The Impact of Information Technology Risks on Audit Quality: Evidence from Egypt

تأثير أثر مخاطر تكنولوجيا المعلومات على جودة المراجعة: دليل من مصر

Dr. Ayman Mohamed Sabry Nokhal

Associated Professor of Accounting

Faculty of Commerce – Kafr El Sheikh University

مجلة الدراسات التجارية المعاصرة

كلية التجارة – جامعة كفر الشيخ

المجلد (١١) - العدد (٢١) - الجزء الثاني

يوليو ٢٠٢٥م

رابط المجلة: https://csj.journals.ekb.eg

Abstract

This study investigates the impact of information technology (IT) risks on audit quality, with a focus on the Egyptian context. As organizations increasingly rely on IT systems for operational efficiency, data management, and competitive advantage, the associated risks—such as cyber-attacks, data breaches, and system failures—pose significant challenges to audit quality. The study explores how IT risks influence material misstatements, audit risks, and earnings management, aiming to provide insights into the complexities auditors face in an increasingly digital environment.

A theoretical framework was developed, and a field study was conducted using a survey questionnaire distributed to sample of academic staff and external auditors in Egypt. The findings reveal that IT risks significantly impact audit quality, with virus-related risks being the most prominent, leading to material misstatements. Additionally, the integration of IT has enhanced auditing methods and procedures, enabling auditors to leverage technology for greater efficiency and effectiveness. However, to effectively manage these risks and maximize the benefits of IT, auditors require specialized skills and advanced proficiency, which can be developed through continuous education and practical experience.

The study concludes that while IT risks pose significant challenges to audit quality, they also offer opportunities for improving audit processes. Recommendations include staying updated with technological advancements, enhancing information security measures, and developing specialized auditor skills. The findings contribute to the growing body of knowledge on IT risks and audit quality, offering practical insights for auditors and organizations

striving to maintain high standards of audit quality in a rapidly evolving technological landscape.

Keywords: Information Technology Risks, Audit Quality, Material Misstatements, Audit Risks, Earnings Management, Egypt.

الملخص

هدفت هذه الدراسة إلى تحليل تأثير مخاطر تكنولوجيا المعلومات (IT) على جودة المراجعة، مع التركيز على البيئة المصرية. ومع اعتماد المنظمات بشكل متزايد على أنظمة تكنولوجيا المعلومات لتعزيز الكفاءة التشغيلية، وإدارة البيانات، وتحقيق المزايا التنافسية، فإن المخاطر المرتبطة بها—مثل الهجمات الإلكترونية، وانتهاكات البيانات، وفشل الأنظمة—تشكل تحديات كبيرة لجودة المراجعة. وقد تناولت الدراسة ذلك من خلال دراسة اثر مخاطر تكنولوجيا المعلومات على الأخطاء الجوهرية، ومخاطر المراجعة، وإدارة الأرباح .

تم تقديم إطار نظري، وإجراء دراسة ميدانية باستخدام قائمة استقصاء تم توزيعها على عينة من أعضاء هيئة التدريس والمراجعين الخارجيين في مصر. كشفت النتائج أن مخاطر تكنولوجيا المعلومات تؤثر بشكل كبير على جودة المراجعة، حيث تعد المخاطر المتعلقة بالفيروسات الأكثر تأثيرا، مما تؤدى إلى زيادة الأخطاء الجوهرية في البيانات. بالإضافة إلى ذلك، أدى الاعتماد على تكنولوجيا المعلومات إلى تحسين أساليب وإجراءات المراجعة، مما يمكن المراجعين من الاستفادة من التكنولوجيا لتحقيق كفاءة وفعالية أكبر.

وقد خلصت الدراسة إلى أن مخاطر تكنولوجيا المعلومات، على الرغم من كونها تشكل تحديات كبيرة لجودة المراجعة، فإنها توفر أيضًا فرصًا لتحسين عمليات المراجعة. لذا فقد اوصت الدراسة الى ضرورة التعليم المستمر للمراجعين للاطلاع الدائم على التطورات التكنولوجية، وضرورة تعزيز إجراءات أمن المعلومات، وضرورة تطوير مهارات المراجعين الخارجيين المتخصصة.

الكلمات المفتاحية: مخاطر تكنولوجيا المعلومات، جودة المراجعة، الأخطاء الجوهرية في البيانات، مخاطر المراجعة، إدارة الأرباح، مصر.

1-Introduction

In the contemporary business landscape, the integration of information technology (IT) into organizational processes is not just a convenience but a necessity. This digital transformation, while offering numerous benefits such as increased efficiency and enhanced data management, also introduces a spectrum of risks that can profoundly affect the quality of audits. As businesses rely more heavily on sophisticated IT systems, auditors are tasked with navigating these complexities to ensure the accuracy, security, and compliance of financial data.

The impact of IT risks on audit quality is multifaceted. Firstly, the complexity of modern IT systems demands that auditors possess specialized knowledge and skills to effectively evaluate these systems. Without this expertise, there is a risk of inadequate audit coverage and oversight. Secondly, IT risks such as cyber-attacks, data breaches, and system failures pose significant threats to the integrity and security of financial data. Ensuring that data remains accurate and reliable is paramount for maintaining high audit quality (Bierstaker et al., 2001).

Moreover, the planning and execution of audits are directly influenced by IT risks. Effective audit planning requires a comprehensive understanding of the IT environment and its associated risks. Inadequate planning can lead to poor risk assessments and insufficient audit procedures, ultimately compromising audit quality. Additionally, regulatory compliance is a critical aspect that can be affected by IT risks. Organizations must adhere to various regulations such as GDPR, HIPAA, and PCI DSS, and non-compliance can result in legal penalties and reputational damage (Azizi et al., 2024).

The relationship between auditors and clients is also at stake when IT risks are not properly managed. Clear communication and collaboration are essential to address these risks and ensure a smooth audit process. To mitigate the impact of IT risks on audit quality, auditors must engage in continuous education and development, robust audit planning, and a thorough understanding of the IT landscape (Stoel& Havelka, 2021)

This paper aims to delve into the intricate relationship between IT risks and audit quality, exploring the challenges and proposing strategies to enhance audit

practices in an increasingly digital world. By examining these dynamics, the study seeks to provide valuable insights for auditors and organizations striving to maintain high standards of audit quality amidst the evolving technological landscape.

2- Literature Review and hypotheses development

To achieve the aim of the study, the researcher will present the previous studies related to the subject of the study in three groups as follows:

- The first group is previous studies about information technology risks.
- The second group is previous studies about audit quality.
- The third group is previous studies about the impact of information technology risks on audit quality.

2.1 Previous studies related to information technology risks.

Numerous studies have explored the multifaceted nature of information technology (IT) risks across various domains. Researcher have sought to analyze and understand these risks by reviewing existing literature and conducting empirical studies. Below is a synthesis of key findings from these studies:

- Sjöberg & Fromm (2001) examined the social and psychological impacts of IT use, particularly email and the Internet. Their survey of the Swedish population revealed that increased Internet use is associated with reduced social engagement and higher feelings of loneliness and depression, except for individuals with strong local social networks. The study also highlighted ethical and legal risks related to privacy, personal integrity, and freedom of speech, despite the Internet's potential to foster social connections through platforms like email and chat rooms.

- Abu-Musa (2001) investigated risks to electronic accounting systems in Egyptian banks, identifying threats such as unauthorized data destruction, incorrect data entry, password sharing, virus

introduction, and data dissemination. The study found no significant differences among bank types, except for external hacking incidents.

- Whitman (2003) focused on information security risks in Georgia, identifying prevalent and severe threats. The study emphasized the need for organizations to improve their awareness and understanding of these risks to better protect their systems.

- Malami et al. (2012) explored risks to banking information systems from the perspective of Malaysian bank managers. The study identified human, technological, environmental, and natural threats, stressing the importance of internal control systems and employee training in information security.

- Ackermann et al. (2012) developed a framework to assess IT security risks in cloud computing, identifying six key dimensions: Confidentiality, Integrity, Availability, Performance, Accountability, and Maintainability. The study highlighted the complexity of IT security risks and the need for a comprehensive framework to evaluate them.

- Mason et al. (2014) created the Cyber-Paranoia and Fear Scale to measure perceptions of IT-related threats. The study found that cyber-paranoia is linked to age, technology use, and awareness, suggesting that improving technological competence could reduce such fears.

- Rangarajan et al. (2019) developed a conceptual model to understand how perceived information security threats influence user resistance to technological innovation. The study found that these risks affect trust and adoption, with intrinsic benefits and costs playing a critical role in user behavior.

- Dokuchaev et al. (2020) analyzed risks related to personal data handling in information systems, emphasizing the need to categorize

threats based on user behavior and unauthorized activities to protect privacy and constitutional rights.

- Tangprasert (2020) evaluated IT risk management using COBIT 5 standards, demonstrating that implementing risk management across all phases of the COBIT 5 life cycle reduces risk levels in both government and commercial sectors. The study underscored the importance of IT risk management for security and user confidence.

