JOURNAL OF MANAGEMENT AND BUSINESS SOLUTIONS

An Integrated Cybersecurity Audit Model for Intelligent Systems with Emphasis on Risk Assessment and Digital Resilience

1. Amir. Naseri : Department of Accounting, Ara.C., Islamic Azad University, Aras, Iran
2. Heydar. Mohammadzadeh Salteh*: Department of Accounting, Mara.C., Islamic Azad University, Marand, Iran
3. Robab. Mogadamzadeh: Department of Accounting, Mara.C., Islamic Azad University, Marand, Iran

*corresponding author's email: h_salteh@iau.ac.ir

ABSTRACT

The present study aimed to develop an integrated cybersecurity auditing model for intelligent systems with an emphasis on risk assessment and digital resilience within contemporary digital and AI-driven organizational environments. This study was conducted using a qualitative exploratory approach based on grounded theory-oriented analysis. The statistical population consisted of experts in internal auditing, cybersecurity, information technology risk management, chief information officers (CIOs), members of audit committees, and university professors specializing in intelligent systems and cybersecurity governance in Tehran. Participants were selected through purposive and snowball sampling methods, and data collection continued until theoretical saturation was achieved. In total, 23 in-depth semi-structured interviews were conducted. The collected data were transcribed and analyzed using MAXQDA software through open, axial, and selective coding procedures. To ensure the trustworthiness of the findings, member checking, peer review, and continuous comparison techniques were utilized throughout the analytical process. The findings revealed that cybersecurity auditing in intelligent systems is a multidimensional and adaptive governance process integrating technological, organizational, behavioral, operational, and resilience-oriented dimensions. The open coding stage identified major concepts including intelligent infrastructure vulnerabilities, cyber risk governance, AI assurance, digital resilience capabilities, continuous monitoring systems, incident response management, and human-centered cybersecurity controls. Axial coding demonstrated that these dimensions are interconnected through strategic governance mechanisms, predictive risk assessment processes, and resilience-oriented auditing structures. Selective coding ultimately led to the development of a comprehensive integrated cybersecurity auditing model in which digital resilience functioned as the central organizing principle connecting continuous monitoring, intelligent risk management, governance accountability, and adaptive operational response capabilities. The results indicated that traditional cybersecurity auditing frameworks are insufficient for addressing the complexity of intelligent digital ecosystems and AI-driven infrastructures. Organizations require integrated and resilience-oriented cybersecurity auditing models capable of combining continuous monitoring, strategic governance, intelligent threat analysis, AI assurance, and adaptive risk management. The proposed model provides a comprehensive framework for strengthening organizational digital resilience, improving cybersecurity governance effectiveness, and enhancing preparedness against emerging cyber threats in intelligent systems environments.

Keywords: Cybersecurity Auditing, Intelligent Systems, Digital Resilience, Risk Assessment, Artificial Intelligence, Cyber Governance, Continuous Monitoring, Intelligent Infrastructure, Cyber Risk Management, Adaptive Security Systems

Article history:
Received 10 February 2026
Revised 30 March 2026
Accepted 19 May 2026
Initial Publish 29 May 2026
Published online 01 July 2027

How to cite this article:
Naseri, A., Mohammadzadeh Salteh, H., & Mogadamzadeh, R. (2027). An Integrated Cybersecurity Audit Model for Intelligent Systems with Emphasis on Risk Assessment and Digital Resilience. *Journal of Management and Business Solutions, 5*(4), 1-16. https://doi.org/10.61838/jmbs.321

Introduction

The rapid expansion of intelligent systems, artificial intelligence technologies, cloud computing infrastructures, interconnected digital platforms, and autonomous decision-making mechanisms has fundamentally transformed the operational structure of modern organizations and critical infrastructures. Organizations increasingly rely on intelligent digital ecosystems to manage strategic operations, process sensitive information, automate decisions, and maintain competitive advantage within dynamic technological environments. However, alongside these technological advancements, the complexity, frequency, and sophistication of cyber threats have escalated significantly, creating unprecedented challenges for organizational security, governance, auditing processes, and digital resilience. Contemporary cyberattacks are no longer limited to traditional malware or unauthorized access incidents; instead, organizations now face AI-driven attacks, algorithmic manipulation, ransomware campaigns, advanced persistent threats, supply chain infiltrations, cloud infrastructure breaches, and vulnerabilities associated with autonomous intelligent systems (1-3). As intelligent technologies become deeply integrated into organizational operations and critical infrastructures, cybersecurity has evolved from a purely technical issue into a strategic governance concern requiring multidisciplinary auditing and risk management approaches (4, 5).

The emergence of intelligent systems has introduced new forms of cybersecurity risks that traditional auditing models are often unable to address effectively. Conventional cybersecurity auditing frameworks were primarily designed for static technological environments characterized by predictable infrastructures, limited interconnectivity, and rule-based operational systems. In contrast, intelligent systems operate through adaptive algorithms, machine learning models, distributed cloud architectures, autonomous decision mechanisms, and real-time data processing structures that continuously evolve over time (6, 7). This transformation has significantly increased the attack surface of organizations and created complex vulnerabilities associated with explainability, algorithmic transparency, AI bias, autonomous decision-making, and real-time threat adaptation (8, 9). Consequently, cybersecurity auditing in intelligent environments requires integrated models capable of combining technological assessment, governance mechanisms, resilience evaluation, continuous monitoring, and strategic risk analysis within a unified framework.

One of the most significant developments influencing cybersecurity governance is the increasing integration of artificial intelligence into both defensive and offensive cyber operations. AI technologies are now extensively utilized for predictive threat analysis, automated incident detection, adaptive security architectures, and intelligent risk assessment systems. Simultaneously, cybercriminals increasingly employ generative AI, autonomous agents, and machine learning algorithms to bypass security controls, manipulate intelligent systems, and launch sophisticated cyberattacks against critical infrastructures (9, 10). This dual-use nature of AI has created a highly dynamic cybersecurity environment in which organizations must continuously adapt their defensive capabilities and auditing mechanisms. Researchers have emphasized that AI-driven cybersecurity requires advanced governance structures capable of ensuring accountability, interpretability, ethical compliance, and operational transparency in intelligent systems (11, 12). Therefore, the integration of cybersecurity auditing with intelligent risk management and resilience-oriented governance has become an essential organizational requirement.

