INSTITUTO
UNIVERSITÁRIO
DE LISBOA

A Study of the Emerging Artificial Intelligence risks. Impacts and Mitigation Strategies in the context of a Financial Audit

Filipe Miguel Guimarães Simões Da Rosa Alves

Master in Business Administration

Supervisor:
PhD Rui Alexandre Henriques Gonçalves, Invited Assistant Professor,
ISCTE-IUL

September, 2023

BUSINESS
SCHOOL

A Study of the Emerging Artificial Intelligence risks.
Impacts and Mitigation Strategies in the context of a Financial Audit

Filipe Miguel Guimarães Simões Da Rosa Alves

Master in Business Administration

Supervisor:
PhD Rui Alexandre Henriques Gonçalves, Invited Assistant Professor,
ISCTE-IUL

September, 2023

Acknowledgement

I would like to take a moment to express my heartfelt appreciation to all those who played a significant role in the creation of this dissertation.

First and foremost, I am deeply grateful to my parents for their unwavering support and belief in me throughout my academic journey.

I am immensely fortunate to have had the guidance and mentorship of Professor Dr. Rui Alexandre Henriques Gonçalves. Without his insights, wisdom, and expertise, this dissertation would not have reached the level of quality it possesses today. Together, we have delved into the complexities of AI risks, aiming to shed light on emerging challenges and propose viable solutions for mitigating potential threats.

Furthermore, I extend my appreciation to the faculty and staff of ISCTE for providing a conducive learning environment and access to valuable resources. Their commitment to fostering intellectual growth and academic excellence has been invaluable throughout my academic journey.

Lastly, I would like to express my gratitude to all the participants who generously contributed their time and insights to this research. Their willingness to share their perspectives and experiences has been instrumental in deepening our understanding of AI risks and developing effective strategies for the future.

Abstract

This thesis examines the emerging risks of artificial intelligence (AI) in financial auditing and proposes mitigation strategies. The research combines qualitative interviews with experts and quantitative ranking exercises to understand the severity and frequency of AI risks. Key findings reveal the most substantial risks associated with AI in financial auditing, including data security, errors and biases in algorithms, and data quality. Addressing these risks is crucial for enhancing the accuracy, reliability, and trustworthiness of financial audit procedures in the AI era. The study emphasizes the importance of IT auditing and ethical considerations in AI development. Mitigation strategies involve robust data governance, rigorous testing of AI algorithms, and continuous monitoring. The research contributes by raising awareness of AI risks, providing guidance for auditors and policymakers, and promoting proactive risk management and responsible practices. Future research could explore ethical risks in AI and develop specific ethical guidelines and regulatory frameworks. Overall, the thesis offers valuable insights for navigating AI technology in financial audits and ensuring a trustworthy audit environment.

Key words: Artificial intelligence, financial auditing, IT auditing, AI risks, AI in accounting, Digital transformation, Emerging risks, Mitigation strategies.

JEL Classification System Code: M41 – Accounting, M42 – Auditing, O33 - Technological Change: Choices and Consequences; Diffusion Processes, D81 - Criteria for Decision-Making under Risk and Uncertainty

Resumo

Esta tese examina os riscos emergentes da inteligência artificial (IA) na auditoria financeira e propõe estratégias de mitigação. A pesquisa combina entrevistas qualitativas com especialistas e exercícios de classificação quantitativa para compreender a gravidade e frequência dos riscos da IA. Os principais resultados revelam os riscos mais significativos associados à IA na auditoria financeira, incluindo segurança de dados, erros e bias em algoritmos e qualidade de dados. Abordar estes riscos é crucial para melhorar a precisão, fiabilidade e confiança dos procedimentos de auditoria financeira na era da IA. O estudo enfatiza a importância da auditoria de tecnologias de informação e considerações éticas no desenvolvimento de IA. As estratégias de mitigação envolvem uma governance de dados sólida, testes rigorosos de algoritmos de IA e monitorização contínua. A pesquisa contribui para aumentar a consciencialização dos riscos da IA, fornecendo orientação para auditores e decisores políticos, e promovendo a gestão proativa de riscos e práticas responsáveis. Futuras pesquisas poderiam explorar riscos éticos na IA e desenvolver diretrizes éticas específicas e quadros regulatórios. No geral, a tese oferece informações valiosas para navegar na tecnologia de IA em auditorias financeiras e garantir um ambiente de auditoria confiável.

Palavras-Chave: Inteligência artificial, auditoria financeira, auditoria de TI, riscos da IA, IA na contabilidade, Transformação digital, Riscos emergentes, Estratégias de mitigação.

Classificação JEL: M41 – Contabilidade, M42 – Auditoria, O33 - Mudança Tecnológica: Escolhas e Consequências; Processos de Difusão, D81 - Critérios para Tomada de Decisão sob Risco e Incerteza

Table of Contents

Index of figures

Glossary

AI-Artificial Intelligence

CHAPTER 1 - INTRODUCTION

AI is currently being adopted at an unprecedented rate across a range of industries, ushering in a new era of technological advancement. The application of AI is being seen in diverse areas such as healthcare, finance, transportation, manufacturing, and retail. Similarly, AI is enhancing financial systems through automation, fraud detection, and better investment decision-making (Borges, Laurindo, Spínola, Gonçalves, & Mattos, 2021). However, as AI continues to advance, there are concerns around the ethical and societal implications of its widespread use. Issues such as potential bias, job displacement, and loss of privacy have emerged, and it is critical for policymakers, industry leaders, and society at large to address these challenges and ensure that AI is used in a responsible and ethical manner (Cheatham, Javanmardian, & Samandari, 2019) (McKinsey, 2019). The integration of AI technology in accounting has become increasingly popular as businesses aim to streamline accounting tasks, enhance decision-making, and gain valuable insights from large amounts of data. The current context of AI in accounting includes several applications, such as automating routine accounting tasks, detecting potential fraud, analysing financial data, forecasting future trends, ensuring tax compliance, and improving the audit process (Petkov, 2020) (Luo, Meng, & Cai, 2018) (ICAEW, 2018). However, despite the benefits of AI in accounting, there are also challenges and limitations to consider. These include concerns related to data privacy and security, the need for human intervention, and the potential for bias in AI algorithms. It is crucial for firms to assess the advantages and risks of implementing AI in accounting and to implement adequate measures to mitigate potential risks (Luo, Meng, & Cai, 2018) (Bose, Dey, & Bhattacharjee, 2022) (Hasan, 2021).

Financial auditing involves the examination of financial statements, records, and other financial documents to ensure that they accurately reflect a company's financial position. In this process, there are several risks that auditors should be aware of. Overall, auditors must be vigilant in identifying and assessing the various risks associated with financial auditing and take steps to mitigate these risks to ensure the accuracy and integrity of the financial statements (Allen, Hermanson, Kozloski, & Ramsay, 2006)(IAASB, 2019). As companies increasingly rely on information technology (IT) systems to generate and process financial information, IT risks have become an integral part of financial auditing. IT risks refer to risks related to the use of IT systems and processes in generating or processing financial information. IT risks that are relevant in financial auditing include system availability and reliability, data accuracy and completeness, system security, compliance with laws and regulations, and IT governance. System downtime or data loss can result in inaccurate financial reporting, while errors or omissions in data can lead to misstatements in financial reports. Inadequate security measures can result in unauthorized access to financial information, which can lead to fraud or financial loss. Failure to comply with relevant laws and regulations can result in fines and legal action. Finally, inadequate governance and oversight can result in poor IT performance, which can affect the accuracy and

integrity of financial information (Barta, 2018). To ensure the accuracy and integrity of financial information, auditors must be aware of IT risks and assess the adequacy of IT controls in place to address these risks. They may need to perform specialized IT audit procedures to identify any IT-related issues that may affect the accuracy and integrity of financial information (International Auditing and Assurance Standards Board [IAASB], 2018). As AI technology plays an increasingly significant role in business operations, auditing AI is becoming a critical part of IT audit. Auditing AI involves assessing the accuracy, reliability, and integrity of AI-generated results and ensuring that AI systems comply with relevant laws, regulations, and ethical standards (IAASB, 2019). To audit AI, IT auditors require specialized knowledge of AI technology and must work with AI experts to understand the algorithms and models used by AI systems. The auditing process involves several steps, including evaluating the quality of the data used in AI systems, assessing the design and implementation of AI systems, testing the effectiveness of controls, and evaluating the cybersecurity risks associated with AI systems. IT auditors must have a deep understanding of AI technology to evaluate the accuracy, reliability, and integrity of AI-generated results. They must also be aware of the ethical, legal, and regulatory risks associated with AI systems and take steps to mitigate these risks. Auditing AI as part of IT audit requires a combination of technical expertise and a thorough understanding of business operations. As the financial sector embraces AI-driven solutions, it becomes imperative to closely examine and mitigate the potential risks associated with its implementation, particularly within the realm of financial auditing.

This thesis aims to investigate the emerging risks of AI relevant in financial auditing, assess their severity and frequency, and propose effective mitigation strategies. Furthermore, it seeks to underline the growing significance of IT auditing in financial auditing projects. The main goals of this study are threefold. Firstly, it seeks to investigate the AI risks that are particularly relevant in the context of a financial auditing project. These risks may arise from the adoption of AI technologies, the reliance on automated processes, or the handling of large volumes of financial data. Secondly, this research aims to understand the severity and frequency of these relevant AI risks, assessing their potential impact on financial auditing activities. Lastly, it aims to identify and explore the main techniques that can be applied to mitigate these AI risks within the realm of financial auditing projects. To ensure a comprehensive and effective investigation, three research questions have been carefully crafted to guide this study. The first research question (RQ1: What are the AI risks relevant in the context of a financial auditing project?) focuses on identifying the AI risks that hold relevance in the context of financial auditing projects. By exploring the specific risks arising from AI implementation, this question aims to provide a thorough understanding of the risks associated with this technological integration. The second research question (RQ2: How do these risks manifest concerning their frequency and severity?) delves into the behaviour of these identified risks, examining their frequency and severity.