Through analysis of the existing literature, the researcher establishes three fundamental conclusions regarding information technology risks:

- **IT Risks Are Multidimensional :**IT risks span technical vulnerabilities (e.g., system breaches, data integrity), human factors (e.g., user errors, psychological impacts), and organizational weaknesses, requiring holistic management approaches rather than isolated technical fixes.
- **Human Factors Are Central to Risk and Mitigation:** From employee behavior to user adoption resistance, human elements significantly influence both the emergence of IT risks (e.g., data leaks, poor security practices) and their solutions (e.g., training, awareness programs)
- **Core Implication**: Effective IT risk management must integrate technology, people, and processes, supported by adaptable frameworks that address evolving threats.

2.2 Previous studies related to audit quality.

- Nuryaman (2013) examined the impact of earnings management on firm stock returns, with audit quality as a moderating factor. The study found that earnings management negatively affects stock returns, and this negative relationship is intensified by higher audit quality. Specifically, the adverse effect is more pronounced for firms audited by Big 4 Audit Firms compared to non-Big 4 firms, highlighting the moderating role of audit quality.
- Soliman et al. (2014) analyzed the relationship between audit committee effectiveness, audit quality, and earnings management in

over 50 non-financial Egyptian companies listed on the Egyptian Stock Exchange from 2007 to 2010. The study revealed that audit committee independence, member experience, meeting frequency, and audit quality significantly reduce discretionary accruals, a proxy for earnings management. However, audit committee size showed no significant relationship with discretionary accruals.

- Zahmatkesh & Rezazadehb (2017) explored the factors influencing audit quality from the perspective of company-employed auditors. The study found that professional competence, accountability, and objectivity significantly enhance audit quality. Additionally, hiring highly experienced individuals improves audit quality by boosting auditors' professional competence.
- Ado et al. (2020) investigated the direct impact of audit quality on the financial performance of publicly traded companies in Nigeria. The study focused on three variables—audit fee, auditor size, and auditor independence—and their relationship with Return on Assets (ROA). The findings showed a positive correlation between auditor independence and financial performance, consistent with agency theory. The study also suggested that higher audit fees motivate auditors to deliver high-quality services, ensuring value for money.
- Rustiarini et al. (2021) studied how personal factors such as goal orientation, self-efficacy, and professional commitment influence auditors' responsibility to detect fraud, particularly in small accounting firms. Surveying 86 auditors in Bali Province, Indonesia, the study found that self-efficacy mediates the relationship between goal orientation and auditor responsibility. Professional commitment also emerged as a key mediating factor, emphasizing its importance in enhancing auditor performance.

Based on the analysis of these studies, the researcher concludes that the key determinants of audit quality include:

1. **Controlling Earnings Management:** High-quality audits effectively constrain earnings manipulation by detecting and reporting irregular accounting practices, thereby enhancing financial statement transparency and reliability.

2. **Managing Audit Risks:** Audit risk, defined as the probability that financial statements contain material undetected errors despite audit procedures (AICPA, 2020), requires auditors to systematically evaluate and address potential misstatements through comprehensive examination processes.
3. **Detecting Material Misstatements:** A fundamental auditor responsibility involves identifying significant inaccuracies in financial reporting. Competent detection of material misstatements not only ensures reporting accuracy but also reinforces stakeholder trust in financial disclosures.

2.3 Previous studies related to the impact of information technology risks on audit quality.

- Al-Qudah et al. (2013) examine the debate surrounding the integration of information technology (IT) in auditing, focusing on its impact on audit quality and efficiency. Their study indicates that while IT improves audit efficiency, it may also compromise the quality of the review process. Notably, the observed efficiency gains appear to stem more from the discontinuation of outdated audit methods than from the inherent advantages of modern IT-based approaches. Additionally, the study finds that IT adoption across different audit functions can enhance both the efficiency and effectiveness of the review process. Despite these benefits, persistent challenges prevent organizations from making substantial investments in audit-related IT solutions. These barriers constrain the full potential of IT in optimizing audit performance, highlighting the need for strategic decision-making to effectively harness technological advancements for improved audit outcomes.
- Polo & Oima (2013) investigated the effect of computerized accounting systems on audit risk management, linking it to risk assessment, monitoring, and control awareness. Key risks included system security breaches and inadequate information provision, with recommendations to review ERP procedures.

- Saleem and Oleimat (2020) examined the role of employee training programs and accounting information systems (AIS) in mitigating IT-related audit risks within Jordanian audit firms. Their research revealed three key findings: (1) computerized audit software significantly enhances financial performance, (2) adequately trained staff demonstrate effective management of accounting and IT audit systems, and (3) information systems in leading Jordanian firms successfully reduce accounting-related risks. Based on these findings, the study recommends two primary measures: implementing enhanced cybersecurity protocols for computerized auditing environments and developing comprehensive specialized training programs to strengthen auditors' risk management capabilities
- Stoel & Havelka (2021) This study explores factors influencing IT audit quality (ITAQ), comparing professionals' general perceptions with real-world audit experiences. While auditors initially emphasize individual expertise (IT knowledge, business process skills) as key to ITAQ, actual audits reveal organizational factors—such as planning and client relationships—as more critical. The gap between perception and practice suggests that improving pre-audit team preparation and processes could enhance ITAQ. The research highlights the growing importance of IT risk management and calls for better education and structured audit approaches to strengthen IT audit effectiveness
- Al-Taie & Elnagar (2021) studied the reduction of IT risks using the COPIT 2019 framework, finding it effective in enhancing internal audit quality. The study recommended staying updated with technical and professional developments.
- Ali et al. (2022) proposed a framework for auditors to manage blockchain technology risks, highlighting new challenges like network governance, data confidentiality, and scalability. The study found a positive relationship between blockchain auditing practices and risk management.
- Imoniana et al. (2023) examine the impact of technological advancements on financial statement auditing practices. Their

research reveals that modern auditing is being fundamentally transformed through Advanced audit technologies:(Computer-Assisted Audit Techniques (CAATs), Artificial Intelligence applications (including supervised models for data extraction), Deep learning systems, Blockchain-enabled continuous auditing, Robotic Process Automation (RPA)) , Emerging monitoring tools(Internet of Things (IoT), Drone technology, Satellite imagery systems, Remote sensing technologies).Furthermore, the study demonstrates how these innovations are reshaping all critical phases of the audit process - from initial planning through execution to final reporting.

- Azizi et al. (2024) explored the impact of digital transformation on IT audit procedures, emphasizing the need to adapt audit practices to technological advancements to optimize benefits and mitigate risks.
- Nisarga (2024) conducted a comprehensive study examining how emerging technologies are transforming audit practices. The research investigates: (1) the multidimensional impacts of digital tools on traditional audit methodologies, (2) the benefits and implementation challenges of technological adoption, and (3) specific applications of advanced solutions including data analytics, artificial intelligence (AI), robotic process automation (RPA), blockchain, and Power BI in auditing processes. Key findings emphasize technology's pivotal role in modern auditing while providing actionable recommendations for professionals integrating these innovations. Through evidence-based analysis, the study makes significant contributions to understanding digital transformation in accounting, particularly regarding effective implementation strategies for technological tools in audit practice

Based on the analysis of these studies, the researcher concludes that the impact of technology on audit quality manifests in three key dimensions:

1. **Dual Impact of Technology:** While digital tools (AI, blockchain, RPA) significantly enhance audit efficiency and risk detection capabilities, they simultaneously introduce new challenges in maintaining audit

quality and require careful implementation to avoid over-reliance on automated systems.

2. **Human-Centric Adaptation:** Successful technological integration depends fundamentally on auditor expertise and training, as human judgment remains irreplaceable for critical assessment, particularly in addressing emerging IT risks and cybersecurity threats.
3. **Framework-Driven Transformation:** Effective adoption requires structured approaches (like COBIT 2019) to manage new risks and standardized processes to bridge the gap between technological potential and actual audit quality outcomes, emphasizing continuous skill development alongside technological upgrades.

Based on the analysis of the three groups of previous studies, the study proposes the following hypotheses:

-H_1: Information technology risks have a significant impact on constraining earnings management.

-H_2: Information technology risks have a significant impact on audit risks.

-H_3: Information technology risks have a significant impact on detecting material misstatements.

These hypotheses aim to explore the influence of IT risks on critical aspects of audit quality, providing a foundation for further investigation.

3. Information Technology

The term "technology" originates from the Greek words "techno" (skill) and "logia", referring to the science of applying knowledge and skills to achieve specific goals. It encompasses the interaction between humans, tools, and materials, enabling the practical application of expertise to produce desired outcomes (Anissimov, 2023).

