A Systematic Literature Review of Cybersecurity Audit Frameworks and Access Control Mechanisms in Information Systems: Trends and Challenges

***Chika Almalia Agisti., Annisa Nur Hanifah., Luthfiyyah Khaira Zahra., Agus Widarsono**

Master of Accounting, Faculty of Economics and Business Education, Universitas Pendidikan Indonesia

***Corresponding Author**

DOI: https://doi.org/10.47772/IJRISS.2026.100500328

Received: 04 May 2026; Accepted: 09 May 2026; Published: 30 May 2026

ABSTRACT

The rapid advancement of digital transformation has significantly increased cybersecurity risks faced by organizations, making cybersecurity governance and auditing essential components of organizational resilience. This study aims to analyze the development of cybersecurity audit frameworks and access control mechanisms in information systems through a Systematic Literature Review (SLR). The study follows the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines and reviews 30 Scopus-indexed journal articles and conference proceedings published between 2020 and 2025. The review focuses on comparing cybersecurity audit frameworks, identifying recent trends, examining implementation challenges, and analyzing the evolution of access control mechanisms. The findings indicate that widely used frameworks such as ISO/IEC 27001, NIST Cybersecurity Framework (NIST-CSF), COBIT, CIS Controls, SOX, and COSO possess different orientations, strengths, and limitations regarding governance, compliance, flexibility, and technical protection. The study also reveals a shift from traditional compliance-based auditing toward risk-based, continuous, and technology-driven auditing supported by Artificial Intelligence (AI), Machine Learning (ML), blockchain, and continuous monitoring systems. In terms of access control, the findings demonstrate an evolution from traditional models such as DAC, MAC, and RBAC toward more adaptive approaches including ABAC, blockchain-based access control, and Zero Trust Architecture (ZTA). However, the implementation of modern frameworks and technologies still faces challenges related to scalability, interoperability, implementation complexity, operational costs, and the shortage of skilled cybersecurity professionals. This study concludes that no single framework or access control mechanism is universally effective for all organizations, and therefore organizations should adopt adaptive and hybrid approaches based on their risk profiles, governance maturity, and operational requirements. The study contributes theoretically by integrating discussions on cybersecurity audit frameworks and access control mechanisms while providing practical insights for auditors, cybersecurity practitioners, regulators, and organizations in designing more resilient cybersecurity governance strategies.

Keywords: cybersecurity audit, audit framework, access control, blockchain, information systems

INTRODUCTION

In the era of rapid digital transformation, cyber threats have become one of the most significant risks faced by organizations worldwide. The Global Cybersecurity Outlook 2025 report published by the World Economic Forum (WEF) states that 72% of cybersecurity leaders reported an increase in organizational risk over the past year (World Economic Forum, 2025). This condition is further exacerbated by findings from the FBI's Internet Crime Complaint Center (IC3), which recorded 859,532 cybercrime complaints from the American public in 2024, with potential losses exceeding USD 16 billion, an increase of 33% compared to the previous year (Federal Bureau of Investigation, 2024). One major global incident was the SolarWinds supply chain attack in 2020, which stemmed from a lack of control over the software development process and excessive access privileges (Meegammana et al., 2020). Furthermore, failures in access control mechanisms can also be seen in

the ransomware attack on Colonial Pipeline, where hackers gained entry using a single compromised VPN password without additional protection such as multi-factor authentication (MFA) (Geerman, 2026). In Indonesia, cybersecurity breaches have also occurred, including the leak of 91 million Tokopedia user accounts in 2020 (Pahlawati et al., 2025). These figures clearly demonstrate that cyber threats are no longer merely technical risks, but have evolved into strategic business risks that require organizations to implement structured and measurable governance.

The financial impact of cyber incidents continues to rise consistently. According to the *Cost of a Data Breach Report 2024* published by International Business Machines (IBM) and the Ponemon Institute, an ongoing study conducted over 19 consecutive years the global average cost of a data breach reached USD 4.88 million in 2024. This represents a 10% increase from the previous year and marks the largest annual surge since the COVID-19 pandemic (International Business Machines, 2024). The report is based on an in-depth analysis of real data breaches experienced by 604 organizations worldwide, spanning 17 industries and 16 countries. These findings underscore the substantial financial burden caused by cyber incidents.

Therefore, it is crucial to establish effective cybersecurity governance and audit mechanisms. One of the key approaches is conducting a cybersecurity audit. To carry out such an audit effectively, an appropriate and efficient framework is required to serve as a guideline. According to Haapamäki & Sihvonen (2019), out of 39 studies examined, 13 did not systematically conceptualize the effectiveness of cybersecurity audits (CSA) nor operationalize them with measurable indicators. Meanwhile, research by Slapničar et al. (2022) found that 82% of internal auditors reported that their organizations use one or more cybersecurity frameworks in developing audit plans; however, their usage remains fragmented. Furthermore, Toussaint et al. (2024) identified 12 voluntary cybersecurity frameworks and 17 standards, yet found that none of them comprehensively address all audit needs across different sectors.

Based on the discussion above, there is a significant research gap: on one hand, cyber threats continue to increase in both quantity and complexity; on the other hand, existing cybersecurity audit frameworks remain fragmented, lack universal standardization, and do not fully address the continuously evolving risk dimensions. Existing literature reviews are generally limited to a single framework, thus failing to provide a holistic view of the overall cybersecurity audit framework landscape. Therefore, this study aims to conduct a systematic literature review of studies discussing cybersecurity audit frameworks. Through a comparative analysis of Scopus-indexed articles, this research is expected to: map the latest developments in cybersecurity audit frameworks, compare existing frameworks, and analyze the challenges faced in implementing cybersecurity audit frameworks.

In addition, as a novel contribution compared to previous studies, this research also incorporates a discussion on access control mechanisms, considering that many cyber incidents are caused by weaknesses in access control. Therefore, this study also aims to analyze and compare various access control mechanisms, as well as evaluate the effectiveness of implementing technologies such as IoT and blockchain in enhancing access control security compared to traditional methods.

By conducting a literature review, this study aims to help organizations understand the importance of implementing effective cybersecurity audit frameworks, as well as to deepen their understanding of access control mechanisms as a preventive measure against cybersecurity breaches. This research can serve as a reference for auditors and cybersecurity practitioners in developing more comprehensive and flexible audit programs. From a theoretical perspective, this study contributes to the body of knowledge by summarizing the development of cybersecurity audit frameworks from 2020 to 2025, as well as addressing gaps in previous research by incorporating discussions on access control mechanisms.

This study is structured into several sections. Section 2 provides a theoretical overview of cybersecurity audit frameworks and access control mechanisms. Section 3 describes the research methodology used in this study. Section 4 presents the latest developments in cybersecurity audit frameworks, compares existing frameworks, and analyzes the challenges faced in their implementation. Additionally, this section discusses access control mechanisms and evaluates the effectiveness of technologies such as IoT and blockchain in enhancing access

control security compared to traditional methods. Finally, Section 5 presents the conclusions, outlines the limitations of the study, and offers recommendations for future research.

LITERATURE REVIEW

Information Systems Audit

Information systems auditing broadly focuses on assessing internal controls, security, and the governance of an organization's IT infrastructure (Sayankar, 2013). Traditionally, this audit involves reviewing documentation, conducting physical inspections of infrastructure, and performing interviews to ensure the organization complies with internal protocols and regulatory requirements. Its primary focus includes the integrity of financial reporting data, system availability, and operational efficiency.

Many organizations are willing to spend substantial amounts on information technology because they recognize the significant benefits it can provide for their operations and services (Yang et al., 2025). Nevertheless, organizations need to ensure that their IT systems are reliable, secure, and not vulnerable to cyber threats. IT auditing therefore becomes essential, as it provides assurance that IT systems are properly protected, deliver reliable information to users, and are effectively managed to achieve their intended benefits.

The risks associated with the use of information technology systems include operational disruptions, data loss, and security breaches. System weaknesses can lead to serious consequences such as financial losses, business interruptions, and increased security risks. Therefore, the implementation of cybersecurity measures and IT auditing is essential, as they help protect data, prevent unauthorized access, and ensure the continuity and reliability of systems in supporting organizational operations (Tharwat et al., 2025).

Definition of Cybersecurity Audit

Cybersecurity auditing represents a more specialized domain, focusing on identifying vulnerabilities and assessing an organization's resilience against specific cyber threats. This form of audit has evolved from merely testing static technical controls (such as firewalls and antivirus systems) into a dynamic methodology that leverages artificial intelligence and machine learning to detect Advanced Persistent Threats (APTs) in real time.

Cybersecurity auditing serves as a crucial mechanism for evaluating the effectiveness of an organization's information security controls, identifying vulnerabilities, and ensuring compliance with various regulatory mandates. The importance of audit practices in enhancing organizational resilience against cyber threats through adherence to 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) is significant and should not be underestimated (Ilori et al., 2022). The continuously evolving nature of these frameworks requires cybersecurity audits to adapt to reflect current risks and emerging technologies (Rahman et al., 2021; Santoso et al., 2021). For instance, as regulators impose stricter requirements, organizations are compelled to shift from conventional checklist-driven audits to more dynamic, risk-based, and real-time methodologies, ultimately reshaping the landscape of cybersecurity governance (Dimitris Balios et al., 2020; Rahman et al., 2021).

Evolution of Cybersecurity Audit

In the early stages of information technology adoption, cybersecurity auditing emerged primarily as a reactive, manual, and compliance-driven process. Auditors focused on verifying the existence and adequacy of technical controls, including essential measures such as firewalls, antivirus software, and password policies. These practices typically involved conducting periodic assessments, commonly on an annual or semi-annual basis (Dagilienė & Klovienė, 2019). Such evaluations aimed to ensure that organizations complied with regulatory requirements and internal security protocols, relying largely on documentation reviews, physical inspections of IT infrastructure, and interviews with staff (Sulistyowati et al., 2020).