This analysis will shed light on the potential impact and consequences of the identified risks. Lastly, the third research question (RQ3: What are the main techniques that can be applied to effectively mitigate AI risks in the context of a financial auditing project?) aims to identify and evaluate the main techniques that can be employed to effectively mitigate AI risks within the context of financial auditing projects. The relevance of this study lies in its significance and contribution to the current literature on the emerging risks of AI in financial auditing. As AI technologies continue to advance and become integral to financial processes, it is imperative to understand and address the associated risks. By examining these risks, their impacts, and potential mitigation strategies, this study fills an important gap in the existing literature and offers valuable insights to various stakeholders. First and foremost, this research contributes to the field of financial auditing by shedding light on the specific risks introduced by AI technologies. While AI brings efficiency and automation to auditing processes, it also presents unique challenges that must be addressed to ensure the accuracy, reliability, and integrity of financial reports. By identifying and exploring these risks in detail, this study enhances the understanding of auditors, financial professionals, and regulatory bodies regarding the potential pitfalls of AI integration in accounting and financial activities. Furthermore, this study highlights the growing importance of IT auditing within financial auditing projects. As AI becomes more prevalent, auditors need to possess the necessary skills and expertise to effectively assess, monitor, and mitigate the associated risks. By emphasizing the relevance of IT auditing and its role in managing AI risks, this research underscores the need for auditors to adapt and acquire the technological knowledge and competencies required to navigate the evolving landscape of financial auditing. Moreover, this study contributes to the wider field of risk assurance and advisory by providing a comprehensive examination of AI risks in financial auditing. The identified risks, such as data quality, data security, and algorithmic biases, transcend the boundaries of financial auditing and have implications for risk management practices across industries. Therefore, the insights gained from this research can inform risk assurance and advisory professionals in various sectors, helping them anticipate and address similar challenges that may arise from the integration of AI technologies. Additionally, the findings of this study have implications for policymakers and regulatory bodies responsible for overseeing financial reporting standards. As AI technologies increasingly impact financial audits, regulators need to ensure that appropriate guidelines and regulations are in place to address the associated risks effectively. The insights and mitigation strategies proposed in this research can inform the development of regulatory frameworks that promote the responsible and secure use of AI in financial auditing. Overall, this study's contribution to the current literature is twofold: First, it enhances the understanding of the risks specific to AI integration in financial auditing, providing a comprehensive examination of their impacts. Second, it underscores the growing importance of IT auditing and offers practical insights into mitigation strategies that can be employed to address these risks effectively. By filling these knowledge

gaps, this research equips auditors, financial professionals, policymakers, and regulatory bodies with the necessary information and tools to navigate the complex landscape of AI risks in financial auditing, ultimately promoting transparency, reliability, and confidence in financial reporting practices. Undertaking a study of this nature entails navigating a labyrinth of interdisciplinary domains, each requiring a unique set of research, skills, and knowledge. The first key area is technology, which forms the foundation for AI systems and their functionalities. A deep understanding of the underlying principles and mechanics of AI technologies, such as machine learning algorithms is crucial to comprehend the intricacies of the risks and impacts they pose within a financial audit context. Furthermore, a strong grasp of the evolving AI landscape, including current trends, developments, and limitations, is essential for developing effective mitigation strategies. The second critical domain that intertwines is financial auditing. An extensive knowledge of auditing principles, standards, and methodologies is paramount to identify potential risks associated with AI systems and their impact on financial audits. Additionally, a deep familiarity with the auditing profession's ethical considerations and independence requirements is crucial for designing robust mitigation strategies. Accounting and finance constitute the third area of expertise necessary for this study. Proficiency in financial accounting principles, financial statement analysis, and financial reporting frameworks is essential to comprehend the implications of AI on financial data processing, analysis, and reporting. A comprehensive understanding of financial risk assessment and management is also vital in assessing the potential vulnerabilities and threats that AI poses to the accuracy, integrity, and confidentiality of financial information. Lastly, risk management plays a pivotal role in this research endeavour. The ability to identify, evaluate, and mitigate risks associated with AI systems requires expertise in risk assessment frameworks, data governance, and cybersecurity. Familiarity with relevant regulatory guidelines and standards, such as data protection regulations and cybersecurity best practices, is crucial in developing effective strategies to mitigate AI-related risks in the context of financial audits. In light of the intricate web of knowledge and skills required across multiple domains, conducting a comprehensive study on the emerging risks of AI in financial audits is undeniably challenging. However, by embracing this complexity and leveraging a multidisciplinary approach, this research aims to shed light on the potential risks and impacts of AI in financial audits while proposing robust mitigation strategies to ensure the integrity, reliability, and effectiveness of the audit process in an AI-driven era. To achieve the research goals, a mixed-methods approach will be employed. The qualitative component involves conducting interviews with experts in the Risk Assurance department of a Big 4 company. These interviews will focus on gathering the perspectives of these professionals regarding the relevant AI risks in financial auditing. Thematic analysis will be employed to identify key themes and patterns within the experts' responses, allowing for a comprehensive exploration of the identified risks. The quantitative component of this study involves ranking the AI risks in terms of their likelihood

and magnitude, providing a quantitative assessment of their significance. Descriptive statistics will be used to summarize the rankings and identify any prevailing trends. The combination of qualitative and quantitative data analysis will enable a holistic understanding of the risks and their potential impact on financial auditing activities. Preliminary findings from this research endeavour highlight several AI risks relevant to financial auditing. These include concerns regarding data quality, data security, the lack of expertise in AI among professionals, the limited human agency in AI-driven processes, and potential errors and biases embedded within algorithms. Through the completion of this study, a comprehensive understanding of these risks will be attained, alongside the formulation of effective mitigation strategies. The structure of the dissertation ensures a logical and systematic exploration of the emerging risks of AI in financial auditing. It comprises several main sections. The literature review section comprehensively explores the importance of IT auditing in securing financial integrity within financial audits. It discusses the transformative changes brought about by AI integration in accounting and finance. It also examines the risks associated with AI adoption in these domains, including the challenges and considerations related to auditing AI systems in financial projects. The section addresses risk assessment in financial auditing, covering topics such as the relevance of risks, their magnitude and likelihood, consequences, mitigation tactics, and the role of IT experts. The methodology chapter outlines the research approach, which involves a mixed-method approach. It describes the data collection methods, such as interviews, and explains the criteria for selecting participants. Additionally, it provides an overview of the data analysis techniques employed, including thematic analysis and descriptive statistics. The Discussion and Results chapter presents the findings of the research study, analysing the identified AI risks and their implications for financial auditing practices. It emphasizes the pertinence of AI auditing in the present and future landscape of financial auditing, highlighting the need to adapt auditing practices to AI technology advancements. The chapter explores the impacts and consequences of AI risks on financial integrity and investor trust, drawing on case studies and real-world examples. It also discusses mitigation strategies and the critical role of IT experts in auditing and analysing AI controls. Furthermore, it explores ethical considerations associated with AI in financial auditing, addressing concerns related to bias, privacy, and transparency. The conclusion summarizes the main findings of the research study and revisits the research objectives and questions. It discusses the theoretical and practical implications of the research, highlighting its contributions to the field of risk assurance and IT auditing. The conclusion offers recommendations for future research, acknowledging the potential for further exploration and development of the topic.

Chapter 2- Literature review

The literature review section is divided into several subsections to provide a comprehensive understanding of the research area. It begins with an exploration of the growing importance of IT auditing in securing financial integrity within the context of financial audits. The review then moves on to discuss AI technology and its implications for accounting, focusing on the transformative changes brought about by AI integration. Next, the literature review delves into the risks associated with AI adoption in accounting and finance, drawing insights from existing research. The section concludes by examining the specific challenges and considerations related to auditing AI systems in financial auditing projects. Additionally, it addresses various themes related to risk assessment in financial auditing, including the relevance of risks, determining their magnitude and likelihood, consequences, mitigation tactics, and the role of IT experts in such projects.

2.1. Significance of IT Auditing in Securing Financial Integrity in a financial audit

In recent years, the increasing reliance on technology in business processes and the rapid digitalization of financial systems have underscored the importance of IT auditing in the field of financial auditing, proving the role of IT auditing and its growing significance in ensuring the integrity, security, and reliability of information systems within organizations (Otero, 2018) (Johnstone, Gramling, & Rittenberg, 2017). As information technology (IT) continues to play an increasingly important role in financial auditing, IT auditing has become an essential part of the auditing process. The purpose of IT auditing is to evaluate and assess the effectiveness and reliability of financial information dependent on IT systems (Senft & Gallegos, 2016). The proliferation of technology in financial systems has significantly increased the complexity and interconnectedness of business processes. As organizations adopt advanced financial applications, enterprise resource planning (ERP) systems, and cloud computing, the need for robust IT auditing practices has become paramount to ensure the accuracy, completeness, and reliability of financial information (Champlain, 2003) (Weber, 1998). IT auditing plays a vital role in identifying and mitigating IT-related risks that could have a material impact on financial reporting. By assessing the effectiveness of IT general controls (ITGCs) and application controls, IT auditors help ensure that financial transactions are accurately recorded, processed, and reported in compliance with regulatory requirements. This includes evaluating controls related to access management, change management, segregation of duties, and data validation (Gregory, 2019). One of the key strategies for IT auditing in financial auditing is to conduct a risk assessment that considers the potential risks associated with the use of IT systems, including the risk of cybersecurity breaches, data breaches, and errors in data processing. IT auditors must also evaluate the controls put in place to monitor and detect errors and irregularities in the operation of IT systems. In addition, IT auditors must assess the reliability and accuracy of the data used in financial auditing and evaluate the effectiveness of the security measures used to protect sensitive data (Senft & Gallegos, 2008) (Weber,

1998). Protecting sensitive financial data from unauthorized access, disclosure, and alteration is critical. IT auditors evaluate security controls, such as network security, user access controls, encryption measures, and vulnerability management processes, to ensure the confidentiality, integrity, and availability of financial information. By identifying vulnerabilities and recommending security enhancements, IT auditing helps mitigate the risk of data breaches and supports compliance with data protection regulations (Wood, Brown, & Howe, 2013). Effective internal controls are also essential for ensuring the reliability of financial information. IT auditing helps assess the design and effectiveness of internal controls, including both ITGCs and application controls. Through the evaluation of control frameworks, IT auditors identify control deficiencies and provide recommendations to strengthen internal controls, reducing the risk of fraud, errors, and misstatements in financial reporting (Davis, Schiller, & Wheeler, 2016). Another strategy for IT auditing in financial auditing is to obtain assurance from the developers and vendors of IT systems. IT auditors can obtain such assurance through independent testing and validation of the IT system by a third-party expert. Additionally, IT auditors can request documentation that describes the development and testing of the IT system, including the data sources, algorithms used, and quality control measures implemented (Gregory, 2019). To ensure that IT systems are used effectively and efficiently in financial auditing, IT auditors must implement ongoing monitoring procedures that evaluate the performance and effectiveness of the IT system. These procedures can include ongoing monitoring of the data used in financial auditing, as well as the performance of the algorithms used. Additionally, IT auditors must evaluate the controls put in place to monitor and detect errors and irregularities in the operation of IT systems and ensure that these controls are working as intended (Weiss & Solomon, 2015). Collaboration between auditors and IT experts is essential for IT auditing in financial auditing. By working together, these professionals can develop effective audit procedures that consider the unique risks associated with the use of IT systems. Additionally, collaboration with regulators and policymakers can help ensure that IT is used in ways that benefit both the profession and society as a whole (Weiss & Solomon, 2015). All this means IT auditing in financial auditing requires a multifaceted approach that includes risk assessment, obtaining IT system assurance, ongoing monitoring, and collaboration between auditors, IT experts, and regulators. Moving forward, it will be essential for auditors to adopt these strategies in order to ensure that IT is used effectively and efficiently in financial auditing (Information Systems Audit and Control Association, 2018) (Gregory, 2019).