Digital resilience has emerged as a critical concept in cybersecurity management due to the increasing inability of organizations to fully prevent cyber incidents in highly interconnected environments. Rather than focusing exclusively on threat prevention, modern cybersecurity strategies increasingly emphasize organizational resilience,

adaptive response capability, operational continuity, and rapid recovery following cyber disruptions (13, 14). Digital resilience refers to the capability of organizations to anticipate, withstand, respond to, and recover from cyberattacks while maintaining operational continuity and strategic stability. In intelligent systems environments, resilience becomes even more critical because cyber incidents can affect autonomous systems, interconnected infrastructures, data-driven decision processes, and real-time operational networks simultaneously (15, 16). Consequently, cybersecurity auditing frameworks must incorporate resilience-oriented indicators and adaptive governance mechanisms to evaluate organizational preparedness against evolving digital threats.

Another major challenge associated with intelligent systems relates to the growing dependence on cloud computing infrastructures, interconnected IoT ecosystems, blockchain networks, and distributed digital platforms. Organizations increasingly utilize cloud-based architectures and intelligent interconnected systems to improve scalability, operational efficiency, and data accessibility. However, these technologies introduce substantial cybersecurity risks associated with data confidentiality, distributed vulnerabilities, third-party dependencies, and cross-platform attack propagation (17, 18). Blockchain technologies and distributed ledger systems have also introduced new opportunities and risks related to cybersecurity governance, transparency, and decentralized operational control (12, 19). Researchers have argued that cybersecurity auditing frameworks must evolve beyond traditional perimeter-based security approaches and incorporate dynamic assessment models capable of addressing interconnected digital ecosystems and distributed infrastructures (20, 21).

Cybersecurity risks have become particularly critical within sectors involving sensitive information, critical infrastructures, financial systems, healthcare networks, and transportation ecosystems. Financial institutions increasingly face threats targeting digital transactions, cloud-based financial platforms, customer data storage systems, and intelligent financial technologies (22, 23). Healthcare organizations similarly encounter substantial cybersecurity challenges due to the digitization of medical records, telemedicine platforms, AI-assisted diagnostics, and interconnected healthcare infrastructures (24, 25). Furthermore, cybersecurity concerns within transportation systems, autonomous vehicles, maritime logistics, and supply chain networks have intensified due to increasing automation and interconnected operational technologies (7, 26). These developments demonstrate that cybersecurity auditing is no longer confined to information technology departments but instead constitutes a strategic organizational function affecting operational continuity, public trust, regulatory compliance, and national security.

The integration of cybersecurity governance with regulatory compliance has also become increasingly important within modern digital ecosystems. Governments and international institutions have introduced extensive cybersecurity regulations, data protection requirements, AI governance frameworks, and digital accountability standards intended to strengthen organizational security and reduce systemic cyber risks (12, 27). Compliance requirements associated with AI governance, data protection laws, cloud security standards, and critical infrastructure protection necessitate comprehensive auditing mechanisms capable of evaluating both technical and managerial dimensions of cybersecurity governance. Researchers have highlighted that organizations lacking integrated cybersecurity auditing systems face greater vulnerability to operational disruption, reputational damage, financial losses, and regulatory penalties (20, 28). Therefore, cybersecurity auditing frameworks must simultaneously address regulatory alignment, governance accountability, operational transparency, and strategic resilience.

An additional dimension of cybersecurity complexity relates to the human factor and organizational culture. Despite technological advancements in intelligent defense systems, human error, insufficient awareness, weak governance culture, and behavioral vulnerabilities continue to represent major sources of cybersecurity incidents (1, 29). Employees, managers, and organizational stakeholders frequently become targets of social engineering attacks, phishing campaigns, and behavioral manipulation strategies designed to bypass technological controls. Consequently, cybersecurity auditing frameworks must incorporate human-centered assessment dimensions evaluating organizational awareness, governance culture, training effectiveness, and behavioral risk exposure (4, 5). The interaction between technological infrastructures and human behavior significantly influences organizational resilience and the effectiveness of cybersecurity governance mechanisms.

The growing dependence on digital supply chains and third-party infrastructures has further intensified cybersecurity risks in intelligent organizational ecosystems. Organizations increasingly rely on outsourced service providers, cloud vendors, interconnected logistics systems, and external technology platforms to support operational processes. However, vulnerabilities within third-party systems can propagate rapidly across interconnected networks and compromise entire organizational ecosystems (30, 31). Cybersecurity incidents affecting supply chain infrastructures can disrupt operational continuity, compromise sensitive data, and weaken resilience capabilities across multiple organizations simultaneously. Researchers have emphasized the importance of integrated cybersecurity governance models capable of evaluating external dependencies, third-party vulnerabilities, and distributed infrastructure risks within comprehensive auditing frameworks (21, 26). This highlights the need for multidimensional auditing approaches integrating internal controls with ecosystem-wide cybersecurity assessment mechanisms.

The emergence of critical infrastructure protection as a national and strategic priority has also expanded the importance of cybersecurity auditing within intelligent systems. Artificial intelligence, cloud infrastructures, telecommunications networks, transportation systems, healthcare platforms, and financial ecosystems increasingly function as critical national infrastructures whose disruption can create extensive economic, political, and social consequences (3, 9). Researchers have argued that intelligent infrastructures require proactive cybersecurity governance models integrating predictive analytics, continuous monitoring, autonomous threat detection, and resilience-oriented operational management (6, 10). Traditional periodic auditing mechanisms are insufficient for managing rapidly evolving cyber threats targeting intelligent infrastructures. Instead, organizations require adaptive cybersecurity auditing systems capable of real-time analysis, continuous assurance, and strategic resilience evaluation.

