Cyber Security Risks in Automated Systems and Their Impact on Audit Quality: A Conceptual and Empirical Framework

Dr. M. Janakiram
Associate Professor of Commerce
Badruka College Of Commerce and Arts, Kachiguda, Hyderabad

***Abstract*—The fast use of artificial intelligence (AI), machine learning (ML), robotic process automation (RPA), block chain, and cloud computing in auditing has greatly changed the audit profession. These technologies make auditing faster, more accurate, and allow continuous monitoring. However, they also create new and serious cyber security risks. Cyber threats such as data breaches, ransom ware attacks, and manipulation of algorithms, insider misuse, and risks from third-party cloud providers can affect the reliability of audit evidence, the judgment of auditors, and overall audit quality. Even though technology is widely used in auditing today, there is still limited research that clearly studies how cyber security risks impact audit quality. This study develops a clear conceptual framework by combining audit quality theory, information systems risk theory, and technology governance models. It proposes that cyber security risks reduce audit quality, mainly by affecting system integrity. At the same time, strong IT governance systems and auditors' technological skills can reduce these negative effects.**

The paper integrates different theories, develops testable hypotheses, and suggests a strong research design that can be applied across different countries. Overall, the study highlights that managing cyber security effectively is essential to maintaining high audit quality in today's digital environment.

***Index Terms*—Cyber security risk, Automated auditing, Audit quality, Artificial intelligence, IT governance, Cloud auditing, Algorithmic risk.**

I. INTRODUCTION

The auditing profession is changing very quickly because of digital technology. Audit firms now use automated systems that include artificial intelligence (AI), big data analytics, robotic process automation (RPA), blockchain tools, and cloud-based audit platforms. These technologies help auditors work continuously, detect fraud more easily, assess risks in advance, and test large numbers of transactions more effectively. However, this shift to digital systems also increases the risk of cyberattacks. Automated auditing depends on connected computer systems, shared databases, software algorithms, and outside service providers. Because of this, cyber security is no longer just an IT issue—it has become a major threat to the accuracy and reliability of audits. Recent ransomware attacks and major data breaches around the world show that professional firms, including audit firms, are common targets for hackers. In auditing, cyber security failures can damage:

- Confidential financial information
- Audit working papers
- The reliability of audit evidence
- Automated decision-making systems
- Audit deadlines and timelines

Audit quality is defined as the likelihood that an auditor detects and reports important errors in financial statements (DeAngelo, 1981). High audit quality depends on reliable systems and trustworthy evidence. If automated systems are hacked or manipulated, audit quality can decline. Even though these risks are increasing, most research has focused on the advantages of audit automation, with less attention given to how cyber security affects audit quality. This study aims to fill that gap

II. RESEARCH OBJECTIVES

- To identify key cyber security risks inherent in automated auditing systems.

- To examine theoretical linkages between cyber security risk and audit quality.
- To develop a comprehensive conceptual framework integrating cyber security governance into audit quality models.
- To propose empirically testable hypotheses.

III. LITERATURE REVIEW

➢ Evolution of Automated Auditing Systems

Digital technology has greatly changed the way audits are conducted. Some of the major developments include:

- Using AI to identify unusual transactions or errors
- Continuous auditing systems that monitor data regularly instead of once a year
- Blockchain technology to verify transactions securely
- Robotic Process Automation (RPA) to handle routine and repetitive audit tasks
- Cloud-based platforms that allow auditors to work and share information online

Research shows that data analytics helps improve audit quality and makes it easier to detect fraud (Appelbaum et al., 2017). However, depending heavily on technology can also create weaknesses and new risks in audit systems (Alles, 2015).

Most studies focus on how technology increases efficiency and effectiveness. But only a few studies examine the cyber security risks that come with automated auditing systems.

➢ Cyber security Risk in Digital Information Systems

Cybersecurity risk means the chance that someone gains unauthorized access to a system or causes damage by disrupting, changing, or destroying information. In digital systems, cyber risks are usually grouped into the following types:

- Confidentiality risk – when sensitive information is accessed without permission
- Integrity risk – when data is changed or manipulated incorrectly
- Availability risk – when systems or data are not accessible when needed
- Authentication risk – when user identities are not properly verified
- Third-party dependency risk – when risks arise from external service providers

In professional service firms, cyberattacks can harm the company's reputation, lead to legal problems, and result in regulatory penalties.

In auditing, the impact can be even more serious. If audit systems are hacked or manipulated, the evidence collected may be incorrect or unreliable. This can directly affect the accuracy and trustworthiness of financial reports.

➢ Audit Quality: Theoretical Foundations

Audit quality is usually explained using different theories, such as:

- Agency theory – which focuses on reducing conflicts between managers and shareholders
- Reputation theory – which suggests that audit firms maintain high quality to protect their reputation
- Auditor competence and independence frameworks – which emphasize the skills and objectivity of auditors

DeAngelo (1981) defined audit quality as the likelihood that an auditor will both detect important errors and report them honestly.