However, this traditional audit approach has significant limitations. It is often structured as a checklist-based audit that evaluates compliance against predefined standards such as ISO 27001, COBIT, or sector-specific regulations, including HIPAA and PCI DSS. Such frameworks primarily focus on access controls, incident response procedures, and backup mechanisms; nevertheless, the periodic nature of these audits creates gaps in detecting vulnerabilities in real time or anticipating sophisticated cyber threats (Gepp et al., 2018; Sardi et al., 2020). As a result, risks may remain undetected between audit cycles, increasing an organization's exposure to breaches and regulatory penalties. The limitations of this static audit model become even more critical as organizations navigate a rapidly evolving digital landscape characterized by increasingly frequent and advanced cyberattacks (Bernadette Bristol-Alagbariya et al., 2022).

Risk-based audit methodology has now become central to modern auditing practices, where resources are prioritized toward areas with the highest potential exposure and business impact through comprehensive risk assessments. This approach enables organizations to optimize resource allocation while supporting compliance with frameworks such as NIST and regulations like the GDPR. Complementing this, continuous auditing and monitoring systems are gaining increasing prominence, as traditional audit cycles are no longer sufficient to address rapidly emerging cyber threats. By leveraging real-time data analytics, organizations can detect anomalies and policy violations instantly, which is particularly critical in sectors such as finance and healthcare. Furthermore, the integration of Artificial Intelligence (AI) and Machine Learning (ML) represents a transformative advancement, empowering auditors to process large datasets, uncover hidden patterns, and automate repetitive tasks. Although the full implementation of these methodologies faces challenges such as budget constraints and skill shortages, the adoption of adaptive and intelligent auditing practices has become a strategic necessity to safeguard assets and build trust in an increasingly interconnected world.

Definition and Basic Concepts of Access Control

In information security literature, there is a fundamental distinction between the concepts of authorization and access control. Authorization refers to the specification of access rights, while access control focuses on the enforcement of those rights. (Kizza, 2020) defines access control as the process of determining who is allowed to perform what actions on specific objects based on a defined policy. Thus, access control can be understood as the mechanism for implementing the access rights established in authorization policies. It ensures data security by protecting assets and sensitive information from unauthorized access by specified subjects, thereby helping to prevent information leakage or improper modification by potentially malicious parties.

An access control model functions as a framework that defines how authorization is enforced. It determines which parameters must be evaluated to decide whether a subject's access to a protected resource should be granted or denied.

According to Stallings (2018), access control systems operate by receiving access requests, evaluating them against established policies, and producing a final decision in the form of granting or denying access (allow or deny) as a means of enforcing security policies. Access control functions as a fundamental security mechanism that protects system resources from unauthorized access while ensuring that only users with appropriate permissions can interact with protected assets. It operates by evaluating access requests against predefined policies to determine whether such requests comply with the permitted level of access. By enforcing these policies, access control helps prevent unauthorized actions, reduce the risk of data breaches, and safeguard sensitive information within organizational systems (Golightly et al., 2023).

METHOD

This study employs the Systematic Literature Review (SLR) method, following the guidelines of the *Preferred Reporting Items for Systematic Reviews and Meta-Analyses* (PRISMA). This approach is chosen because it enables the systematic and structured identification, evaluation, and synthesis of literature, resulting in findings that are objective and replicable (Kitchenham, 2004). This review is guided by the following research questions:

1. What are the main differences among the cybersecurity audit frameworks currently in use?

2. How has the use of cybersecurity audit frameworks evolved in recent years?
3. What are the challenges in conducting cybersecurity audits?
4. What are the main differences among access control mechanisms?
5. What are the trends in the use of access control mechanisms?
6. What are the challenges in implementing access control mechanisms?

In searching for prior studies, the researcher utilized three Scopus-indexed databases: Scopus, Web of Science, and IEEE Xplore. The search was limited to English-language publications within the period of 2020–2025. The keywords were combined using Boolean operators as follows: ("cybersecurity audit" OR "information security audit") AND ("framework" OR "model") AND ("access control"). The search process was carried out by applying predefined inclusion and exclusion criteria as follows:

Table 1. Inclusion and Exclusion Criteria

Dimension	**Inclusion**	**Exclusion**
Time Range	2020 – April 2025	Before 2020
Language	English	Non-English
Document Type	Peer-reviewed journal articles and conference proceedings	Theses, books, editorials, technical reports
Indexing	Indexed in Scopus, Web of Science, or IEEE Xplore	Not indexed in the target databases
Topic	Cybersecurity audit frameworks and/or access control in information systems	Not relevant to the research topic
Accessibility	Full text available	Abstract only; full text not accessible

The article selection process in this study follows the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) flow, which consists of four stages, as shown in the following table

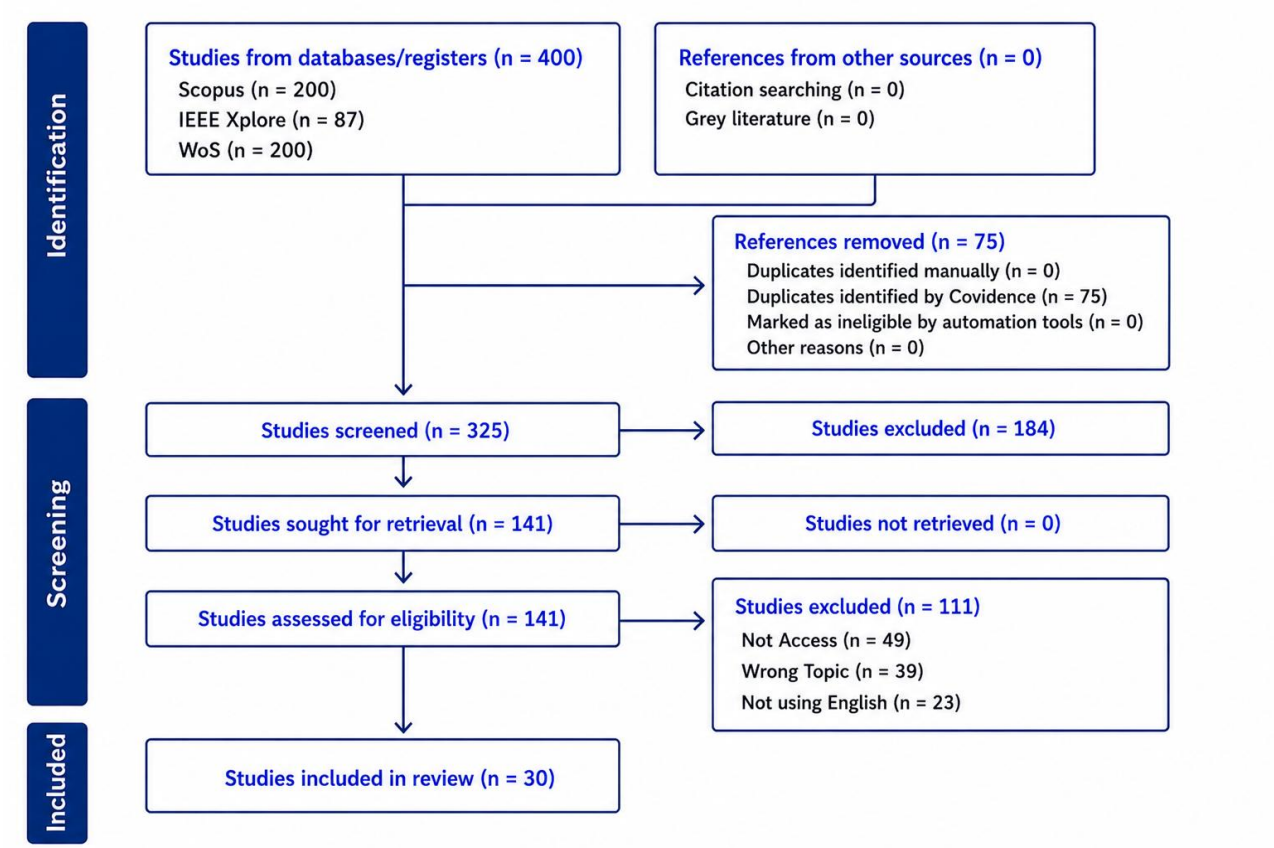

Figure 1 PRISMA

The PRISMA diagram illustrates the article selection process in this study in a systematic manner. In the identification stage, the researcher identified a total of 400 articles from three databases: Scopus, Web of Science, and IEEE Xplore, with no additional records from other sources. Next, 75 duplicate articles were removed, resulting in a set of articles proceeding to the screening stage. During the screening phase, 325 articles were evaluated based on their titles and abstracts, of which 184 were excluded due to lack of relevance. The following stage was the eligibility assessment, where 141 articles were reviewed in full text, all of which were successfully accessed. From this set, 111 articles were further excluded for various reasons, such as lack of appropriate access, irrelevance to the topic, and non-English language. Ultimately, only 30 articles met the criteria and were included in the literature review. The following is a list of the selected prior studies:

Table 2. List of Previous Studies

No	Author (s) & Year	Research Title	Publishing Journal	Country of Study	Methodology	Research Focus	Findings
1	Syed et al. (2024)	Evaluating the Effectiveness of Cybersecurity Protocols in SAP System Upgrades	Iconic Research and Engineering (IRE) Journals	USA	Comparative analysis and case studies	Effectiveness of cybersecurity protocols in SAP upgrades (administrative vs technical)	Requires a holistic approach combining governance and advanced technologies (AI, ML, quantum encryption)
2	Adesokan-Imran (2025)	The Impact of Cybersecurity Governance on National Security by Strengthening Critical Infrastructure through IT Auditing and Risk Management.	Asian Journal of Research in Computer Science	Nigeria	Quantitative statistical analysis	ybersecurity governance impact on national infrastructure	NIST + ISO reduces cyber exploitation significantly; audits and risk management improve resilience
3	Andreanov & Maisyarah (2025)	Cybersecurity Audit and IT Risk Management	2nd International Conference on Islamic Community Studies (ICICS)	Indonesia	Systematic Literature Review	Cybersecurity audits, risk management, and leadership influence	Tech-based audits and leadership improve risk control; transparency increases trust
4	Olawore et al. (2025)	AI-Driven Cybersecurity Governance in Financial Services: Enhancing	Iconic Research and Engineering (IRE) Journals.	USA & Nigeria	Literature review	AI-driven cybersecurity governance	XAI improves transparency and detection; regulation needed for