Despite the increasing importance of cybersecurity governance within intelligent environments, existing auditing models remain fragmented and insufficiently integrated. Many cybersecurity auditing approaches focus exclusively on technical vulnerabilities while neglecting governance structures, resilience capabilities, human factors, strategic risk management, and intelligent system accountability. Similarly, many digital resilience frameworks fail to incorporate comprehensive auditing dimensions capable of evaluating organizational preparedness and operational adaptability within dynamic cyber environments (13, 14). Furthermore, the rapid evolution of AI-driven technologies and autonomous systems has outpaced the development of integrated cybersecurity auditing standards and governance models. This gap highlights the necessity for developing multidimensional frameworks capable of integrating cybersecurity auditing, intelligent risk assessment, digital resilience evaluation, governance accountability, and continuous monitoring within a coherent conceptual structure.

Given the increasing complexity of cyber threats, the strategic importance of intelligent systems, and the limitations of traditional cybersecurity auditing approaches, there is a critical need for integrated models capable of addressing the technological, organizational, governance, behavioral, and resilience-oriented dimensions of cybersecurity management simultaneously. The development of comprehensive cybersecurity auditing frameworks can significantly contribute to organizational preparedness, operational continuity, regulatory compliance, digital trust, and strategic resilience in intelligent digital ecosystems. Therefore, the present study aims to develop an integrated cybersecurity auditing model for intelligent systems with an emphasis on risk assessment and digital resilience.

Methods and Materials

This study was conducted using a qualitative research approach with an exploratory design grounded in thematic analysis and grounded theory-oriented coding procedures. The primary objective of the research was to develop an integrated cybersecurity auditing model for intelligent systems with an emphasis on risk assessment and digital resilience in organizational and technological environments. Given the multidimensional and emerging nature of cybersecurity auditing in intelligent systems, a qualitative methodology was considered the most appropriate approach for identifying the underlying concepts, extracting expert experiences, and constructing a comprehensive conceptual framework. The study focused on understanding the perspectives of professionals and specialists involved in cybersecurity governance, internal auditing, digital risk management, and intelligent technology infrastructures within organizations operating in Tehran.

The statistical population of the study consisted of experts in internal auditing, cybersecurity, information technology risk management, chief information officers (CIOs), members of audit committees, and university professors specializing in cybersecurity, information systems auditing, digital governance, and intelligent systems. Participants were selected from governmental organizations, private technology companies, financial institutions, consulting firms, and academic institutions located in Tehran. In order to ensure the inclusion of knowledgeable and experienced participants with direct involvement in cybersecurity auditing and digital resilience management, purposive sampling was initially employed. Subsequently, snowball sampling was utilized to identify additional experts through professional referrals and expert networks. This sampling process enabled the researchers to access individuals with extensive practical and theoretical expertise in cybersecurity auditing frameworks, intelligent systems governance, and digital infrastructure resilience.

Data collection continued until theoretical saturation was achieved, meaning that no new conceptual categories or meaningful insights emerged from subsequent interviews. In total, 23 in-depth semi-structured interviews were conducted with selected experts. The interviews were carried out individually in either face-to-face or virtual formats depending on participants' availability and organizational constraints. Each interview lasted between 60 and 90 minutes and was recorded with the informed consent of participants. Ethical considerations were carefully observed throughout the research process, including voluntary participation, confidentiality of responses, anonymity of participants, and the right to withdraw from the study at any stage. After the completion of the interviews, the audio recordings were transcribed verbatim and prepared for qualitative analysis.

The primary data collection tool in this study was a semi-structured interview guide specifically designed based on the theoretical foundations of cybersecurity auditing, enterprise risk management, digital resilience, intelligent systems governance, and information systems auditing standards. The interview protocol consisted of open-ended

and exploratory questions intended to elicit participants' experiences, perceptions, and professional judgments regarding cybersecurity auditing mechanisms, digital vulnerabilities, intelligent system threats, resilience strategies, and organizational readiness for cyber incidents. The interview questions were formulated after an extensive review of relevant literature, international cybersecurity frameworks, information systems auditing standards, and digital governance models. To ensure the content validity of the interview guide, the preliminary questions were reviewed and evaluated by several university professors and senior cybersecurity professionals, and their recommendations were incorporated into the final version of the instrument.

The interview process was conducted flexibly to allow participants to elaborate on emerging themes and discuss organization-specific cybersecurity challenges. During the interviews, probing questions were used to clarify ambiguous responses and deepen the understanding of critical issues related to cyber risk identification, intelligent system vulnerabilities, resilience capabilities, incident response mechanisms, governance structures, internal control systems, and cybersecurity audit practices. Field notes were also documented during and immediately after each interview to capture non-verbal cues, contextual observations, and preliminary analytical reflections that contributed to the interpretation of qualitative data.

To enhance the trustworthiness and rigor of the findings, several qualitative validation techniques were applied throughout the data collection process. Member checking was performed by sharing selected interview summaries and preliminary interpretations with participants to confirm the accuracy of the extracted meanings. In addition, peer debriefing was utilized through consultation with qualitative research experts and specialists in cybersecurity governance. The researchers also maintained an audit trail documenting methodological decisions, coding procedures, and analytical developments during the study. These measures contributed to the credibility, dependability, confirmability, and transferability of the qualitative findings.

The collected data were analyzed using qualitative content analysis and grounded theory-oriented coding techniques with the assistance of MAXQDA software. Following the transcription of interviews, the analysis process was conducted systematically in three consecutive stages including open coding, axial coding, and selective coding. In the open coding stage, the interview texts were reviewed line by line and segmented into meaningful units. Initial concepts and codes related to cybersecurity auditing, digital risk assessment, intelligent system vulnerabilities, cyber governance mechanisms, resilience dimensions, internal control structures, and organizational response capabilities were extracted from the participants' statements. This stage generated a large number of primary codes representing diverse dimensions of cybersecurity auditing practices and digital resilience management.

In the axial coding stage, the identified codes were compared, categorized, and linked based on conceptual similarities and causal relationships. The researchers organized the extracted concepts into broader thematic categories reflecting the structural and operational dimensions of cybersecurity auditing within intelligent systems. Relationships among categories such as technological risk factors, governance structures, resilience capabilities, threat detection mechanisms, compliance requirements, auditing processes, incident management, and strategic cybersecurity controls were identified and refined during this stage. The coding process was iterative and involved constant comparison between interview data, emerging categories, and conceptual interpretations.

