;33(4):377-409. https://doi.org/10.1108/maj-07-2017-1595
56. Islam M, Farah N, Stafford T. Factors associated with security/cybersecurity audit by internal audit function. Managerial Auditing Journal. 2018;33(4):377-409. https://doi.org/10.1108/maj-07-2017-1595
57. Joshi K, Elluri L, Nagar A. An integrated knowledge graph to automate cloud data compliance. IEEE Access. 2020;8:148541-148555. https://doi.org/10.1109/access.2020.3008964
58. Joshi K, Elluri L, Nagar A. An integrated knowledge graph to automate cloud data compliance. IEEE Access. 2020;8:148541-148555. https://doi.org/10.1109/access.2020.3008964
59. Kahyaoğlu S, Çalıyurt K. Cyber security assurance process from the internal audit perspective. Managerial Auditing Journal. 2018;33(4):360-376. https://doi.org/10.1108/maj-02-2018-1804
60. Kahyaoğlu S, Çalıyurt K. Cyber security assurance process from the internal audit perspective. Managerial Auditing Journal. 2018;33(4):360-376. https://doi.org/10.1108/maj-02-2018-1804
61. Lankton N, Price J, Karim M. Cybersecurity breaches and the role of information technology governance in audit committee charters. Journal of Information Systems. 2020;35(1):101-119. https://doi.org/10.2308/isys-18-071
62. Lankton N, Price J, Karim M. Cybersecurity breaches and the role of information technology governance in audit committee charters. Journal of Information Systems. 2020;35(1):101-119. https://doi.org/10.2308/isys-18-071
63. Lewallen J. Emerging technologies and problem definition uncertainty: The case of cybersecurity. Regulation & Governance. 2020;15(4):1035-1052. https://doi.org/10.1111/rego.12341
64. Lewallen J. Emerging technologies and problem definition uncertainty: The case of cybersecurity. Regulation & Governance. 2020;15(4):1035-1052. https://doi.org/10.1111/rego.12341
65. Lois P, Drogalas G, Karagiorgos A, Tsikalakis K. Internal audits in the digital era: Opportunities risks and challenges. EuroMed Journal of Business. 2020;15(2):205-217. https://doi.org/10.1108/emjb-07-2019-0097
66. Lowe D, Bierstaker J, Janvrin D, Jenkins J. Information technology in an audit context: Have the Big 4 lost their advantage? Journal of Information Systems. 2017;32(1):87-107. https://doi.org/10.2308/isys-51794
67. Malatji M, Marnewick A, Solms S. Cybersecurity capabilities for critical infrastructure resilience. Information and Computer Security. 2021;30(2):255-279. https://doi.org/10.1108/ics-06-2021-0091
68. Mamahit A, Urumsah D. The comprehensive model of whistle-blowing, forensic audit, audit investigation, and fraud detection. Journal of Accounting and Strategic Finance. 2018;1(2):153-162. https://doi.org/10.33005/jasf.v1i2.43
69. Odio PE, Kokogho E, Olorunfemi TA, Nwaozomudoh MO, Adeniji IE, Sobowale A. Innovative financial solutions: A conceptual framework for expanding SME portfolios in Nigeria's banking sector. International Journal of Multidisciplinary Research and Growth Evaluation. 2021;2(1):495-507.
70. Ogunnowo E, Ogu E, Egbumokei P, Dienagha I, Digitemie W. Theoretical model for predicting microstructural evolution in superalloys under directed energy deposition (DED) processes. Magna Scientia Advanced Research and Reviews. 2022;5(1):76-89.
71. Ogunnowo E, Ogu E, Egbumokei P, Dienagha I, Digitemie W. Theoretical framework for dynamic mechanical analysis in material selection for high-

performance engineering applications. Open Access Research Journal of Multidisciplinary Studies. 2021;1(2):117-131.
72. Ogunwole O, Onukwulu EC, Sam-Bulya NJ, Joel MO, Achumie GO. Optimizing automated pipelines for real-time data processing in digital media and e-commerce. International Journal of Multidisciplinary Research and Growth Evaluation. 2022;3(1):112-120. https://doi.org/10.54660/.IJMRGE.2022.3.1.112-120
73. Ogunwole O, Onukwulu EC, Sam-Bulya NJ, Joel MO, Ewim CP. Enhancing risk management in big data systems: A framework for secure and scalable investments. International Journal of Multidisciplinary Comprehensive Research. 2022;1(1):10-16. https://doi.org/10.54660/IJMCR.2022.1.1.10-16
74. Ogunyankinnu T, Onotole EF, Osunkanmibi AA, Adeoye Y, Aipoh G, Egbemhenghe J. Blockchain and AI synergies for effective supply chain management. 2022.
75. Ohki E, Harada Y, Kawaguchi S, Shiozaki T, Kagaya T. Information security governance framework. In: Proceedings of the first ACM workshop on Information security governance. 2009. p. 1-6.
