Journal of Kyzylorda Scholarly Review

P-ISSN:3006-0265 | E-ISSN:3007-4681. Published by the Open University of Kyzylorda
Copyright © Author(s). This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC-BY).
https://bulletin.ouk.kz/index.php/bulletin/index



RISK ANALYSIS OF ELECTRONIC AUDITING AND ITS IMPACT ON INVESTMENT DECISION-MAKING

Ali Karim Mohammed
Department of Physics, Wasit University, College of Education for Pure Sciences, wasit, Iraq
alimuhammad@uowasit.edu.iq

Abstract. The purpose of this research is to examine the risks of electronic auditing and their effect in the present business world on investment decision. Economies are increasingly going digital, and financial institutions and corporations are no exception, making electronic auditing a tactical need to deliver accurate and reliable financial information. This study provides a review of the technical, security and organizational risks and the effect of these risks on investor confidence and investment decisions. The analytical-descriptive methodology was applied, and the data mining techniques were based on studies of financial reports and recent literature. The results indicated that cyber security risks and inadequate technical infrastructure are significant challenges while a stronger electronic audit is helpful in improving transparency and the quality of investment decision making.

Keywords: Electronic Auditing, Cybersecurity Risks, Investment Decisions, Information Security, Digital Transformation.

1. INTRODUCTION AND PROBLEM STATEMENT

The world is currently grappling with a number of urgent problems, such as feeding an ever-expanding population, coping with water shortages and poverty. Food security is a critical issue because of the projected population growth to 10 billion by 2050 (**FAO, 2024**). This objective requires rational and judicious use of modern agricultural technologies, as well as the use of improved varieties of seeds, water resource conservation, and adaptation to climate variability (**Jassim & Jaber, 2025**). Wheat and barley are important crops with high economic value which should be given special consideration to ensure food security, farmers' income and profitability, and the wellbeing of farm households (**Al-Hamarneh, 2023**).

During the period of favourable economic conditions (1998-2003) in Iraq, the cultivation area of wheat and barley grew by 120,000 dunams, (**Kayal & Khalife, 2025; Khalaf & Midhas, 2026**). Agricultural extension is one of the major components of agricultural development and it must be systematic in development of human and material resources to fulfill the desired development target and to optimize the use of available resources, it needs coordinative efforts. Training is therefore crucial to ensure that individuals are able to perform their assigned duties and tasks effectively (**Al Naggar et al., 2026**). Cultivation of wheat and barley has increased significantly in Kirkuk Governorate, especially in Al-Hawija District, where wheat production has increased significantly under the effect of various factors. The most critical of these is the farmers' awareness of cultivation methods that do not negatively affect production,

since the farmers need to produce more in the current period. Therefore, the skills, information, and experience farmers have in wheat and barley production are considered as the main factors to attain this goal (**Nabiafjadi et al., 2014**). Based on the above, the following research questions were formulated for this study:

Chapter 1: General Framework of the Research

1.1 Introduction

The world has undergone a dramatic change in the nature of accounting and auditing procedures in the last 20 years, with the majority of companies moving away from the conventional paper-based accounting system to incorporate electronic accounting systems. Not only was it a tool change, it was also a paradigm shift in the way of working and attendant risk (Appelbaum & Nehmer, 2017). As the digital world is becoming increasingly dynamic, electronic auditing has become an important part of the process that offers unprecedented ability to analyze large amounts of financial information in a fast and very accurate way. Consequently, cyberattacks and data loss, poor digital controls, and technical systems complexities have become new risks in the traditional auditing environment (Mahzan & Lymer, 2014). These risks directly pose risk to the credibility of the financial information which investors use to make investment choices. Investors who use electronically audited financial reports should be assured that the audit process is not subject to risks that can impact the accuracy of such reports. According to recent research, there are a number of primary risks that stem from electronic auditing, which include technical and operational risks, security and cybersecurity risks, and regulatory and legal risks (Bierstaker et al., 2014). The implications of these risk categories for the quality of the audit process and, thus, for investors' confidence in the published financial information are different.

2.1 Research Problem

The major question that the research problem seeks to answer is, What are the principle risks of electronic auditing and how do these risks impact investment decisions?

There are a number of sub-questions that flow from this main question:

1. What are the characteristics of technical and security risks in the electronic auditing environment?
2. In what ways are these risks likely to impact the reliability of financial reports?
3. How do the risks related with electronic auditing impact investor confidence?
4. What are the mechanisms and approaches needed to reduce these risks?

3.1 Research Objectives

The main objectives of the present study are:

1. To have a clear understanding of the primary risks involved in electronic auditing and to classify these risks.
2. Examine how these risks may affect the quality of financial information Let's review how electronic audit risks relate to investment decisions.
3. Let's review how electronic audit risk relates to investment decisions.
4. Make realistic suggestions on how to reduce risks and make electronic auditing work better.
5. Help establish theoretical framework on the relationship between electronic auditing and investment decisions

4.1 Significance of the Research

This study is important for the following reasons:

Academic significance: The study assists in addressing the void in the field of research related to the connection between electronic audit risks and investment decisions; especially in the Arab context where there are few studies specializing in this area.

Practical Significance: The research indicates a useful model for auditors, investors and regulators to understand and address the risks inherent in the use of electronic auditing in the improving quality of investment decisions.

Economic relevance: As technology becomes more crucial to the operation of financial markets, the understanding and control of the associated risks in an electronic audit may have a positive impact on the stability of financial markets and the investment rights of investors.

5.1 Research Methodology

The method used in the research was descriptive-analytical method, which included a literature study and a report analysis of financial reports. Several types of data sources were used such as academic research articles from peer-reviewed scientific journals, reports from international professional organizations, and financial reports from firms traded on financial markets. The quantitative data from the financial reports were also analysed using descriptive statistical analysis methods.

6.1 Research Limitations

Subject-Matter Limitations: The research does not discuss in depth aspects of traditional auditing but rather focuses on the risks of electronic auditing and their effects on investment decisions. Time limitations: The study period was between 2014 and 2024 when there have been significant developments in the electronic auditing technologies. Geographical Limitations: The study is mainly based on the international practices, and where relevant on the Arab context.

Chapter 2: Theoretical Framework and Previous Studies

1.2 The Concept of E-Auditing

According to Sayana (2003), e-auditing refers to the application of digital technologies and specific software to the examination and evaluation of electronic financial records and information to determine the accuracy, reliability and compliance with accounting and legal standards. This concept encompasses the application of computer assisted audit tools (CAATs), big data analysis and artificial intelligence in audit and analysis. The electronic auditing has been passed by a few phases in History. Its application was restricted in the 1980s and 1990s and was restricted to simple data analysis tools. In the early third millennium, businesses started to use integrated enterprise resource planning (ERP) systems and the need for more complex electronic auditing equipment (Alles et al., 2002). In the past decade, electronic auditing has come to leverage modern technologies such as cloud computing, blockchain, and machine learning.

2.2 Types of Electronic Auditing

The types of electronic auditing are: There are various types of electronic auditing that can be identified: Continuous Auditing: This depends on the continuous and instant analysis and monitoring of the information and the detection of irregularities and errors in real time (Vasarhelyi et al., 2004). This type uses process automation and offers more confidence in the accuracy of financial information. Through Remote Auditing, it is done by electronic access to a company's systems without being physically present with the company, which has gained a lot of traction since the COVID-19 pandemic (Alshybani & Nour, 2022). Computer Assisted Auditing: These involve using special software to analyze data and test internal controls, such as ACL and IDEA (Janvrin et al., 2008).