Information technology (IT) is defined as "hardware and software products, information system operations and management processes, as well as the human resources and skills needed to apply these products and processes to

information production, system development, operation, management, and control" (IFAC, 2009, p. 30). IT knowledge involves understanding the theoretical or conceptual aspects of technology, while IT skills refer to the ability to apply this knowledge in real-world scenarios (IFAC, 2009). (Skelton ,2012) emphasizes that "knowledge is the most essential foundation for developing skills." Furthermore, IT can be described as "any activity involving information processing and integrated communication through electronic equipment" (Victoria, 2020).

3-1 **Information Technology Attributes** (Setiawati et al., 2022; Zhu, 2019)

1. Quality of Operations

IT ensures stability and operational excellence, acting as the foundation that keeps well-designed business systems running efficiently. It is essential for maintaining seamless business operations.

2. Proficiency with Digital Tools

The primary goal of IT is to leverage technology and information to enhance operations, reduce costs, and increase revenue. Digitally proficient IT teams focus on using data to gain business insights and employing technology to achieve organizational objectives.

3. Originality and Innovation

As businesses mature digitally, they expect IT to introduce creative solutions for managing complexity, improving quality, and accelerating digital transformation. Modern digital tools make innovation more accessible and cost-effective. Examples include soft innovations (cultural or communication changes), efficiency innovations (process improvements), sustainability innovations (enhanced products or services), and breakthrough innovations (pushing boundaries to new levels).

4. Use of Artificial Intelligence

AI plays a critical role in advancing knowledge and empowering users by enhancing inclusion and control over production processes.

5. Equilibrium

The integration of modern technologies with other key business attributes amplifies their impact, especially as ecosystems evolve. IT must balance traditional practices with new approaches to develop future-ready digital strategies, rather than relying solely on outdated best practices.

6. Flexibility

Adaptability refers to the ability of individuals or systems to adjust swiftly to changing conditions. In the fast-paced digital era, characterized by constant disruptions, information overload, and shorter knowledge lifecycles, success depends on how quickly and effectively an organization can adapt to challenges.

7. Adaptability

Unlike rigid mechanical systems, digital organizations evolve gradually through pattern-making, structure-building, and innovation, similar to biological systems. As long as the core structure and interfaces remain stable, individual components can be modified without disrupting the entire system.

8. Speed

Progressive IT organizations accelerate innovation by separating outdated technologies and processes from new approaches. They rapidly and cost-effectively validate changes to ensure they align with business goals, enhance productivity, reduce costs, and meet customer expectations. IT acceleration aims to increase organizational agility and strategic responsiveness.

9. Wealth and Investment

IT effectiveness is dynamic, often requiring significant investments rather than incremental changes. To enhance business capabilities, IT needs top-level support, expertise, continuous investment, and evolution. When businesses invest in IT resources, they entrust the IT department with managing these investments to maximize commercial value.

10. Resilience

Resilient IT organizations adapt quickly to changing business needs, reducing risks and improving overall risk management. They embrace a "fail fast, fail cheap, and recover quickly" approach, enabling them to navigate disruptions effectively and maintain business continuity.

3.2 Information Technology Risk Analysis.

Despite the significant benefits of the Internet and technological advancements, which have transformed communication, information transfer, and access to data, businesses are increasingly adopting the latest electronic systems and software to streamline operations. These tools have made computer usage more accessible, enabling organizations to complete tasks faster and with greater accuracy. However, as practices and controls have not evolved at the same pace as advancements in computers and information technology, serious vulnerabilities and risks related to the security and integration of electronic accounting systems have emerged (Abu-Musa, 2006, p. 510).

The primary risk involves the potential for organizational losses or damage to assets due to either unintentional accounting errors or deliberate misconduct aimed at exploiting opportunities for irregular activities.

The following is a classification of security threats associated with electronic accounting information systems, examined from multiple perspectives:

- **Classification of Risks by Source:**

1. Internal Risks:

Employees, being familiar with the weaknesses and gaps in the control systems of an organization, are the primary source of internal risks in information systems. Dishonest employees with access to the system and data may intentionally destroy, distort, or modify information. According to El-Ebiary&Nahg (2020), internal risks are those that may arise during the planning, design, and operation of technology, communication channels, and computers used in accounting information systems. These risks can occur during programming, data collection, entry, processing, result extraction, or system configuration.

2. External Risks:

External risks originate from entities outside the organization, such as competitors or hackers, who attempt to bypass security measures to access proprietary information. Additionally, natural disasters like earthquakes, volcanoes, and floods can partially or completely disrupt the facility's systems (Abu-Musa, 2006).

- **Categories of Risks Based on Cause**

1. Human Risks:

Human risks stem from errors or intentional actions by employees or management, such as manipulation and fraud. These risks can occur during the preparation, design, and implementation of accounting information systems, including the setup of equipment, communication channels, and computers. Human risks are a major challenge to the security and safety of accounting information systems, whether during development, testing, data collection, or system input (El-Ebiary&Nahg,2020).

Control and Protection Measures:

- Restrict access to or use of computers in the computer room.

- Install computers in secure, monitored locations to prevent unauthorized movement.

- Use backup power sources to maintain operations during power outages.

- Monitor access to computer peripherals, the computer room, and external devices.

- Implement controls for issuing or revoking physical access methods (e.g., keys, badges).

- Ensure all physical access processes are supervised by a responsible official (Abu Atiwi, 2012).

2. Management Fraud and Cheating:

Management fraud is a significant issue in auditing electronic accounting information systems, especially advanced ones. Fraudulent activities, such as altering databases or creating fictitious documents, are facilitated by computer capabilities. Weak internal controls exacerbate the problem, leading to substantial losses. The complexity of electronic systems makes monitoring and auditing more challenging. While management bears primary responsibility for detecting fraud, external auditors also play a critical role, as undetected fraud can result in inaccurate financial statements that misrepresent the organization's true financial position (Elshrief, 2010, p. 63).

3. Environmental Risks:

Environmental risks include natural disasters like earthquakes, storms, floods, and hurricanes, by power failures, fires, and malfunctioning air conditioning or refrigeration systems. These risks can significantly compromise the security and functionality of accounting information systems (Alsakiny & Aleawawda, 2011, p. 225).

Control and Protection Measures:

- Install and maintain fire extinguishers.

- Use protective covers to shield equipment from dust and water damage.

- Position computer devices away from water sources and pumps.

- Ensure the computer room is equipped with air conditioners.

- Use earthquake-resistant and vibration-proof equipment (Abu Atiwi, 2012, p. 24).-

4. Computerized Crimes:

Computerized crimes result in significant losses due to challenges in managing information systems, including unauthorized access, use, or modification of software and data. Examples include the unauthorized use of computers for personal purposes, where organizational assets may be transferred to unauthorized accounts. Specific types of computerized crimes include:

- Computer Viruses:

Independent programs that operate within software, spreading across systems or residing in memory to disrupt or alter programs and data (Ilmudeen, 2013).

- Piracy:

The illegal copying of software or data to steal information, often for commercial or marketing purposes. This can lead to unauthorized access to organizational accounts (Bandyopadhyay & Bandyopadhyay, 2015)

- Cybercrime:

Threats to privacy, electronic identities, and personal information held by organizations, departments, and government entities are growing.

- System Quality Problems:

Beyond disasters, viruses, and security breaches, missing data and software inconsistencies pose ongoing threats to information systems.

- **Types of Risks According to Intentionality**

1. Intentional Risks:

These involve deliberate actions, such as entering incorrect data or deleting information with the intent to commit fraud, manipulation, or theft. Such actions significantly impact the system (Abu-Musa, 2006).

Control and Protection Measures (Abu Atiwi, 2012):

- Implement methods to control, protect, and maintain information confidentiality.

- Educate employees on ethical responsibilities when handling third-party information.

- Conduct periodic and non-periodic evaluations to assess system protection levels.

- Train employees on risks to accounting information systems and appropriate mitigation strategies.

- Emphasize the importance of protecting passwords.

2. Unintentional Risks:

These arise from ignorance or lack of experience, such as incorrect data entry or omissions during registration. While less severe than intentional risks, they still require attention and can often be corrected (Abu-Musa, 2006).

- **Types of Risks According to Its Impact:**

1.Material Damage Risks:

Risks that cause physical harm to systems, computers, or data storage mechanisms, resulting from natural disasters or human actions, whether intentional or unintentional (Abu-Musa, 2006).

2. Technical and Logical Risks:

Risks that affect data accessibility, integrity, or confidentiality, such as system memory disruptions or virus infections. These risks can compromise an organization's competitive position.

- **Types of Risks According to System Phase:**

1. Input Risks:

Risks associated with inaccurate or untimely data entry or errors in data transfer across communication lines (Abu-Musa, 2006). These include:

- Creating Incorrect Data:

Using legitimate documents to hide fraudulent activities, such as adding fictitious employees to payrolls or submitting fake invoices.

- Modifying or Distorting Data:

Altering authorized entries before they are entered into the system.

- Deleting Data: Removing data intentionally or unintentionally before processing.

- Duplicate Data Entry: Entering the same data multiple times, either deliberately or accidentally.

2. Data Processing Risks:

Risks related to unauthorized use, modification, or theft of data and programs stored in the system.