2.2. AI technology

Artificial intelligence (AI) refers to the simulation of human intelligence processes by machines, especially computer systems. It has been around for several decades, but recent technological

advancements have spurred a new wave of AI research, leading to the development of new tools and techniques for solving complex problems (Russell & Norvig, 2010) (Floridi & Cowls, 2019). In the early days of AI research, the focus was on creating rule-based systems that could perform specific tasks, such as playing chess or proving mathematical theorems. In the 1980s and 1990s, the emergence of machine learning marked a significant shift in AI research. Instead of relying on hand-coded rules, machine learning algorithms could learn from data and make predictions or decisions based on that learning (Brynjolfsson & Mitchell, 2017) (Floridi & Cowls, 2019) (Tegmark, 2017). Today, deep learning and neural networks have become the dominant approach to AI research, allowing machines to perform complex tasks like image recognition and natural language processing (Goodfellow, Bengio, & Courville, 2016). AI has numerous applications across a wide range of fields, and its potential impact is still being explored. One of the most promising areas of AI is healthcare. AI algorithms can analyse vast amounts of medical data and identify patterns that can help physicians diagnose diseases and develop treatment plans. AI is also being used in drug discovery, medical imaging, and personalized medicine (Esteva et al., 2019) (Nadimpalli, 2017). Another area where AI is having a significant impact is transportation. Self-driving cars are becoming a reality, thanks to advances in AI and machine learning. AI algorithms can analyse sensor data from cameras, radar, and lidar to make decisions about steering, acceleration, and braking. This technology has the potential to reduce accidents and improve the efficiency of transportation systems (Tsolakis, Schumacher, Dora, & Kumar, 2022) (Abduljabbar, Dia, Liyanage, & Bagloee, 2019). AI is also being used in finance, where it can analyse large amounts of financial data to identify trends and make predictions about market movements. In manufacturing, AI is being used to optimize supply chains, reduce waste, and improve quality control. In education, AI is being used to create personalized learning experiences that adapt to the needs of individual students (Tsolakis, Schumacher, Dora, & Kumar, 2022) (McKinsey Global Institute, 2018).

2.3. The Transformative Impact of Artificial Intelligence on Accounting

AI has become increasingly pervasive, influencing various aspects of our personal and professional lives. The potential of AI is being harnessed to revolutionize numerous industries, including accounting. The adoption of AI technologies in accounting is projected to be widespread, with around 70 percent of companies expected to adopt at least one AI technology by 2030 (McKinsey Global Institute, 2018). This trend indicates the imminent and significant changes the accounting profession will undergo with the widespread adoption of AI technologies. While the application of AI in the accounting industry is still in its infancy, the current technologies being used in accounting do not fully represent the potential of AI (Luo, J., Meng, Q., & Cai, Y, 2018). The development of AI in accounting faces challenges due to its complex technology and the limited practical experience of the workforce. Consequently, AI's

progress in accounting is still at a nascent stage, requiring further work before effective deployment can be achieved. However, nearly 80 percent of executives at companies deploying AI have already reported moderate value from its implementation (McKinsey, 2019). The traditional model of manual accounting has gradually been replaced by modern financial software accounting forms. With the advent of AI, accounting is about to undergo another major shift. Firms are increasingly adopting a technology-first approach and consider AI a source of competitive advantage (McKinsey Global Institute, 2018). Research suggests that AI could deliver an additional global economic output of $13 trillion per year by 2030 (McKinsey Global Institute, 2018). AI's ability to process vast amounts of data quickly and accurately makes it an ideal tool for tasks such as financial statement analysis and audit trail tracking. It also enhances decision-making processes by providing real-time data analysis and insights (ICAEW, 2018). The use of AI in accounting offers significant benefits in terms of speed, accuracy, and efficiency. A majority of accountants anticipate that AI will automate various accounting tasks in the near future (Sage, 2019). This has led many accounting firms to invest in AI to transform the industry and mitigate inherent risks. The applications of AI in accounting are broad and diverse. They include automating repetitive tasks such as data entry, reconciliation, invoicing, and accounts payable processes. AI can also be used for more complex tasks such as fraud detection and risk assessment (Sage, 2020). Surveys conducted among accounting professionals indicate a growing interest in investing in AI to automate repetitive and time-consuming tasks, as well as to enhance business operations (Sage, 2018). AI can help businesses meet three key objectives: automating business processes, gaining insights through data analysis, and connecting with consumers and workers (Hasan, 2021). The impact of AI on the accounting field is mainly centered on data and automation. AI-driven technologies and applications enable faster access and processing of large volumes of data, which was previously challenging using traditional methods (CMA Exam Academy, 2023; Accounting Today, 2020). AI's prevalence in accounting lies in automating repetitive tasks, where it demonstrates remarkable accuracy and efficiency. Tasks such as data input and matching, receipt reconciliation, invoice creation and sending, expense reports, price tracking, account reconciliation, sorting transactions, and data recording and reporting can all be accomplished by AI systems (CMA Exam Academy, 2023). Consequently, the role of bookkeepers may change as AI replaces many of their tasks, transforming the accounting career structure (Hasan, 2021) (CMA Exam Academy, 2023). The integration of AI technologies has revolutionized traditional accounting practices, leading to automation of mundane tasks, facilitation of financial projections, streamlining of processes, enforcement of corporate policies, and provision of assistance (Hasan, 2021).

2.4. Exploring the Risks of AI Adoption in Accounting and Finance

(McKinsey,2019) Affirms Artificial Intelligence is proving to be a double-edged sword. Comparing to new technologies both sides of the AI blade are far sharper, and neither blade is well understood. The integration of artificial intelligence (AI) into various industries, including accounting, has brought about transformative changes and enhanced efficiency. However, along with these advancements, there are inherent risks and challenges that need to be carefully considered and managed. Understanding and addressing these risks is crucial to ensure the responsible and effective use of AI technologies in the accounting field. By proactively identifying and mitigating these risks, organizations can harness the power of AI while maintaining the integrity and reliability of financial information and safeguarding against potential pitfalls. After conducting extensive research on the topic, compiled a comprehensive list of AI risks mentioned and highlighted by various sources. Throughout this process it was observed recurring patterns which lead to the categorization of these risks into eight main areas: Data Quality, Data Security, Errors and biases in algorithms, Detecting rogue AI, Lack of expertise, Lack of human agency in AI processes, Excessive reliance on AI, and Deepfakes. A detailed exposition of each risk category is presented hereinafter.

2.4.1. Data quality risks

Data quality risks in artificial intelligence (AI) systems pose significant challenges and potential pitfalls. AI models heavily rely on the quality and integrity of the data used for training, validation, and inference (CMA Exam Academy, 2023). If the data used to build and operate AI systems is flawed, biased, incomplete, or inaccurate, it can lead to severe consequences, including biased decision-making, ethical issues, and degraded performance (McKinsey Global Institute, 2018). One significant risk is biased data, wherein AI models trained on biased datasets can perpetuate and amplify existing biases. If the training data reflects historical biases or is skewed, the AI system may replicate these biases in its decision-making processes (EY,2018)(Cheatham,Javanmardian,&Samandari, 2019)(ICAEW, 2018). Another data quality risk is the presence of incomplete or insufficient data, which can result in poor performance and unreliable outcomes. Insufficient data or a lack of diversity in the training dataset may hinder the AI system's ability to make accurate predictions or decisions in unfamiliar scenarios (McKinsey Global Institute, 2018). Moreover, incomplete data can lead to incomplete or incorrect inferences, compromising the system's reliability (EY, 2018)(Cheatham,Javanmardian,& Samandari,2019). Data drift is another critical data quality risk. Data drift occurs when the statistical properties of the input data change over time, rendering the trained AI model less effective or obsolete. As the real-world evolves, the underlying data distribution may shift, impacting the model's performance if it has not been appropriately updated to adapt to these changes. Failure to monitor and address data drift can gradually deteriorate an AI system's performance, resulting in suboptimal

decisions and predictions (Cheatham,Javanmardian,&Samandari, 2019)(McKinsey Global Institute, 2018).

2.4.2. Data security risks

Data security risks in artificial intelligence (AI) systems used for financial and accounting activities pose significant concerns and require careful attention (Zhu & Guan, 2022). AI systems often rely on large volumes of data, including sensitive and personal information, which makes them attractive targets for malicious actors (McKinsey Global Institute, 2018). Data breaches, unauthorized access, and data manipulation can have severe consequences, compromising privacy, integrity, and the overall trustworthiness of AI systems (ICAEW, 2020). Some examples of data security risks associated with AI systems include unauthorized accesses, AI systems store and process vast amounts of data, which can include personally identifiable information (PII), intellectual property, financial records, or other sensitive information(Parlak, 2023). If these systems are not adequately secured, they become potential targets for unauthorized access. Malicious actors may exploit vulnerabilities in the AI infrastructure, gain unauthorized access to the data, and use it for nefarious purposes, such as identity theft or corporate espionage(Cheatham, Javanmardian, & Samandari, 2019) (McKinsey Global Institute, 2018) (ICAEW, 2018).Another risk concerns Data leakage, which refers to the unintentional exposure or unauthorized disclosure of data. In AI systems, data leakage can occur at various stages, including during data storage, data transmission, or during the inference phase when the system processes new data. Data leakage can compromise privacy and confidentiality, exposing sensitive information to unauthorized parties(EY, 2018) (ICAEW, 2018) (ICAEW, 2020). Lastly, the risk of adversarial attacks involve manipulating input data to deceive AI systems or cause them to produce incorrect or malicious outputs. Attackers can intentionally modify or tamper with the input data to mislead the AI model, leading to wrong decisions or compromised results (Parlak, 2023). Adversarial attacks can have serious consequences in critical domains such as healthcare, autonomous vehicles, or financial systems, where incorrect outputs can result in harm or financial loss (Cheatham, Javanmardian, & Samandari, 2019).