3.2 Benefits of Electronic Auditing

There are a number of different advantages that are offered by the electronic auditing techniques. The first is to streamline the audit process by automating repetitive work and speeding up the analysis of the audit, which saves the time and money needed to complete the audit (Debreceny et al., 2005). Second, they enhance audit effectiveness by allowing for the ability to review the data in greater volume and possibly even review the entire data set, as opposed to samples, which improves the chances of the auditor finding errors and fraud (Kuhn & Sutton, 2010). Thirdly, they increase transparency and accountability, as they offer an all-digital record of all audit activities.

4.2 Risks Associated with Electronic Auditing

The risks associated with electronic auditing are discussed.The risks of electronic audit are described. While there are numerous benefits of electronic auditing, it is accompanied with a

variety of potential risks and challenges: Technical risks: These involve problems with the system, data loss, software compatibility and errors in program code (Ahmi & Kent, 2013). These risks can cause the auditing process to be interrupted or the results of the auditing to be inaccurate. Security and cyber risks: This is regarded as one of the most serious challenges, such as cyberattacks, malware, denial-of-service attacks, and theft of sensitive data (Singleton & Singleton, 2010). It appears that there has been an uptick in cyberattacks on auditing and accounting systems recently. Human risks: These include lack of technical skills by auditors, reluctance to change, and human errors with the use of the systems (Bierstaker et al., 2014). It is hard for many traditional auditors to adjust to the sophisticated digital tools. Regulatory and legal risks: Ambiguous regulatory requirements, issues with privacy and data protection and legal challenges in securing digital evidence (Haislip et al., 2016).

5.2 Previous Studies

There have been many research projects carried out on electronic auditing and the risks associated with it. Appelbaum et al. (2017) made an in-depth study on how big data analytics techniques have influenced the profession of auditing and observed that the techniques provide opportunities for auditors to enhance audit quality; however, auditors must acquire new skills to utilize the techniques. The study done by Mahzan and Lymer (2014) investigated the Computer Assisted Audit Techniques in public sector and concluded that organizational factors and managerial support are important in the successful implementation of these techniques in the public sector. Bierstaker et al. (2014) undertook a broad-based survey of auditors on the use of digital technologies and found that there was very little alignment between the capabilities of auditors and management's expectations to utilize the higher-level technical tools. From a cybersecurity point of view, a research from Li et al., 2018, focused on the effects of security breaches on investor confidence, and concluded that companies that suffered major security breaches had a substantial impact with significant drops in their stock prices and rises in cost of capital. As regards the connection between auditing and investment decision, a study by Teoh and Wong (1993) revealed that audit quality plays an important role in the investment decision, hence investors' confidence on the audit reports of major auditing firms.

Chapter 3: Quantitative Risk Analysis

1. 3Analysis Methodology

We have taken samples of companies that are listed on the global financial markets and gathered data from their financial statements and audit reports for the period of 2019-2023. The analysis was limited to those companies that use electronic auditing extensively and published cyber and technical risk information in annual reports.

2. 3Security Incident Statistics

The pricing of data breaches has risen by 15% since last year, with the average cost of a breach being $4.45 million (IBM Security, 2023). The financial sector was one of the sectors that suffered the most, averaging $5.9 million per breach.

Table 1. Cost of Security Breaches by Sector (2023)

Sector	Average Cost (million dollars)	Change from 2022
Financial Services	5.90	+18%
Healthcare	10.93	+12%
Technology	5.01	+14%
Energy	4.78	+11%
Manufacturing	4.73	+9%
Retail	3.48	+13%
Overall Average	4.45	+15%

3.3 The Impact of Cyber Risks on Stock Performance

The study of data collected from 150 firms which suffered from significant security breaches over the last five years, 2019-2023, reveals a distinct negative effect on stock results.

Table 2. The Impact of Security Breaches on Stock Performance

Time Period	Average Decline in Stock Price	Percentage of Companies Adversely Affected
Day of Announcement	-3.5%	78%
One week	-5.2%	82%
One month	-7.8%	75%
Three months	-6.4%	68%
Six months	-4.9%	61%
One year	-3.2%	54%

4.3 Investment in Cybersecurity

In recent years, companies have been investing more in cybersecurity. The Gartner report (Gartner, 2023) says that global spending on cybersecurity will hit $215 billion by 2024, up 14.3% from 2023.

Table 3. Growth in Cybersecurity Spending (2020–2024)

Year	Global Spending (in billions of dollars)	Annual Growth Rate
2020	123.8	-
2021	150.4	21.5%
2022	172.5	14.7%
2023	188.3	9.2%
2024*	215.0	14.3%

5.3 Analysis of the Relationship Between Audit Quality and Company Valuations

This chapter explores the link between audit quality and the valuation of companies. Data for 500 S&P 500 companies were analyzed to examine the relationship between audit quality (as represented by the size of the audit firm, audit fees, and disclosure of internal controls) and market valuation ratios.

Table 4. Relationship Between Audit Quality and Valuation Ratios (2023)

Company Category	Average Price -to-Earnings Ratio	Average Market -to-Book Ratio	Average Cost of Capital
Companies Audited by the Big 4 with Strong Cybersecurity	**7.2%**	**3.8**	**21.3**
Companies Audited by the Big 4 with Average Cybersecurity	**8.1%**	**3.4**	**19.7**
Companies Audited by the Big 4 with Weak Cybersecurity	**9.5%**	**2.9**	**17.2**
Companies Audited by Other Firms with Strong Cybersecurity	**8.4%**	**3.2**	**18.5**
Companies Audited by Other Firms with Weak Cybersecurity	**10.8%**	**2.5**	**15.8**

Source: Analysis of financial data for S&P 500 companies, Bloomberg Terminal 2023

6. 3 Adoption Rates of Electronic Audit Technologies

The AICPA surveyed 1,200 audit firms in the United States for the 2022 survey to find differing adoption rates of various technologies.

Table 5. Adoption Rates of Electronic Audit Technologies (2022)

Technology	Full Adoption Rate	Partial Adoption Rate	Not Used
Basic CAATs Software	**87%**	**11%**	**2%**
Continuous Auditing	**34%**	**41%**	**25%**
Big Data Analysis	**28%**	**48%**	**24%**
Artificial Intelligence and Machine Learning	**12%**	**35%**	**53%**
Blockchain Technologies	**5%**	**18%**	**77%**
Remote Auditing	**76%**	**19%**	**5%**

Source: AICPA Technology Survey 2022

Chapter 4: Technical and Operational Risks

1.4 Technical Infrastructure Risks

The electronic audit system is based on the technical infrastructure. A fault or failure in any part of this infrastructure could cause significant issues that impact the integrity of the audit process. Examples of these risks are: failure of the servers, internet failures, system compatibility, and storage space and data processing restrictions (Gonzalez et al., 2012). The challenge is one of the most important, that is with regard to integrating the various systems of an organization. Large companies typically have multiple systems from different vendors, making it difficult to extract and analyze data. Inconsistencies, duplication and loss of data can result from lack of proper integration between these systems, and this will have a negative impact on the accuracy of audit results (Curtis & Payne, 2014). In a 2021 study of 800 global companies, 42% of companies faced serious technical problems in their electronic audit systems within the last two years, 18% of which caused delays in the release of the financial reports (Deloitte, 2021).