Today, the concept of audit quality has expanded. It now also includes:

- The reliability of audit evidence
- The use of professional skepticism
- Strong governance within audit firms
- The technological skills of auditors

However, most current models of audit quality do not clearly include cyber security and system integrity as key factors that influence audit quality.

IV. IDENTIFIED RESEARCH GAP

Existing research shows three main gaps:

- There is little connection made between cyber security risk and audit quality theory.
- There are very few empirical models that link weaknesses in digital systems to actual audit results.
- There is not enough research on how governance systems can reduce cyber security risks in auditing.

This study aims to fill these gaps by combining information systems risk theory with existing audit quality frameworks.

Cyber security Risks in Automated Auditing Systems

➢ Data Breaches and Confidentiality Threats

Automated audit systems handle very sensitive financial and business information. If a data breach happens, it can lead to:

- Exposure of confidential client information
- Competitive disadvantage for the client or audit firm
- Fines and penalties from regulators

Impact on audit quality:

- Lower trust and confidence among stakeholders
- Higher risk of legal action against the audit firm
- Possible damage to the auditor's independence and objectivity.

➢ Ransomware and System Disruption

Ransomware attacks can block access to audit files and systems, especially during important reporting periods.

Consequences:

- Delays in completing audit procedures
- Reduction in the scope of the audit work
- Increased time pressure on auditors

Research shows that when auditors face high time pressure, their professional skepticism may decrease, and overall audit performance can decline.

Algorithm Manipulation and AI Risk

AI systems used in auditing can face several risks, such as:

- Data poisoning – when false or harmful data is added to mislead the system
- Adversarial attacks – when attackers intentionally trick the AI system
- Biased training data – when the data used to train the AI is incomplete or unfair

If algorithms are manipulated, they may give wrong results. This can lead to:

- False confidence that everything is correct
- Failure to detect fraud
- Poor allocation of audit time and resources

Insider Threats

Audit firms also face cyber risks from people inside the organization, such as:

- Unhappy or dissatisfied employees
- Misuse of access rights or special privileges
- Theft of login credentials and passwords

When insiders misuse their access, they may change audit working papers or tamper with important data. This can damage the reliability and integrity of audit evidence.

Cloud and Third-Party Risk

Using cloud services creates new risks, such as:

- Weak security systems at the vendor's side
- Risks from shared infrastructure used by many organizations
- Limited control over where and how data is stored (data sovereignty issues)

When audit firms depend on cloud providers and other third parties, they may lose direct control over the security of their systems and data.

Theoretical Framework Development

This study combines three main theories:

- Agency Theory – explains the auditor's role in reducing the information gap between managers and stakeholders.
- Information Systems Risk Theory – focuses on weaknesses in digital systems and the need for proper controls.
- Technology Governance Theory – highlights the importance of monitoring, rules, and oversight in managing technology.

Based on these theories, the study proposes that cyber security risks reduce audit quality because they weaken the integrity and reliability of automated audit systems.

Conceptual Model

- Independent Variables (Main Risk Factors):
- Risk of data breaches
- Risk of ransomware attacks
- Risk of AI or algorithm manipulation
- Risk of insider threats
- Risk related to cloud system weaknesses

Mediating Variable (Connecting Factor):
- Integrity and reliability of the automated audit system

Dependent Variable (Final Outcome):
- Audit quality

Moderating Variables (Factors that Influence the Relationship):
- Level of IT governance maturity in the audit firm
- Technological skills and competence of auditors

V. HYPOTHESIS DEVELOPMENT

H1: Higher cyber security risk reduces the integrity and reliability of automated audit systems.
H2: When automated audit systems are reliable and secure, audit quality improves.
H3: The integrity of automated systems acts as a link between cyber security risk and audit quality. In other words, cyber security risk affects audit quality mainly by weakening system integrity.
H4: Strong and mature IT governance can reduce the negative effect of cyber security risk on system integrity.
H5: When auditors have strong technological skills, the positive impact of system integrity on audit quality becomes stronger.

VI. RESEARCH METHODOLOGY

➢ Research Design

This study uses a quantitative cross-sectional survey design. This means data will be collected at one point in time using a structured questionnaire, and the results will be analyzed using statistical methods.

➢ Sample

The target respondents for the study include:
- External auditors
- Internal auditors
- IT audit professionals
- Professionals working in Big 4 and mid-sized audit firms

The expected sample size is between 300 and 500 respondents.

➢ Measurement of Variables

- Cybersecurity Risk:

Cyber security risk will be measured using multiple questions on a Likert scale (for example, from strongly disagree to strongly agree). These questions are adapted from previous studies in information security research.