In the final stage of selective coding, the central phenomenon of the study was identified and integrated with the major categories to construct the final integrated cybersecurity audit model. The researchers synthesized the relationships among the categories and developed a coherent conceptual framework explaining how cybersecurity auditing mechanisms, digital risk assessment practices, and resilience-oriented governance structures interact

within intelligent systems. Throughout the analysis process, efforts were made to ensure analytical consistency and theoretical coherence by continuously revisiting the raw data and comparing interpretations with participants' viewpoints. The final model was developed based on the recurring themes, causal relationships, contextual conditions, and strategic dimensions extracted from the qualitative data analysis.

Findings and Results

The qualitative analysis of the interviews conducted with 23 experts in the fields of cybersecurity auditing, intelligent systems governance, information technology risk management, internal auditing, digital resilience, and information systems security resulted in the extraction of a comprehensive set of concepts and categories related to the development of an integrated cybersecurity auditing model for intelligent systems. The demographic analysis of participants indicated that the interviewees possessed extensive professional and academic experience in the areas relevant to the study objectives. Among the participants, 8 individuals were university faculty members specializing in information systems, cybersecurity, and auditing, 5 participants were senior cybersecurity managers, 4 participants served as chief information officers (CIOs), 3 individuals were members of audit committees in financial and governmental organizations, and 3 participants were senior internal auditors with expertise in information systems auditing and digital risk governance. The majority of participants had more than 10 years of professional experience in cybersecurity governance, auditing, or digital infrastructure management. Furthermore, participants represented a diverse range of industries including banking, governmental institutions, telecommunications, healthcare technology, digital service providers, higher education institutions, and consulting organizations operating in Tehran.

Table 1. Open Coding Results of the Integrated Cybersecurity Auditing Model for Intelligent Systems

Primary Concepts	Initial Open Codes
Cyber threat identification	Malware attacks, ransomware incidents, phishing campaigns, insider threats, AI-based cyberattacks, unauthorized access attempts
Intelligent system vulnerabilities	Algorithmic weaknesses, insecure APIs, cloud infrastructure gaps, weak authentication protocols, IoT vulnerabilities
Digital resilience capabilities	System recovery capacity, business continuity preparedness, adaptive response mechanisms, resilience-oriented architecture
Governance and compliance mechanisms	Cybersecurity policies, governance frameworks, regulatory compliance, audit committee oversight, accountability structures
Risk assessment processes	Continuous risk monitoring, threat prioritization, vulnerability assessment, cyber risk scoring, impact analysis
Internal control effectiveness	Access control systems, segregation of duties, real-time monitoring controls, automated auditing procedures
Incident response management	Detection speed, incident escalation, response coordination, crisis management procedures, forensic readiness
Human factor vulnerabilities	Employee negligence, insufficient awareness, lack of cybersecurity culture, social engineering susceptibility
Technological infrastructure challenges	Legacy systems, fragmented digital architecture, insufficient integration, outdated security protocols
Artificial intelligence auditing concerns	Algorithm transparency, explainability issues, AI bias detection, autonomous decision auditing
Data protection mechanisms	Encryption systems, privacy controls, data classification policies, secure data transmission
Strategic cybersecurity management	Cybersecurity investment planning, resilience-oriented strategies, digital transformation governance
Continuous auditing capabilities	Automated monitoring, real-time analytics, predictive auditing models, intelligent audit dashboards
Organizational readiness	Crisis preparedness, digital maturity, cybersecurity awareness training, resilience planning
Third-party and supply chain risks	Vendor vulnerabilities, outsourced service risks, external platform dependency, cloud provider risks
Cybersecurity performance indicators	Incident frequency, resilience metrics, recovery time, audit effectiveness indicators

The findings presented in Table 1 demonstrate that the open coding process generated a broad range of conceptual categories reflecting the complexity and multidimensionality of cybersecurity auditing within intelligent systems. During the initial analysis, numerous fragmented concepts emerged from participants' narratives concerning technological vulnerabilities, governance deficiencies, digital resilience requirements, and auditing limitations in intelligent environments. The coding process revealed that cybersecurity auditing in intelligent systems extends beyond traditional control assessment and requires an integrated perspective combining technological, organizational, strategic, and behavioral dimensions. Participants repeatedly emphasized the increasing sophistication of cyber threats, particularly AI-driven attacks, cloud-related vulnerabilities, and interconnected digital ecosystems, which significantly complicate auditing processes and risk evaluation mechanisms. The findings also indicated that digital resilience was consistently perceived as a central organizational capability rather than merely a technical recovery mechanism. Experts highlighted the importance of adaptive governance structures, real-time auditing systems, predictive monitoring technologies, and continuous risk assessment procedures in maintaining resilience against dynamic cyber threats. Additionally, the analysis identified the human factor as one of the most influential sources of cybersecurity risk, with participants emphasizing the critical role of cybersecurity culture, employee awareness, and governance accountability in strengthening intelligent system security. Overall, the open coding stage provided the conceptual foundation for identifying relationships among technological, managerial, operational, and governance-oriented dimensions of cybersecurity auditing.

Table 2. Axial Coding Results of the Integrated Cybersecurity Auditing Model for Intelligent Systems

Axial Categories	Related Open Codes	Conceptual Dimension
Cyber Risk Governance	Governance frameworks, compliance mechanisms, audit committee oversight, accountability systems	Governance Dimension
Intelligent Infrastructure Vulnerability Management	Cloud vulnerabilities, API weaknesses, IoT security gaps, legacy system risks	Technological Dimension
Resilience-Oriented Auditing	Recovery capacity, adaptive response, continuity preparedness, resilience metrics	Resilience Dimension
Continuous Cybersecurity Monitoring	Real-time auditing, predictive analytics, automated controls, intelligent dashboards	Operational Dimension
Human-Centered Cybersecurity Controls	Cybersecurity awareness, employee behavior risks, organizational culture, social engineering prevention	Behavioral Dimension
AI and Intelligent Systems Assurance	Algorithm auditing, AI transparency, explainability assessment, autonomous decision evaluation	Intelligent Systems Dimension
Integrated Incident Response Management	Incident detection, crisis management, escalation procedures, forensic readiness	Response Dimension
Strategic Digital Risk Assessment	Risk scoring, vulnerability prioritization, threat forecasting, strategic risk analysis	Strategic Dimension
Third-Party Security Governance	Vendor risk assessment, outsourced infrastructure control, cloud governance, external dependency management	External Governance Dimension
Data Security and Privacy Assurance	Encryption controls, secure transmission, privacy management, access protection systems	Information Protection Dimension