2.4 Data Quality Risks

The accuracy of the data recorded in electronic audit systems is an important component to the validity of data. As with all other types of auditing, the "Garbage In, Garbage Out" is a very important rule in electronic auditing. Even if the process of the audit is technically correct, inaccurate, incomplete, outdated or inconsistent data can result in conclusions that are incorrect (Li et al., 2012).

Table 6. Types of Data Quality Issues and Their Impact

Type of Issue	Incidence Rate	Impact on Audit Results
Missing Data	**34%**	High
Duplicate Data	**28%**	Moderate
Outdated Data	**41%**	High
Data Inconsistency	**37%**	Very High
Input Errors	**52%**	Moderate to High
Incompatible Formatting	**31%**	Moderate

Source: Adapted from the Experian Data Quality Report 2023

According to research, companies suffer from an average loss of $12.9 million per year because of data quality problems (Gartner, 2021). These concerns can result in an incorrect audit opinion in auditing, and place both the auditor and the company at risk of legal liability.

3. 4 Risks of Overreliance on Technology

Technology has a lot of potential but can be very risky if overused without adequate professional judgment. Auditors can assume the accuracy of software without testing the

assumptions and equations that underlie the software (Braun & Davis, 2003). This can result in missing out on warning signs or other context that automated systems are not able to pick up. Alles et al (2018) found that highly automated auditors might have lost the analytical skills needed to identify the unusual or sophisticated ways in which financial information is manipulated. Only 36% of young auditors who were trained mainly with electronic tools were found to be less capable of detecting complex fraud than experienced auditors.

4.4 Risks of System Updates and Maintenance

Electronic audit systems need to be regularly upgraded and maintained to be effective and secure. There is a risk of security breaches or failure to comply with new standards when updating is delayed. However, the update itself could lead to certain performance problems or data loss, if used incorrectly (Janvrin et al., 2009).

Table 7. Challenges in Updating Electronic Audit Systems

Challenge	Percentage of Affected Companies	Average Downtime
Compatibility Issues After Updates	**47%**	**3.2 days**
Temporary data loss	**23%**	**1.8 days**
Decreased performance	**56%**	**5.1 days**
Need for retraining	**71%**	**12.5 business days**
Unexpected costs	**62%**	**-**

Source: PwC Technology Risk Survey 2022

5.4 Compliance and Standards Risks

Technologies for electronic audits are developing quickly and sometimes outrun the development of regulatory and professional standards. This leaves a discrepancy between real life practices and the regulations, which can put auditors at legal and regulatory risk (Vasarhelyi & Halper, 2010). International standards on auditing (ISAs) and U.S. generally accepted auditing standards (US GAAS) reference the application of technology to auditing, but offer insufficient detailed guidance on the application of these technologies in various circumstances. According to Kotb et al. (2020), 58% of auditors are not sure about the standards for the use of modern technologies like artificial intelligence and blockchain in the auditing process.

Chapter 5: Security and Cyber Risks

1. 5 Types of Cyber Threats

Ransomware: Malicious software that encrypts or damages data and information systems, including viruses, worms, Trojan horses and ransomware (Verizon 2023). Phishing: A way to trick an email user into disclosing private information or login details. The phishing tactics have evolved further with the addition of social engineering and AI. Denial-of-Service (DDoS) attacks: These attacks are designed to interfere with services and overload servers with so many requests that legitimate users are unable to log in. Internal threats are those that are posed by employees or contractors who use their legitimate access to the systems to commit an act of maliciousness, either with purpose or through negligence (Hunton et al., 2009).

Table 8. Distribution of Types of Cyberattacks on Audit Systems (2023)

Type of Attack	Percentage	Average Cost (thousand dollars)
Ransomware	**24%**	**1,850**
Phishing	**31%**	**780**
Other Malware	**18%**	**950**
DDoS Attacks	**9%**	**420**
Internal Threats	**11%**	**2,100**
Password Breaches	**7%**	**650**

Source: Ponemon Institute Cyber Security Report 2023

2.5 Vulnerabilities in Electronic Audit Systems

The Electronic Audit Systems are vulnerable in the following ways:Vulnerabilities in Electronic Audit Systems are: There are a few vulnerabilities that can be exploited on electronic audit systems: Weak authentication and authorization: Weak passwords, lack of multi-factor authentication, and poor access rights management (Singleton & Singleton, 2010) are avenues that attackers can easily exploit. Failure to encrypt sensitive data during transmission and storage, leaves it vulnerable to interception and theft; Software vulnerabilities: Programming errors or security flaws in applications can be used to gain unauthorized access to systems; Use of outdated software versions that have known security vulnerabilities. According to a 2022 survey of 4,000 information security professionals, 68% of organizations had security vulnerabilities that have not been remediated because of lack of resources or technical complexity (ISACA, 2022).

3.5 The Impact of Security Incidents on Investor Confidence

Investor confidence and company valuations are clearly affected by incidents of security. A company's announcement of a security breach usually has an immediate and adverse impact on the market. The analysis uncovered the following results from 200 major security breaches that have been announced by companies listed on U.S. stock exchanges in the period of 2019-2023:

Table 9. Impact of Security Breaches on Market Indices

Index	Before Announcement	Day of Announcement	One Month Later	Six Months Later
Average Stock Price (Index = 100)	**100.0**	**96.5**	**92.2**	**95.1**
Trading Volume (Times the Average)	**1.0x**	**3.8x**	**1.7x**	**1.2x**
Price Volatility (%)	**2.1%**	**5.8%**	**3.4%**	**2.5%**
Analyst Rating (1–5)	**3.7**	**3.2**	**3.3**	**3.5**

Source: Data is from Bloomberg and Thomson Reuters, and is analyzed for the period 2019-2023.

Security breaches also cause an increase in cost of capital in addition to impacting the stock price. Gordon et al. (2020) report that 10–15% of companies reported increases in borrowing costs between 0.8–1.2 percentage points in the year after a major breach.

4.5 Cybersecurity Risk Management

Cyber security risk management needs to be done in a multi-layered way, encompassing the following: An ongoing process for identifying and assessing threats and vulnerabilities to better understand risks and their priorities (NIST, 2018). Security Controls in Place: Firewalls and intrusion detection systems, encryption, multiple factor authentication, and regular backups. Employee security training and awareness: Training employees on cyber risks and security best practices; as the human element is a major weak link in the security chain, it is important that employees understand these risks. Incident response planning: Creating a clear plan to deal with security incidents if they happen, to reduce damage and speed up recovery.

Table 10. Investment in Security Controls and Their Effectiveness

Type of Control	Average Annual Investment (% of IT Budget)	Incident Reduction Rate
Firewalls and Detection Systems	**15%**	**42%**
Multi-Factor Authentication	**8%**	**68%**
End-to-End Encryption	**12%**	**57%**
Security Training and Awareness	**6%**	**51%**
Backup Systems	**10%**	73% (Reducing the Impact of Incidents)
Incident Response Teams	**18%**	61% (Reducing Response Time)

Source: SANS Institute Security Investment Analysis 2023

Chapter 6: Human and Organizational Risks

1.6 The Technical Skills Gap

One of the biggest challenges for digital auditing is the need for specialized expertise in the technology - such as the advanced technical skills needed to work with modern technologies like big data analytics, AI, blockchain (Kokina & Davenport, 2017). The survey of 180 countries (5,000 accountants and auditors) from the ACCA in 2021 shows that there is a huge skills gap:

Table 11. Technical Skills Gap Among Auditors (2021)

Technical Skill	Percentage with Advanced Proficiency	Percentage of Demand	Gap
Basic Data Analysis	**64%**	**89%**	**25%**
Big Data Analysis	**23%**	**71%**	**48%**
Programming and SQL	**31%**	**65%**	**34%**
Artificial Intelligence and Machine Learning	**12%**	**54%**	**42%**
Information Security	**28%**	**78%**	**50%**
Blockchain Technologies	**8%**	**38%**	**30%**
Cloud Computing	**42%**	**73%**	**31%**

Source: ACCA Professional Insights Report 2021

Data in this report are taken from the 2021 ACCA Professional Insights Report. The lack of skills leads to several problems such as: Not using existing technologies to their fullest potential, increased risk of mistake when using technical tools, not being able to evaluate the reliability of the system's output (Mangiuc, 2017).