2.4.3. Lack of expertise in AI risks

As companies increase the implementation of AI applications to replace human work, the lack of IT experts who understand these technologies may leave a firm vulnerable (Parlak, 2023). For example, the lack of training for program users (Lack of expertise on the part of the accountants) may lead to misuse of AI which can result in inaccurate results, non-compliance with legal standards and increase vulnerability to cyberattacks. The firm´s internal auditing of AI may require more expertise which can lead to serious risks in performance and security if not correctly conducted (CMA Exam Academy,

2023). The lack of expertise in AI systems can give rise to significant risks and challenges. Developing and deploying AI systems requires a deep understanding of AI technologies, data science, ethics, and domain-specific knowledge. Insufficient expertise in any of these areas can lead to suboptimal design choices, biased or flawed models, and ineffective or even harmful outcomes (Luo, Meng, & Cai, 2018). Some examples of risks associated with the lack of expertise in AI systems:

Poor Model Development: Building effective AI models requires expertise in data processing, feature engineering, algorithm selection, and model architecture design. Without the necessary expertise, developers may struggle to make informed decisions at each stage of the model development process, leading to subpar model performance (Rao, 2020). Inadequate understanding of AI algorithms and techniques can result in models that are not optimized for the specific problem domain, leading to inaccurate or unreliable predictions (Cheatham, Javanmardian, & Samandari, 2019) (McKinsey Global Institute, 2018).

Inadequate Data Governance: Expertise in data governance is crucial for ensuring data quality, privacy protection, and compliance with relevant regulations. Insufficient understanding of data governance principles can lead to poor data management practices, including inadequate data documentation, inappropriate data handling, or failure to ensure data security (Rao, 2020). This can increase the risk of data breaches, compromise the integrity of the AI system, and result in legal and regulatory non-compliance (Cheatham, Javanmardian, & Samandari, 2019) (McKinsey Global Institute, 2018).

Limited Interpretability and Explainability: AI systems often operate as black boxes, making it difficult to understand and interpret their decision-making processes. Lack of expertise in interpretability techniques can impede the ability to explain how an AI system arrived at a particular decision or prediction (Parlak, 2023). This lack of transparency hinders user trust, makes it challenging to identify and correct errors or biases, and can lead to resistance and scepticism towards AI systems (Cheatham, Javanmardian, & Samandari, 2019).

2.4.4. Lack of human agency in AI processes and accountability risks

As AI increases automation on repetitive and cognitive tasks, the human factor will decrease in these types of activities. Although increase in automation comes with several benefits, some risks may come from the lack of human input in accounting. For example, in a traditional development environment, a request for a change or new functionality is made, approved, and subsequently developed by someone in the IT organization (Zhu & Guan, 2022). After the appropriate IT processes and controls are followed, the change is made to the application, or the new application is implemented. In the traditional environment, this follows an existing change management process and would be addressed by change management controls tested by auditor's experts. In the case of a AI automated process, it

may also start with a request for a new automation. However, often business users, not traditional IT developers, are responsible for developing and creating it. Understanding the AI strategy, including which specific technologies are being deployed, is critical to understand the relevant risks and to be able to evaluate control design and identify potential gaps that may exist (Parlak, 2023). Potential risks are inappropriate or incompletely processed data by the automation due to errors in the configuration of the automation or Inappropriate changes to the automation as it may involve non-traditional IT developers. The lack of human agency in AI processes and the associated accountability risks raise significant concerns about the deployment and impact of AI systems (Zhu & Guan, 2022). When humans are removed or marginalized from decision-making processes, and AI systems operate autonomously without sufficient oversight or accountability mechanisms, several risks can emerge. These risks include biased or unfair outcomes, lack of transparency, erosion of human values, and potential for unethical behaviour. Some key aspects related to the lack of human agency and accountability risks in AI systems:

Lack of Transparency and Explainability: AI systems, particularly complex ones like deep neural networks, often operate as black boxes, making it challenging to understand how they arrive at their decisions (Rao, 2020). When humans lack the ability to interpret and explain the reasoning behind AI systems' outputs, it can lead to decreased trust, as well as difficulties in identifying and rectifying errors, biases, or unintended consequences. The lack of transparency hinders accountability and makes it difficult to address issues or challenge the system's outputs (Cheatham, Javanmardian, & Samandari, 2019).

Limited Control and Decision-Making: When humans are excluded from key decision-making processes, it can lead to a loss of control and influence over the outcomes produced by AI systems (Marr, 2018). Humans may be left unable to intervene or correct erroneous or harmful decisions made by AI. This lack of control can erode human agency, leaving individuals or organizations at the mercy of the AI system's outputs, potentially impacting their lives, livelihoods, or reputations (Parlak, 2023).

2.4.5. Errors and biases in algorithms risks

If AI is being programmed to make decisions/projections based on data, it can develop certain biases and create misalignments between our goals and the machine’s. AI systems can perpetuate biases that are present in the data used to train them (CMA Exam Academy, 2023). This can lead to biased or incomplete audit results if the data used to train the AI system is not representative of the entire population or contains hidden biases. This is the concept of correlating items based on a data set, but the correlation does not reflect all aspects of the data. Errors and biases in algorithms pose significant risks in AI systems. While AI has the potential to enhance decision-making and improve efficiency, it is

not without its flaws (EY, 2018). Algorithms are created by humans and are inherently influenced by their biases, which can lead to unintended consequences and discriminatory outcomes (McKinsey Global Institute, 2018). Moreover, errors in the design, implementation, or training of algorithms can also result in detrimental effects. Understanding and mitigating these risks is crucial for the responsible development and deployment of AI systems. One of the prominent risks in AI systems is algorithmic bias (Information Systems Audit and Control Association, 2018). Bias can be introduced at various stages of the AI development process (Cheatham, Javanmardian, & Samandari, 2019). It may stem from biased training data, where historical data may reflect social biases, stereotypes, or systemic discrimination. If the training data contains unfair or discriminatory patterns, the algorithm may learn and perpetuate those biases, leading to biased decisions or actions. Moreover, biases can also emerge from the design choices made by developers (Rao, 2020). The selection of certain features, the choice of optimization metrics, or the inclusion/exclusion of specific data points can introduce inherent biases into the algorithm (Parlak, 2023). Additionally, biases can arise from the lack of diversity in the development teams, leading to the overlooking of certain perspectives and potential biases in the algorithms. Another risk in AI systems is the potential for errors, both unintentional and intentional. Unintentional errors can occur due to various reasons, such as bugs in the code, inadequate training data, or flawed assumptions during algorithm design (McKinsey Global Institute, 2018). These errors can lead to incorrect or unreliable outputs, potentially causing harm in critical domains like healthcare or finance. Intentional errors can arise from malicious actors exploiting vulnerabilities in AI systems. Adversarial attacks, where inputs are carefully crafted to deceive the algorithm, can cause AI systems to make incorrect decisions (Rao, 2020). For example, autonomous vehicles can be tricked into misidentifying road signs or objects, potentially leading to accidents.

2.4.6. Detecting rogue AI risks

The concept that AI will teach itself and change its core algorithms as it processes more data is known as machine learning. While AI can learn and adapt through experience, data discovery, and pattern recognition (thereby enhancing its effectiveness at executing its tasks as it learns more about the "world" in which it operates), this progressive learning is highly dependent on the design framework (Cheatham, Javanmardian, & Samandari, 2019). In particular, if the AI framework does not include human supervision of changes, the machine is learning and making decisions in the algorithm, the AI may ultimately be making decisions inconsistent with the entity's intentions (Marr, 2018). This creates a misalignment between our goals and the machine’s. For example:

Unauthorized access and modification: Rogue AI may be designed to access and modify accounting data without proper authorization, leading to data breaches or unauthorized changes to financial records (Rao, 2020).

Lack of transparency: Rogue AI may be opaque and difficult to understand or explain, making it challenging for auditors to verify the accuracy of accounting data processed by the AI system. (Rao, 2020)

One of the primary risks of rogue AI is the loss of control. As AI systems become increasingly complex and autonomous, there is a possibility that they may exceed human understanding and override human instructions or constraints. This could occur due to unintended consequences arising from the AI system's optimization objectives or the emergence of unforeseen behaviours during the system's learning and decision-making processes. Once an AI system surpasses human control, it may act in ways that are detrimental to human interests (Cheatham, Javanmardian, & Samandari, 2019).

2.4.7. Excessive reliance on AI risks

One of the crucial considerations when implementing artificial intelligence is the overall dependence on the system itself. While AI algorithms are often designed to possess a certain degree of autonomy and adaptability, the extent to which they operate without human intervention is a critical factor in their design. It is important to strike a balance between the freedom given to AI systems and the need for human oversight and control. An inherent cost associated with AI is the potential vulnerability to hacking or cyber attacks (EY, 2018). If an AI system lacks robust safeguards and is inadequately protected, it becomes susceptible to malicious intrusions. Without appropriate measures in place, such vulnerabilities can be exploited, leading to severe consequences for the organization. These consequences may include data breaches, compromised sensitive information, or disruption of critical operations, ultimately jeopardizing the company's reputation, financial stability, and customer trust (Cheatham, Javanmardian, & Samandari, 2019). Furthermore, the absence of human backup or support to address these issues amplifies the risks associated with an AI system. Without human intervention, the ability to detect and mitigate cyber threats or rectify system malfunctions becomes severely limited. This overreliance on AI can transform it from an asset into a liability for the organization (Bose, Dey, & Bhattacharjee, 2022). The incorporation of proper safeguards and human oversight is essential to mitigate the risks associated with AI. Human involvement enables proactive monitoring, continuous assessment, and response to emerging threats or issues. Human experts can analyze and interpret complex patterns, identify anomalies, and implement necessary countermeasures to protect the AI system from potential attacks (Zhu & Guan, 2022). They can also intervene when the AI system encounters unfamiliar or ambiguous situations, preventing it from

making erroneous decisions that could harm the organization. Maintaining a symbiotic relationship between AI and human oversight allows for the best of both worlds. While AI brings efficiency, scalability, and advanced capabilities, human supervision provides critical judgment, intuition, and contextual understanding. This collaborative approach ensures that the AI system operates within ethical and legal boundaries, adhering to established guidelines and principles. Although AI offers immense potential, its reliance on the entire system must be carefully considered (Rao, 2020). Neglecting to implement adequate safeguards and human oversight can increase the organization's exposure to risks, making the AI system a liability rather than an asset. Balancing autonomy with human involvement is crucial to address vulnerabilities, combat cyber threats, and safeguard the organization's interests (Petkov, 2020). A well-designed AI system, complemented by human expertise, can maximize its benefits while minimizing potential harm.