76. Oluoha O. Project management innovations for strengthening cybersecurity compliance across complex enterprises. International Journal of Multidisciplinary Research and Growth Evaluation. 2021;2(1):871-881. https://doi.org/10.54660/.ijmrge.2021.2.1.871-881
77. Onukwulu EC, Fiemotongha JE, Igwe AN, Ewim CPM. International Journal of Management and Organizational Research. 2022.
78. Otokiti BO, Igwe AN, Ewim CPM, Ibeh AI. Developing a framework for leveraging social media as a strategic tool for growth in Nigerian women entrepreneurs. Int J Multidiscip Res Growth Eval. 2021;2(1):597-607.
79. Otokiti BO, Igwe AN, Ewim CP, Ibeh AI, Sikhakhane-Nwokediegwu Z. A framework for developing resilient business models for Nigerian SMEs in response to economic disruptions. Int J Multidiscip Res Growth Eval. 2022;3(1):647-659.
80. Oyedokun OO. Green human resource management practices and its effect on the sustainable competitive edge in the Nigerian manufacturing industry (Dangote) [Doctoral dissertation]. Dublin Business School; 2019.
81. Oyegbade IK, Igwe AN, Ofodile OC, Azubuike C. Innovative financial planning and governance models for emerging markets: Insights from startups and banking audits. Open Access Research Journal of Multidisciplinary Studies. 2021;1(2):108-116.
82. Oyegbade IK, Igwe AN, Ofodile OC, Azubuike C. Advancing SME financing through public-private partnerships and low-cost lending: A framework for inclusive growth. Iconic Research and Engineering Journals. 2022;6(2):289-302.
83. Oyegbade IK, Igwe AN, Ofodile OC, Azubuike C. Transforming financial institutions with technology and strategic collaboration: Lessons from banking and capital markets. International Journal of Multidisciplinary Research and Growth Evaluation. 2022;4(6):1118-1127.
84. Oyeniyi LD, Igwe AN, Ajani OB, Ewim CPM, Adewale TT. Mitigating credit risk during macroeconomic volatility: Strategies for resilience in emerging and developed markets. International Journal of Science and Technology Research Archive. 2022;3(1):225-231. https://doi.org/10.53771/ijstra.2022.3.1.0064
85. Oyeniyi LD, Igwe AN, Ofodile OC, Paul-Mikki C. Optimizing risk management frameworks in banking: Strategies to enhance compliance and profitability amid regulatory challenges. 2021.
86. Ozobu CO, Adikwu F, Odujobi O, Onyekwe FO, Nwulu EO. A conceptual model for reducing occupational exposure risks in high-risk manufacturing and petrochemical industries through industrial hygiene practices. International Journal of Social Science Exceptional Research. 2022;1(1):26-37.
87. Pace L, Cornish P. Cybersecurity capacity building. 2021. p. 463-476. https://doi.org/10.1093/oxfordhb/9780198800682.013.29
88. Paul PO, Abbey ABN, Onukwulu EC, Agho MO, Louis N. Integrating procurement strategies for infectious disease control: Best practices from global programs. Prevention. 2021;7:9.
89. Perdana A, Rob A, Rohde F. Does visualization matter? The role of interactive data visualization to make sense of information. Australasian Journal of Information Systems. 2018;22. https://doi.org/10.3127/ajis.v22i0.1681
90. Rahman C. Organizational culture and its influence on auditing practices: A case study in audit firms. Golden Ratio of Auditing Research. 2020;1(1):24-33. https://doi.org/10.52970/grar.v1i1.363
91. Rahman F, Putri G, Wulandari D, Pratama D, Permadi E. Auditing in the digital era: Challenges and opportunities for auditor. Golden Ratio of Auditing Research. 2021;1(2):86-98. https://doi.org/10.52970/grar.v1i2.367
92. Repetto M, Striccoli D, Piro G, Carrega A, Boggia G, Bolla R. An autonomous cybersecurity framework for next-generation digital service chains. Journal of Network and Systems Management. 2021;29(4):37.
93. Sabillón R. A practical model to perform comprehensive cybersecurity audits. Enfoque Ute. 2018;9(1):127-137. https://doi.org/10.29019/enfoqueute.v9n1.214
94. Sabillon R. National cybersecurity strategies. In: National Cybersecurity Strategies. IGI Global; 2021. p. 1-23. https://doi.org/10.4018/978-1-7998-4162-3.ch005
95. Sabillón R. Audits in cybersecurity. 2022. p. 1-18. https://doi.org/10.4018/978-1-6684-3698-1.ch001
96. Sabillón R. Audits in cybersecurity. 2022. p. 1-18. https://doi.org/10.4018/978-1-6684-3698-1.ch001
97. Sabillón R. The cybersecurity audit model (CSAM). 2022. p. 77-139. https://doi.org/10.4018/978-1-6684-3698-1.ch005
98. Sabillón R, Serra-Ruiz J, Cavaller V, M. J. A comprehensive cybersecurity audit model to improve cybersecurity assurance: The cybersecurity audit model (CSAM). 2017. p. 253-259. https://doi.org/10.1109/inciscos.2017.20
99. Sabillón R, Serra-Ruiz J, Cavaller V, M. J. A comprehensive cybersecurity audit model to improve cybersecurity assurance: The cybersecurity audit model (CSAM). 2017. p. 253-259. https://doi.org/10.1109/inciscos.2017.20
100. Salek M, Khan S, Rahman M, Deng H, Islam M, Khan Z, *et al*. A review on cybersecurity of cloud computing for supporting connected vehicle applications. IEEE Internet of Things Journal. 2022;9(11):8250-8268.