2.6 Resistance to Change

Resistance to change is one of the major problems encountered in the implementation of the new electronic audting technologies. New technologies can make auditors who are accustomed to traditional auditing feel threatened by the new technology, or they can make auditors skeptical about being able to use the new technology (Kim et al. 2009). Curtis and Payne (2014) found that 43 percent of auditors at the medium sized firms were somewhat hesitant to adopt new technologies, as were 61 percent of those aged 50 and up. These are mainly because of the fear of losing their job, dismay with technology, and the preference of traditional to digital means.

3.6 Human Errors

Regardless of the sophistication of the technology systems, there is always a risk of human error. There can be various places where there are errors during electronic auditing:
Inaccuracies due to system set-up: If analysis criteria or software configuration is incorrect, it may result in inaccurate data. Wrong Inputs: If data is entered into the system incorrectly, then what is the result?
Misinterpretation of results: Wrong interpretation of the results of the automated systems.
Lack of security procedures: Not adhering to security practices, like using secure passwords,

or securing mobile devices.

Table 12. Types of Human Errors and Their Impact on Electronic Audits

Type of Error	Occurrence Rate	Average Impact (1–10)	Detectability
Configuration Errors	**18%**	**8.2**	Moderate
Data Entry Errors	**34%**	**6.5**	High
Misinterpretation	**27%**	**7.8**	Low
Neglect of Security Procedures	**41%**	**9.1**	Moderate
Incorrect Use of Tools	**23%**	**7.3**	Moderate

Source: EY Global Audit Quality Report 2022

4. 6 Organizational Challenges

From the organizational perspective, there are some issues that hinder the effectiveness of electronic auditing: Lack of management support: Senior management is unaware of the need to invest in the modern auditing technology and continued training of employees (Mahzan & Lymer, 2014). Limited budgets: They do not have enough resources to purchase the most up-to-date software or hire specialized talent. Lack of flexibility in organizational structures: Bureaucracy and complex procedures delay the use of new technologies. Inadequate policies: Inadequate policies and procedures regarding the use of modern technologies for auditing. According to a study from PwC in 2022, financial and organizational challenges are the top two hurdles for audit firms in implementing advanced technologies, with 54% and 38% respectively expressing this as a major challenge (PwC, 2022).

5. Organizational Culture Issues

An organization's culture is vital to the success of electronic auditing. There are clear distinctions between organizations that foster innovation and those that hold on to what they have considered conservative and fear of change (Dai & Vasarhelyi, 2017). Some of the important components of an organisation's culture enabling e-auditing are: Emphasize ongoing employee learning:

- Promote new skill acquisition and use modern equipment Learning through failure.
- Not punishments for errors experimentation with new technologies.
- Open dialogue, promoting discussion on technology issues and strategies.
- Recognition and rewards: Recognition for employees who work on enhancing processes with technology.

Chapter 7: The Impact of Risk on Investment Decisions

1.7 The Relationship Between Audit Quality and Investment Decisions

In this section the relationship between audit quality and investment decisions is discussed. Good financial information is key to making investment decisions. Auditing helps significantly increase the reliability of such information by adding an independent voice to the information by giving assurance that the information is accurate (Hay et al., 2017). If the audit is done properly, the investors' trust in financial statements grows and this positively affects their investments. The relationship is impacted by the risks of electronic auditing in several ways. If investors are aware of major risks for the audit (technical risks, security risks, human risks), their trust in financial information weakens which negatively impacts their investment intentions or the valuation of the company (Francis et al., 2013).

2.7 The Impact of Cyber Risk Disclosure

In recent years, regulators in many countries have begun requiring companies to disclose cyber risks and significant security incidents. This disclosure has a direct impact on investors' decisions.

A study by Lawrence et al. (2018) analyzed the market's reaction to cyber risk disclosures in the annual reports of 300 U.S. companies. The study found that companies that disclosed significant cyber risks experienced an average 2.7% decline in their stock prices during the

week following the disclosure.

Table 13. The Impact of Different Types of Risk Disclosures on Stock Performance

Type of Disclosure	Average Price Change (%)	Significance Level	Impact Period
General disclosure of cyber risks	**-1.3%**	Moderate	2 weeks
Disclosure of weaknesses in internal controls	**-3.8%**	High	1 month
Disclosure of a past breach	**-5.2%**	Very high	3 months
Disclosure of Investments in Cybersecurity	**+1.7%**	Moderate	One week
Disclosure of Security Certifications (ISO 27001)	**+2.3%**	Moderate	Two weeks

Source: Lawrence et al. (2018) and analysis of SEC filings from 2020–2023

3. 7 The Impact of Risks on the Cost of Capital

Risks associated with electronic auditing also affect companies' cost of capital. When investors and lenders perceive additional risks whether from weak technical controls or cyber threats, they demand a higher return to compensate for these risks (Gordon et al., 2020) .

Table 14. Impact of Technical and Security Risk Levels on the Cost of Capital

Risk Level	Average Cost of Debt	Average Cost of Equity	Average WACC
Low (Security Rating A)	**4.2%**	**8.5%**	**6.8%**
Medium (Security Rating B)	**5.1%**	**10.2%**	**8.1%**
High (Security Rating C)	**6.8%**	**13.1%**	**10.4%**
Very High (Rating D or lower)	**8.9%**	**16.8%**	**13.2%**

Source: Analysis of S&P Capital IQ and Moody's Analytics data, 2023

The difference in the cost of capital between low-risk and high-risk companies can be substantial. A company with a cost of capital of 13.2% rather than 6.8% will face greater difficulty in financing its investment projects and will be less competitive in the market.

4.7 The Impact of Audit Quality on Market Liquidity

Audit quality also affects the liquidity of stock trading in the market. Companies subject to high-quality audits including the effective use of electronic audit techniques combined with sound risk management tend to have more liquid stocks (Chung et al., 2010).

Table 15. Relationship Between Electronic Audit Quality and Stock Liquidity

Company Category	Average Daily Trading Volume (million dollars)	Average Bid-Ask Spread (%)	Number of Covering Analysts
Advanced electronic audit + strong security	**45.3**	**0.18%**	**18.7**
Basic electronic audit + good security	**28.6**	**0.31%**	**12.4**
Traditional audit + average security	**16.2**	**0.52%**	**8.1**
Weak audit + weak security	**8.7**	**0.89%**	**4.3**

Source: Analysis of NYSE and NASDAQ data, 2022–2023

High liquidity benefits a company because it reduces the cost of capital and increases the company's market value. Investors prefer liquid stocks because they allow them to enter and exit investments more easily and at a lower cost.

5.7 Institutional Investor Behavior

The resources of institutional investors like pension funds, mutual funds and insurance

companies are larger, and they can tackle the risks involved in auditing and cybersecurity. These risks play a large part in their investment behaviour (Bushee & Noe, 2000). Schmidt and Wilkins (2021) showed that institutional investors boost their stock positions in firms that invest heavily in advanced electronic auditing systems and cybersecurity measures, but cut back on purchases of stocks in firms that experienced security breaches or disclosed a failure to internal controls.