3. Output Risks:

Risks associated with the misuse, deletion, or unauthorized disclosure of processed data and reports, such as displaying or printing sensitive information without authorization (Abu Atiwi, 2012).

- **Types of Risks According to Its components:**

Information technology (IT) systems are composed of various components, each of which introduces specific risks that can compromise data integrity, security, and operational efficiency. This section categorizes and discusses the risks associated with key IT components, including hardware, software, databases, communication systems, and networks. These risks are critical to understanding the vulnerabilities inherent in IT systems and are integral to the development of the questionnaire for this study

1. Hardware Risk

Hardware risk refers to threats that can damage or compromise data stored on computer systems or allow unauthorized access to these systems. Such risks can arise from malicious software (malware), which includes viruses, worms, ransomware, spyware, and Trojan horses. Additionally, misconfigurations of hardware components and unsafe computing practices can exacerbate these risks. For example, improper settings or outdated firmware can create vulnerabilities that attackers exploit to gain unauthorized access or disrupt operation (ICAEW, 2020).

2. Software Risk

Software risk is defined as the potential for loss or failure during the software development process. This risk stems from uncertainties and unforeseen challenges that cannot be fully accounted for in project planning. Losses may manifest as increased production costs, poor-quality software, or project delays. Software risks can be categorized into two types: (1) internal risks, which are within the control of the project manager, and (2) external risks, which are beyond their control. These risks highlight the importance of robust risk management practices in software development to mitigate potential negative outcomes (Bannerman, 2008).

3.Database Risk

Database risk encompasses the potential for business losses due to poor data governance, mismanagement, or inadequate security measures. Specific risks include (Otto & Jarke, 2023):

- **Poor Data Governance**: Inability to maintain high-quality data throughout its lifecycle.
- **Data Mismanagement**: Weak processes for acquiring, validating, storing, protecting, and processing data.
- **Insufficient Data Security**: Vulnerabilities that expose digital data to cyber-attacks, data breaches, or unauthorized access. Additional risks include storage device failures, data corruption, and the accumulation of unused data, all of which can compromise data integrity and availability.

4. Communication Risk

Communication risk refers to the potential for losses resulting from breaches of confidentiality, failures in system or data integrity, or the unavailability of critical systems. This risk also includes the inability to adapt IT systems to changing business requirements in a timely and cost-effective manner. Examples of communication risks include system reliability issues, data theft, malware dissemination, and persistent unauthorized access within networks. These risks underscore the importance of securing communication infrastructures to ensure data availability, integrity, and accessibility (Saeed et al., 2023).

5. Network Risks

Network risks involve threats to an organization's digital assets, including data stored on internal and external servers or cloud services. Common network security threats include:

- **Malware**: Malicious software designed to disrupt, damage, or gain unauthorized access to systems.
- **Phishing Schemes**: Fraudulent attempts to obtain sensitive information by disguising as a trustworthy entity.
- **Distributed Denial of Service (DDoS)**: Attacks that overwhelm networks, rendering them unavailable to users.

- **Viruses**: Malicious programs that replicate and spread, often causing harm to systems and data (Williams et al., 2023).

These risks not only threaten data security but also increase the likelihood of regulatory non-compliance, which can result in legal and financial penalties.

4- Audit Quality

4-1 The Concept of Audit Quality

Despite its importance, there is no universally accepted definition of audit quality. Researchers and academics have approached the concept from various perspectives, leading to differing interpretations.

- **Definition of Audit Quality in Terms of Compliance with GAAS**

Auditors often define a quality audit as one that adheres to Generally Accepted Auditing Standards (GAAS), resulting in accurate and reliable financial statements. Such audits are well-planned, conducted by competent and independent auditors, and free from errors upon subsequent review. Investors, on the other hand, emphasize the importance of well-trained auditors, proper planning, and the independence of the auditing team. Compliance with GAAS, accurate financial reporting, and reliance on transparent financial statements are also critical metrics for investors (ICAEW, 2020).

Audit quality can also be defined as the probability that an auditor will detect and report errors or fraud within a client's accounting system. This definition highlights the role of auditor competence and independence in ensuring audit quality (Christensen et al., 2022).

Other definitions focus on adherence to professional standards and ethical behavior. For instance, Svanström (2016) described audit quality as the auditor's commitment to professional standards, rules, and ethics, while Serdouk et al., (2024) defined it as the adherence to standards that result in error-free financial statements.

The American Institute of Certified Public Accountants (AICPA) emphasized that audit quality is achieved through compliance with auditing standards and the application of quality control measures (AICPA, 2019). Similarly, the Public Company Accounting Oversight Board (PCAOB) defined audit quality as meeting investor needs through an independent and reliable audit process, effective communication with audit committees, and assurances regarding internal controls and financial disclosures (PCAOB, 2013).

While compliance with professional standards is a critical component of audit quality, it may not fully capture the concept's complexity. Other perspectives, such as the relationship between audit quality and audit risk, provide additional insights.

- **Definition of Audit Quality in Terms of Its Relationship to Audit Risk**

Audit quality is inversely related to audit risk. Higher audit risk typically results in lower audit quality, and vice versa. This relationship underscores the importance of minimizing audit risk to achieve high-quality audits (Saeed et al., 2023).

DeAngelo (1981) defined audit quality as the auditor's ability to minimize the risk of errors in financial statements while considering agreed-upon fees. However, this definition has been criticized for being incomplete, as it does not account for situations where auditors may choose not to report detected errors (DeAngelo, 1981).

The audit risk model, as outlined in Statement on Auditing Standards (SAS) No. 47, provides a framework for understanding this relationship. The model defines audit risk as the product of inherent risk, control risk, and detection risk. Auditors must manage these risks to ensure the accuracy and reliability of financial statements (AICPA, 1983).

- **In Relation to the Detection of Material Misstatements**

This perspective focuses on the auditor's ability to detect errors, fraud, and material misstatements in financial statements. High-quality audits are

characterized by the auditor's ability to identify and report such irregularities, thereby reducing information asymmetry between management and shareholders (Williams et al., 2023)

4-2 Factors Affecting Audit Quality

The quality of an audit is influenced by a variety of factors, which can be categorized into three main groups: factors related to the audit firm, factors related to the audit team, and factors related to the audited entity. Below is an analysis of the most significant factors affecting audit quality:

1. Factors Related to the Audit Firm

- Characteristics of the Audit Team

The audit team plays a critical role in determining the quality of an audit. Key characteristics include:

- **Independence and Impartiality**: Independence is a cornerstone of the auditing profession. Auditors must avoid any material interests or relationships with the audited entity that could compromise their objectivity. Even the interests of an auditor's relatives must be considered, as they could influence impartiality (ICAEW, 2020).
- **Scientific Qualification and Professional Experience**: The competence and expertise of auditors are vital for ensuring the effectiveness and efficiency of the audit process. Well-qualified and experienced auditors are better equipped to identify and address potential issues.
- **Auditor Qualifications and Proficiency**: The primary goal of an audit is to provide assurance that financial statements are free from material misstatements. The value of an audit depends on the auditor's ability to detect and report errors or breaches in the reporting system. Developing leadership, management skills, and staff knowledge is essential for maintaining high audit quality (IASSB., 2020).

- Characteristics of the Audit Office

- **Audit Office Size**: The size of the audit firm significantly impacts audit quality. Larger firms typically have greater resources, specialized expertise, and advanced technological capabilities, enabling them to deliver higher-quality audits. Smaller firms, on the other hand, may lack the resources to meet the demands of complex audits. Studies have shown a positive correlation between firm size and audit quality, as larger firms are more likely to invest in quality control measures and maintain their reputation (Boone et al.,2010)
- **Auditor's Fees**

Audit fees encompass all costs associated with audit services, including staff salaries, travel expenses, and other operational costs. While higher fees may reflect a higher level of service quality, they can also pose challenges to auditor independence, especially when non-audit services are involved. Research suggests that audit fees are a noisy proxy for quality, as they are influenced by various factors beyond the scope of the audit itself (Saeed et al., 2023).

- Auditor's Reputation

The reputation of an audit firm is a key determinant of audit quality. A firm with a strong reputation for delivering high-quality audits is more likely to gain the trust of investors and stakeholders. Conversely, any decline in reputation can negatively impact the perceived quality of the firm's audits. Reputation is built over time through consistent performance and adherence to professional standards (Williams et al., 2023).

2. Factors Related to the Audit Process

- Audit Planning

Effective planning is essential for ensuring that the audit is conducted efficiently and that risks are minimized to an acceptable level. Proper planning involves identifying potential risks, allocating resources, and setting clear objectives for the audit (Yones & Aissa, 2016).

- **Evidence**

The quality of audit evidence is critical for supporting the auditor's conclusions. Evidence must be reliable, relevant, and sufficient to provide a basis for the auditor's judgment. High-quality evidence enhances the auditor's ability to detect errors and irregularities in financial statements.