		Ethical Auditing, Automated Compliance Monitoring and Explainable AI for Stakeholder Trust.					bias/privacy
5	Abbas et al. (2021)	Blockchain-assisted secured data management framework for health information analysis based on Internet of Medical Things.	Personal and Ubiquitous Computing (Springer	Saudi Arabia & Pakistan, Tunisia and India	Experimental framework (BSDMF)	Secure IoMT healthcare data	High accuracy, improved efficiency and latency
6	Zhao et al.(2024)	Blockchain-Based Lightweight Authentication Mechanisms for Industrial Internet of Things and Information Systems	International Journal on Semantic Web and Information Systems.	China	Experimental + comparative	Cross-domain authentication in IIoT	Higher throughput and strong attack resistance
7	Akbar et al. (2024)	Blockchain-based cyber-security trust model with multi-risk protection scheme for secure data transmission in cloud computing	Cluster Computing (Springer)	Oman, Uni Emirat Arab (UEA), India, and Chili.	Simulation (MATLAB)	Secure cloud data transmission	High accuracy, fast encryption, strong security
8	Akhtar & Rawol (2024)	Enhancing Cybersecurity through Artificial Intelligence (AI) - Powered Security	IT Journal Research and Development (ITJRD	UK & Bangladesh	Mixed (survey + experiment)	AI-powered cybersecurity	Improves detection accuracy and enables real-time threat response

		Mechanisms					
9	Faruq (2025)	A Meta-Analysis of Cybersecurity Framework Integration in GRC Platforms: Evidence from U.S. Enterprise Audits.	Journal of Sustainable Development and Policy	USA	Meta-analysis	Framework integration in GRC	Enhances audit performance and compliance
10	Folorunso et al. (2024)	The impact of ISO security standards on enhancing cybersecurity posture in organizations	World Journal of Advanced Research and Reviews (WJARR).	USA & India	Literature review	ISO standards in cybersecurity	Improves risk management and compliance
11	McIntosh et al. (2024)	From COBIT to ISO 42001: Evaluating Cybersecurity Frameworks for Opportunities, Risks, and Regulatory Compliance in Commercializing Large Language Models	Computers & Security, Elsevier	Australia and New Zealand (La Trobe University., Massey University., Victoria Univ.)	Qualitative analysis	Frameworks for AI/LLM governance	ISO 42001 strongest; all frameworks need updates
12	Pal, D orri & Jurdak (2022)	Blockchain for IoT Access Control: Recent Trends and Future Research Directions	Journal of Network and Computer Applications, Vol. 203, Elsevier	Australia	Systematic Literature Review	Blockchain IoT access control	Blockchain improves security but faces scalability issues
13	Toussaint et al. (2024)	Industry 4.0 Data Security: A Cybersecurity Frameworks Review	Journal of Industrial Information Integration, Vol. 39, Elsevier	France & USA	Literature review + analisis komparatif framework	Industry 4.0 security frameworks	No universal framework; customization required

14	Vuko et al. (2025)	Key Drivers of Cybersecurity Audit Effectiveness: A Neo-Institutional Perspective	International Journal of Auditing, Vol. 29(1), pp. 188–206, Wiley	Kroasia & Australia	Quantitative survey	Audit effectiveness drivers	Certification and regulation improve audit effectiveness
15	Ameer et al. (2023)	Hybrid Approaches (ABAC and RBAC) Toward Secure Access Control in Smart Home IoT	IEEE Transactions on Dependable and Secure Computing, IEEE	USA	Model design	Hybrid access control (ABAC+RBAC)	More flexible and suitable for IoT
16	Ragothaman et al. (2023)	Access Control for IoT: A Survey of Existing Research, Dynamic Policies and Future Directions	Sensors, 23(4):1805, MDPI	USA	Survey	IoT access control models	Blockchain promising but scalability issues remain
17	Punia et al. (2024)	A Systematic Review on Blockchain-Based Access Control Systems in Cloud Environment	Journal of Cloud Computing, Vol. 13, Art. 146, Springer	India & UK	Systematic review	Blockchain access control (cloud)	Smart contracts effective but scalability challenges
18	Yeoh, Liu, Shore & Jiang (2023)	Zero Trust Cybersecurity : Critical Success Factors and a Maturity Assessment Framework	Computers & Security, Vol. 133, Elsevier	Australia (Univ. of South Australia)	Framework development	Zero Trust Architecture	Effective but complex and costly
19	Singh et al. (2023)	Blockchain-Enabled Access Control to Prevent Cyber Attacks in IoT:	Frontiers in Big Data, Vol. 5, Frontiers	India	Systematic review	Blockchain IoT access control	Ethereum dominant; scalability issues persist

		Systematic Literature Review					
20	Aftab et al. (2022)	Traditional and Hybrid Access Control Models: A Detailed Survey	Security and Communication Networks (Hindawi)	Pakistan & China	Comparative review	Access control models	Hybrid models outperform traditional ones
21	Omotunde & Ahmed (2023)	A Comprehensive Review of Security Measures in Database Systems: Assessing Authentication, Access Control, and Beyond	Mesopotamian Journal of Cybersecurity	Saudi & Canada	Literature review	Database security mechanisms	Requires multi-layered security approach
22	Jiang et al. (2023)	IoT Access Control Model Based on Blockchain and Trusted Execution Environment	Processes (MDPI)	China	Model + experiment	Blockchain + TEE access control	Improves security and auditability
23	Hu et al. (2023)	N-Accesses: A Blockchain-Based Access Control Framework for Secure IoT Data Management	Sensors (MDPI)	China	Framework design	Blockchain IoT data access control	Enhances control and auditability, minor scalability limits
24	Mohamed et al. (2022)	A Systematic Literature Review for Authorization and Access Control: Definitions, Strategies and Models	International Journal of Web Information Systems	Austria	Systematic Literature Review	Access control classification	Clear taxonomy improves model selection
25	Zhai et al.	Blockchain-Based Internet	Applied Sciences	China	Model	Blockchain +	Improves flexibility and

	(2022)	of Things Access Control Technology in Intelligent Manufacturing	(MDPI)		design	ABAC	efficiency
26	Ilori et al. (2022)	Cybersecurity Auditing in the Digital Age: A Review of Methodologies and Regulatory Implications	Journal of Frontiers in Multidisciplinary Research	Canada & Nigeria	Systematic Literature Review	Cybersecurity auditing methods	Modern audits are proactive but face integration challenges
27	Reuben-Owoh & Haig (2025)	A Systematic Review of Voluntary Cybersecurity Standards and Frameworks	International Journal of Information Security	United Kingdom	Systematic Literature Review	Cybersecurity standards/frameworks	ISO, COBIT, NIST dominant; customization needed
28	Al-Matari et al. (2020)	Integrated Framework for Cybersecurity Auditing	Information Security Journal: A Global Perspective	Mesir	Framework Development + Case Study	Integrated audit framework	Improves threat detection and audit reporting
29	Antunes et al. (2022)	A Client-Centered Information Security and Cybersecurity Auditing Framework	Applied Sciences (MDPI)	Portugal	System implementation	Client-centered audit system	Improves audit efficiency and automation
30	Slapničar et al. (2022)	Effectiveness of Cybersecurity Audit	International Journal of Accounting Information Systems	Multi-country	Quantitative survey	Cybersecurity audit effectiveness	Improves governance but not direct attack reduction

FINDING AND DISCUSSION

Differences in Cybersecurity Audit Frameworks

Differences among cybersecurity audit frameworks indicate significant variations in approaches to managing information security governance, cyber risk management, and the evaluation of organizational security controls. According to Taherdoost (2022), frameworks such as the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27001, the National Institute of Standards and Technology Cybersecurity Framework (NIST-CSF), Control Objectives for Information and

Related Technologies (COBIT), Center for Internet Security Controls (CIS Controls), and the Sarbanes–Oxley Act (SOX) differ in both methodology and implementation orientation. ISO/IEC 27001 emphasizes an Information Security Management System (ISMS)-based approach and continuous improvement, whereas NIST-CSF focuses on a risk management lifecycle through five core functions: identify, protect, detect, respond, and recover. In contrast, COBIT places greater emphasis on the alignment between IT governance and organizational business objectives, meaning its scope extends beyond cybersecurity to overall IT governance (Taherdoost, 2022). These differing orientations demonstrate that each framework is designed to address distinct organizational needs; therefore, no single universal framework can simultaneously satisfy all cybersecurity audit requirements.

In terms of audit methodology, Antunes et al. (2022) explain that ISO 27001-based audit frameworks tend to rely on compliance checklists and systematic, well-documented evaluations of security controls. This approach differs from NIST-CSF, which is more flexible because it allows organizations to prioritize risks according to the level of threats they face. According to Slapničar et al. (2022), NIST-based audits are more adaptive to modern cyber threats because they emphasize continuous monitoring and cyber resilience rather than traditional compliance audits. However, the high degree of flexibility within NIST-CSF also introduces weaknesses, particularly inconsistencies in implementation across organizations due to the absence of strictly standardized controls comparable to ISO 27001 (Slapničar et al., 2022). Thus, the primary trade-off between ISO 27001 and NIST-CSF lies in control stability versus implementation flexibility.

Another distinction can be observed between governance-oriented frameworks, such as COBIT, and technically oriented frameworks, such as CIS Controls. According to Melaku (2023), COBIT positions cybersecurity audits as part of broader organizational governance, with audit processes focusing on accountability, strategic alignment, and value delivery. Conversely, CIS Controls emphasize technical safeguards such as vulnerability management, access control, and intrusion prevention, making them more operational and easier to implement in organizations with limited resources (Melaku, 2023). Haapamäki & Sihvonen (2019) argue that this difference leads to the consequence that COBIT is more effective for large organizations with complex governance structures, while CIS Controls are more suitable for organizations requiring practical and cost-efficient security implementation. Nevertheless, technical frameworks such as CIS Controls are often criticized for lacking comprehensive strategic guidance regarding governance and organizational compliance (Haapamäki & Sihvonen, 2019).