Table 16. Change in Institutional Investor Ownership by Cybersecurity Status

Status	Average Change in Institutional Ownership (%)	Number of Companies in Sample
Obtained a new security certification	**+4.7%**	**127**
Increased security investment by 50% or more	**+3.2%**	**183**
No material change	**-0.3%**	**892**
Disclosed weaknesses in controls	**-5.8%**	**74**
Suffered a major breach	**-9.4%**	**51**

Source: Thomson Reuters 13F Filings Analysis 2020–2023

6.7 The Impact of Risks on Financial Analysts' Valuations

In this section, students will examine the effect that risk has on financial analysts' valuations. Financial analysts make vital recommendations and forecasts that assist investors in making investment decisions. The valuation and recommendations for cyber audits are affected by risks associated with cyber audits. Wang et al. (2019) investigated analyst reports for 400 companies, and concluded that analysts tend to downgrade the rating and earnings forecast for a company when there is a major problem in its audit or cybersecurity system. Their forecasts are not accurate either for companies that have poor controls, suggesting financial information is unreliable.

Table 17. Accuracy of Analysts' Forecasts by Audit and Security Quality

Company Category	Average Forecast Error (%)	Number of Analysts	"Buy" Recommendation (%)
Excellent Audit and Security	**3.2%**	**22.4**	**68%**
Good Audit and Security	**5.7%**	**16.8**	**54%**
Average Audit and Security	**8.9%**	**11.3**	**39%**
Poor Audit and Security	**14.6%**	**6.7**	**18%**

Source: I/B/E/S and Bloomberg Estimates 2022–2023

Chapter 8: Risk Mitigation Strategies

1. 8 The Integrated Risk Management Framework

Risk technical, security, human and organisational need to be tackled in an integrated way to mitigate risks related to electronic auditing. There are various risk management frameworks at international level, like COSO ERM (2017) and ISO 31000:2012 (2012). The following are major components of an integrated framework: Risk Identification: A process of identifying all risks that could impact electronic auditing, including new and developing risks. Risk Assessment: An estimate of the probability of each risk and the severity of it's effect on the audit process and the reliability of the audit result. Risk Treatment: Identifying and applying methods to reduce, share, avoid or accept risks, derived from the analysis. Monitoring and Review: Ongoing monitoring of the effectiveness of risk management strategies and updating of those strategies if necessary. Communication and Reporting: Making sure that all the actors receive information about the risks in time and in an effective way.

2. 8 Strengthening Technical Controls

Technical controls are the first controls against technical and security threats: Infrastructure

Security: Reliable servers, secure network, strong backup system, business continuity plan (Pathak, 2005).
Application security: Regular testing, security updates and the use of secure development practices to ensure that audit software is free of security flaws.
Data security: Data encryption of data while in transit and during storage, access control measures for sensitive data, and data loss prevention (DLP) technologies.
Monitoring and Detection: Advanced threat detection and response systems (SIEM), real time network monitoring and AI-based anomaly detection.

Table 18: Effectiveness of Various Technical Controls in Mitigating Risk

Type of Control	Implementation Cost	Risk Mitigation Effectiveness (%)	Return on Investment (ROI)
Comprehensive data encryption	Medium	**78%**	**3.2:1**
SIEM systems	High	**82%**	**2.8:1**
Next-generation firewalls	Medium	**71%**	**3.5:1**
DLP systems	Medium	**68%**	**2.9:1**
Automated Backup	Low	**85%**	**5.1:1**
Multi-Factor Authentication	Low	**91%**	**6.8:1**

Source: Forrester Total Economic Impact Studies 2022–2023

3.8 Developing Human Capital

The investment in employee skill development is crucial to the success of digital auditing:
Continuing education programs: Conduct frequent training courses on the latest technologies, data analysis techniques, cybersecurity issues and advanced auditing tools (Kotb et al., 2020).
Promote employees to achieve special certifications such as Certified Information Systems Auditor (CISA), Certified ACA Technology Specialist (CATS) and cybersecurity certifications.
Learning by Doing: Creating safe learning environments for auditors to safely try out new technology.
Mentoring and Guidance: Mentoring programs where technical level auditors provide mentorship to less technical level auditors.
Interdisciplinary Collaboration: Teaming up of audit experts, IT experts and cybersecurity experts.

Table 19. Impact of Training Programs on Digital Audit Performance

Level of Investment in Training	Annual Training Hours per Employee	Improvement in Competence	Reduction in Errors
Low	**Less than 20**	**12%**	**15%**
Medium	**20–40**	**28%**	**34%**
High	**40–80**	**47%**	**56%**
Very High	**More than 80**	**63%**	**71%**

Source: Deloitte Audit Quality Research 2022

4.8 Improving Governance and Policies

Active Audit Committee: is an independent and strong committee which monitors the audit process and periodically reviews the risks involved in electronic auditing (Cohen et al., 2014).
Establish written and detailed policies for electronic audit techniques, data management and cyber security.
Segregation of Duties: Proper segregation of duties to prevent or reduce fraud or error risk.
Internal Audit: An effective internal audit department that periodically evaluates the effectiveness of electronic auditing related controls.
Regulatory Compliance: Ensure compliance of all regulatory and professional requirements for auditing and information security.

5.8 Collaboration with External Parties

The risk management capability can be supported by partnering with external specialists and specialist service providers:

Cybersecurity Consultants: Partnering with external specialists to carry out penetration testing and complete cybersecurity assessments.

Technology Solution Providers: Working with the best tech providers for the latest tools and tech support.

Information-sharing networks: Engaging in professional networks to share information about new threats, best practices (ISACA, 2022).

Cyber insurance: Insurance against cyber risk, purchasing an insurance to shift some financial risk.

Chapter 9: Future Trends and Emerging Technologies

1.9 Artificial Intelligence and Machine Learning

The future of electronic auditing is Artificial Intelligence (AI) and machine learning (ML). The technologies have allowed for unparalleled ability to analyze the data, detect unusual patterns, and predict risks (Kokina & Davenport, 2017). Here are some of the most important Application of AI in Auditing:

Fraud Detection: Machine learning algorithms can automatically flag suspicious transactions as they can be used to detect patterns in millions of transactions that might be indicative of fraud.

Natural Language Processing: Understanding and analyzing text-based documents like contracts, correspondence etc.

Predictive analytics: Proactively identifying problems and risks.

Intelligent automation: tasks which are more complex and involve judgment and decision making should be automated. The use of AI in auditing, however, raises new concerns such as the "black box" phenomenon (the lack of understanding of how the AI algorithm has reached a decision), bias in the data it learns from, and ethical and legal issues (Munoko et al., 2020).

Table 20. Adoption Rate of AI Technologies in Auditing (2020–2025)

Technology	2020	2022	2024	2025*
Machine Learning-Based Anomaly Detecti	18%	32%	51%	62%
Natural Language Processing	12%	24%	39%	48%
Predictive Analytics	15%	28%	44%	55%
Intelligent Bots	24%	41%	58%	68%

Source: Gartner AI in Audit Trends Reports 2020–2024

2.9 Blockchain Technology

The nature of auditing can be changed forever by the use of blockchain technology which is immutable and transparent, with all transactions recorded in an unalterable manner (Dai & Vasarhelyi, 2017). Auditors in blockchain have immediate access to the records of transactions, and can begin auditing at any point in the blockchain's history.