The axial coding results presented in Table 2 illustrate the process through which the fragmented open codes were systematically integrated into broader conceptual categories representing the core dimensions of the integrated cybersecurity auditing model. During this analytical stage, relationships among concepts were identified based on causal links, contextual similarities, operational dependencies, and strategic interactions. The analysis revealed that cybersecurity auditing in intelligent systems is fundamentally shaped by the interaction between governance structures, technological infrastructure, resilience mechanisms, and operational monitoring capabilities. Participants consistently emphasized that cybersecurity auditing can no longer be treated as a periodic compliance-oriented activity, but instead must evolve into a dynamic and resilience-oriented governance process supported by

continuous monitoring technologies and intelligent analytical systems. The findings further demonstrated that digital resilience operates as an overarching organizational capability integrating technological preparedness, operational flexibility, crisis response readiness, and strategic adaptation. Another major finding emerging from the axial coding stage was the increasing importance of AI assurance and intelligent systems transparency within cybersecurity auditing frameworks. Experts noted that the rapid adoption of intelligent technologies has introduced new forms of algorithmic risks, automated decision-making vulnerabilities, and explainability challenges that traditional auditing models are not adequately prepared to address. Furthermore, participants highlighted that cybersecurity governance effectiveness is highly dependent on organizational culture, executive commitment, interdepartmental coordination, and employee cybersecurity awareness. The axial coding structure therefore clarified the interdependence between technological controls, governance mechanisms, resilience capacities, and behavioral dimensions in the development of an integrated cybersecurity auditing framework.

Table 3. Selective Coding Results and Final Integrated Cybersecurity Auditing Model

Core Category	Main Integrated Dimensions	Strategic Outcomes
Integrated Cybersecurity Auditing for Intelligent Systems Based on Risk Assessment and Digital Resilience	Cyber risk governance, intelligent infrastructure security, resilience-oriented auditing, AI assurance, continuous monitoring, incident response integration, human-centered cybersecurity management, strategic risk analysis, third-party governance, data protection mechanisms	Enhanced digital resilience, proactive cyber risk management, intelligent threat detection, improved governance transparency, sustainable cybersecurity capability, adaptive organizational response, strategic decision support

The selective coding stage resulted in the identification of the central phenomenon of the study, namely the development of an integrated cybersecurity auditing model for intelligent systems based on risk assessment and digital resilience. The findings presented in Table 3 indicate that the final conceptual model emerged through the integration of multiple interconnected dimensions involving governance, technology, resilience, human behavior, operational monitoring, and strategic risk management. At this stage, the relationships among all major categories were synthesized into a coherent explanatory framework illustrating how cybersecurity auditing functions as an adaptive and intelligence-driven organizational capability. The analysis demonstrated that effective cybersecurity auditing within intelligent systems requires the simultaneous integration of predictive risk assessment mechanisms, resilience-oriented governance structures, continuous technological monitoring, and intelligent decision-support systems. Participants emphasized that traditional audit frameworks focused solely on compliance verification are insufficient for addressing the dynamic and evolving nature of cyber threats in intelligent digital environments. Instead, organizations must adopt proactive and adaptive auditing models capable of continuously identifying vulnerabilities, monitoring emerging risks, evaluating intelligent system behaviors, and supporting rapid organizational responses to cyber incidents.

The selective coding results further revealed that digital resilience serves as the foundational principle connecting all dimensions of the proposed model. According to participants, resilience-oriented auditing enables organizations not only to detect cybersecurity weaknesses but also to enhance their adaptive capacity, operational continuity, and strategic flexibility in response to cyber disruptions. Experts repeatedly highlighted the importance of integrating AI assurance mechanisms, predictive analytics, automated auditing technologies, and governance accountability structures into cybersecurity auditing frameworks to improve organizational readiness against sophisticated digital threats. Additionally, the findings demonstrated that cybersecurity auditing effectiveness is strongly influenced by organizational digital maturity, executive leadership support, cross-functional coordination, and the establishment

of a cybersecurity-oriented organizational culture. The final integrated model therefore represents a multidimensional governance and assurance framework designed to strengthen intelligent systems security, improve digital resilience, support strategic cybersecurity decision-making, and enhance the sustainability of organizational digital infrastructures in complex technological environments.

Discussion and Conclusion

The findings of the present study demonstrated that cybersecurity auditing in intelligent systems has evolved into a multidimensional and resilience-oriented governance process that extends far beyond conventional compliance verification and technical control assessment. The qualitative analysis revealed that effective cybersecurity auditing frameworks must simultaneously integrate intelligent risk assessment, governance accountability, continuous monitoring, digital resilience capabilities, AI assurance mechanisms, and organizational preparedness dimensions within a unified operational structure. The extracted model emphasized the dynamic interaction between technological infrastructures, human-centered security controls, adaptive resilience mechanisms, and strategic governance processes in shaping cybersecurity effectiveness within intelligent digital ecosystems. These findings indicate that organizations operating within highly interconnected and AI-driven environments can no longer rely on fragmented or static cybersecurity auditing mechanisms. Instead, organizations require integrated and adaptive auditing systems capable of continuously identifying vulnerabilities, evaluating intelligent system behaviors, monitoring emerging threats, and supporting resilience-oriented decision-making processes.

One of the central findings of the study was the importance of digital resilience as the foundational principle underlying cybersecurity auditing in intelligent systems. Participants repeatedly emphasized that modern organizations cannot fully eliminate cyber risks due to the increasing complexity and unpredictability of digital threats. Consequently, organizational capability to withstand, respond to, recover from, and adapt to cyber incidents becomes a critical determinant of cybersecurity effectiveness. This finding is strongly aligned with previous studies emphasizing resilience-oriented cybersecurity governance and adaptive defense architectures (13, 14). Researchers have argued that resilience has become a strategic organizational capability rather than merely a technical recovery process because cyber incidents increasingly affect interconnected infrastructures, operational continuity, and strategic organizational functions simultaneously. The findings of the current study further support the perspective that cybersecurity auditing should evaluate not only vulnerability exposure and control effectiveness but also organizational adaptability, recovery preparedness, continuity mechanisms, and resilience maturity levels. This interpretation is consistent with the findings of (21), who emphasized the necessity of integrating resilience metrics into cybersecurity governance frameworks for critical digital infrastructures.