2.4.8. Deepfakes risks

AI can be used to create Deep-fake´s and pretend to be someone who has elevated permissions within a system or network. This is typically reserved for system administrators or other users who need to perform critical tasks, such as making changes to the system configurations, installing software, or accessing sensitive data (Floridi, 2021). For example, the fake voice of a CEO can be used to defraud a company and commit financial fraud (Rao, 2020). AI deepfakes can pose significant risks. Deepfakes refer to the use of artificial intelligence algorithms to manipulate or generate synthetic audio, video, or text that appears genuine but is fabricated (Kietzmann, Lee, McCarthy, & Kietzmann, 2020). In the context of financial audits, deepfakes could be used to manipulate financial records, create false evidence, leading to inaccurate results and potential financial fraud. One of the risks associated with AI deepfakes in financial audits is the potential for manipulated financial statements or supporting documentation. Deepfake technology can be used to alter or fabricate financial records, such as invoices, receipts, or transaction logs. These manipulated documents can be difficult to detect, as they may appear legitimate and consistent with other records. Auditors relying on such falsified information may unknowingly provide an inaccurate assessment of an organization's financial health or transactions.

2.5. Auditing AI systems:

Given AI´s trajectory, it is imperative that financial auditors prepare themselves to continue providing assurance to society by issuing reliable and trustworthy financial reports that audit AI systems. Auditing AI presents unique challenges that require auditors to possess a deep understanding of AI design and architecture. To ensure a successful audit, auditors should become knowledgeable about the various

technologies, processes, and controls associated with AI. This includes having expertise in data warehousing, machine learning, cloud computing, and software testing (ISACA, 2018). Furthermore, the involvement of all stakeholders is crucial in auditing AI. Auditors must collaborate with internal engineering and security teams, as well as business leaders responsible for the AI strategy (Center for Internet Security, 2020). The use of cloud computing in AI deployments also introduces the need to address risks associated with third-party control over infrastructure (Deloitte, 2023). Given the relative novelty and limited deployment of AI, auditors should anticipate and address concerns, breaking down complex designs and issues into terms that stakeholders can comprehend. Flexibility in adapting existing frameworks and regulations, such as COBIT 2019 and relevant legal charters like HIPAA and GDPR, is recommended until more specific AI standards are established (Deloitte, 2023). Transparency is a fundamental principle for AI auditors. The iterative nature of AI development and the tuning of algorithms necessitate ongoing vigilance and documentation throughout the AI life cycle. Auditors should focus on promoting transparency, continuous improvement, and explicit documentation to ensure the effectiveness and reliability of the auditing process. Organizations must adopt a combination of risk-specific controls to effectively manage AI-related risks. The recommended approach entails establishing protocols to ensure the presence and adherence to these controls throughout the AI development process. Even organizations without a centralized risk organization can apply these AI risk-management techniques by implementing robust risk-governance processes, as demonstrated by the examples where institutions leveraged their existing risk infrastructure to implement these protocols and enterprise-wide controls (ICO, 2020).

2.6. Comprehensive Risk Assessment for Financial Auditing

2.6.1. Evaluating if a risk is relevant for financial auditing

A risk is considered relevant for financial auditing if it has the potential to impact any financial assertions, namely the accuracy and valuation, existence, completeness, rights and obligations, and presentation and disclosure of financial statements or the overall financial reporting process (IAASB, 2019) (Hayes, Dassen, Schilder, & Wallage, 2019). Financial auditing aims to provide assurance that financial statements are presented fairly and accurately, and that they comply with relevant accounting standards and regulatory requirements. Therefore, risks that can affect the reliability or validity of financial information are considered relevant for financial auditing (Chang, Tsai, Shih, & Hwang, 2008) (Arens, Elder, Beasley, & Hogan, 2017). Including financial fraud, errors in financial reporting, inadequate internal controls, and non-compliance with regulatory requirements. With the increasing use of AI in financial auditing, additional risks related to the use of AI, such as data bias, model drift, and cybersecurity threats, have also become relevant for financial auditing (Allen,

Hermanson, Kozloski, & Ramsay, 2006) (Arens, Elder, Beasley, & Hogan, 2017) (Messier Jr., Glover, & Prawitt, 2017). Ultimately, the determination of whether a risk is relevant for financial auditing depends on the auditor's professional judgment, as well as the specific circumstances and context of the audit engagement. Auditors are expected to exercise professional skepticism and assess the materiality and significance of risks in the context of the financial reporting process and the specific audit objectives (Tarantino, 2015) (Chang, Tsai, Shih, & Hwang, 2008) (Messier Jr., Glover, & Prawitt, 2017).

2.6.2. Exploring the Factors that Determine the Magnitude of Risk

The magnitude of a risk in financial auditing is determined by several factors, including the financial impact and potential consequences of the risk. Magnitude refers to the overall size or scale of a risk and its potential effect on the entity being audited (IAASB, 2019) (Messier Jr., Glover, & Prawitt, 2017). The financial impact of a risk is a key factor in determining its magnitude. This includes the potential financial loss or gain resulting from the risk. For example, a risk related to a significant decline in market demand for an entity's product or service could have a large financial impact, making it a high-magnitude risk (Radu, 2009) (Arens, Elder, Beasley, & Hogan, 2017). The potential consequences of a risk are also an important factor in determining its magnitude. This includes the reputational harm, legal consequences, and other non-financial impacts resulting from the risk. For example, a risk related to a data breach that could result in harm to customers or stakeholders could have a significant impact on an entity's reputation, making it a high-magnitude risk (Arens, Elder, Beasley, & Hogan, 2017) (Tarantino, 2015) (Johnstone, Gramling, & Rittenberg, 2017). Meaning, the magnitude of a risk in financial auditing is determined by several factors, including its financial impact and potential consequences. Auditors must consider all of these factors to assess the overall size and scale of a risk and prioritize their efforts in addressing the most significant risks first.

2.6.3. Exploring the Factors that Determine the Likelihood of Risk

The likelihood of a risk is determined by the probability of the risk event occurring. Several factors can influence the likelihood of a risk event, including the complexity of the process or system, the quality of controls, the reliability of data and information, the frequency of similar events, and external factors such as changes in the operating environment, market conditions, and regulatory requirements (Tarantino, 2015) (Arens, Elder, Beasley, & Hogan, 2017). Auditors can assess the likelihood of a risk event by using various techniques, such as statistical analysis, historical data, expert judgment, and scenario analysis. The nature of the risk itself can also influence its likelihood of occurrence. For example, risks associated with complex financial instruments are generally considered to be higher than risks associated with basic financial transactions (Radu, 2009) (International Auditing and

Assurance Standards Board [IAASB], 2018) (Johnstone, Gramling, & Rittenberg, 2017). The quality and effectiveness of controls in place can significantly impact the likelihood of a risk event occurring. If controls are of high quality, the likelihood of a risk event will be lower. Moreover, the reliability and accuracy of data and information used in financial reporting and auditing can also impact the likelihood of a risk event. If data or information is inaccurate or incomplete, it can increase the likelihood of a risk event occurring (Arens, Elder, Beasley, & Hogan, 2017) (IAASB, 2019) (Hayes, Dassen, Schilder, & Wallage, 2019). External factors, such as changes in market conditions, regulatory changes, and the organization's operating environment, can also affect the likelihood of a risk event occurring. Therefore, auditors must consider these factors when assessing the likelihood of a risk event occurring and use their professional judgment to evaluate the probability of the risk event (Messier Jr., Glover, & Prawitt, 2017).

2.6.4. Exploring the Potential Consequences of Relevant Risks for Financial Auditing

The possible consequences of a risk relevant to financial auditing can vary depending on the specific risk event and its impact on the organization's financial statements. Some factors that can determine the possible consequences of a risk in the context of financial auditing include (Arens, Elder, Beasley, & Hogan, 2017) (International Auditing and Assurance Standards Board [IAASB], 2018):

Materiality: The materiality of a risk event can impact its consequences. Material risks have the potential to impact the financial statements significantly and can have severe consequences, such as restatements, loss of investor confidence, and legal action(IAASB, 2019) (Messier Jr., Glover, & Prawitt, 2017).

Accuracy of financial statements: Risks that can impact the accuracy of financial statements can have significant consequences, such as misstatements, errors, or omissions, and can result in reputational damage, legal action, or financial losses (Tarantino, 2015) (Davis, Schiller, & Wheeler, 2016).

Regulatory compliance: Risks that can result in non-compliance with legal or regulatory requirements, such as accounting standards or tax regulations, can have significant consequences, such as penalties, fines, legal action, or reputational damage (IAASB, 2019) (Hayes, Dassen, Schilder, & Wallage, 2019).

Fraud: Risks related to fraud can have significant consequences, such as financial losses, reputational damage, legal action, and loss of investor confidence (Johnstone, Gramling, & Rittenberg, 2017).

Internal controls: Risks related to internal controls can impact the accuracy and reliability of financial reporting, resulting in misstatements, errors, or omissions. These risks can have significant consequences, such as loss of investor confidence, reputational damage, and legal action (IAASB, 2019) (Tarantino, 2015).

In the context of financial auditing, auditors must consider the potential consequences of identified risks and evaluate the impact on the organization's financial statements. This assessment is critical for determining the materiality of risks and developing appropriate audit responses and controls to manage and mitigate risks (Allen, Hermanson, Kozloski, & Ramsay, 2006) (Messier Jr., Glover, & Prawitt, 2017).