Differences among frameworks are also evident in compliance-based audit approaches compared with risk assessment-based audit approaches. According to Ilori et al. (2022), compliance-based audits such as SOX and ISO tend to focus on regulatory fulfillment and formal documentation, whereas risk assessment-based frameworks such as NIST and the Committee of Sponsoring Organizations of the Treadway Commission (COSO) place greater emphasis on threat identification and dynamic risk impact evaluation. Compliance approaches provide advantages in terms of standardization and ease of regulatory evaluation, but they are often considered less responsive to rapidly evolving cyber threats (Ilori et al., 2022). On the other hand, risk assessment-based audits are more adaptive and proactive but require highly competent personnel and continuous monitoring processes. This trade-off suggests that highly regulated sectors, such as finance and healthcare, are more likely to adopt compliance-oriented frameworks, while technology companies tend to favor risk-oriented approaches.

In research concerning the effectiveness of cybersecurity audits, Slapničar et al. (2022) developed the Cybersecurity Audit Index, which consists of planning, performing, and reporting dimensions. This model differs from traditional audit frameworks because it evaluates audit effectiveness not only in terms of control compliance but also based on the overall quality of the audit process. According to Vuko et al. (2025), audit effectiveness is also influenced by institutional factors such as auditor competence, board of directors' support, and collaboration among organizational lines of defense. This perspective suggests that the success of an audit framework is determined not only by technical control structures but also by governance factors and organizational culture. However, the weakness of maturity assessment-based approaches lies in the high level of subjectivity in measuring audit effectiveness, as it heavily depends on auditors' perceptions and the organization's internal conditions (Vuko et al., 2025).

Differences in cybersecurity audit frameworks become increasingly apparent with the integration of emerging technologies such as artificial intelligence (AI) and blockchain. According to Leo (2025), modern frameworks have begun integrating AI for anomaly detection, automated compliance monitoring, and predictive risk assessment. Meanwhile, blockchain-based frameworks, as discussed by Antunes et al. (2022) and various access control studies, introduce a more decentralized and immutable audit approach because all activities are permanently recorded within distributed ledgers. The primary advantage of blockchain lies in the transparency and traceability of audit trails; however, its implementation often faces challenges related to scalability, latency, and high computational costs. Conversely, AI improves audit efficiency and speed but introduces risks associated with black-box decision-making and low explainability in cybersecurity decision-making processes (Leo, 2025). Therefore, integrating emerging technologies into audit frameworks creates trade-offs among automation, transparency, efficiency, and implementation complexity.

In synthesis, various studies demonstrate that differences in cybersecurity audit frameworks are not limited to control structures and audit methodologies but also extend to the underlying philosophies used to manage cyber risks. According to Taherdoost (2022), frameworks such as ISO and SOX emphasize standardization and compliance, whereas NIST and CIS Controls are more adaptive to the dynamics of modern cyber threats. On the other hand, COBIT and other governance-based frameworks seek to connect cybersecurity audits with strategic business alignment. These differences imply that framework selection should consider organizational size, regulatory requirements, available resources, and the complexity of IT infrastructure. Therefore, no framework is entirely superior; the effectiveness of a framework largely depends on the organizational context and the organization's ability to adapt the framework to its operational needs and risk profile. The following table presents a comparison of Cybersecurity Audit Frameworks:

Table 2. Comparison of Cybersecurity Audit Frameworks

Framework	**Main Characteristics**	**Audit Approach**	**Primary Focus**	**Strengths**	**Weaknesses**	**Trade-off / Implications**
ISO/IEC 27001	Based on Information Security Management System (ISMS) and continuous improvement	Compliance-based audit	Information security governance, compliance, and control standardization	Well-structured controls, internationally recognized, supports certification, strong documentation	Less flexible toward emerging threats, complex documentation, costly implementation	Provides high standardization and regulatory assurance, but slower adaptation to dynamic cyber threats
NIST Cybersecurity Framework (NIST-CSF)	Based on risk management lifecycle with Identify, Protect, Detect, Respond, and Recover functions	Risk-based and continuous monitoring	Cyber resilience and adaptive risk management	Flexible, adaptive to modern threats, supports continuous assurance	Implementation inconsistency across organizations due to non-rigid controls	High flexibility and adaptability, but lower implementation consistency
COBIT	IT governance-oriented framework linking cybersecurity with business objectives	Governance and performance audit	Strategic alignment, accountability, and value delivery	Strong integration between IT governance and business strategy	Complex implementation, requires high governance maturity and substantial resources	Strong governance capability, but expensive and difficult to implement
CIS Controls	Technical safeguard-oriented	Technical control	Vulnerability management, access control,	Practical, relatively easy and cost-	Limited support for strategic governance and	Technically effective but weaker in

	framework	assessment	and intrusion prevention	efficient implementation	regulatory compliance	governance and organizational alignment
SOX / Compliance Framework	Focused on formal regulations and internal control compliance	Compliance auditing	Regulatory compliance and accountability	Facilitates regulatory evaluation and formal documentation	Less responsive to rapidly evolving cyber threats	Strong regulatory compliance, but lower adaptability to modern cyber risks
COSO	Risk management and internal control framework	Risk assessment audit	Threat identification and risk impact evaluation	Supports proactive risk-oriented auditing and internal control integration	Requires continuous and complex risk evaluation processes	More proactive in risk management, but demands highly competent auditors

Trends in Cybersecurity Audits: The Most Widely Used and Effective Frameworks

Research trends in cybersecurity audits indicate that frameworks such as ISO/IEC 27001, the NIST Cybersecurity Framework (NIST-CSF), COBIT, and CIS Controls are among the most dominant frameworks used across various industrial sectors. According to Taherdoost (2022), the dominance of ISO 27001 is attributed to its structured approach through the Information Security Management System (ISMS), which can be easily integrated into organizational business processes. Furthermore, ISO 27001 has gained international recognition, encouraging many organizations to adopt it to meet compliance requirements and enhance their information security reputation. According to Antunes et al. (2022), Adebola Folorunso et al. (2024) also explain that ISO/IEC 27001 offers a systematic approach to managing sensitive information and helps organizations identify, manage, and mitigate cybersecurity risks through ISMS while improving regulatory compliance. Its popularity is further reinforced by its position as one of the most comprehensive frameworks for managing opportunities related to Large Language Models (LLMs), while COBIT is considered the framework most aligned with the European Union AI Act (McIntosh et al., 2024). ISO is also supported by the availability of well-documented security controls, making it easier for auditors to conduct systematic compliance evaluations.

In addition to ISO 27001, NIST-CSF has become one of the most widely used frameworks, particularly in organizations that require flexibility and a risk-based approach. According to Faruq (2025), NIST-CSF is widely adopted because it supports the integration of governance, risk management, and compliance (GRC) in a more dynamic manner compared to traditional compliance frameworks. The study demonstrates that organizations using NIST-CSF exhibit stronger threat detection capabilities and better audit preparedness due to its emphasis on continuous monitoring and cyber resilience. This is consistent with the findings of Al-Matari et al. (2021), who argue that NIST is widely utilized because it helps organizations manage cybersecurity risks systematically, following a clear process from risk identification to incident recovery. However, the high flexibility of NIST also creates a trade-off in the form of considerable implementation variation among organizations, meaning that the framework's effectiveness largely depends on the organization's level of security maturity (Faruq, 2025).

Within the context of IT governance, COBIT remains a dominant framework among large organizations and highly regulated sectors. According to Melaku (2023), organizations choose COBIT because the framework effectively connects cybersecurity audits with strategic governance, performance measurement, and business objectives. COBIT's dominance is particularly evident in multinational corporations and financial institutions that require comprehensive integration between IT governance and enterprise-wide risk management. Nevertheless, several studies indicate that COBIT implementation tends to be complex and resource-intensive,

making it less effective for small and medium-sized organizations (Melaku, 2023). This reflects a trade-off between the depth of governance frameworks and ease of implementation.

Another emerging trend is the increasing use of hybrid frameworks that combine multiple standards simultaneously. According to Melaku (2023), modern organizations no longer rely on a single framework but instead integrate ISO 27001, NIST-CSF, COBIT, and CIS Controls to achieve a balance between compliance, governance, and technical protection. Hybrid approaches have become popular because each framework provides complementary strengths. ISO offers formal control structures, NIST provides flexibility in risk management, COBIT supports governance, while CIS Controls deliver more practical technical safeguards. However, integrating multiple frameworks also increases audit complexity, implementation costs, and the demand for highly competent auditors (Antunes et al., 2022).

Trends in cybersecurity audits also demonstrate increasing adoption of automation technologies such as artificial intelligence (AI), machine learning, and blockchain. According to Ilori et al. (2022), AI is increasingly used in continuous auditing, anomaly detection, and predictive analytics because it accelerates audit processes and reduces human error. In addition, AI supports real-time monitoring, enabling organizations to detect threats more quickly compared to traditional periodic audit approaches. However, the use of AI has also been criticized due to concerns regarding limited explainability and potential algorithmic bias, meaning that auditors still need to perform manual validation of AI-generated analyses (Ilori et al., 2022).

Meanwhile, the use of blockchain in cybersecurity audits is growing, particularly in access control systems and audit trail management. According to various studies on blockchain-based access control, blockchain technology is considered effective because it provides immutable audit trails and decentralized verification, thereby improving transparency and data integrity in auditing processes. However, blockchain implementation still faces challenges related to scalability, latency, and high resource consumption, preventing it from fully replacing traditional audit frameworks. Consequently, blockchain is more commonly used as a complementary technology within cybersecurity audit frameworks rather than as a primary framework itself.