➢ Audit Quality:

Audit quality will be measured based on how respondents perceive the following factors:
- Reliability of audit evidence
- Ability to detect errors or fraud
- Level of professional skepticism
- Timely completion of audit work

➢ System Integrity:

System integrity will be measured using indicators such as:
- Reliability of data
- System availability and uptime
- Effectiveness of security controls

➢ Data Analysis

The collected data will be analyzed using the following methods:
- Reliability testing (Cronbach's alpha) – to check whether the survey questions are consistent and reliable.
- Confirmatory Factor Analysis (CFA) – to confirm whether the data fits the expected measurement model.
- Structural Equation Modeling (SEM) – to test the relationships between the variables in the study.
- Mediation and moderation analysis – to examine indirect effects (mediation) and the influence of moderating variables.

The analysis will be carried out using software such as AMOS, SmartPLS, or STATA.

VII. EXPECTED CONTRIBUTIONS

➢ Theoretical Contribution
- Expands audit quality theory to better fit today's digital and technology-based audit environment.
- Identifies cyber security governance as an important factor that directly influences audit results.

- Connects accounting research with cyber security studies, bringing both areas together in one framework.

➢ Practical Contribution

- Encourages audit firms to include cyber security risks in their audit planning process.
- Supports the development of proper governance frameworks for using AI in auditing.
- Helps regulators update audit inspection standards to address new digital and cyber security risks.

➢ Policy Implications

Regulators should:

- Make cyber security assessments a compulsory part of audit inspections.
- Create clear standards for managing and governing the use of AI in audit firms.
- Require audit firms to disclose their level of cyber security and technology governance maturity in audit reports

VIII. CONCLUSION

Automated auditing systems offer both benefits and risks. They improve the efficiency and effectiveness of audits, but they also expose audit firms to serious cyber security threats. These risks can directly and indirectly reduce audit quality by weakening the integrity and reliability of audit systems.

Therefore, managing cyber security should become a key part of audit firm strategy, regulatory monitoring, and academic research.

Future research should use long-term data and data from different countries to test and confirm the proposed model.

REFERENCES

[1] J. Kokina *et al.*, "Challenges and opportunities for artificial intelligence in auditing," *International Journal of Accounting Information Systems*, 2025.

[2] E. Pérez-Calderón, "Impact of artificial intelligence on auditing: Auditor perceptions and quality implications," Springer, 2025.

[3] Y. Li *et al.*, "Artificial intelligence auditability and auditor readiness for auditing AI systems," *International Journal of Accounting Information Systems*, 2025.

[4] C. Nott, "Organizational adaptation to generative AI in cybersecurity: A systematic review," 2025.

[5] B. Zweers, D. Dey, and D. Bhaumik, "The AI-fraud diamond: A novel lens for auditing algorithmic deception," 2025.

[6] F. Fajrillah, "Improving information system audit security through artificial intelligence: A literature review," 2025.

[7] "The quality of cybersecurity audits: Do synergies among the internal audit function matter?" 2025.

[8] "Integrating AI in audit workflow: Opportunities and challenges," 2026.

[9] "AI software selection for cybersecurity auditing using neutrosophic CRITIC CODAS," *Applied Soft Computing*, 2025.

[10] "Adaptive structural audit processes as shaped by emerging technologies," 2025.

[11] "AI and internal audit quality," SSRN Working Paper, 2025.

[12] "Artificial intelligence in internal auditing: Enhancing audit effectiveness," *Decision Making: Applications in Management and Engineering*, 2024.

[13] "The future of auditing: How AI will transform the profession by 2030," *Journal of International Commercial Law and Technology*, 2025.

[14] N. A. Noordin *et al.*, "The use of artificial intelligence and audit quality: Perspectives of external auditors," *Journal of Risk and Financial Management*, vol. 15, 2022.

[15] J. L. S. Riega-Virú *et al.*, "Cybersecurity and the NIST framework: System implementation and effectiveness," *International Journal of Advanced Computer Science and Applications*, 2025.

[16] D. M. Rofi'ah, "NIST cybersecurity framework in internal auditors' perspective," *Indonesian Interdisciplinary Journal of Sharia Economics*, 2025.

[17] J. A. Calvo-Manzano *et al.*, "CyberESP: Integrated cybersecurity framework for SMEs," *Journal of Software: Evolution and Process*, 2025.

[18] M. Toussaint *et al.*, "Industry 4.0 data security: Review of cybersecurity frameworks," *Journal of Industrial Information Integration*, 2024.

[19] "A decade of cybersecurity research in internal auditing: A bibliometric analysis," *Discover Sustainability*, 2025.
[20] "Automating security audit using LLM agents," arXiv preprint, 2025.
[21] "Revolutionizing cybersecurity audit through AI automation," *International Journal of Advanced Research in Computer and Communication Engineering*, 2024.
[22] "AI for AI audit: Vision from legacy to multi-layered AI auditing," *International Journal of Advanced Research*, 2025.