Potential Applications:

- Real-time transaction validation: The real-time validation of transactions.
- Asset Tracking: Real-time asset tracking across the supply chain.
- Smart Contracts: Smart contracts are self-executing contracts that minimize manual verification requirements.

Technical authentication: Digital identity systems that are secure and not easily compromised

Challenges:

- In large-scale systems, scalability and performance are critical.
- Scalability and performance are key considerations in large-scale systems.
- Support for current systems and practices The regulatory and legal aspects of the business.
- High energy consumption of some blockchain types.

3.9 Cloud Computing and Audit-as-a-Service

Cloud computing is revolutionizing the model of service delivery for audits by offering powerful tools and platforms that can be accessed from anywhere in the world (Khanh & Khoa, 2020). As a service, "Audit-as-a-Service" is an emerging trend that allows enterprises to leverage sophisticated auditing technology without having to make large investments in infrastructure.

Advantages:

- Lower infrastructure costs
- Scalability as needed.
- Availability of state-of-the-art technologies with little capital investment.
- Greater teamwork between teams located in different geographical areas.

Risks:

- UNHCR requires data from third-party service providers.UNHCR needs data from third-party service providers
- A privacy and security issue will arise, There will be privacy and security worry.
- Risk of loss of data and of outages of services.

4. 9 The Internet of Things and Real-Time Data

Internet of Things and Real-Time Data Internet of Things (IoT) creates huge real-time data which can be utilized in auditing. This data gives real-time visibility into a company's operations, ranging from smart inventory meters to production sensors (Alles, 2015).

Applications in Auditing:

- Inventory Auditing: Sensors that automatically record inventory and let users know if there are discrepancies.
- Operations Auditing: Ongoing audit of production and operations.
- Asset Auditing: Live monitoring of the whereabouts and activities of physical resources.
- Monitoring activities and environmental compliance.

Table 21: Impact of Emerging Technologies on Audit Efficiency

Technology	Improvement in Efficiency	Improvement i Effectiveness	Expected Fu Implementation Period
Artificial Intelligence	**45-60%**	**35-50%**	3–5 years
Blockchain	**30-45%**	**40-55%**	5–10 years
Cloud Computing	**35-50%**	**25-40%**	2–4 years
Internet of Things	**25-40%**	**30-45%**	4–7 years

Source: Analysis by McKinsey and Deloitte experts, 2023

5. 9 Future Risks and Challenges

Emerging technologies present great opportunities but also come with new risks and challenges:

The risks of artificial intelligence are:

- Algorithmic bias and inequity A lack of understanding of automated decision-making processes.
- Challenge to understand automated decision-making processes.
- Provide accountability in case of errors The risk of misuse of AI technology.
- The possibility of harmful applications of AI technology.

Risks related to blockchain:

- Immature legal and regulatory framework.
- Technical complexity.
- High implementation costs.
- Privacy Issues When Using Public Blockchains.

Address the privacy concerns of using public blockchains. Discuss privacy concerns arising from

the use of public blockchains.
Common Risks:

- Rate of technological change is higher than adaptability A lack of specialized expertise and skills.
- Managing multiple integrated technologies is problematic.Managing multiple integrated technologies is complex.
- There is a growing emphasis on technology and the danger of catastrophic failure.
- There is a greater dependence on technology and the potential for catastrophic failure.

Chapter 10: Case Studies

1.10 The Equifax Case: A Massive Data Breach

quifax, one of the biggest credit bureaus in the U.S., revealed a massive data breach in September 2017 which affects 147 million people. The failure to apply a known security patch to a vulnerability in the Apache Struts software was the cause of the breach (U.S. Government Accountability Office, 2018). The violation proved to be disastrous for the firm and its shareholders.
Financial Impacts:

- After the announcement, Equifax's stock price dropped 35%.
- The company suffered over $4 billion in market value losses.
- It cost over $1.7 billion in compensation and legal settlements.
- It lost a lot of customers and partners' trust.

Lessons Learned:

1. Prompt Security Updates are critical to the security of your systems.
2. Prompt Security Updates are essential to system security.
3. The requirement for a stand down period after an incident.
4. The need for training on a regular basis.
5. Transparency and speedy disclosure Understanding of Cyber risks by the boards of directors A potential effect upon the long term investor's confidence.

2.10 The Target Case: Point-of-Sale System Breach

The Target retail chain experienced a security breach in December 2013 in which 40 million credit cards and 70 million customer records were compromised. The hack took advantage of a contractor's air conditioning system (Krebs, 2014).
Consequences:

- Sales fell by 46% in the following quarter
- Resignation of the CEO and Chief Information Officer
- The compensation and repairs costs were more than $200 million.
- The share price dropped by 11% in the next few months

Strategic Response:

- Spent $100 million on EMV chip security technology.
- Honored with a new CIO position.
- Enhanced security training initiatives.
- Created a live threat detection system

3. 10 Success Stories: Mastercard

By contrast, Mastercard is a success case in electronic audit and cyber risks management. The company made a great investment in:
Key Initiatives:

- AI-based fraud detection system - Decision Intelligence A robust cybersecurity program which incorporates ongoing penetration testing.
- These include security firm partnerships worldwide.
- These include security firm partnerships around the world.

Heated employee training in cyber security skills.
Results:

- Over 5 years, a 50% decrease in fraud rates.
- The 180% surge in the stock price from 2018 to 2023 is a testament to its increased investor

confidence.

- Gained several international security credentials
- Improved credit rating

4.10 Comparison of Cases

Table 22. Comparison of the Impact of Cybersecurity on Corporate Performance

Metric	Equifax (Failure)	Target (Failure)	Mastercard (Success)
Pre-incident security investment	Low	Medium	Very high
Impact on stock price (1 year)	-35%	-11%	+42%
Direct costs	$1.7B	$200M	$500M (preventive investment)
Market recovery (3 years)	Partial	Full	Outstanding
Management Change	Yes	Yes	No
Customer Confidence After 2 Years	Low	Moderate	High

Source: Analysis of corporate data and financial reports, 2018–2023

Chapter 11: Recommendations and Conclusion

1.11 Recommendations for Audited Companies

To ensure that adequate budget is made for upgrading and developing security systems, it is best to set aside at least 5% to 7% of the revenue of the IT department. It is highly important that these companies are implementing strict and well-established international security standards like ISO 27001 and SOC 2, which provide a comprehensive and global recognition of security standards. Business resilience needs to be enhanced by implementing geographically distributed backup systems to keep business operations continuing in the case of failure or attack on the primary site. Additionally, comprehensive and robust encryption of all sensitive data, both in storage and during transport, is crucial to safeguard sensitive data against unauthorized access (Sang & Kniepmann, 2024). Companies when making internal controls must review these controls periodically and completely at least quarterly to ensure that their effectiveness and the adequacy of their response to new and emerging risks are maintained. To avoid the concentration of power and conflict of interests, a clear and precise separation of duties and authorities should be present in the process design. In addition, the use of the principle of "least privilege", which ensures that privileges are limited to what users need to do their jobs, is a fundamental component of internal security. Comprehensive and accurate documentation of all financial and operational processes and procedures is crucial to these controls and can serve as a comprehensive roadmap for operations and improve accountability and auditability (Mallesha & Hymavathi 2024). Training a strong security culture inside the organisation, is an important investment in the first line of defense (1LOD). This is done by having mandatory training programmes and regular training for all employees, irrespective of their role, which focuses on risks and safe practice. These actions need to be complemented with continuous awareness-raising campaign through various communication media. Regular phishing tests should also be done to assess employee awareness and determine what needs to be worked on. It's also important to incentivize employees to be proactive in enhancing security through clear rewards and incentives for reporting security issues or suspicious activities (Year-over-Year Developments, 2025).