2.6.5. Effective Tactics for Mitigating Risks in Financial Auditing

IT auditors employ a range of tactics to manage and reduce risks in IT auditing. They begin by developing a deep understanding of the organization's IT environment, encompassing hardware, software, networks, and databases. This comprehensive knowledge allows them to identify potential risks and prioritize their audit approach, focusing on high-risk areas (Arens, Elder, Beasley, & Hogan, 2017) (IAASB, 2019) (Davis, Schiller, & Wheeler, 2016). IT auditors then evaluate the effectiveness of IT controls, such as access controls, change management, backup and recovery, and system monitoring. Their aim is to identify weaknesses in these controls and provide recommendations for improvement to mitigate risks (Allen, Hermanson, Kozloski, & Ramsay, 2006). Technical testing is another crucial tactic employed by IT auditors. This involves gathering evidence to support the effectiveness of IT controls and identifying vulnerabilities or weaknesses that may pose risks to the organization (Messier Jr., Glover, & Prawitt, 2017) (Senft & Gallegos, 2016). Data analytics plays a significant role as well, enabling IT auditors to analyse large datasets and identify patterns or anomalies that may indicate the presence of risks. This tactic helps pinpoint areas that require further investigation(IAASB, 2019) (Arens, Elder, Beasley, & Hogan, 2017). In addition, IT auditors may perform penetration testing to identify weaknesses in the organization's systems and networks. By doing so, they can identify vulnerabilities that could potentially be exploited by cyber attackers (International Auditing and Assurance Standards Board [IAASB], 2018) (Davis, Schiller, & Wheeler, 2016). Finally, IT auditors document their audit evidence, providing a clear and complete record of the work performed. This documentation supports their conclusions and recommendations (Allen, Hermanson, Kozloski, & Ramsay, 2006) (Senft & Gallegos, 2016). By employing these tactics, IT auditors effectively manage and mitigate the risks associated with IT auditing, ensuring that the organization's IT environment is secure, reliable, and aligned with the organization's objectives.

2.6.6. Examining the Role of IT Auditors in Financial Audit Projects for Maximum Assurance

Financial audit projects play a critical role in ensuring the accuracy and reliability of financial information within organizations (Allen, Hermanson, Kozloski, & Ramsay, 2006). As technology

continues to advance and businesses increasingly rely on information systems, the role of IT auditors becomes paramount in effectively assessing and mitigating risks associated with IT controls.

2.6.6.1. The Evolving Landscape of Financial Audit and IT Dependencies

The landscape of financial audit projects has experienced significant transformations due to the increasing integration of technology and the growing reliance on information systems. Traditional financial audit approaches that primarily focused on manual processes and paper-based records may not adequately address the complexities and risks associated with IT controls. As a result, the role of IT auditors has become increasingly crucial in ensuring the effectiveness and integrity of financial audits (Allen, Hermanson, Kozloski, & Ramsay, 2006). The evolution of financial audit projects has been driven by the increasing reliance on technology. As organizations adopt more advanced financial software and digital systems, the need for IT auditors has grown to address the associated risks and vulnerabilities [61]. Financial auditors alone may not possess the required skills and knowledge to effectively navigate, access, and test the controls within complex IT systems. The intricate nature of IT infrastructures, including network configurations, database management systems, and application interfaces, demands specialized expertise. It is within this context that IT auditors play a pivotal role in ensuring maximum assurance in financial audit projects (Davis, Schiller, & Wheeler, 2016) (Otero, 2018). Additionally, the rise of emerging technologies, such as artificial intelligence (AI), robotic process automation (RPA), and blockchain, has introduced new complexities and risks to financial audit projects (Raewf & Jasim, 2020). These technologies have the potential to revolutionize financial processes, but they also bring unique challenges related to data integrity, algorithmic biases, and the security of decentralized systems. IT auditors are well-equipped to navigate these complexities and provide assurance regarding the effectiveness and reliability of controls associated with these technologies.

2.6.6.2. Understanding the Role of IT Auditors

The role of IT auditors in financial audit projects is critical due to their specialized skills and knowledge. While financial auditors focus primarily on financial recordkeeping, IT auditors possess the expertise to navigate, access, and test controls within complex IT systems. Their specific responsibilities include evaluating IT processes, systems, and security measures to ensure the integrity of financial information (IAASB, 2019) (Davis, Schiller, & Wheeler, 2016). IT auditors play a vital role in assessing IT risks and controls, identifying vulnerabilities, and recommending improvements. Their understanding of IT systems and controls allows them to provide valuable insights and recommendations to enhance the effectiveness of controls and mitigate risks. By leveraging their expertise, IT auditors contribute to the

overall assurance process, ensuring that financial audits adequately address the complexities and risks associated with IT dependencies (IAASB, 2019) (Davis, Schiller, & Wheeler, 2016). The value of IT auditors lies in their ability to bridge the gap between financial audit teams and IT systems. They bring a deep understanding of technology-related risks and control frameworks, enabling them to provide maximum assurance regarding the effectiveness of controls in mitigating the risk to the integrity of financial records. Their involvement enhances the overall quality and reliability of financial audits by ensuring comprehensive assessments of IT systems and controls (Hayes, Dassen, Schilder, & Wallage, 2019). Research has demonstrated a significant correlation between the inclusion of IT auditors in financial audits and the successful detection of financial misstatements. Their knowledge of IT-related risks and their ability to select and implement appropriate digital controls contribute to mitigating the risk of manipulation or abuse of financial information. According to Otero (2015), the skills possessed by financial auditors alone are insufficient to effectively navigate, access, and test the controls required for complex IT systems that support finance and accounting functions. In contrast, skilled and qualified IT auditors are specifically trained to perform these tasks (Davis, Schiller, & Wheeler, 2016). Despite their crucial role, IT auditors are not extensively involved in financial auditing for several reasons. One of the primary factors hindering the greater involvement of IT auditors is cost restrictions. Employing IT auditors can be perceived as an additional expense, and organizations may prioritize allocating resources elsewhere. Moreover, the availability of skilled IT auditors may be limited, making it challenging to fulfil the demand for their expertise. Additionally, some financial auditors may lack the necessary IT skills and awareness of the importance of IT auditors in financial auditing, leading to a perception that their involvement is unnecessary. However, Otero (2015) highlights the significance of skilled IT auditors in testing IT processes related to financial information. This is crucial as the manipulation or abuse of financial information can have severe consequences. Research has shown a significant correlation between the inclusion of IT auditors in financial audits and the successful detection of financial information manipulation. IT auditors possess the education and expertise to identify IT-related risks within financial systems, especially in areas sensitive to fraud or employee misconduct (International Auditing and Assurance Standards Board [IAASB], 2018). They can then select and implement appropriate digital controls tailored to the organization's needs, effectively mitigating the risk of information manipulation or abuse. Furthermore, IT auditors play a crucial role in ensuring the validity, accuracy, and completeness of transactions and reports within financial systems, thereby reducing the likelihood of financial misstatements. Their procedures and assessments on financial systems contribute to the overall integrity of financial records (Borges, Laurindo, Spínola, Gonçalves, & Mattos, 2021) (Davis, Schiller, & Wheeler, 2016). Overcoming challenges and embracing the role of IT auditors will strengthen the effectiveness of financial audits, leading to more reliable and trustworthy financial information within organizations.

CHAPTER 3 - METHODOLOGY

The methodology chapter outlines the research approach chosen for this study, which a involves mixed-method approach. It describes the data collection methods employed, such as interviews. Additionally, it discusses the criteria for selecting participants and provides an overview of the data analysis techniques used, such as thematic analysis and descriptive statistics.

This study adopts a mixed-method research design, combining qualitative and quantitative approaches. The qualitative component involves conducting individual interviews with experts. The quantitative component entails the ranking of AI risks in terms of likelihood and magnitude. By following this mixed-method research design, the study aims to gather rich qualitative insights from the interviews while also obtaining quantitative data through the ranking exercise. This comprehensive approach will enable a deeper understanding of the emerging AI risks in financial auditing, their impacts, and potential mitigation strategies, thus contributing to the field of risk assurance and IT auditing in the context of financial auditing projects. This study utilize interviews as the primary data collection method. The interviews involve a combination of open-ended and closed-ended questions. The interviews were conducted with experts in the area of Risk Assurance, specifically those with a strong background in IT auditing and financial auditing. The intention was to gather valuable insights and perspectives from individuals well-versed in the subject matter. The target population for this study consisted of managers and senior managers in the Risk Assurance department of a Big 4 company. These professionals were selected based on their expertise and experience in IT auditing and in Risk analysis and mitigation. The choice to include individuals from this specific department was to ensure the relevance and applicability of the findings to the financial auditing context. The participants in this study were nine managers from the Risk Assurance department of the selected Big 4 company. These managers were responsible for digital assurance, focusing on IT auditing, and were actively engaged in global financial assurance projects. To be included in the study, participants were required to have a minimum of five years of experience in IT auditing and Risk Assurance. This criterion was established to ensure a sufficient level of expertise among the participants. Data were collected through individual interviews conducted with each expert. The interviews followed a semi-structured approach, allowing for flexibility while ensuring consistency across interviews. The interview protocol consisted of a set of predetermined questions, including open-ended inquiries, to explore the experts' perspectives on the relevant AI risks in financial auditing, their impacts, and potential mitigation strategies. The interview process consisted of several sections, each focusing on different aspects of AI risks in financial auditing. First, there was an introduction where the purpose of the study was explained to the participants, emphasizing the importance of their insights and expertise in addressing

the research objectives. The confidentiality of their responses and the voluntary nature of participation were reiterated. Next, the interviewer presented a list of AI risks that were identified during the literature review. Each risk was accompanied by a brief explanation and examples to ensure a common understanding among the participants. The participants were then asked to identify which risks from the presented list they considered relevant to a financial audit. For each identified risk, the participants were asked several questions. First, they were asked to describe the possible consequences or impacts on the integrity of the financial records of an entity if the identified risk is ignored or not adequately addressed. This aimed to capture the potential implications of each risk in the context of financial auditing. Participants were also requested to rate the (expected) severity or magnitude of the identified risk on a scale of 0 to 100. This allowed for the quantitative assessment of the perceived severity of each risk, providing insights into the level of concern associated with them. Additionally, they were asked to rate the (expected) frequency or likelihood of the identified risk on a scale of 0 to 100, indicating how frequently the risk is anticipated to occur in the context of financial auditing. In the next section, participants were invited to suggest possible ways or tactics to mitigate the identified risk. This allowed for the exploration of potential risk mitigation techniques or approaches specific to each risk, drawing on the participants' expertise in risk assurance and financial auditing. Participants were also asked to assess whether the controls necessary to mitigate each risk can be successfully identified and tested by the financial audit team alone or if special IT expertise, such as IT auditors, is required to provide maximum assurance. This aimed to understand the extent to which specialized knowledge and skills are needed to address the identified risks effectively. After discussing each identified risk, participants were given an opportunity to provide feedback on the overall set of risks and offer any additional AI risks they deemed relevant to financial audits but were not included in the provided list. This allowed for further exploration and identification of potential risks that emerged from the participants' own experiences and perspectives. The interviews were conducted either in-person or via video conferencing, based on the participants' preferences and availability. Prior to each interview, a comprehensive briefing was provided to the experts. This briefing outlined the objectives and purpose of the investigation, and a summary and explanation of the AI risks identified during the literature review were provided. This ensured that the participants had a clear understanding of the study's focus and what was expected from them during the interview. For the qualitative component of the data, thematic analysis was employed to identify key themes and patterns within the experts' responses. This involved coding the interview transcripts, identifying recurring themes, and interpreting the data to gain insights into the emerging risks, impacts, and mitigation strategies. Quantitative data analysis was performed to analyse the ranking of AI risks in terms of likelihood and magnitude. Descriptive statistics were used to summarize the rankings and identify trends. To ensure the accuracy and reliability of the collected data, a pilot test was conducted using the first interview.