Critically, the dominance of a particular framework does not necessarily indicate that it is the most effective framework in every organizational context. According to Slapničar et al. (2022), the effectiveness of cybersecurity audits is influenced more by implementation quality, auditor competence, and governance support than by the mere selection of a framework. Popular frameworks such as ISO 27001 and NIST-CSF may provide strong structures and flexibility, but poor implementation can still result in weak security performance. Conversely, less popular frameworks may prove more effective when tailored to the specific needs of an organization. Therefore, the dominance of certain frameworks reflects organizations' preference for frameworks that balance compliance, flexibility, scalability, and ease of integration with modern business requirements.

Overall, cybersecurity audit trends demonstrate a shift from compliance-based auditing toward risk management-based auditing and continuous assurance. According to Ilori et al. (2022), modern organizations increasingly adopt frameworks that support agility, automation, and cyber resilience rather than focusing solely on formal regulatory compliance. However, studies also indicate that framework popularity is often influenced by regulatory requirements, international recognition, and certification convenience rather than purely by technical effectiveness. Thus, the primary trade-off in cybersecurity audit framework adoption trends lies in balancing global standardization, implementation flexibility, operational efficiency, and the framework's ability to address continuously evolving cyber threats.

Challenges of Cybersecurity Audit Frameworks

According to Taherdoost (2022), one of the primary challenges in implementing cybersecurity audit frameworks is the complexity of translating security standards into practical organizational operations. Frameworks such as ISO/IEC 27001, NIST-CSF, COBIT, and SOX contain different documentation requirements, controls, and audit procedures, making integration with existing business structures and technological systems increasingly difficult. Antunes et al. (2022) further explain that implementation becomes more complicated when organizations must adapt audit checklists, mitigation tasks, and compliance

requirements to dynamic operational needs. In addition, governance-oriented frameworks often require organizational culture changes, business process restructuring, and stronger interdepartmental coordination, which limits the speed and effectiveness of implementation (Melaku, 2023). These findings demonstrate that implementing cybersecurity audit frameworks involves not only technical adaptation but also broader organizational transformation.

The effectiveness of cybersecurity audits also depends heavily on organizational readiness and governance quality rather than solely on the selected framework. According to Slapničar et al. (2022), effective cybersecurity auditing requires organizations to consistently perform planning, execution, and reporting activities. However, many organizations struggle to maintain audit consistency because of limited resources, insufficient continuous monitoring, and the growing complexity of modern IT systems. Vuko et al. (2025) additionally emphasize that weak board-level support and poor coordination among organizational lines of defense significantly reduce audit effectiveness. These challenges become more serious as the role of auditors continues to evolve from compliance inspectors into strategic risk evaluators who must simultaneously understand cybersecurity risks, cloud infrastructure, data analytics, AI-based monitoring, and regulatory compliance (Rahman et al., 2021). Haapamäki and Sihvonen (2019) further argue that modern cybersecurity environments require auditors to possess not only technical expertise but also managerial and business knowledge. Consequently, organizations increasingly face shortages of qualified cybersecurity auditors and must continuously invest in training and upskilling to keep pace with evolving cyber threats (Ilori et al., 2022).

Implementation challenges also differ according to organizational size and infrastructure maturity. Antunes et al. (2022) explain that small and medium-sized enterprises (SMEs) often encounter greater barriers because of limited budgets, lower IT maturity, and shortages of cybersecurity professionals. Many cybersecurity audit tools remain proprietary and expensive, making them difficult for SMEs to adopt effectively. In contrast, large organizations face challenges related to integrating cybersecurity frameworks into extensive governance structures, business processes, and enterprise infrastructures (Melaku, 2023). Yang et al. (2025) additionally note that implementing and upgrading security systems may temporarily reduce operational efficiency because organizations require adaptation periods for new procedures and controls. These findings indicate that both small and large organizations experience implementation difficulties, although the nature of these challenges differs depending on organizational scale and technological complexity.

Another major challenge involves the integration of emerging technologies such as artificial intelligence and blockchain into cybersecurity auditing. Research on AI-powered security mechanisms shows that artificial intelligence improves anomaly detection, predictive analytics, and continuous auditing capabilities, enabling organizations to identify cyber threats more quickly and efficiently. However, AI implementation also introduces concerns regarding explainability, accountability, and algorithmic bias because auditors often struggle to validate automated decisions generated by opaque machine learning models (Ilori et al., 2022). Furthermore, integrating AI into cybersecurity audits requires advanced digital infrastructure, high-quality data, and auditors with machine learning expertise, thereby increasing implementation costs and complexity. Similarly, blockchain-based cybersecurity models improve transparency and create immutable audit trails, but they also introduce scalability, latency, and computational resource challenges. Organizations must additionally adapt traditional audit processes to decentralized verification mechanisms that are still unfamiliar to many auditors. Several studies further note that integrating blockchain with legacy systems often creates interoperability issues because existing infrastructures were not originally designed to support distributed ledger technologies. These developments illustrate that while emerging technologies strengthen cybersecurity capabilities, they simultaneously increase operational complexity and resource requirements.

Regulatory and compliance pressures also represent significant obstacles in implementing cybersecurity audit frameworks. According to Santoso et al. (2021), organizations must simultaneously comply with multiple regulations such as SOX, GDPR, ISO standards, and NIST guidelines, causing audit processes to become increasingly administrative and complex. Haapamäki and Sihvonen (2019) argue that excessive regulatory pressure often encourages organizations to prioritize documentation and audit formalities over substantive security improvements. Ilori et al. (2022) additionally explain that repeated audit processes, assessments, and evidence collection activities may create audit fatigue, particularly in highly regulated industries. This situation

can lead to over-compliance, where organizations become excessively focused on administrative obligations at the expense of operational flexibility and practical cyber resilience. The challenge becomes even more critical in sectors managing essential services and national infrastructure. According to Sardi et al. (2020), healthcare organizations must conduct cybersecurity audits without disrupting medical services or compromising patient safety, highlighting the trade-off between strengthening security controls and maintaining operational continuity.

Finally, cybersecurity audit frameworks face the broader challenge that even well-designed audits cannot always directly prevent cyberattacks. Slapničar et al. (2022) explain that cyber threats continue to evolve more rapidly than formal standardization and auditing processes, requiring organizations to continuously update security controls and mitigation strategies. Melaku (2023) further argues that many organizations still perceive cybersecurity primarily as a technical issue rather than as a strategic governance and business resilience concern. As a result, audit frameworks are often implemented merely to satisfy regulatory obligations rather than to establish a strong organizational security culture.

In synthesis, according to Taherdoost (2022), Antunes et al. (2022), Slapničar et al. (2022), Melaku (2023), Rahman et al. (2021), and Ilori et al. (2022), the most common challenges in implementing cybersecurity audit frameworks involve framework integration, limited auditor competencies, implementation costs, regulatory complexity, and the need for continuous monitoring. Santoso et al. (2021) and Haapamäki and Sihvonen (2019) further emphasize that organizations also face the risk of over-compliance, which may reduce the practical effectiveness of cybersecurity audits. Therefore, successful implementation of cybersecurity audit frameworks requires balancing security, operational flexibility, governance readiness, human resource competencies, and the organization's ability to adapt to continuously evolving cyber threats.

Differences Among Access Control Mechanisms

Cybersecurity governance and access control are inherently interconnected because both support each other in maintaining the security of information systems. Cybersecurity governance frameworks such as ISO/IEC 27001, COBIT, and NIST CSF function to regulate policies, risk management, compliance procedures, and security audit mechanisms at the organizational level. These frameworks provide rules and guidelines regarding how information security should be managed. However, these rules cannot operate effectively without technical mechanisms that directly enforce them within systems. This is where access control plays a crucial role. Access control models such as Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), and Policy-Based Access Control (PBAC) are used to determine who is allowed to access data, when access is granted, and what actions users are permitted to perform within the system. Thus, cybersecurity governance can be understood as the strategic layer that defines security policies and objectives, whereas access control represents the operational layer that enforces those policies in the daily activities of information systems. For example, governance may establish that only certain employees are authorized to access sensitive data, while access control ensures that such rules are automatically implemented within the system. This relationship demonstrates that information security depends not only on technology but also on organizational policies and user behavior. Therefore, effective cybersecurity audits require alignment between governance frameworks and access control mechanisms so that security policies can be implemented consistently and cyber risks can be minimized optimally.

Traditional access control mechanisms such as Discretionary Access Control (DAC), Mandatory Access Control (MAC), and Role-Based Access Control (RBAC) adopt different approaches to managing access rights and user authorization (Mohamed et al., 2022). DAC provides flexibility by allowing data owners to determine access permissions for other users, although this flexibility may increase the risk of misuse because security decisions heavily depend on user judgment. In contrast, MAC applies centralized security-classification policies that enforce stricter control over user access, making it more suitable for highly secure environments. However, the rigidity of MAC reduces its effectiveness in environments requiring dynamic access changes. To address the complexity of access management in large organizations, RBAC was introduced as a mechanism that assigns permissions according to user roles rather than individual identities (Mohamed et al., 2022). This approach improves administrative efficiency because permissions can be managed collectively through

organizational roles. Nevertheless, RBAC may suffer from role explosion when organizations possess excessive combinations of roles and permissions, while its relatively static structure limits its ability to adapt access decisions according to contextual factors such as location, device conditions, or access time (Singh & Singh, 2023).

The limitations of traditional role-based approaches have encouraged the development of more adaptive mechanisms such as Attribute-Based Access Control (ABAC). According to Hu et al. (2023), ABAC enhances access control flexibility by using user, object, and environmental attributes in authorization decisions, making it highly suitable for cloud computing, IoT, and distributed systems that require dynamic authorization. Zhai et al. (2022) further explain that ABAC enables devices in intelligent manufacturing environments to obtain access based on specific operational conditions, while Abbas et al. (2024) note that similar approaches are increasingly adopted in distributed healthcare and IoMT systems. Despite these advantages, ABAC introduces greater policy complexity because administrators must manage large numbers of rules and attribute relationships simultaneously (Hu et al., 2023). This demonstrates that increased contextual flexibility often comes at the cost of more complicated security administration and policy management.