https://doi.org/10.1109/jiot.2022.3152477
101. Santoso F, Wijaya A, Pramudita C, Permata D, Suryani E. The influence of government regulations on auditing practices: A qualitative research. Golden Ratio of Auditing Research. 2021;1(2):54-63. https://doi.org/10.52970/grar.v1i2.366
102. Sardi A, Rizzi A, Sorano E, Guerrieri A. Cyber risk in health facilities: A systematic literature review. Sustainability. 2020;12(17):7002. https://doi.org/10.3390/su12177002
103. Sardi A, Rizzi A, Sorano E, Guerrieri A. Cyber risk in health facilities: A systematic literature review. Sustainability. 2020;12(17):7002. https://doi.org/10.3390/su12177002
104. Schmidt T, Nøhr C, Koppel R. A simple assessment of information security awareness in hospital staff across five Danish regions. 2021. https://doi.org/10.3233/shti210248
105. Sobowale A, Odio PE, Kokogho E, Olorunfemi TA, Nwaozomudoh MO, Adeniji IE. Innovative financial solutions: A conceptual framework for expanding SME portfolios in Nigeria's banking sector. International Journal of Multidisciplinary Research and Growth Evaluation. 2021;2(1):495-507.
106. Sobowale A, Odio PE, Kokogho E, Olorunfemi TA, Nwaozomudoh MO, Adeniji IE. A conceptual model for reducing operational delays in currency distribution across Nigerian banks. International Journal of Social Science Exceptional Research. 2022;1(6):17-29.
107. Sow M, Gehrke C. Evaluating information security system effectiveness for risk management, control, and corporate governance. Business and Economic Research. 2019;9(1):164. https://doi.org/10.5296/ber.v9i1.13994
108. Sulistyowati D, Handayani F, Suryanto Y. Comparative analysis and design of cybersecurity maturity assessment methodology using NIST CSF, COBIT, ISO/IEC 27002 and PCI DSS. JOIV International Journal on Informatics Visualization. 2020;4(4):225-230. https://doi.org/10.30630/joiv.4.4.482
109. Sulistyowati D, Handayani F, Suryanto Y. Comparative analysis and design of cybersecurity maturity assessment methodology using NIST CSF, COBIT, ISO/IEC 27002 and PCI DSS. JOIV International Journal on Informatics Visualization. 2020;4(4):225-230. https://doi.org/10.30630/joiv.4.4.482
110. Sun T. Applying deep learning to audit procedures: An illustrative framework. Accounting Horizons. 2019;33(3):89-109. https://doi.org/10.2308/acch-52455
111. Sun T, Vasarhelyi M. Embracing textual data analytics in auditing with deep learning. IJDAR. 2018. p. 49-67. https://doi.org/10.4192/1577-8517-v18_3
112. Taherdoost H. Understanding cybersecurity frameworks and information security standards—A review and comprehensive overview. Electronics. 2022;11(14):2181. https://doi.org/10.3390/electronics11142181
113. Tiwari R, Debnath J. Forensic accounting: A blend of knowledge. Journal of Financial Regulation and Compliance. 2017;25(1):73-85. https://doi.org/10.1108/jfrc-05-2016-0043
114. Tronnier F, Pape S, Löbner S, Rannenberg K. A discussion on ethical cybersecurity issues in digital service chains. 2022. p. 222-256. https://doi.org/10.1007/978-3-031-04036-8_10
115. Tula OA, Adekoya OO, Isong D, Daudu CD, Adefemi A, Okoli CE. Corporate advising strategies: A comprehensive review for aligning petroleum engineering with climate goals and CSR commitments in the United States and Africa. Corporate Sustainable Management Journal. 2004;2(1):32-38.
116. Wang Y, Wang Y, Qin H, Ji H, Zhang Y, Wang J. A systematic risk assessment framework of automotive cybersecurity. Automotive Innovation. 2021;4(3):253-261. https://doi.org/10.1007/s42154-021-00140-6
117. Yuara S, Ibrahim R, Diantimala Y. Pengaruh sikap skeptisme profesional auditor, kompetensi bukti audit dan tekanan waktu terhadap pendeteksian kecurangan pada inspektorat kabupaten bener meriah. Jurnal Perspektif Ekonomi Darussalam. 2019;4(1):69-81. https://doi.org/10.24815/jped.v4i1.10924
118. Коваленко С, Smolyev Y, Bargylevych O. Cybersecurity audit technology of corporate information system according to ISO / IES: 27001. Modern Information Security. 2021;47(3). https://doi.org/10.31673/2409-7292.2021.032935