- **Report and Disclosure**

The audit report is the final output of the audit process, and its quality directly impacts the credibility of the financial statements. A well-prepared report facilitates clear communication with stakeholders and reflects positively on the overall quality of the audit.

- **Size of Reports Required**

The complexity and volume of reports required can influence audit quality. Some argue that reducing the size of reports may compromise their quality, as important details could be omitted. Conversely, overly lengthy reports may dilute key findings and reduce their effectiveness.

11- Field Study

-Study tool design**.**

The researcher utilized a survey questionnaire as one of the primary tools for data collection. The questions were carefully designed after completing the theoretical study, with a strong emphasis on precision and clarity. To ensure the accuracy and effectiveness of the questionnaire, the researcher took the following steps:

1. Clarification of Terms

Some terms and concepts were explicitly defined to ensure that respondents fully understood the questions and could provide accurate responses.

2. General Information Collection

The questionnaire included questions to gather general information about the respondents, such as their current job roles and educational backgrounds, to provide context for their answers.

3. Five-Point Likert Scale

The survey was structured using a five-point Likert scale to measure the respondents' level of agreement or disagreement with the statements. This scale allowed for a clear and standardized measurement of responses, as illustrated in the table below:

Table 1: Five-point Likert scale

Strongly disagree	Disagree	Neutral	Agree	Strongly agree	Category
1	2	3	4	5	Degree

By incorporating these elements, the researcher aimed to create a reliable and valid survey instrument that would yield meaningful insights into the study's objectives.

- Testing the Stability and Validity

The reliability and validity of the scales used in the study were assessed as follows:

Checking the Level of Consistency in the Scales

Consistency is a critical feature of any measurement tool. It refers to the stability and uniformity of the measurements produced by the tool. In other words, consistency indicates the tool's ability to yield similar or equal results when applied multiple times to the same sample under identical conditions. To test the stability and validity of the survey, several methods were employed, with Cronbach's alpha coefficient being the most widely accepted measure. The coefficient ranges between 0 and 1, with values closer to 1 indicating higher

reliability. A Cronbach's alpha value of 60% or higher is generally considered acceptable for judging the stability of a survey. Additionally, any variable with a total correlation coefficient of less than 30% with the other variables in the same scale was excluded to ensure consistency.

Table 2: Results of the Validity and Reliability Test

Items	**Category**	**No**	**reliability**
Hypotheses 1	X1.1 --- X1.7	7	.845
Hypotheses 2	X2.1 --- X2.12	12	.909
Hypotheses 3	X3.1 --- X3.5	5	.833
Total		24	**.935**

From the table above, it is evident that the Cronbach's alpha values ranged between 0.833 and 0.909 These values are well within the acceptable range, reflecting the reliability and confidence of the research variables. This confirms their validity for use in subsequent stages of analysis.

Field Study Population and Sample

To achieve the objectives of the study, a random sampling method was employed to select the study sample, which included members of the teaching staff and external auditors. The researcher distributed the survey questionnaires electronically using the following link: https://forms.gle/P5ZvSRLYz7xo4xmr9.

A total of **155 completed questionnaires** were received, all of which were deemed suitable for statistical analysis

Sample Characteristics

The demographic characteristics of the study sample were analyzed using frequencies and percentages to provide insights into the composition of the sample. The results are presented as follows:

First: Job Title

The frequencies and percentages for the distribution of the study sample based on their current job titles are shown in the table below

Table 3: Frequencies and percentages by Job Title

Categories	Member of teaching staff		Auditor		Other		Total
	N0.	%	N0.	%	N0.	%	
Total	17	11	21	13.5	117	75.5	155

Second: Educational Level:

The frequencies and percentages were calculated to analyze the distribution of the study sample based on their educational level. The results are presented in the table below:

Table 4: Frequencies and percentages by Educational Level

Categories	Bachelor's		Graduate Diploma		Master's degree		Ph.D		Total
	N0.	%	N0.	%	N0.	%	N0.	%	
Total	103	66.5	15	9.7	31	20	6	3.8	155

This table highlights the educational background of the respondents, with the majority holding a Bachelor's degree (66.5%), followed by Master's degree holders (20%), Graduate Diploma holders (9.7%), and Ph.D. holders (3.8%). These results provide valuable insights into the academic qualifications of the study participants.

Third: Experience:

The frequencies and percentages were extracted for the distribution of the study sample according to number of years of job experience, as shown in the following table:

Table (5/5)

Frequencies and percentages by Experience

Categories	Less than 1 year		1 To 5 Years		5 To 10 Years		Over 10 Years		**Total**
	N0.	%	N0.	%	N0.	%	N0.	%	
Total	76	49	53	34	14	9	12	8	**155**

This table illustrates the distribution of respondents based on their years of professional experience. The majority of participants have **less than 1 year of experience (49%)**, followed by those with **1 to 5 years of experience (34%)**, **5 to 10 years of experience (9%)**, and **over 10 years of experience (8%)**. These findings provide insights into the experience levels of the study sample

6-5 The statistical Symbols.

For the purposes of statistical analysis, the researcher coded the survey questions related to the Variables axes as follows:

Items for H0.1 --- from X1.1 to X1.7

Items for H0.2 --- from X2.1 to X2.12

Items for H0.3 --- from X3.1 to X3.5

5.9 Statistical Methods

To test the hypotheses of the study, a variety of statistical methods were employed using the statistical software package SPSS 26. Determining the appropriate statistical methods required an understanding of the statistical distribution of the population from which the sample was drawn. To assess whether the study data followed a normal distribution, the Kolmogorov-Smirnov Test was conducted. The results are presented in the table below:

Table 6: Results of Kolmogorov-Smirnov Test

Items	**Kolmogorov-Smirnov Z**	**Asymp. Sig. (2-tailed)**	**Items**	**Kolmogorov-Smirnov Z**	**Asymp. Sig. (2-tailed)**
X1.1	0.235	.000[c]	X2.6	0.260	.000[c]

Items	Kolmogorov-Smirnov Z	Asymp. Sig. (2-tailed)	Items	Kolmogorov-Smirnov Z	Asymp. Sig. (2-tailed)
X1.2	0.235	.000[c]	X2.7	0.247	.000[c]
X1.3	0.266	.000[c]	X2.8	0.256	.000[c]
X1.4	0.255	.000[c]	X2.9	0.258	.000[c]
X1.5	0.252	.000[c]	X2.10	0.232	.000[c]
X1.6	0.231	.000[c]	X2.11	0.268	.000[c]
X1.7	0.231	.000[c]	X2.12	0.249	.000[c]
X2.1	0.239	.000[c]	X3.1	0.224	.000[c]
X2.2	0.256	.000[c]	X3.2	0.244	.000[c]
X2.3	0.231	.000[c]	X3.3	0.269	.000[c]
X2.4	0.251	.000[c]	X3.4	0.249	.000[c]
X2.5	0.247	.000[c]	X3.5	0.239	.000[c]

As shown in Table 6, the Asymp. Sig. (2-tailed) values for all items are 0.000, indicating that the data does not follow a normal distribution. Therefore, the researcher relied on non-parametric tests for further analysis.

After confirming the nature of the data and ensuring the validity of using non-parametric tests, the researcher proceeded to test the study hypotheses as follows:

5.10 Examination of Study Hypotheses

The results of the statistical analysis and the testing of the study hypotheses are presented as follows:

- Testing Hypothesis No. 1

"There is a significant impact of information technology risks on material misstatements."

First: Descriptive Statistics for $H_{0.1}$ Items

Table7 :Descriptive statistics for $H_{0.1}$ Items

Items	Mean	Std. Deviation	Mode	General trend
X1.1	4.1613	.79351	4	Agree
X1.2	4.0323	.92876	4	Agree
X1.3	4.0194	.96343	4	Agree
X1.4	3.8516	1.0051	4	Agree
X1.5	4.2000	.79282	4	Agree
X1.6	4.0645	.97819	5	Strongly agree
X1.7	4.0516	.86635	4	Agree

Source: SPSS statistical analysis results

The table above indicates that the study sample generally **agreed** (Agree) on the impact of information technology risks on material misstatements.