Recent developments in access control have also highlighted the growing importance of blockchain-based mechanisms and Zero Trust Architecture (ZTA). Blockchain-based access control utilizes distributed ledgers and smart contracts to perform authentication and authorization in a decentralized manner, thereby improving auditability and traceability because all access activities are permanently recorded on the blockchain (Hu et al., 2023). Zhai et al. (2022) explain that smart contracts can improve transparency and security in communication among IoT devices, cloud service providers, and system users within intelligent manufacturing environments. Abbas et al. (2024) additionally emphasize that blockchain technologies strengthen data integrity and secure data exchange in the Internet of Medical Things (IoMT). However, blockchain implementation also introduces significant challenges, including latency, high computational resource consumption, and increased system complexity (Singh & Singh, 2023). Alongside blockchain, Zero Trust Architecture has emerged as another major trend because organizations can no longer rely solely on perimeter-based security models. According to Omotunde & Ahmed (2023), Zero Trust adopts the principle of “never trust, always verify,” requiring continuous authentication and behavioral monitoring for all users and devices. This approach is particularly relevant in cloud computing, hybrid infrastructure, and remote access environments where insider threats and unauthorized access risks continue to increase (Singh & Singh, 2023). Nevertheless, continuous monitoring and authentication significantly increase administrative complexity and operational security costs because organizations require more advanced monitoring infrastructures (Hu et al., 2023).

Modern access control trends also demonstrate stronger integration between security mechanisms, privacy protection, and regulatory compliance. According to Omotunde and Ahmed (2023), searchable encryption and encryption-based authorization have become increasingly important because they allow users to search encrypted data without exposing its contents, thereby preserving data confidentiality in cloud and database environments. However, these mechanisms increase computational overhead because encrypted search operations require additional resources. Similarly, trusted execution environments improve the security of access policy execution through secure enclaves, although the integration of hardware and software components significantly increases implementation costs. In addition, organizations increasingly require access control systems that support logging, monitoring, forensic analysis, and audit trails to meet compliance requirements and strengthen cybersecurity governance (Hu et al., 2023). These developments indicate that modern access control mechanisms are evolving beyond simple authorization systems into comprehensive governance-support technologies that integrate security, compliance, monitoring, and operational accountability.

In synthesis, according to Mohamed et al. (2022), Hu et al. (2023), Zhai et al. (2022), Abbas et al. (2024), Omotunde and Ahmed (2023), and Singh and Singh (2023), the evolution of access control mechanisms demonstrates a clear transition from static and centralized models toward more adaptive, context-aware, decentralized, and continuously verified approaches. DAC and MAC emphasize traditional access restriction, RBAC improves administrative efficiency, ABAC enhances contextual flexibility, while blockchain and Zero Trust strengthen transparency, auditability, and continuous verification. However, each mechanism involves

trade-offs among security, flexibility, scalability, management efficiency, implementation complexity, and operational cost. Therefore, no single access control mechanism can be considered universally ideal for all organizational contexts, and organizations must select mechanisms based on their governance requirements, infrastructure maturity, operational needs, and cybersecurity risk profiles

Table 3. Access Control Mechanism Comparison Table

Access Control Mechanism	**Main Characteristics**	**Access Management Approach**	**Security Level**	**Flexibility**	**Scalability**	**Strengths**	**Weaknesses**	**Trade-off / Implications**
Discretionary Access Control (DAC)	Access rights are controlled by data owners	User-based permission assignment	Moderate	High	Limited	Flexible and easy to implement	Vulnerable to insider threats and privilege propagation	High flexibility but weaker security control
Mandatory Access Control (MAC)	Access decisions are based on security classifications and labels	Centralized policy enforcement	Very High	Low	Limited	Strong confidentiality and strict control	Rigid and difficult to adapt to dynamic environments	Strong security but low operational flexibility
Role-Based Access Control (RBAC)	Access rights are assigned according to organizational roles	Role-oriented authorization	High	Moderate	High	Simplifies permission management and administration	Role explosion and limited context-awareness	Efficient administration but less adaptive to dynamic access requirements
Attribute-Based Access Control (ABAC)	Access decisions are based on attributes of users, resources, and environments	Context-aware and policy-based authorization	High	Very High	High	Supports dynamic and fine-grained access control	Complex policy management and configuration	High flexibility but increased administrative complexity
Blockchain-Based Access Control	Uses distributed ledger and smart contracts for decentralized authorization	Decentralized verification and immutable audit trail	Very High	High	Moderate	Strong transparency, traceability, and auditability	Scalability, latency, and high computational cost	Improved trust and security but reduced efficiency and performance
Zero Trust Architecture (ZTA)	Based on “never trust, always verify” principle	Continuous authentication and verification	Very High	High	High	Strong protection against insider threats and unauthorized access	Requires continuous monitoring and complex infrastructure	Higher security assurance but increased operational complexity
Searchable Encryption-Based Access Control	Allows encrypted data search without revealing data content	Encryption-oriented authorization	High	Moderate	Moderate	Enhances privacy and confidentiality	Increased computational overhead during encrypted searches	Strong privacy protection but reduced system performance
Trusted Execution Environment (TEE)-Based Access Control	Uses secure enclaves for policy execution and data processing	Hardware-assisted secure execution	Very High	Moderate	Moderate	Strong protection for sensitive execution environments	High implementation and infrastructure cost	Enhanced execution security but expensive integration

Cloud-Based Access Control	Designed for distributed and cloud environments	Centralized and federated identity management	High	High	Very High	Supports remote access and distributed systems	Complex interoperability and identity synchronization	Scalable access management but difficult cross-platform integration
IoT/IoMT Access Control	Tailored for resource-constrained devices and distributed environments	Lightweight and context-aware authorization	Moderate to High	High	High	Supports dynamic device authentication and distributed communication	Limited device resources and monitoring challenges	Adaptive for IoT ecosystems but constrained by device limitations

Trends in Access Control Mechanisms

According to Mohamed et al. (2022), the rapid development of cloud computing, distributed systems, and IoT has exposed the limitations of traditional access control mechanisms such as DAC and MAC in supporting dynamic access requirements. Modern organizations increasingly require mechanisms that are more flexible, scalable, and adaptive than traditional static models. Consequently, RBAC and ABAC have emerged as the most widely adopted mechanisms because they are better suited to managing access within modern organizational environments. RBAC remains dominant due to its relatively simple implementation and effectiveness in organizations with clearly defined role structures (Mohamed et al., 2022). Omotunde and Ahmed (2023) further explain that RBAC is widely implemented in database systems and enterprise environments because it simplifies permission administration and supports compliance requirements. However, RBAC has also been criticized for its limited flexibility in handling context-aware authorization, while the growing number of roles and permissions may lead to role explosion and increased administrative complexity (Singh & Singh, 2023).

At the same time, ABAC has gained increasing attention because it enables access decisions based on user, device, location, and environmental attributes (Hu et al., 2023). This capability makes ABAC particularly suitable for intelligent manufacturing, IoT, cloud computing, and distributed environments that require dynamic authorization mechanisms (Zhai et al., 2022). Abbas et al. (2021) also note that ABAC is widely adopted in IoMT and cloud systems because it supports distributed access management more effectively than traditional role-based approaches. Nevertheless, the greater flexibility provided by ABAC also increases policy complexity and requires more advanced security administration to manage attributes, policies, and authorization rules effectively (Omotunde & Ahmed, 2023). These findings indicate that the evolution from RBAC to ABAC reflects a broader transition from static authorization models toward more context-aware and adaptive access control mechanisms.

Another major trend in modern access control is the increasing adoption of blockchain-based mechanisms and Zero Trust Architecture (ZTA). According to Hu et al. (2023), blockchain-based access control provides immutable audit trails, decentralized authentication, and trusted authorization without relying on a central authority. Zhai et al. (2022) explain that blockchain is particularly relevant in intelligent manufacturing environments because smart contracts improve transparency and security in communication among IoT devices, cloud services, and system users. Similarly, Abbas et al. (2021) emphasize that the healthcare sector has increasingly adopted blockchain technologies to strengthen data integrity and improve user access auditability. However, Singh and Singh (2023) argue that blockchain-based access control still faces significant challenges related to latency, computational overhead, and resource consumption. Alongside blockchain, Zero Trust Architecture has become another important trend because organizations can no longer rely solely on perimeter-based security approaches (Omotunde & Ahmed, 2023). Zero Trust supports continuous authentication and behavioral monitoring, making it highly relevant for hybrid cloud systems, remote working environments, and BYOD practices (Singh & Singh, 2023). Nevertheless, Hu et al. (2023) point out that implementing Zero Trust significantly increases the need for continuous monitoring and verification, thereby raising operational security costs and administrative complexity.

Modern access control trends also demonstrate stronger integration between security mechanisms and compliance requirements. Organizations increasingly require mechanisms that not only control access but also provide logging, monitoring, and audit trails to support regulatory compliance and forensic analysis (Omotunde & Ahmed, 2023). Hu et al. (2023) explain that blockchain-based mechanisms are particularly attractive because immutable logging improves transparency and accountability. Abbas et al. (2021) further emphasize that auditability has become a critical requirement in healthcare systems and distributed environments, where organizations must ensure that user access can be securely monitored and traced. This trend illustrates that modern access control is no longer limited to authorization management but has evolved into a broader governance and compliance-support mechanism.

In synthesis, according to Mohamed et al. (2022), Hu et al. (2023), Zhai et al. (2022), Abbas et al. (2021), Omotunde and Ahmed (2023), and Singh and Singh (2023), trends in access control mechanisms are shifting from static models toward more adaptive, context-aware, decentralized, and continuously verified approaches. RBAC remains dominant because of its ease of implementation and administrative efficiency, while ABAC continues to grow due to its support for dynamic authorization and contextual flexibility. Blockchain and Zero Trust are increasingly adopted because they enhance transparency, auditability, and continuous verification in cloud and IoT environments. However, the growing dominance of these mechanisms does not necessarily indicate complete effectiveness, as organizations must still balance security, flexibility, implementation complexity, scalability, and operational efficiency when selecting appropriate access control models.