Another important finding emerging from the study relates to the increasing role of artificial intelligence within cybersecurity governance and auditing processes. Participants highlighted that AI technologies simultaneously strengthen cybersecurity defenses and create new categories of vulnerabilities, governance challenges, and accountability concerns. Intelligent systems increasingly rely on autonomous decision-making algorithms, predictive analytics, adaptive monitoring systems, and machine learning infrastructures that operate dynamically and continuously evolve over time. As a result, traditional auditing approaches based on static control assessment are insufficient for evaluating intelligent digital environments. This finding is strongly supported by studies examining the impact of AI-driven cybersecurity systems and intelligent infrastructures (9, 10). These studies emphasized that AI-enabled cyber environments require auditing frameworks capable of assessing algorithmic transparency,

explainability, adversarial robustness, ethical governance, and autonomous system accountability. Similarly, (11) argued that modern cybersecurity governance frameworks must integrate interpretability and organizational modeling mechanisms to ensure secure and transparent intelligent systems. The findings of the present study therefore reinforce the necessity of incorporating AI assurance dimensions into integrated cybersecurity auditing models.

The results also demonstrated that continuous monitoring and predictive cybersecurity analytics represent essential operational components of modern cybersecurity auditing frameworks. Participants consistently emphasized the importance of real-time auditing mechanisms, automated threat detection systems, intelligent dashboards, and predictive risk analysis technologies in identifying cyber threats before they escalate into large-scale operational disruptions. This finding corresponds with the increasing shift from periodic auditing toward continuous cybersecurity assurance models highlighted in recent literature (8, 17). AI-driven cloud security systems and next-generation intelligent firewalls increasingly enable organizations to conduct adaptive threat monitoring and dynamic vulnerability assessment in real time. The findings of this study suggest that cybersecurity auditing effectiveness is significantly enhanced when organizations utilize intelligent monitoring systems capable of identifying abnormal patterns, predicting cyber incidents, and supporting rapid operational responses. This interpretation is also consistent with the arguments presented by (2), who emphasized the transformative role of AI in predictive cybersecurity governance and threat analysis.

The present study additionally identified governance accountability and organizational culture as critical dimensions influencing cybersecurity resilience and audit effectiveness. Participants highlighted that cybersecurity governance failures frequently emerge not only from technological vulnerabilities but also from insufficient executive commitment, fragmented governance structures, weak accountability mechanisms, and inadequate organizational awareness. Human error, social engineering exposure, and behavioral vulnerabilities were repeatedly identified as major contributors to cybersecurity incidents within intelligent systems environments. These findings align closely with studies emphasizing the role of human factors and organizational culture in cybersecurity governance (1, 29). Researchers have increasingly recognized that technological security controls alone are insufficient without organizational awareness, executive engagement, and cybersecurity-oriented behavioral practices. Furthermore, the findings support the conclusions of (4), who emphasized that emerging technology risk management requires integrated governance structures combining strategic leadership, human-centered security policies, and technological resilience mechanisms. The integrated model developed in this study therefore highlights the necessity of combining technical auditing processes with organizational governance assessment and behavioral cybersecurity evaluation.

The findings further revealed that interconnected infrastructures and third-party digital ecosystems significantly increase organizational cybersecurity complexity. Participants emphasized that organizations increasingly rely on cloud providers, outsourced platforms, digital supply chains, IoT ecosystems, and interconnected infrastructures that expand operational dependencies and create distributed vulnerabilities. This interconnectedness increases the probability of cyberattack propagation across organizational ecosystems and complicates cybersecurity governance processes. These findings are highly consistent with studies focusing on supply chain cybersecurity and interconnected digital infrastructures (30, 31). Similarly, (26) demonstrated that maritime logistics and supply web systems face escalating cybersecurity challenges due to increasing digital interconnectivity and autonomous operational infrastructures. The current study contributes to this body of literature by emphasizing that integrated

cybersecurity auditing frameworks must extend beyond internal organizational controls and include ecosystem-wide governance assessment, third-party risk evaluation, and distributed infrastructure monitoring capabilities.

Another important aspect of the findings concerns the increasing strategic importance of cybersecurity within critical infrastructures and intelligent operational systems. Participants repeatedly emphasized that cybersecurity auditing has become a strategic governance necessity in sectors such as healthcare, finance, telecommunications, transportation, logistics, and national digital infrastructures. Intelligent systems supporting these sectors process highly sensitive information and operate through interconnected digital ecosystems vulnerable to sophisticated cyberattacks. This finding aligns with the arguments presented by (3), who conceptualized AI infrastructures as strategic national assets requiring advanced cybersecurity governance and protection mechanisms. Similarly, studies conducted in financial, healthcare, and telecommunications sectors highlighted the increasing vulnerability of critical infrastructures to cyber threats and the necessity of integrated cybersecurity governance frameworks (21, 22, 24). The present study extends these findings by demonstrating that cybersecurity auditing must evolve into a strategic organizational capability capable of supporting resilience-oriented governance, operational continuity, and intelligent threat management across critical digital ecosystems.

The role of blockchain technologies and distributed systems also emerged as an important dimension within the integrated cybersecurity auditing model. Participants noted that blockchain-based infrastructures may improve transparency, traceability, and decentralized security management within intelligent systems. However, they also highlighted challenges associated with interoperability, governance complexity, and distributed attack surfaces. These findings are consistent with studies examining the relationship between blockchain technologies and cybersecurity governance (18, 19). Researchers have argued that blockchain integration can strengthen cybersecurity resilience and trustworthiness within distributed intelligent ecosystems while simultaneously introducing new governance and operational complexities. Additionally, (12) emphasized the role of blockchain technologies in strengthening AI governance compliance and cybersecurity transparency within distributed digital environments. The findings of the present study therefore suggest that integrated cybersecurity auditing models should incorporate distributed governance assessment and blockchain assurance mechanisms as part of broader intelligent systems auditing frameworks.