Second: Chi-Square Test

Table 8: Chi-Square Test for $H_{0.1}$ Items

Items	Chi-Square	df	Asymp. Sig
X1.1	65.103	3	.000
X1.2	90.839	4	.000
X1.3	98.710	4	.000
X1.4	73.097	4	.000
X1.5	139.355	4	.000
X1.6	92.452	4	.000
X1.7	47.555	3	.000

Source: SPSS statistical analysis results

The table shows that the calculated **Chi-Square values** for all items are greater than the tabular Chi-Square value, and the **significance level (Sig)** for all items is less than **0.05**. This indicates that the study sample members **accepted** the statements of the first sub-hypothesis, supporting the claim that **"There is a significant impact of information technology risks on material misstatements.**

Third: Friedman Test

Table 9: Friedman Test for $H_{0.1}$ Items

Items	Mean Rank	Ranking	Chi-Square	Sig
X1.1	4.22	2	22.300	.001
X1.2	3.99	4		
X1.3	3.95	5		
X1.4	3.56	7		
X1.5	4.32	1		
X1.6	4.01	3		
X1.7	3.94	6		

Source: SPSS statistical analysis results

The table reveals the following:

1. The **significance level (Sig)** for this hypothesis is less than **0.05**, indicating a **significant difference** in the respondents' opinions about the impact of information technology risks on material misstatements. This means there is **no consensus** on the relative importance of the statements related to this hypothesis.
2. The **highest mean rank** is **4.32** for item **X1.5**, which states that *"Risks resulting from viruses impact the corruption of data files, leading to an increase in material misstatements."* This indicates that this statement is the **most agreed-upon** among the respondents.
3. The **lowest mean rank** is **3.56** for item **X1.4**, which states that *"Information technology risks contribute to increasing errors and deviations in the audit process."* This suggests that this statement is the **least agreed-upon** among the respondents.

Based on the statistical analysis of the first sub-hypothesis, the researcher **accepts** the hypothesis that **"There is a significant impact of information technology risks on material misstatements."**

Testing Hypothesis No. 2

The second hypothesis, "Information technology risks significantly influence audit risks," was examined using descriptive statistics for the items related to $H_{0.2.}$

Table (10)Descriptive Statistics for $H_{0.2}$ Items

Items	Mean	Std. Deviation	Mode	General trend
X2.1	4.0194	.79341	4	Agree
X2.2	4.1871	.82798	4	Agree
X2.3	4.0387	.88921	4	Agree
X2.4	4.1677	.84377	5	Strongly agree
X2.5	4.0452	.85540	4	Agree
X2.6	4.2258	.81821	5	Strongly agree
X2.7	4.0968	.82000	4	Agree
X2.8	4.2000	.81703	5	Strongly agree
X2.9	4.1935	.81461	5	Strongly agree
X2.10	4.1226	.86291	4	Agree
X2.11	4.1419	.87117	4	Agree
X2.12	4.0129	.90444	4	Agree

Source: SPSS statistical analysis results

The table above indicates that the study sample generally agreed (Agree) on the impact of information technology risks on audit risks. The majority of responses leaned toward "Agree," with some items showing a stronger tendency toward "Strongly Agree." The mean values ranged between 4.01 and 4.23, further supporting the consensus on the significant influence of IT risks on audit risks.

Second: Chi-Square Test

Table 11Chi-Square Test for H0.2 Items

Items	Chi-Square	df	Asymp. Sig
X2.1	58.084	3	.000
X2.2	136.968	4	.000

X2.3	95.677	4	.000
X2.4	58.910	3	.000
X2.5	106.387	4	.000
X2.6	71.297	3	.000
X2.7	117.742	4	.000
X2.8	121.097	4	.000
X2.9	63.090	3	.000
X2.10	54.884	3	.000
X2.11	128.581	4	.000
X2.12	98.258	4	.000

Source: SPSS statistical analysis results

The table above presents the results of the Chi-Square test for the items related to the second hypothesis. The calculated Chi-Square values for all statements are higher than the tabular Chi-Square values, and the significance levels (Sig) for all items are below 0.05. This indicates that the members of the study sample accept the statements of the second sub-hypothesis, which suggests that "Information technology risks have a significant impact on audit risks."

Third: Friedman Test

Table (5/12) Friedman Test for H0.2 Items

Items	Mean Rank	Ranking	Chi-Square	Sig
X2.1	5.97	2	33.237	.000
X2.2	6.92	3		
X2.3	6.05	12		
X2.4	6.66	6		
X2.5	6.21	10		
X2.6	7.05	1		
X2.7	6.33	9		
X2.8	6.71	5		
X2.9	6.81	4		
X2.10	6.58	8		
X2.11	6.63	7		
X2.12	6.08	11		

Source: SPSS statistical analysis results

The table above presents the results of the Friedman Test for the items related to the second hypothesis. The findings reveal the following:

1. The significance level for this hypothesis is less than 0.05, indicating a significant difference in the respondents' opinions regarding the impact of information technology risks on increasing audit risks. This suggests a lack of consensus on the relative importance of the statements associated with this hypothesis.
2. The statement with the highest mean rank (7.05) is X2.6, which states, "The existence of a database with accurate information leads to reducing audit risks." This indicates that this statement received the highest level of agreement among respondents.
3. The statement with the lowest mean rank (6.05) is X2.3, which states, "Software-related risks affect inherent risk." This suggests that this statement received the least agreement compared to the others.

Based on the statistical analysis of the second sub-hypothesis, which examines the impact of information technology risks on audit risks, the researcher can accept the hypothesis: **"There is a significant impact of information technology risks on audit risks."**

3. Test Hypothesis No. 3
"There is a significant impact of information technology risks on earnings management."

First: Descriptive Statistics for $H_{0.3}$ Items

Table 13 Descriptive Statistics for $H_{0.3}$ Items

Items	Mean	Std. Deviation	Mode	General trend
X3.1	3.5806	1.1387	4	Agree
X3.2	3.8129	.93827	4	Agree
X3.3	3.8194	.99656	4	Agree
X3.4	3.8839	.88240	4	Agree
X3.5	3.9161	.94632	4	Agree

Source: SPSS statistical analysis results

The table above indicates that the study sample generally agreed (Agree) on the impact of information technology risks on earnings management. The mean values ranged between 3.58 and 3.92, reflecting a consensus on the influence of IT risks on earnings management practices.

Second: Chi-Square Test

Table 14
Chi-Square Test for H0.3 Items

Items	Chi-Square	df	Asymp. Sig
X3.1	37.935	4	.000
X3.2	90.645	4	.000
X3.3	80.774	4	.000
X3.4	100.065	4	.000
X3.5	80.903	4	.000

Source: SPSS statistical analysis results

The table shows that the calculated Chi-Square values for all statements exceed the tabular Chi-Square values, and the significance levels (Sig) for all items are below 0.05. This indicates that the study sample members accept the statements of the third sub-hypothesis, which suggests that **"There is a significant impact of information technology risks on earnings management.**

Third: Friedman Test

Table 15 : Friedman Test for H0.3 Items

Items	Mean Rank	Ranking	Chi-Square	Sig.
X3.1	2.74	5	13.916	.008
X3.2	2.98	4		
X3.3	3.00	3		
X3.4	3.10	2		
X3.5	3.18	1		

Source: SPSS statistical analysis results

The table reveals the following:

1. The significance level for this hypothesis is less than 0.05, indicating a significant difference in the respondents' opinions regarding the impact of information technology risks on earnings management. This suggests a lack of consensus on the relative importance of the statements associated with this hypothesis.
2. The statement with the highest mean rank (3.18) is X3.5, which states, **"Information technology-related risks affect the external auditor's ability to detect earnings management practices."** This indicates that this statement received the highest level of agreement among respondents.
3. The statement with the lowest mean rank (2.74) is X3.1, which states, **"Information technology plays an important role in reducing earnings management opportunities."** This suggests that this statement received the least agreement compared to the others.

Based on the statistical analysis of the third sub-hypothesis, which examines the impact of information technology risks on earnings management, the researcher can accept the hypothesis: **"There is a significant impact of information technology risks on earnings management."**

12- results :

The findings of the field study are summarized as follows:

1. IT risks, particularly virus-related data corruption, significantly increase material misstatements. Respondents agreed on this impact, though opinions varied on other related factors. The hypothesis **"IT risks increase material misstatements"** was accepted.
2. IT risks contribute to higher audit risks, with the existence of accurate databases seen as a mitigating factor. Respondents agreed that software-related risks affect inherent risk, but this statement received the least agreement. The hypothesis **"IT risks increase audit risks"** was accepted.
3. IT risks affect auditors' ability to detect earnings management practices, receiving the highest agreement. However, the idea that IT increases earnings management opportunities received the least agreement. The hypothesis **"IT risks impact earnings management"** was accepted.

4. Respondents showed significant variation in their views on the relative importance of IT risks in material misstatements, audit risks, and earnings management, indicating a lack of consensus.
5. **Key Agreed Statements:**
    - Virus-related risks corrupt data and increase material misstatements.
    - Accurate databases reduce audit risks.
    - IT risks hinder auditors' ability to detect earnings management.

4. Recommendations

Based on the findings and conclusions of the study, the following recommendations are proposed:

1- Stay Updated with Technological Advancements: Auditors and professionals should actively engage in conferences, seminars, and specialized courses to keep pace with modern developments in information and communication technology. Regularly following advancements in IT is essential to remain competent in addressing emerging risks.

2- Enhance Information Security Measures: It is crucial to protect information security from loss or breaches by storing data in secure locations. Additionally, organizations should maintain standby devices and systems to ensure continuity in case of hardware or software failures.

3- Develop Specialized Auditor Skills: Auditors must acquire specialized skills and expertise through scientific knowledge and targeted training programs. This will enable them to effectively manage and mitigate IT-related risks in the audit process.