Challenges of Access Control Mechanisms

According to Mohamed et al. (2022), one of the primary challenges in implementing access control mechanisms is the complexity of managing access rights in organizations with large numbers of users, systems, and connected devices. Changes in roles, permissions, and organizational structures often create administrative difficulties, particularly in RBAC and ABAC environments. These challenges become even more significant in cloud computing, distributed systems, and IoT environments, where organizations require access control mechanisms that are scalable, adaptive, and capable of supporting dynamic authorization. Scalability issues are particularly evident in blockchain-based access control systems because increasing numbers of transactions and authorization requests may significantly affect system performance (Hu et al., 2023). Zhai et al. (2022) further explain that implementing access control in intelligent manufacturing environments requires integration among IoT devices, smart contracts, and cloud services, thereby increasing overall system complexity. Similarly, Abbas et al. (2021) note that distributed systems such as the Internet of Medical Things (IoMT) face additional challenges related to data synchronization and real-time access management among heterogeneous medical devices.

Another major challenge involves interoperability and the integration of modern access control mechanisms with legacy systems. According to Omotunde and Ahmed (2023), many organizations still rely on older infrastructures that do not support context-aware authorization or dynamic access management. As a result, interoperability among systems becomes increasingly difficult when organizations combine multiple access control models within cloud and distributed environments (Mohamed et al., 2022). Singh and Singh (2023) also argue that hybrid infrastructures, remote access environments, and cross-platform systems complicate identity synchronization and access management. At the same time, blockchain-based mechanisms, while improving auditability and transparency through immutable logging and decentralized verification, also introduce latency and high computational resource consumption (Hu et al., 2023). Zhai et al. (2022) explain that smart contracts may slow authorization processes as transaction volumes increase, while Abbas et al. (2021) highlight the trade-off in healthcare systems between strengthening medical data security and ensuring rapid access to patient information. These findings demonstrate that stronger security mechanisms often reduce operational efficiency and increase infrastructure complexity.

Monitoring and continuous verification also represent critical implementation challenges in modern access control systems. According to Omotunde and Ahmed (2023), the growing volume of user activities and system logs in cloud and distributed environments makes monitoring and auditability increasingly difficult to manage. This challenge is amplified in Zero Trust Architecture (ZTA), where continuous verification and real-time

monitoring are required for every user and device interaction (Singh & Singh, 2023). Hu et al. (2023) further explain that continuous authentication significantly increases administrative complexity and operational security costs because organizations must maintain more advanced monitoring infrastructures. In addition, human error and policy misconfiguration remain among the leading causes of unauthorized access because modern access policies are often too complex to manage manually (Mohamed et al., 2022).

Another important issue is the trade-off between usability and security in modern access control implementation. According to Mohamed et al. (2022), security mechanisms that are excessively strict may reduce user convenience and negatively affect organizational productivity. Omotunde and Ahmed (2023) explain that users frequently perceive multi-factor authentication, strict authorization policies, and continuous verification as operational barriers. Conversely, Singh and Singh (2023) argue that overly flexible access control mechanisms may increase the risks of insider threats and privilege abuse. Furthermore, organizations often face limitations in human resources and technical expertise when implementing modern access control systems. Abbas et al. (2021) and Hu et al. (2023) explain that organizations require administrators and auditors with expertise in blockchain, IoT security, cloud access management, and policy enforcement. Zhai et al. (2022) additionally note that implementing modern access control mechanisms requires substantial investment in infrastructure and training, making adoption difficult for organizations with limited resources.

In synthesis, according to Mohamed et al. (2022), Hu et al. (2023), Zhai et al. (2022), Abbas et al. (2021), Omotunde and Ahmed (2023), and Singh and Singh (2023), the implementation of modern access control mechanisms is challenged by issues related to scalability, interoperability, policy complexity, monitoring requirements, and continuous verification. Organizations must also balance security, operational efficiency, usability, and flexibility when selecting and implementing access control models. Therefore, the successful implementation of access control mechanisms depends not only on choosing appropriate technologies but also on governance quality, organizational readiness, human resource competencies, and the maturity of the supporting security infrastructure.

CONCLUSION

This study demonstrates that cybersecurity audit frameworks and access control mechanisms continue to evolve in response to the increasing complexity of cyber threats, digital transformation, cloud computing, IoT, and distributed information systems. Based on the systematic literature review of 30 Scopus-indexed studies published between 2020 and 2025, it can be concluded that no single cybersecurity audit framework is universally capable of addressing all organizational security needs. Frameworks such as ISO/IEC 27001, NIST Cybersecurity Framework (NIST-CSF), COBIT, CIS Controls, SOX, and COSO each possess distinct orientations, strengths, and limitations. ISO/IEC 27001 and SOX emphasize standardization, compliance, and formal documentation, whereas NIST-CSF and COSO prioritize risk-based and adaptive approaches. Meanwhile, COBIT focuses on strategic IT governance alignment, while CIS Controls provide more practical and technical security safeguards. Consequently, organizations increasingly adopt hybrid approaches that integrate multiple frameworks simultaneously in order to balance governance, compliance, flexibility, and technical protection.

The findings also reveal a significant transformation in cybersecurity auditing practices, shifting from traditional compliance-based auditing toward continuous, risk-oriented, and technology-driven auditing. Emerging technologies such as Artificial Intelligence (AI), Machine Learning (ML), blockchain, and continuous monitoring systems are increasingly integrated into cybersecurity audits to enhance anomaly detection, predictive analytics, automation, transparency, and auditability. However, these technologies also introduce new challenges, including explainability issues, algorithmic bias, scalability limitations, interoperability problems, and high implementation costs. Therefore, organizations must carefully balance automation, operational efficiency, transparency, and governance accountability when integrating emerging technologies into cybersecurity auditing processes.

Furthermore, this study confirms that the effectiveness of cybersecurity audits is not determined solely by the selected framework but is also strongly influenced by organizational readiness, governance quality, auditor

competence, management support, and cybersecurity culture. Many organizations still encounter major challenges related to framework integration, regulatory complexity, limited human resources, implementation costs, and the need for continuous monitoring. Excessive compliance orientation may also create "over-compliance," where organizations prioritize documentation and administrative requirements over substantive cybersecurity resilience improvements. Thus, successful cybersecurity governance requires not only technical controls but also strategic organizational commitment and adaptive governance mechanisms.

In terms of access control mechanisms, this review identifies a clear evolution from traditional static models toward more adaptive, context-aware, decentralized, and continuously verified approaches. Traditional mechanisms such as DAC, MAC, and RBAC remain widely used due to their simplicity and administrative efficiency; however, they exhibit limitations in dynamic and distributed environments. Consequently, more flexible models such as ABAC, blockchain-based access control, Zero Trust Architecture (ZTA), searchable encryption, and Trusted Execution Environments (TEE) are increasingly adopted to address modern cybersecurity requirements in cloud computing, IoT, IoMT, and hybrid infrastructures. Blockchain and Zero Trust approaches are particularly prominent because they strengthen transparency, auditability, and continuous verification. Nevertheless, these mechanisms also increase implementation complexity, monitoring requirements, operational costs, and computational overhead.

Overall, this study concludes that both cybersecurity audit frameworks and access control mechanisms involve unavoidable trade-offs among security, flexibility, scalability, governance complexity, operational efficiency, and implementation cost. Therefore, organizations must select and adapt frameworks and access control mechanisms according to their specific risk profiles, regulatory requirements, technological maturity, operational needs, and governance capabilities. The study also highlights that future cybersecurity governance will increasingly depend on adaptive, intelligent, and continuously monitored security ecosystems that integrate governance frameworks, automated auditing technologies, and context-aware access control systems.

Finally, this research contributes theoretically by providing a comprehensive synthesis of recent developments in cybersecurity audit frameworks and access control mechanisms from 2020–2025, while also addressing gaps in previous literature through the integration of governance-oriented auditing perspectives with technical access control discussions. Practically, the findings may serve as a reference for auditors, cybersecurity practitioners, regulators, and organizations in designing more effective, flexible, and resilient cybersecurity governance strategies in the face of continuously evolving cyber threats.

This study provides important theoretical and practical implications for the development of cybersecurity governance and access control mechanisms in modern information systems. Theoretically, this study expands the literature on cybersecurity auditing by integrating discussions on cybersecurity audit frameworks and access control mechanisms in a comprehensive manner, while also highlighting the paradigm shift from compliance-based approaches toward more adaptive, risk-based, and continuous assurance-oriented approaches. Practically, the findings indicate that organizations cannot rely on a single framework alone; instead, they should adopt a hybrid approach by combining frameworks such as ISO/IEC 27001, NIST-CSF, COBIT, and CIS Controls to achieve a balance between compliance, governance, flexibility, and technical protection. Furthermore, organizations need to improve auditor competencies and infrastructure readiness in responding to the implementation of modern technologies such as Artificial Intelligence (AI), blockchain, cloud computing, and the Internet of Things (IoT), as these technologies can enhance audit effectiveness and system security despite introducing challenges related to complexity, costs, and increased monitoring requirements.

For future research, it is recommended that empirical studies be conducted across various industries, such as finance, healthcare, education, and government sectors, in order to evaluate the effectiveness of cybersecurity audit framework implementation more specifically. Future studies should also develop quantitative evaluation models to measure cybersecurity audit effectiveness and organizational security maturity levels more objectively. In addition, further research is needed to explore the integration of AI, machine learning, blockchain, and Zero Trust Architecture into cybersecurity auditing and access control, particularly regarding explainability, decision transparency, scalability, and operational efficiency. In the context of access control,

future studies may focus on developing hybrid access control models that combine the strengths of RBAC, ABAC, and Zero Trust to provide greater flexibility and suitability for cloud computing, IoT, and distributed system environments. Therefore, future research is expected to contribute to the development of more adaptive, integrated, and resilient cybersecurity governance models that are capable of addressing continuously evolving cyber threats.