The findings of this study also revealed the growing inadequacy of traditional cybersecurity auditing models in addressing the complexity of modern intelligent systems. Conventional auditing frameworks are often designed around static infrastructures, periodic assessments, and compliance-oriented evaluation mechanisms that fail to capture the adaptive and continuously evolving nature of intelligent cyber environments. Participants emphasized the necessity of transitioning toward dynamic, predictive, and resilience-oriented cybersecurity auditing approaches capable of integrating technological monitoring, strategic governance, AI assurance, and adaptive operational management. This finding is strongly supported by previous literature emphasizing the limitations of traditional cybersecurity frameworks in AI-driven ecosystems (6, 15). These studies highlighted the increasing need for trustworthy autonomous systems governance and integrated cybersecurity architectures capable of supporting complex intelligent infrastructures. Therefore, the integrated model proposed in the current study contributes to the existing body of knowledge by offering a multidimensional framework that addresses technological, organizational, strategic, and resilience-oriented dimensions simultaneously.

The study ultimately demonstrates that cybersecurity auditing in intelligent systems should be conceptualized as a continuous and adaptive governance capability rather than an isolated technical assessment function. The

integrated model developed through qualitative analysis highlights the necessity of combining risk assessment, digital resilience evaluation, governance accountability, AI assurance, continuous monitoring, and human-centered security management within a coherent auditing framework. Such an approach can significantly enhance organizational preparedness, strengthen operational continuity, improve strategic decision-making, and increase resilience against emerging cyber threats within intelligent digital ecosystems. The findings therefore provide both theoretical and practical contributions to the evolving field of cybersecurity governance and intelligent systems auditing.

One of the limitations of the present study relates to the qualitative nature of the research design and the relatively limited number of expert participants involved in the interviews. Although theoretical saturation was achieved and the participants possessed substantial expertise in cybersecurity governance and intelligent systems, the findings may not fully represent the perspectives of all industries, organizational contexts, or geographical regions. Additionally, the study focused primarily on organizations and experts located in Tehran, which may limit the generalizability of the findings to other national or international environments with different technological infrastructures, governance structures, and cybersecurity maturity levels. Another limitation concerns the rapidly evolving nature of intelligent technologies and cyber threats, which may influence the long-term stability of some identified dimensions within the proposed model.

Future research can extend the findings of the present study by quantitatively validating the proposed integrated cybersecurity auditing model across different industries and organizational settings. Researchers may also examine the effectiveness of the model within specific sectors such as banking, healthcare, telecommunications, transportation, and governmental infrastructures. Comparative studies between countries or regulatory environments may provide additional insights regarding the influence of governance structures and digital maturity on cybersecurity auditing effectiveness. Future investigations may further explore the role of emerging technologies such as generative AI, blockchain ecosystems, quantum-resistant security mechanisms, and autonomous intelligent agents in reshaping cybersecurity governance and resilience-oriented auditing frameworks.

From a practical perspective, organizations should prioritize the development of integrated cybersecurity governance systems that combine continuous monitoring, resilience-oriented risk management, intelligent threat analysis, and adaptive auditing mechanisms. Executive leaders and audit committees should strengthen organizational cybersecurity culture by investing in awareness programs, resilience planning, and strategic governance accountability structures. Organizations should also adopt AI-enabled auditing technologies capable of real-time threat detection and predictive cybersecurity analysis to improve operational preparedness against evolving cyber risks. Furthermore, policymakers and regulatory institutions should support the development of unified cybersecurity governance standards specifically designed for intelligent systems and interconnected digital infrastructures in order to strengthen organizational resilience and improve national cybersecurity readiness.

Acknowledgments

We would like to express our appreciation and gratitude to all those who helped us carrying out this study.

Authors' Contributions

All authors equally contributed to this study.

Declaration of Interest

The authors of this article declared no conflict of interest.

Ethical Considerations

All ethical principles were adheried in conducting and writing this article.

Transparency of Data

In accordance with the principles of transparency and open research, we declare that all data and materials used in this study are available upon request.

Funding

This research was carried out independently with personal funding and without the financial support of any governmental or private institution or organization.

References

1. Familoni BT, Shoetan PO. Cybersecurity in the Financial Sector: A Comparative Analysis of the Usa and Nigeria. Computer Science & It Research Journal. 2024;5(4):850-77. doi: 10.51594/csitrj.v5i4.1046.
2. Mandal S, Patra SK. Artificial Intelligence and Cybersecurity: A Global Scenario. 2024. doi: 10.20944/preprints202405.0415.v1.
3. Yu C. AI as Critical Infrastructure: Safeguarding National Security in the Age of Artificial Intelligence. 2024. doi: 10.31219/osf.io/u4kdq.
4. Yaacob MN, Idrus SZS, Idris M. Managing Cybersecurity Risks in Emerging Technologies. Ijbt. 2023;13(3):253-70. doi: 10.58915/ijbt.v13i3.297.
5. Shoetan PO, Amoo OO, Okafor ES, Olorunfemi OL. Synthesizing Ai's Impact on Cybersecurity in Telecommunications: A Conceptual Framework. Computer Science & It Research Journal. 2024;5(3):594-605. doi: 10.51594/csitrj.v5i3.908.
6. Flammini F, Alcaraz C, Bellini E, Marrone S, López J, Bondavalli A. Towards Trustworthy Autonomous Systems: Taxonomies and Future Perspectives. Ieee Transactions on Emerging Topics in Computing. 2024;12(2):601-14. doi: 10.1109/tetc.2022.3227113.
7. Durlik I, Miller T, Kostecka E, Zwierzewicz Z, Łobodzińska A. Cybersecurity in Autonomous Vehicles—Are We Ready for the Challenge? Electronics. 2024;13(13):2654. doi: 10.3390/electronics13132654.
8. Ahmadi S. Next Generation AI-Based Firewalls: A Comparative Study. 2024. doi: 10.31219/osf.io/3kg6f.
9. Yigit Y, Ferrag MA, Ghanem MC, Sarker IH, Μαγλαράς Λ, Chrysoulas C, et al. Generative AI and LLMs for Critical Infrastructure Protection: Evaluation Benchmarks, Agentic AI, Challenges, and Opportunities. Sensors. 2025;25(6):1666. doi: 10.3390/s25061666.
10. Adabara I, Sadiq BO, Shuaibu AN, Danjuma YI, Venkateswarlu M. A Review of Agentic AI in Cybersecurity: Cognitive Autonomy, Ethical Governance, and Quantum-Resilient Defense. F1000research. 2025;14:843. doi: 10.12688/f1000research.169337.1.
11. Keshavamurthy D. An <scp>AI</Scp> -Based Framework for Secure and Transparent Banking: Integrating Adversarial Robustness, Interpretability, and Organizational Modeling. Security and Privacy. 2025;9(1). doi: 10.1002/spy2.70153.