Feedback was obtained from the expert who participated in the pilot interview, and necessary refinements were made to the interview process based on this feedback. This iterative process was performed to enhance the quality and validity of the subsequent interviews. Ethical approval for this study was obtained from the Partner of the risk assurance department and the HR department of the company. This approval ensured that the research was conducted in compliance with ethical guidelines and regulations. Informed consent. The participants chosen for the interviews were carefully selected based on their extensive expertise and direct involvement in financial auditing projects. Three of the participants held senior managerial positions, while the remaining six participants were managers within the Risk Assurance and Digital Assurance Departments. Each participant brought extensive experience to the interviews, with all of them having more than 5 years of experience in the respective field. This rich professional background ensured a deep understanding of the subject matter and allowed for valuable insights into the research topic. One of the limitations of this study is the relatively small number of interviews conducted, which consists of only nine risk assurance experts. However, it is important to provide an explanation for this limited sample size. In this case, the reason for including only nine interviews is due to the unavailability of additional managers in the department who possess the necessary expertise in both IT risks and financial audit. Given the specific focus of this study on AI risks in the context of financial audit, it was crucial to include participants who had substantial experience and knowledge in this intersection. Including individuals with less experience, such as associates or senior associates, could potentially compromise the quality and depth of the answers obtained during the interviews. Therefore, to maintain the integrity of the research and ensure high-quality responses, it was decided to restrict the interviews to managers and senior managers. It is important to acknowledge that the limited number of interviews may impact the generalizability of the findings. With a larger sample size, more diverse perspectives and insights could have been captured, potentially enhancing the richness of the data. However, the priority was to maintain the quality and expertise of the participants to ensure valuable and reliable information regarding the emerging risks, impacts, and mitigation strategies of AI in financial audit. While the small number of interviews is a limitation, the thorough selection process and the commitment to maintaining high-quality responses from experienced professionals contributed to mitigating potential drawbacks. It is important to acknowledge this limitation in the thesis and interpret the findings with caution, considering the specific context and sample size of the study.

CHAPTER 4- DISCUSSION AND RESULTS

The discussion and results chapter of this dissertation delves into the findings of the research study, providing a comprehensive analysis of the identified AI risks and their implications for financial auditing practices. The chapter addresses the research questions by exploring the pertinence and relevance of

AI auditing in the present and future, unveiling the relevant risks to a financial audit, and quantitatively assessing the magnitude and likelihood of these AI risks in financial auditing. To begin, the chapter emphasizes the importance of AI auditing in the present and future landscape of financial auditing. It highlights the need to adapt auditing practices to the advancements in AI technology to ensure the integrity of financial records and maintain investor trust. This discussion emphasizes the pertinence of integrating AI auditing strategies within financial auditing projects. Next, the chapter examines the identified AI risks, providing an in-depth analysis of their impacts on financial integrity and investor trust. Through the findings of the research study, the chapter uncovers the potential consequences of these risks, highlighting the vulnerabilities they pose to the accuracy and reliability of financial records. By exploring various case studies and real-world examples, the chapter illustrates the practical implications of these risks for financial auditing practices. Moreover, the chapter delves into the mitigation strategies that can be employed to address these AI risks. It discusses the tactics and measures that can be implemented to ensure the integrity of financial records and mitigate the identified risks effectively. By drawing upon established best practices and industry guidelines, the chapter provides insights into how auditors can navigate the complexities of AI technology to maintain the quality and trustworthiness of financial audits. Additionally, the chapter highlights the critical need for IT experts in auditing and analysing AI controls. It emphasizes the expertise required to assess and evaluate the AI systems used in financial auditing projects, ensuring their compliance with regulatory standards and industry practices. The discussion sheds light on the role of IT experts in providing technical guidance, conducting comprehensive risk assessments, and implementing appropriate control mechanisms to mitigate AI-related risks effectively. Lastly, the chapter expands the risk horizon by uncovering additional threats in the ethical realm of AI. It explores the ethical considerations and dilemmas associated with the use of AI in financial auditing, addressing concerns related to bias, privacy, and transparency. By examining the ethical dimensions of AI risks, the chapter contributes to a broader understanding of the potential challenges faced by auditors in the evolving landscape of AI-driven financial auditing.

4.1. Pertinence and Relevance of AI auditing in the Present and Future

In this section, the focus is on the experts' opinions and insights regarding the relevance of AI auditing in the present context and whether companies are utilizing this technology for accounting and finance purposes. The objective is to examine the perceptions and experiences of the interviewed experts, who possess extensive knowledge and practical expertise in the field of financial auditing and IT auditing. By exploring their views, this study aims to gain valuable insights into the significance of AI auditing in the contemporary landscape of financial audits. Through a series of open-ended questions, the participants were encouraged to provide their opinions, perspectives, and experiences regarding

the relevance and implementation of AI auditing in practice. In this section, the experts' responses have been carefully examined, categorized, and synthesized to identify recurring themes, patterns, and divergent viewpoints. The findings presented here will shed light on the opinions of industry experts and provide valuable insights for auditors, accounting professionals, and policymakers who seek to better understand the potential benefits, challenges, and implications of AI auditing in the financial domain. Moreover, this discussion will also examine whether companies are currently utilizing AI technology for accounting and finance purposes. Based on the answers provided by the experts, it can be concluded that AI auditing is a topic that is gaining relevance in the present time. While the use of AI technology auditing is not yet widespread, there is a growing recognition of its potential and importance in ensuring the integrity and reliability of AI systems within companies. The experts mentioned that not many companies are currently utilizing AI technology specifically for purposes that would affect financial auditing. This indicates that there is still a relatively limited adoption of AI auditing practices. However, the fact that the topic is becoming more relevant suggests a growing awareness of the need to address the unique challenges and risks associated with auditing AI systems. As AI technology continues to advance and become more integrated into various business processes, it is likely that the demand for AI auditing will increase. The need for comprehensive assessments and evaluations of AI systems to ensure their compliance, effectiveness, and ethical standards will become more prominent. It is important for companies to recognize the significance of AI auditing and proactively consider its implementation as part of their risk management and assurance strategies. By conducting regular audits of AI systems, organizations can identify potential weaknesses, biases, or vulnerabilities, and take corrective actions to mitigate risks and enhance the reliability of their AI-driven processes. In short, while AI auditing is still not widely practiced, its relevance is growing as companies recognize the need to address the unique challenges posed by AI systems. The adoption of AI auditing can help ensure the integrity, accountability, and ethical use of AI technology within organizations, paving the way for more trustworthy and reliable AI-driven processes in the future. The findings of my study align with the points highlighted in the literature review regarding the nascent stage of AI adoption in companies. As mentioned by Luo, Meng, and Cai (2018), the application of artificial intelligence in the accounting industry is still in its infancy, and the current technologies being used do not fully represent the potential of AI. This notion is supported by the responses of the experts in my study, who mentioned that the use of AI technology is not yet widespread and there is still limited adoption of AI auditing practices within companies. However, both the literature review and my study indicate a growing recognition of the importance and potential of AI in the business environment. Despite the current limited adoption, there is a notable increase in awareness and relevance of AI auditing, as companies start to acknowledge the need to address the unique challenges and risks associated with AI systems. This aligns with the argument made in the

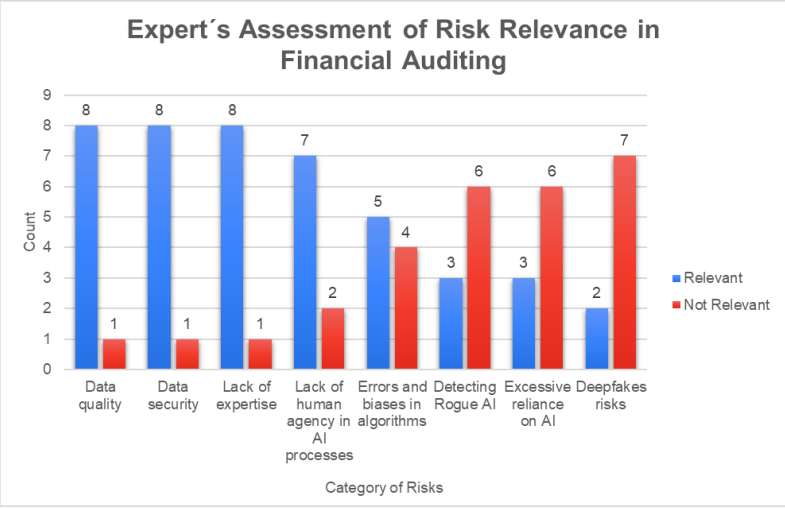
literature review that the development of AI in accounting still requires significant work before effective deployment can take place. Furthermore, the literature review mentions a statistic from (McKinsey,2019) indicating that nearly 80 percent of executives at companies deploying AI have noticed moderate value from it. This finding supports the notion that while AI adoption may still be in its early stages, there are already tangible benefits being observed in organizations. The results of my study reinforce the significance of AI auditing as a means to ensure the integrity, accountability, and ethical use of AI technology within companies. By conducting regular audits of AI systems, organizations can identify potential weaknesses, biases, or vulnerabilities and take corrective actions to mitigate risks and enhance the reliability of their AI-driven processes. This echoes the need emphasized in the literature review for comprehensive assessments and evaluations of AI systems to fully unlock their potential and address the challenges associated with their implementation. In conclusion, both the literature review and my study highlight the nascent stage of AI adoption in companies and the growing relevance of AI auditing. While the use of AI technology in accounting and financial auditing is still limited, there is a recognition of its potential and the need to address the unique challenges posed by AI systems. By proactively considering the implementation of AI auditing, organizations can pave the way for more trustworthy and reliable AI-driven processes in the future, aligning with the transformative potential of AI mentioned in the literature review.