REFERENCES

1. Abbas, A., Alroobaea, R., Krichen, M., Rubaiee, S., Vimal, S., & Almansour, F. M. (2024). Blockchain-assisted secured data management framework for health information analysis based on Internet of Medical Things. Personal and Ubiquitous Computing, 28(1), 59–72. https://doi.org/10.1007/s00779-021-01583-8
2. Adebola Folorunso, Viqaruddin Mohammed, Ifeoluwa Wada, & Bunmi Samuel. (2024). The impact of ISO security standards on enhancing cybersecurity posture in organizations. World Journal of Advanced Research and Reviews, 24(1), 2582–2595. https://doi.org/10.30574/wjarr.2024.24.1.3169
3. Al-Matari, O. M. M., Helal, I. M. A., Mazen, S. A., & Elhennawy, S. (2021). Integrated framework for cybersecurity auditing. Information Security Journal, 30(4), 189–204. https://doi.org/10.1080/19393555.2020.1834649
4. Antunes, M., Maximiano, M., & Gomes, R. (2022). A Client-Centered Information Security and Cybersecurity Auditing Framework. Applied Sciences (Switzerland), 12(9). https://doi.org/10.3390/app12094102
5. Bernadette Bristol-Alagbariya, Latifat Omolara Ayanponle, & Damilola Emmanuel Ogedengbe. (2022). Developing and implementing advanced performance management systems for enhanced organizational productivity. World Journal of Advanced Science and Technology, 2(1), 039–046. https://doi.org/10.53346/wjast.2022.2.1.0037
6. Dagilienė, L., & Klovienė, L. (2019). Motivation to use big data and big data analytics in external auditing. Managerial Auditing Journal, 34(7), 750–782. https://doi.org/10.1108/MAJ-01-2018-1773
7. Dimitris Balios, Panagiotis Kotsilaras, Nikolaos Eriotis, & Dimitrios Vasiliou. (2020). Big Data, Data Analytics and External Auditing. Journal of Modern Accounting and Auditing, 16(5). https://doi.org/10.17265/1548-6583/2020.05.002
8. Faruq, M. O. (2025). A Meta-Analysis Of Cybersecurity Framework Integration In Grc Platforms: Evidence From U.S. Enterprise Audits. Journal of Sustainable Development and Policy, 01(01), 224–249. https://doi.org/10.63125/kwhkmb57
9. Federal Bureau of Investigation. (2024). Internet Crime Report. https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf
10. Geerman, G. et al. (2026). Colonial Pipeline Ransomware Attack: Computational Analysis Based on an Adaptive Network Model. Focus on Artificial Intelligence in Intelligent Systems Design .
11. Gepp, A., Linnenluecke, M. K., O'Neill, T. J., & Smith, T. (2018). Big data techniques in auditing research and practice: Current trends and future opportunities. Journal of Accounting Literature, 40, 102–115. https://doi.org/10.1016/j.acclit.2017.05.003
12. Golightly, L., Modesti, P., Garcia, R., & Chang, V. (2023). Securing distributed systems: A survey on access control techniques for cloud, blockchain, IoT and SDN. In Cyber Security and Applications (Vol. 1). KeAi Communications Co. https://doi.org/10.1016/j.csa.2023.100015
13. Haapamäki, E., & Sihvonen, J. (2019). Cybersecurity in accounting research. In Managerial Auditing Journal (Vol. 34, Number 7, pp. 808–834). Emerald Group Holdings Ltd. https://doi.org/10.1108/MAJ-09-2018-2004
14. Hu, T., Yang, S., Wang, Y., Li, G., Wang, Y., Wang, G., & Yin, M. (2023). N-Accesses: A Blockchain-Based Access Control Framework for Secure IoT Data Management. Sensors, 23(20). https://doi.org/10.3390/s23208535
15. Ilori, O., Lawal, C. I., Friday, S. C., Isibor, N. J., & Eke, E. C. C.-. (2022). Cybersecurity Auditing in the Digital Age: A Review of Methodologies and Regulatory Implications. Journal of Frontiers in Multidisciplinary Research, 3(1), 174–187. https://doi.org/10.54660/.ijfmr.2022.3.1.174-187

16. International Business Machines. (2024). Cost of a data breach 2024: Financial industry.
17. Kitchenham, B. (2004). Procedures for Performing Systematic Reviews. NICTA Technical Report.
18. Kizza, J. M. (2020). Access Control and Authorization. Guide to Computer Network Security. Texts in Computer Science. Springer.
19. Leo, O. (2025). AI-Driven Cybersecurity Governance in Financial Services: Enhancing Ethical Auditing, Automated Compliance Monitoring and Explainable AI for Stakeholder Trust SANUEL OLATUNJI OLAWORE 1 , CHUKWUEBUKA OKOLI 2 , OREOLUWA ABIMBOLA SERIFAT 3 , BLESSING UNWANA UNOH 4 UGOCHUKWU DANIEL OFURUM. IRE Journals.
20. McIntosh, T. R., Susnjak, T., Liu, T., Watters, P., Xu, D., Liu, D., Nowrozy, R., & Halgamuge, M. N. (2024). From COBIT to ISO 42001: Evaluating cybersecurity frameworks for opportunities, risks, and regulatory compliance in commercializing large language models. Computers and Security, 144. https://doi.org/10.1016/j.cose.2024.103964
21. Meegammana, N. W., Vishva, N. P., & Sri, K. (2020). SolarWinds Attack 2020: A Cyber Security and Legal Perspective. https://doi.org/DOI:10.13140/RG.2.2.13076.56963
22. Melaku, H. M. (2023). A Dynamic and Adaptive Cybersecurity Governance Framework. Journal of Cybersecurity and Privacy, 3(3), 327–350. https://doi.org/10.3390/jcp3030017
23. Mohamed, A. K. Y. S., Auer, D., Hofer, D., & Küng, J. (2022). A systematic literature review for authorization and access control: definitions, strategies and models. In International Journal of Web Information Systems (Vol. 18, Numbers 2–3, pp. 156–180). Emerald Publishing. https://doi.org/10.1108/IJWIS-04-2022-0077
24. Omotunde, H., & Ahmed, M. (2023). A Comprehensive Review of Security Measures in Database Systems: Assessing Authentication, Access Control, and Beyond. In Mesopotamian Journal of CyberSecurity (Vol. 2023, pp. 115–133). Mesopotamian Academic Press. https://doi.org/10.58496/MJCS/2023/016
25. Pahlawati, C. S., Pebriani, D., Studi Teknik Informatika, P., & Tinggi Teknologi Wastukancana, S. (2025). Analisis Insiden Kebocoran Data 91 Juta Akun Tokopedia: Dampak Dan Upaya Penanganannya. Integrative Perspectives of Social and Science Journal, 2(3), 4858.
26. Rahman, F., Putri, G., Wulandari, D., Pratama, D., & Permadi, E. (2021). Auditing in the Digital Era: Challenges and Opportunities for Auditor. Golden Ratio of Auditing Research, 1(2), 86–98. https://doi.org/10.52970/grar.v1i2.367
27. Santoso, F., Wijaya, A., Pramudita, C., Permata, D., & Suryani, E. (2021). The Influence of Government Regulations on Auditing Practices: A Qualitative Research. Golden Ratio of Auditing Research, 1(2), 54–63. https://doi.org/10.52970/grar.v1i2.366
28. Sardi, A., Rizzi, A., Sorano, E., & Guerrieri, A. (2020). Cyber risk in health facilities: A systematic literature review. In Sustainability (Switzerland) (Vol. 12, Number 17). MDPI. https://doi.org/10.3390/su12177002
29. Sayankar, V. N. (2013). A Review on Information Systems Audit. Research J. Engineering and Tech, 4(3). www.anvpublication.org
30. Singh, I., & Singh, B. (2023). Access management of IoT devices using access control mechanism and decentralized authentication: A review. Measurement: Sensors, 25. https://doi.org/10.1016/j.measen.2022.100591
31. Slapničar, S., Vuko, T., Čular, M., & Drašček, M. (2022). Effectiveness of cybersecurity audit. International Journal of Accounting Information Systems, 44. https://doi.org/10.1016/j.accinf.2021.100548
32. Stallings, W. (2018). Network Security Essentials Applications and Standards (6th ed.). Pearson Education Limited.
33. Sulistyowati, D., Handayani, F., & Suryanto, Y. (2020). Comparative Analysis and Design of Cybersecurity Maturity Assessment Methodology Using NIST CSF, COBIT, ISO/IEC 27002 and PCI DSS. International Journal On Informatics Visualization.
34. Taherdoost, H. (2022). Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview. In Electronics (Switzerland) (Vol. 11, Number 14). MDPI. https://doi.org/10.3390/electronics11142181

35. Tharwat, H., Hafez, S. T., Elgohary, I. E., & Hassanein, A. (2025). A decade of cybersecurity research in internal auditing: bibliometric mapping and future research agenda. In Discover Sustainability (Vol. 6, Number 1). Springer Nature. https://doi.org/10.1007/s43621-025-02031-w
36. Toussaint, M., Krima, S., & Panetto, H. (2024). Industry 4.0 data security: A cybersecurity frameworks review. In Journal of Industrial Information Integration (Vol. 39). Elsevier B.V. https://doi.org/10.1016/j.jii.2024.100604
37. Vuko, T., Slapničar, S., Čular, M., & Drašček, M. (2025). Key drivers of cybersecurity audit effectiveness: A neo-institutional perspective. International Journal of Auditing, 29(1), 188–206. https://doi.org/10.1111/ijau.12365
38. World Economic Forum. (2025). Resilience Pulse Check: Harnessing Collaboration to Navigate a Volatile World. https://reports.weforum.org/docs/WEF_Resilience_Pulse_Check_2025.pdf
39. Yang, X., Tu, H., Li, Y., & Wang, Q. (2025). The impact of IT system implementation and upgrade on firm operational and financial performance. Journal of Digital Management, 1(1). https://doi.org/10.1007/s44362-025-00005-6
40. Zhai, P., He, J., & Zhu, N. (2022). Blockchain-Based Internet of Things Access Control Technology in Intelligent Manufacturing. Applied Sciences (Switzerland), 12(7). https://doi.org/10.3390/app12073692