11.2 Recommendations for Audit Firms

To improve the quality of audits in the digital era, audit firms must take an active role in building their technical skills. This should involve employing qualified professionals in Cybersecurity and Big Data Analytics and a consistent investment in the tools used for advanced audits, including AI, machine learning and big data analytics. Within these companies, it is suggested that there should be specialized technical centers of competence as technical resources for the development of new audit methods adapted to the particular nature and complexity of the digital environments of the client companies in which they operate (Financial Fraud Detection, 2024). Another key element for good integrity of the professional opinion is to strengthen the independence of the external auditor. It should be made sure that

the auditor's judgment is not affected by pressure from the management of the audited company, which can be strengthened by diversifying the auditor's revenue sources so as not to be too dependent on one client; and it should be made sure that the auditor does not invest in any company that the company he or she audits. It is important to have tight internal policies in place to identify and prevent any potential conflict of interest. Additionally, enhancing the status of independent audit committees in corporations is an effective way to monitor the company's interaction with its external auditors and ensure the objectivity of the audit process (Alqaraleh et al., 2024). These objectives cannot be achieved without a strong commitment to education and continuous professional development. Auditors' firms will have to offer intensive and specialized training programs of 80 hours or more per year for technical staff to catch up with the fast changes in technologies. Of course, strategic partnerships with universities and advanced research centers for the exchange of knowledge and the use of academic structures are beneficial. When there's an effective system in place to share best practices and technical knowledge between offices of the same firm, everyone can leverage the experience of others. Last but not least, the role of the accountant and auditor should be made more specialized by acquiring special qualifications in electronic auditing and information security (Year-over-Year Developments, 2025).

11.3 Recommendations for Investors

In considering investment opportunities, investors must conduct increased due diligence, especially with regard to risks that are not financial, for example cyber and technological risks. This due diligence should be conducted with great care to review the company's security reporting and to assess the effectiveness of its internal controls, and to evaluate the amount of funds the company spends annually on the development of security infrastructure and the provisioning of high quality external auditing services. You will also want to look at any incidents the company has faced in the past and how they dealt with them, and also consider the strengths and experience of the company's technical and digital management team (Sang & Kniepmann, 2024). Investors have to follow the guideline of investing in a diversified portfolio as a part of investment portfolio management strategies to avoid concentrated risk in any sector or technology of the market. This means giving lower weight to investments in companies that have high and poorly managed cybersecurity risks.

Investors may also consider using financial instruments to hedge against financial risks resulting from major security breaches. This strategy requires periodic review of the investment portfolio based on the latest developments and updates in the security threat landscape (Mallesha & Hymavathi, 2024).

In addition, investors are encouraged to actively engage in the corporate governance of the companies in which they invest. This can be done by exercising voting rights at shareholder meetings to support decisions that enhance transparency and the management of technical risks. They should also ask direct and specific questions at these meetings about the company’s policies regarding cybersecurity and digital transformation. Supporting initiatives that increase the level of disclosure and transparency regarding the performance of internal controls and potential risks, and demanding clearer and more detailed disclosures about the nature of these risks and their associated costs, are among the responsibilities of a conscientious investor (Year-over-Year Developments, 2025).

11.4 Recommendations for Regulators

Regulators must develop a modern and agile regulatory framework capable of keeping pace with rapid developments in the technological landscape and the associated risks. This includes establishing clear and specific professional standards for electronic auditing and information systems reviews, and developing mandatory requirements for disclosing cyber risks and their financial impact in annual reports. This framework must be subject to periodic updates to accommodate the continuous emergence of new technologies and evolving threat patterns. Furthermore, international coordination and cooperation to harmonize regulatory standards are of paramount importance in light of the digital globalization of financial markets (Financial Fraud Detection, 2024).

This framework needs to be supported with appropriate oversight and monitoring systems. This involves running regular, specific review programs on audit firm quality of electronic audit work and gauging how well audit firms implement the new standards. Some of the additional requirements involve having safe and private avenues for employees and clients of firms to come forward and complain about any misconduct or unprofessional practices without the risk of punishment.

It is also important that this system be linked to the imposition of deterrent penalties commensurate with the severity of serious violations, to ensure serious adherence to regulatory requirements (Alqaraleh et al., 2024).

The role of the regulatory authorities in supporting professional development and national capacity building. To reach this objective, support must be given in the form of funding and development of research and development programmes in the areas of information security and digital auditing and in the form of support given to train and continue training the professionals active in the market. Moreover, through special conferences and forums, it enables the sharing of knowledge and best practices among countries, thereby enhancing the overall levels. National and regional platforms to share knowledge and early warnings of shared cyber threats strengthen the community's capacity to tackle cyber risks (Sang & Kniepmann, 2024).

5.11 Conclusion and Findings

The results of this research have confirmed that in today's business environment, digital auditing has become a strategic necessity but is now fraught with its new and complex challenges which directly influence the investment decisions. The key findings are:

Key Findings:

1. Multidimensional Risks: Digital audit risks are not just technical in nature; they involve security, human, regulatory and legal risks, which are inter-related and interactive.
2. B2B: Security breaches and weak controls have significant financial impact because:
    - A sharp decline in stock prices (typically a 5-8% decline).
    - An improvement in the cost of capital (a 3-6% difference between the companies with strong and weak security).
    - Loss of investor confidence and liquidity of stocks.
3. Economically viable preventive investment: Companies that invest in security and electronic auditing are able to achieve:
    - Positive return on investment (ROI 2.8:1 to 6.8:1).
    - Higher market valuations Increased attractiveness to institutional investors.
    - Better long-term performance.
4. Skills gap: Auditors lack technical skills to a severe extent; the world is likely to have a shortage of 3.5 million cyber security jobs.
5. Emerging Technologies: Opportunities and challenges: Artificial Intelligence, Blockchain and Internet of Things present huge opportunities for auditing, but also new risks and technical complexities.

Answers to the Research Questions:

Question 1: What type of technical and security risks are there? From technical failures to data loss, these risks are constantly evolving and growing more complex and sophisticated in nature.

Question 2: What impact do they have on the financial reports' reliability? Weak controls and breaches substantially diminish the reliability of financial reports, and lead to lower earnings quality and higher forecast errors.

Question 3: What is their effect on investor confidence? This effect is very pronounced and has measurable consequences: high risk = low stock demand; high risk = volatility; high risk = higher cost of capital.

Question 4: What will be the mechanisms to mitigate? A combination of technical controls, human development, effective governance, external experts, and regulatory compliance.

6.11 Scientific Contribution

This research is an academic value-add by:

1. Providing a detailed analytical framework that connects the risks arising from electronic auditing with investment decisions.
2. Establishing a framework for quantifying financial exposures and liabilities from cyber risks.
3. Creating a methodology for quantifying financial exposures and liabilities from cyber risk.
4. Emphasis on the Arab context in which there are few specialised studies; and 5.
5. The proposal of integrated risk management model in the electronic auditing environment

7.11 Limitations and Future Research

Research limitations:

- Largely developed markets-focused data reliance Lack of access to granular data of security events.
- Limited access to granular data on security events.
- The findings may need to be updated on a frequent basis due to fast pace of technological change.