4- Encourage Further Research: More studies and research should be conducted on the risks of information technology and their impact on audit quality. There is a noticeable gap in this area, and additional research is needed to provide deeper insights and practical solutions.

13- Suggestions for future research:

1. Impact of Emerging Technologies on Auditing:

Investigate how emerging technologies such as artificial intelligence (AI), blockchain, and machine learning are transforming auditing practices and their implications for audit quality and risk management.

2. Cybersecurity Risks and Audit Implications:

Examine the growing threats of cybersecurity breaches and their impact on financial reporting, audit processes, and the role of auditors in mitigating these risks.

3. IT Governance and Audit Effectiveness:

Study the relationship between IT governance frameworks (e.g., COBIT, ITIL) and their effectiveness in enhancing audit processes and reducing IT-related risks.

4. Auditor Preparedness for IT Risks:

Assess the current level of auditor preparedness in dealing with IT risks and identify gaps in knowledge, skills, and training that need to be addressed.

5. Role of Data Analytics in Auditing:

Explore how data analytics tools and techniques can improve audit efficiency, accuracy, and the detection of anomalies or fraudulent activities.

6. Impact of IT on Fraud Detection and Prevention:

Study how IT tools and systems can enhance auditors' ability to detect and prevent fraud, including the use of predictive analytics and real-time monitoring.

References

Abdul Razzaq, M. (2019). The influence of IT advancements on auditing practices: A review of traditional and modern methods. *Journal of Accounting and Auditing*, 15(4), 112-130.

Abu Atiwi, R, (2012), The impact of the risks of using information technology in the audited establishments on the quality of the external auditor's work https://www.mobt3ath.com/uplode/book/book-32984.pdf?ver=accessable

Abu-Musa, A. (2006). Investigating the Perceived Threats of Computerized Accounting Information Systems in Developing Countries: An Empirical Study on Saudi Organizations. *Journal of King Saud University - Computer and Information Sciences, 18*, 1-30. doi:https://doi.org/10.1016/S1319-1578(06)80001-

Abu-Musa, A. A. (2001). *Evaluating the security of computerised accounting information systems : an empirical study on the Egyptian banking industry*. Retrieved from Evaluating the security of computerised accounting information systems : an empirical study on the Egyptian banking industry | Semantic Scholar

Ackermann, T., Widjaja, T., Benlian, A., & Buxmann, P. (2012). *Perceived IT Security Risks of Cloud Computing: Conceptualization and Scale Development* (Vol. 4).

AICPA. (2019). *"Audit Quality Indicators: A Tool for Audit Committees." Retrieved from AICPA Audit Quality Indicators*

Al-Hattami, H., et al. (2020). Risks of computerized AIS and their impact on external auditors' work quality: Evidence from Yemen. *Journal of Accounting and Auditing*, 12(3), 78-95.

Ali, S., et al. (2022). Managing blockchain technology risks: A framework for auditors. *Journal of Information Systems*, 33(2), 78-95.

Al-Qudah, A. A., Baniahmad, A. Y., & Al-Fawaerah, N. (2013). The Impact of Information Technology on the Auditing Profession. *Management and Administrative Sciences Review, 2*(5), 423-430

Alsakiny, A., & Aleawawda, M. (2011). Environmental risks to accounting information systems: A case study of natural disasters. *Journal of Risk Management*, 15(4), 112-130.

Al-Taie, M., & Elnagar, S. (2021). Reducing IT risks using the COPIT 2019 framework: Implications for internal audit quality. *Journal of Risk Management*, 15(4), 112-130.

American Institute of Certified Public Accountants (AICPA). (1983). *Statement on Auditing Standards (SAS) No. 47: Audit Risk and Materiality in Conducting an Audit.* AICPA.

Anissimov, M. (2023). What is Technology? available from https://www.easytechjunkie.com/what-is-technology.htm

Aral, S., & Weill, P. (2007). IT assets, organizational capabilities, and firm performance. *Journal of Management Information Systems*, 24(2), 45-60.

Azizi, M., Hakimi, M., Amiri, F., & Shahidzay, A. (2024). The Role of IT (Information Technology) Audit in Digital Transformation: Opportunities and Challenges. *Open Access Indonesia Journal of Social Sciences, 7*, 1473-1482. doi:10.37275/oaijss.v7i2.230

Bala Ado, A., Rashid, N., Mustapha, U., & Lateef, S. (2020). Journal of Critical Reviews the Impact of Audit Quality on the Financial Performance of Listed Companies Nigeria. *Journal of Critical Reviews, 7*, 2020. doi:10.31838/jcr.07.09.07.

Bandyopadhyay, S., & Bandyopadhyay, K. (2015). *The Effects of Software Piracy on Cybersecurity and Economic Development. Journal of Information Security, 6*(3), 167-176.

Bannerman, P. L. (2008). Risk and risk management in software projects: A reassessment. *Journal of Systems and Software, 81*(12), 2118-2133. Doi: https://doi.org/10.1016/j.jss.2008.03.059

Bierstaker, J., Burnaby, P., & Thibodeau, J. (2001). The impact of information technology on the audit process: An assessment of the future of auditing. *Journal of Information Systems*, 15(1), 49-64.

Boone, J. P., Khurana, I. K., & Raman, K. K. (2010). "Do the Big 4 and the second-tier firms provide audits of similar quality?" *Journal of Accounting and Public Policy*, *29*(4), 330-352.

Christensen, B. E., Glover, S. M., & Wood, D. A. (2022). Auditor competence in the era of big data: Evidence from fraud detection. Journal of Accounting Research, 60 (3), 751-796. https://doi.org/10.1111/1475-679X.12415.

DeAngelo, L. E. (1981). Auditor size and audit quality. *Journal of Accounting and Economics, 3*(3), 183-199. https://doi.org/10.1016/0165-4101(81)90002-1

Dewan, S., & Ren, F. (2007). Risk and return of information technology investments: Evidence from firm-level data. *Journal of Information Systems*, 22(2), 112-130.

Dokuchaev V.A., Maklachkova V.V., Statev V.Yu. (2020) Classification of personal data security threats in information systems. T-Comm, vol. 14, no.1, pp. 56-60. (in Russian)

El-Ebiary, Yousef & Alawi, Nahg. (2020). The Risks of Accounting Information Systems. International Journal of Engineering Trends and Technology. 2231-5381. 10.14445/22315381/CATI3P220.

Elshrief, M. (2010). Management fraud in electronic accounting systems: Challenges for auditors. *Journal of Accounting and Auditing*, 12(3), 78-95.

Han, J., et al. (2016). The risks of IT investments: A study of economic unpredictability and technological complexity. *Journal of Information Systems*, 22(2), 112-130.

IFAC. (2009). Handbook of International Quality Control, Auditing, Review, Other Assurance, and Related Services Pronouncements. *International Federation of Accountants*.

Ilmudeen, A. (2013). The Impact of Computer Virus Attacks and Its Preventive Mechanisms among Personal Computer (PC) Users. *Paper presented at the Third International Symposium, South Eastern University of Sri Lanka.*

Imoniana, J. O., Nava Filho, D. C., Cornacchione, E. B., Reginato, L., & Benetti, C. (2023). Impact of technological advancements on auditing of financial statements. *European Research Studies Journal, XXVI* (4), 131-159.

Institute of Chartered Accountants in England and Wales. (n.d.) (ICAEW). (2020). Audit quality standards. Retrieved from https://www.icaew.com/-/media/corporate/files/technical/audit-and-assurance/the-future-of-audit/audit-quality-standards.ashx

International Auditing and Assurance Standards Board (IAASB). (2020). International Standard on Auditing 220 (Revised): Quality Management for an Audit of Financial Statements. IFAC

Kobelsky, K., et al. (2008). The impact of IT budget deviations on firm performance. *Journal of Information Systems*, 22(2), 112-130.

Malami, A. B., Zainol, Z., & Nelson, S. P. (2012). Security Threats Of Computerized Banking Systems (Cbs): The Managers'perception In Malaysia. International Journal of Economics and Finance Studies, 4(1), 21-30.

Mason, O., Stevenson, C., & Freedman, F. (2014). Ever-present threats from information technology: the Cyber-Paranoia and Fear Scale. *Frontiers in Psychology*, *5*, 1298. doi:10.3389/fpsyg.2014.01298

Nisarga, N. (2024). Impact On Technology on Audit Quality and Efficiency. *International Journal of Creative Research Thoughts,* 2(5), 623-657.

Nuryaman, N. (2013). The influence of earnings management on stock return and the role of audit quality as a moderating variable. International Journal of Trade, Economics and Finance, 4(2), 73-78.

Otto, B., & Jarke, M. (2023). Data governance 4.0: A framework for modern data ecosystems. Journal of Data and Information Quality, 15 (1), 1-25. https://doi.org/10.1145/3570910

Polo, F., & Oima, D. (2013). Effect Of Computerised Accounting Systems on Audit Risk Management in Public Enterprises: A Case of Kisumu County, Kenya. *International Journal of Education and Research,* ١(٥), ١-١٠.