12. Ramos S, Ellul J. Blockchain for Artificial Intelligence (AI): Enhancing Compliance With the EU AI Act Through Distributed Ledger Technology. A cybersecurity Perspective. International Cybersecurity Law Review. 2024;5(1):1-20. doi: 10.1365/s43439-023-00107-9.

13. Al-Hawamleh A. Cyber Resilience Framework: Strengthening Defenses And Enhancing Continuity in Business Security. International Journal of Computing and Digital Systems. 2024;15(1):1315-31. doi: 10.12785/ijcds/150193.

14. Gadhi A, Gondu RM, Chaudhary H, Abiona O. Cyber Resilience Through Real-Time Threat Analysis in Information Security. International Journal of Communications Network and System Sciences. 2024;17(04):51-67. doi: 10.4236/ijcns.2024.174004.

15. Semenenko O, Kirsanov S, Movchan A, Ihnatiev M, Dobrovolskyi U. Impact of Computer-Integrated Technologies on Cybersecurity in the Defence Sector. Naukovij Žurnal «tehnìka Ta Energetika». 2024;15(2):118-29. doi: 10.31548/machinery/2.2024.118.

16. Tabish N, Chaur-Luh T. Maritime Autonomous Surface Ships: A Review of Cybersecurity Challenges, Countermeasures, and Future Perspectives. Ieee Access. 2024;12:17114-36. doi: 10.1109/access.2024.3357082.

17. Rehan H. AI-Driven Cloud Security: The Future of Safeguarding Sensitive Data in the Digital Age. Jaigs. 2024;1(1):132-51. doi: 10.60087/jaigs.v1i1.89.

18. Ahakonye LAC, Nwakanma CI, Kim DS. Tides of Blockchain in IoT Cybersecurity. Sensors. 2024;24(10):3111. doi: 10.3390/s24103111.

19. Zebari GM, Musalhi NA. A Comprehensive Review of Integrating <scp>AI</Scp> and Blockchain Security: Innovations, Challenges, and Future Directions. Security and Privacy. 2025;8(5). doi: 10.1002/spy2.70094.

20. Obiki-Osafiele AN, Agu EE, Chiekezie NR. Protecting Digital Assets in Fintech: Essential Cybersecurity Measures and Best Practices. Computer Science & It Research Journal. 2024;5(8):1884-96. doi: 10.51594/csitrj.v5i8.1449.

21. Folorunsho SO, Adenekan OA, Ezeigweneme C, Somadina IC, Okeleke PA. Ensuring Cybersecurity in Telecommunications: Strategies to Protect Digital Infrastructure and Sensitive Data. Computer Science & It Research Journal. 2024;5(8):1855-83. doi: 10.51594/csitrj.v5i8.1448.

22. Familoni BT. Cybersecurity Challenges in the Age of Ai: Theoretical Approaches and Practical Solutions. Computer Science & It Research Journal. 2024;5(3):703-24. doi: 10.51594/csitrj.v5i3.930.

23. Okoye CC, Nwankwo EE, Usman FO, Mhlongo NZ, Odeyemi O, Ike CU. Securing Financial Data Storage: A Review of Cybersecurity Challenges and Solutions. International Journal of Science and Research Archive. 2024;11(1):1968-83. doi: 10.30574/ijsra.2024.11.1.0267.

24. Layode O, Naiho HNN, Adeleke GS, Udeh EO, Labake TT. The Role of Cybersecurity in Facilitating Sustainable Healthcare Solutions: Overcoming Challenges to Protect Sensitive Data. International Medical Science Research Journal. 2024;4(6):668-93. doi: 10.51594/imsrj.v4i6.1228.

25. Palanichamy A, Sivakumar D. Data Security Challenges in Hospitals: A Survey on Cyber Security Issues in HealthCare Sector and Their Applications. 2025. doi: 10.21203/rs.3.rs-7238646/v1.

26. Samanta K. Maritime Cyber Security Transformation Impacting Supply Web and Logistics. 2025. doi: 10.21203/rs.3.rs-7734201/v1.

27. Abrahams TO, Ewuga SK, Kaggwa S, Uwaoma PU, Hassan AO, Dawodu SO. Mastering Compliance: A Comprehensive Review of Regulatory Frameworks in Accounting and Cybersecurity. Computer Science & It Research Journal. 2024;5(1):120-40. doi: 10.51594/csitrj.v5i1.709.

28. Anyanwu A, Olorunsogo T, Abrahams TO, Akindote OJ, Reis O. Data Confidentiality and Integrity: A Review of Accounting and Cybersecurity Controls in Superannuation Organizations. Computer Science & It Research Journal. 2024;5(1):237-53. doi: 10.51594/csitrj.v5i1.735.

29. Silva F. Evolving Approaches in Cybersecurity: Metrics and Human Factors. International Seven Journal of Multidisciplinary. 2024;1(2). doi: 10.56238/isevmjv1n2-010.

30. Ibiyemi MO, Olutimehin DO. Cybersecurity in Supply Chains: Addressing Emerging Threats With Strategic Measures. International Journal of Management & Entrepreneurship Research. 2024;6(6):2024-47. doi: 10.51594/ijmer.v6i6.1241.

31. Odimarha AC, Ayodeji SA, Abaku EA. Securing the Digital Supply Chain: Cybersecurity Best Practices for Logistics and Shipping Companies. World Journal of Advanced Science and Technology. 2024;5(1):026-30. doi: 10.53346/wjast.2024.5.1.0030.