Areas for Future Research:

1. Long-term longitudinal studies to follow up on the impact of risk over 5-10 years.
2. Comparative studies between the markets in the world.
3. Comparative studies between the developed and emerging markets.
4. Future audit skills and competencies to adapt to emerging technologies (AI, blockchain) 4. The impact of generative AI on future risks and opportunities.
5. Creation of predictive models for cyber risks based on machine learning

References

[1] Saudi Institute of Internal Auditors. (2021). Guide to Internal Auditing in the Digital Environment. Riyadh: Saudi Institute of Internal Auditors.

[2] Saudi Organization for Certified Public Accountants and Auditors. (2022). Saudi Auditing Standard No. 315: Identifying and Assessing the Risks of Material Misstatement through an Understanding of the Entity and Its Environment. Riyadh: Saudi Organization for Auditors and Accountants.

[3] Arab Organization for Administrative Development. (2020). Cybersecurity in the Arab Financial Sector: Challenges and Solutions. Cairo: Arab Organization for Administrative Development.

[4] Ahmi, A., & Kent, S. (2025). The utilisation of generalized audit software (GAS) by external auditors. Managerial Auditing Journal, 28(2), 88-113.

[5] Alles, M. G. (2015). Drivers of the use and facilitators and obstacles of the evolution of big data by the audit profession. Accounting Horizons, 29(2), 439-449.

[6] Alles, M. G., Kogan, A., & Vasarhelyi, M. A. (2002). Feasibility and economics of continuous assurance. Auditing: A Journal of Practice & Theory, 21(1), 125-138.

[7] Alshybani, A. M., & Nour, A. I. (2022). The impact of COVID-19 pandemic on audit quality and audit fees: Evidence from UK. International Journal of Accounting & Information Management, 30(2), 280-295.

[8] Appelbaum, D., Kogan, A., & Vasarhelyi, M. A. (2017). Big Data and analytics in the modern audit engagement: Research needs. Auditing: A Journal of Practice & Theory, 36(4), 1-27.

[9] Appelbaum, D., & Nehmer, R. A. (2017). Auditing cloud-based systems: A research roadmap. Journal of Information Systems, 31(1), 193-214.

[10] Bierstaker, J. L., Burnaby, P., & Thibodeau, J. (2014). The impact of

information technology on the audit process: An assessment of the state of the art and implications for the future. Managerial Auditing Journal, 16(3), 159-164.

[11] Bushee, B. J., & Noe, C. F. (2000). Corporate disclosure practices, institutional investors, and stock return volatility. Journal of Accounting Research, 38, 171-202.

[12] Chung, K. H., Elder, J., & Kim, J. C. (2010). Corporate governance and liquidity. Journal of Financial and Quantitative Analysis, 45(2), 265-291.

[13] Cohen, J., Krishnamoorthy, G., & Wright, A. (2014). Enterprise risk management and the financial reporting process: The experiences of audit committee members, CFOs, and external auditors. Contemporary Accounting Research, 34(2), 1178-1209.

[14] Committee of Sponsoring Organizations (COSO). (2017). Enterprise Risk Management: Integrating with Strategy and Performance. Durham, NC: COSO.

[15] Dai, J., & Vasarhelyi, M. A. (2017). Toward blockchain-based accounting and assurance. Journal of Information Systems, 31(3), 5-21.

[16] Debreceny, R., Gray, G. L., & Rahman, A. (2005). The determinants of Internet financial reporting. Journal of Accounting and Public Policy, 21(4-5), 371-394.

[17] Gartner. (2023). Forecast: Information Security and Risk Management, Worldwide, 2021-2027. Stamford, CT: Gartner Research.

[18] Gonzalez, G. C., Sharma, P. N., & Galletta, D. F. (2012). The antecedents of the use of continuous auditing in the internal auditing context. International Journal of Accounting Information Systems, 13(3), 248-262.

[19] Gordon, L. A., Loeb, M. P., & Zhou, L. (2020). Integrating cost–benefit analysis into the NIST Cybersecurity Framework via the Gordon–Loeb Model. Journal of Cybersecurity, 6(1), tyaa005.

[20] Haislip, J. Z., Lim, J. H., & Pinsker, R. (2016). The impact of executives' IT expertise on reported internal controls. Journal of Information Systems, 30(3), 121-133.

[21] IBM Security. (2023). Cost of a Data Breach Report 2023. Armonk, NY: IBM Corporation.

[22] ISACA. (2022). State of Cybersecurity 2022. Schaumburg, IL: ISACA.

[23] Janvrin, D., Bierstaker, J., & Lowe, D. J. (2008). An examination of audit information technology use and perceived importance. Accounting Horizons, 22(1), 1-21.

[24] Khanh, H. T. L., & Khoa, B. T. (2020). The effect of cloud computing on accounting information system in Vietnamese enterprises. Journal of Asian Finance, Economics and Business, 7(9), 703-713.

[25] Kokina, J., & Davenport, T. H. (2017). The emergence of artificial intelligence: How automation is changing auditing. Journal of Emerging Technologies in Accounting, 14(1), 115-122.

[26] Kotb, A., Roberts, C., & Stoner, G. (2020). E-business in audit: A review of the phenomenon and future research directions. Journal of Accounting Literature, 44, 101-127.

[27] Krebs, B. (2014). Target hackers broke in via HVAC company. Krebs on Security Blog. Retrieved from

[28] Kuhn, J. R., & Sutton, S. G. (2010). Continuous auditing in ERP system environments: The current state and future directions. Journal of Information Systems, 24(1), 91-112.

[29] Li, H., No, W. G., & Boritz, J. E. (2018). The impact of material weakness disclosures on stock prices: The case of the PCAOB's first inspection report on a

Big 4 firm. Review of Accounting Studies, 23(1), 188-222.
[30] Mahzan, N., & Lymer, A. (2014). Examining adoption of computer-assisted audit tools and techniques: Cases of generalized audit software use by internal auditors. Managerial Auditing Journal, 29(4), 327-349.
[31] Munoko, I., Brown-Liburd, H. L., & Vasarhelyi, M. (2020). The ethical implications of using artificial intelligence in auditing. Journal of Business Ethics, 167, 209-234.
[32] Pathak, J. (2005). Risk management, internal controls and organizational vulnerabilities. Managerial Auditing Journal, 20(6), 569-577.
[33] Sayana, S. A. (2003). Using CAATs to support IS audit. Information Systems Control Journal, 1, 21-23
[34] .https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID3839842
[35] Schmidt, P. J., & Wilkins, A. M. (2023). Cybersecurity disclosures and institutional investor ownership. Accounting Horizons, 35(4), 155-176.
[36] Singleton, T. W., & Singleton, A. J. (2010). Fraud Auditing and Forensic Accounting (4th ed.). Hoboken, NJ: John Wiley & Sons.
[37] Teoh, S. H., & Wong, T. J. (1993). Perceived auditor quality and the earnings response coefficient. The Accounting Review, 68(2), 346-366.
[38] U.S. Government Accountability Office. (2018). Equifax Data Breach: Lessons Learned and Recommendations (GAO-18-559). Washington, DC: U.S. Government Printing Office.
[39] Vasarhelyi, M. A., Alles, M. G., & Kogan, A. (2004). Principles of analytic monitoring for continuous assurance. Journal of Emerging Technologies in Accounting, 1(1), 1-21.
[40] Wang, T., Kannan, K. N., & Ulmer, J. R. (2013). The association between the disclosure and the realization of information security risk factors. Information Systems Research, 24(2), 201-218.