Public Company Accounting Oversight Board (PCAOB). (2013). *"Report on the PCAOB's 2012 Inspection of Domestic Annually Inspected Firms."* (PCAOB Release No. 2013-006).

Rangarajan, A., Batts, D., & Dunn, C. K. (2019). Impact of perceived information technology security risks on user resistance to information technology innovations. Proceedings of Society for the Advancement of Information System, March, 27-29.

Rustiarini, N. W., Yuesti, A., & Gama, A. W. S. (2021). Public accounting profession and fraud detection responsibility. *Journal of Financial Crime, 28*(2), 613-627. doi:10.1108/JFC-07-2020-0140.

Saeed, S., Altamimi, S., Alkayyal, N., Alshehri, E., & Alabbad, D. (2023). Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. *Sensors*, *23*(15), 6666. https://doi.org/10.3390/s23156666

Saleem, K. S. M. A., & Oleimat, I. M. (2020). The Impact of Computerized Auditing in Reducing audit risks in Jordan. International Journal of Academic Research in Business and Social Sciences, 10(6), 284 298.

Samir, A. (2019). IT risks and their impact on internal control systems: A study of auditor responsibilities. *Journal of Accounting Research*, 58(3), 45-60.

Serdouk, F., Khalida, A., Bachir, M., & Abdelatif, T. (2024). A Comprehensive Analytical Framework of Audit Quality. *Journal of Informatics Education and Research, 4*, 3654-3671.

Setiawati, R., Eve, J., Syavira, A., Ricardianto, P., Nofrisel, & Endri, E. (2022). The Role of Information Technology in Business Agility: Systematic Literature Review. *Quality - Access to Success, 23*, 144-149. doi:10.47750/QAS/23.189.16

Sjöberg, L., & Fromm, J. (2001). Information Technology Risks as Seen by the Public. *Risk Analysis, 21*(3), 427-442. Doi: https://doi.org/10.1111/0272-4332.213123

Skelton, M. (2012). What to Value: Knowledge, Skills or Understanding? *Academy magazine*, 1(2), 30-33.

Soliman, M. M., & Ragab, A. A. (2014). Audit committee effectiveness, audit quality and earnings management: an empirical study of the listed companies in Egypt. Research journal of finance and accounting, 5(2), 155-166.

Stoel, M. D., & Havelka, D. (2021). Information Technology Audit Quality: An Investigation of the Impact of Individual and Organizational Factors. *Journal of Information Systems, 35*(1), 135-154. doi:10.2308/isys-18-043

Svanström, T. (2016). "Audit Quality and Auditor Behavior." *Journal of Accounting Literature, 36*, 1-16.

Tangprasert, S. (2020). A study of information technology risk management of government and business organizations in Thailand using COSO-ERM based on the COBIT 5 framework. Journal of Applied Science and Emerging Technology, 19(1), 13-24.

Victoria, L. (2020). Information technology: Definitions and applications in modern business. *Journal of Business Technology*, 14(3), 78-95.

Whitman, M. E. (2003). Enemy at the gate. Communications of the ACM, 46(8), 91–95. https://doi.org/10.1145/859670.859675

Williams, A., Harris, B., & Clark, D. (2023). The role of IT in enhancing audit quality. *Journal of Information Systems*, 37(2), 55-70.

Yones, M., & Aissa, S. (2016). Audit planning and risk management. *Journal of Accounting and Auditing*, 12(4), 369-385.

Zahmatkesh, S., & Rezazadeh, J. (2017). The effect of auditor features on audit quality. *Tékhne, 15*(2), 79-87. doi:https://doi.org/10.1016/j.tekhne.2017.09.003

Zhu, P. (2019). 15 characteristics of IT digital maturity. Retrieved from : 15 characteristics of IT digital maturity | CIO.

Appendix A

The Questionnaire

Dear Sir,

I am conducting a research study titled "The Impact of Information Technology Risks on Audit Quality: Evidence from Egypt." This study focuses on exploring the influence of information technology risks in the following areas:

1. Their effect on material misstatements.
2. Their contribution to audit risks.
3. Their role in earnings management.

I kindly request a few moments of your time to complete the attached questionnaire. Your participation in this survey is highly valued and will greatly contribute to the success of the study. Rest assured; your responses will remain completely anonymous. I sincerely appreciate your assistance and thank you in advance for your contribution to this research.

Yours sincerely,

Researcher

First: Concepts Used in the Questionnaire

First: Concepts Used in the Questionnaire

1. Information technology risks: It is a type of business risk defined as the possibility of any technical failure occurring to disrupt the business. There are many types of technology risks, such as information security incidents, electronic attacks, password theft, and service interruptions.

2. Risks related to IT components:

Hardware risk: It is anything on your computer that may damage or steal your data without your knowledge, including malicious software that can create security risks such as viruses.

Software risk: The possibility of suffering loss in the software development process is called software risk.

Database risk: These risks occur due to mismanagement of data, which may lead to weak processes for obtaining data and verifying its storage and protection, such as electronic attacks, storage device failure, and weak security.

Communication risk: It means the risk of loss due to breach of confidentiality or failure of systems integrity, and may lead to the spread of malware, theft and manipulation of data, and continuous unauthorized access within networks.

Network risk: Threats to an organization's digital assets, including information stored on both internal and external servers and public cloud services, such as phishing schemes.

3. Material misstatements: is the appearance of an item of financial lists contrary to fact and misrepresentation is divided into unintentional misrepresentation (error) and deliberate misrepresentation (fraud).

4. Audit risk: It is the failure of the auditor to express an opinion correctly about the financial statements that contain material errors found in the accounting records and books.

5. Inherent risk: It is defined as the possibility of an error in the financial statements without taking internal control into account.

6. Control risk: It is defined as the risk of material misstatements in account balances or a category of transactions that are significant either alone or when

combined with misstatements in other balances or categories or are not detected by internal control.

7. Non detection risk: It is defined as the risk resulting from the failure of audit evidence to detect errors that exceed the maximum acceptable errors in a specific group of accounts. The error of non-detection depends on both the inherent risk and the internal control risk in its estimation.

8. Earnings management: Earnings management is defined as purposeful and deliberate intervention by management in the process of preparing external financial reports with the intention of obtaining some private gains.

Second: General Information

1. Name (Optional): _____

• Please tick "✓" on the appropriate box for each question:

1. Your Educational Level:

□ PhD. □ Diploma

□ Master. □ Bachelor.

2. What is your current job title?

□ Member of teaching staff

□ Auditor

□ Other

4. How many years of experience do you have at your current position?

□ Less than 1 year □ 1-5

□ 5-10 □ Over 10

Please, tick (✓) on front of the level of importance you see suitable for each of the following phrases.

The following statements measure the impact of information technology risks on material misstatements.

No	category	Strongly agree	Agree	Neutral	Disagree	Strongly disagree
1	Risks related to computers affect in increase material misstatements.					
2	Software and database risks reduce the transparency of disclosure of users' financial information.					
3	Risks related to communications lead to increased effort and time spent on reducing material misstatements.					
4	Information technology risks contribute to increasing errors and deviations in the audit process.					

5	Risks resulting from viruses impact the corruption of data files, leading to an increase in material misstatements.					
6	Scientific and practical experience in the field of information technology affects information technology risks.					
7	Information technology risks contribute to the effectiveness of the internal control system.					

The following statements measure the Impact of information technology risks on audit risk.

No	**category**	**Strongly agree**	**Agree**	**Neutral**	**Disagree**	**Strongly disagree**
1	Risks related to computers affect the inherent risk.					
2	Enhancing data security and confidentiality prevents unauthorized data access.					

3	Software-related risks affect inherent risk.					
4	Expertise programs contribute to providing solutions to audit problems.					
5	Database risks affect internal control risk.					
6	Existence of a database with accurate information leads to reducing the censorship					
7	Communication risks affect information security and therefore audit risks.					
8	Lack of adequate protection against network and virus risks affects audit risk.					
9	Auditors' insufficient awareness of the need to examine software when entering devices affects the detection risk.					
10	The risks of unauthorized access to computers by					

	employees affect the audit risk.					
11	Security and encryption methods related to information technology contribute to reducing the risk of censorship.					
12	Software approved for the audit process is affected by IT risks.					

The following statements measure the impact of information technology risks on Earnings management.

No	category	Strongly agree	Agree	Neutral	Disagree	Strongly disagree
1	Information technology plays an important role in reducing earnings management opportunities.					
2	Risks related to hardware, software, and communication networks affect the profit management of the entity under auditing.					
3	Information technology affects the manipulation of financial reporting.					
4	Information technology risks affect the procedures used to verify and document accounts.					
5	Information technology-related risks affect the					

	external auditor's ability to detect earnings management practices.					

Please use this space to write any comments you wish to make

Thank you for your time and participation.