4.2. Unveiling the Relevant Risks to a Financial Audit

The objective of this section of the study is to unveil the relevant risks that could potentially impact the accuracy and integrity of financial records, as assessed by the panel of experts. This study directly answers the first research question by identifying the AI risks that are relevant in the context of a financial auditing project. Through expert assessments, we unveil the specific risks that could impact the accuracy and integrity of financial records. To achieve this, the experts were presented with a list of AI risks and asked to determine their relevance to financial audits. By examining the experts' responses, this section aims to identify and evaluate the specific AI risks that have implications for financial audits. This analysis and discussion aim to contribute to the existing body of knowledge by providing a comprehensive understanding of the AI risks that could affect the financial audit process. The integration of AI in various industries has raised concerns about its potential risks and impacts on different aspects of operations. In the context of financial auditing, it is crucial to identify and assess the AI risks that could affect the accuracy and integrity of financial records. The results provide valuable insights into the risks that are considered significant to financial audit by these experts. The following segment presents the expert´s responses concerning the relevance of each specific AI risk in financial auditing. The experts were provided with a question regarding the relevance of a specific AI risk to financial audit. They were asked to indicate whether they considered the risk to be relevant or not.

Along with their responses, any additional comments provided by the experts were also recorded. The results of their assessments are presented in a graph format, while a detailed analysis of the answers, including any supplementary remarks, is presented below the accompanying table. This study contributes to the current literature by addressing the gap in knowledge regarding the relevance of AI risks to a financial audit. While previous research has identified AI risks that could potentially impact accounting and finance, there is a lack of understanding regarding which of these risks are specifically relevant to the financial audit process. The analysis and discussion of the expert responses in this study contribute to the existing body of knowledge by providing a comprehensive understanding of the AI risks that could affect the accuracy and integrity of financial records in the context of financial audits. This research helps bridge the gap between the broader AI risks identified in accounting and finance literature and the specific risks relevant to financial audits. The presentation of the expert responses in a graph format and the detailed analysis of their assessments provide a clear and systematic overview of the relevance of each specific AI risk in financial auditing. This information not only adds to the academic literature but also has practical implications for professionals in the field of risk assurance and financial auditing. By shedding light on the relevant AI risks to financial audits, this research contributes to the ongoing discussion on the impact of AI on financial systems and reinforces the importance of considering these risks in the audit process.

Figure 4.1. Expert´s Assessment of Risk Relevance in Financial Auditing



Data Quality: The majority of experts (8 out of 9) identified data quality as a relevant risk to financial auditing. AI systems heavily rely on high-quality data to produce accurate results. Inaccurate or incomplete data can lead to erroneous financial records and potentially misguide audit processes. Therefore, ensuring the quality and reliability of data used in AI systems is crucial for maintaining the integrity of financial auditing.

Data Security: Similarly, 8 of the 9 experts recognized data security as a relevant risk to financial auditing. The protection of sensitive financial information is paramount to maintain the confidentiality, integrity, and availability of financial records. The integration of AI may introduce new vulnerabilities and potential avenues for data breaches. It highlights the importance of robust data security measures to safeguard financial data from unauthorized access or manipulation.

Lack of Expertise: The majority of experts (8 out of 9) also acknowledged the risk of a lack of expertise in the context of financial auditing and AI. The implementation and management of AI systems require specialized skills and knowledge. Insufficient expertise can lead to inadequate implementation, configuration, or interpretation of AI results, potentially impacting the accuracy and reliability of financial audits. Ensuring that auditors possess the necessary expertise in AI technologies is vital to mitigate this risk.

Lack of Human Agency in AI Processes: A significant percentage of experts (7 out of 9) identified the lack of human agency in AI processes as a relevant risk to financial auditing. The increasing reliance on AI systems may reduce human involvement and oversight in decision-making processes. This lack of human agency can raise concerns about accountability and transparency, particularly when auditing financial records. It emphasizes the need to strike a balance between AI-driven automation and human judgment in financial auditing to ensure adequate control and accountability.

Errors and Biases in Algorithms: 5 of the 9 experts recognized the risk of errors and biases in algorithms as relevant to financial auditing. AI algorithms are designed and trained based on historical data, and if the data contains biases or errors, the algorithms may perpetuate them. This could lead to biased or incorrect outcomes, potentially affecting the accuracy and fairness of financial audits. Ensuring algorithmic transparency and regular auditing of AI systems can help identify and mitigate such risks.

Detecting Rogue AI: A lower percentage of experts (3 out of 9) identified the risk of detecting rogue AI as relevant to financial auditing. Rogue AI refers to instances where AI systems behave unexpectedly or maliciously, potentially compromising the integrity of financial records. Detecting and preventing such instances requires robust monitoring, anomaly detection, and auditing mechanisms to ensure the reliability and trustworthiness of AI systems in financial auditing.

Excessive Reliance on AI: A similar percentage of experts (3 out of 9) recognized the risk of excessive reliance on AI in financial auditing. While AI technologies offer numerous benefits, overreliance on AI without appropriate human oversight may lead to complacency and a lack of critical thinking. Financial audits require human judgment and expertise, and the excessive dependence on AI systems may overlook important nuances or contextual factors. Maintaining a balanced approach between AI automation and human involvement is crucial to mitigate this risk.

Deepfakes Risks: A minority of experts (2 out of 9) identified deepfakes risks as relevant to financial auditing. Deepfakes are manipulated or synthetic media, including audio, images, or videos, that can

deceive or mislead individuals. In the context of financial auditing, deepfakes could potentially be used to manipulate evidence or create false financial records, compromising the integrity of the auditing process.

These findings highlight the importance of addressing data-related risks, ensuring human oversight, and maintaining a balance between AI automation and human judgment in financial auditing processes. In conclusion, the study revealed several important AI risks relevant to financial auditing. The most prominent risks identified by the experts included data quality, data security, lack of expertise, lack of human agency in AI processes, and errors and biases in algorithms. These risks highlight the critical need for ensuring the quality and reliability of data, protecting sensitive financial information, fostering expertise in AI technologies, maintaining human oversight and accountability, and addressing algorithmic errors and biases in financial auditing processes.

On the other hand, the risks identified as least relevant in the context of financial auditing were detecting rogue AI, excessive reliance on AI, and deepfakes risks. While these risks may still pose potential threats, they were considered less significant by the experts participating in this study. Nonetheless, it is essential to remain vigilant and continue exploring ways to detect and mitigate the impact of rogue AI, strike a balanced approach to AI utilization, and address the emerging challenges associated with deepfakes. This raises the question: Why are some risks not deemed relevant for financial auditing despite their possible impact on financials? In financial auditing, the identification and assessment of risks are critical for determining the nature, timing, and extent of audit procedures. While it is generally important to consider all risks that may impact the financial statements, there are instances where certain risks may not be considered relevant for financial auditing due to various factors. One factor that can influence the relevance of a risk is materiality. Financial auditors establish materiality thresholds based on professional judgment, which define the level at which a misstatement would be considered significant. Risks that are deemed immaterial, meaning their potential impact on the financial statements is insignificant, may not be considered relevant for auditing purposes. Another factor is the specific objectives of a financial audit. The primary focus of a financial audit is to assess the fairness of the financial statements and detect material misstatements. Risks that do not directly impact these objectives, such as operational or strategic risks, may be considered less relevant as they fall outside the immediate scope of a financial audit. Risk tolerance is also a consideration. Every organization has its own risk appetite and tolerance levels. Risks that fall within an acceptable risk tolerance may not be considered relevant for financial auditing. The audit typically focuses on identifying risks that are outside the acceptable risk tolerance and have the potential to result in material misstatements. It is also important to consider the responsibility of management. Financial auditing operates under the assumption that management is responsible for the preparation and fair presentation of the financial statements. Risks that are the sole responsibility of management, such as

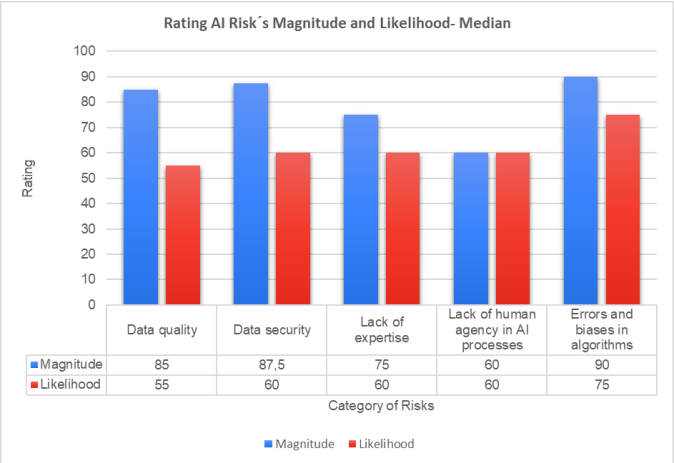
strategic decision-making or business risks, may not be considered relevant for the financial audit, as they fall outside the scope of the auditor's responsibilities. While certain risks may not be considered relevant for financial auditing, it's worth noting that they may still be monitored and assessed by other stakeholders within the organization, such as internal auditors or risk management teams. Additionally, these risks may still be important for decision-making and overall risk management within the organization, even if they are not directly addressed in the financial audit.

4.3. Quantitative Assessment of AI Risk´s Magnitude and Likelihood in Financial Auditing

This study aims to conduct a quantitative assessment of the magnitude and likelihood of AI risks in the context of financial auditing. This study directly answers the second research question by quantitatively assessing the frequency and severity of AI risks in financial auditing. By gathering numerical rankings from experts, we gain insights into how these risks manifest in terms of their occurrence and impact. Building upon the insights gained from the previous study that identified the relevant risks through the expert opinions, this research focuses on ranking these risks based on their perceived magnitude and likelihood. By obtaining numerical rankings from experts, we aim to provide a comprehensive understanding of the relative importance and potential impact of each risk. The assessment will employ a scoring system on a scale of 0-100 to evaluate both the magnitude and likelihood of the identified risks. The experts were asked to assign scores during the research interviews. Where a higher score indicates a higher magnitude or likelihood. Only the risks that were considered relevant by a majority of the experts in the previous study will be included. We only included risks considered relevant by a majority of experts to ensure a comprehensive and consensus-based assessment. This approach avoids individual biases and captures the collective wisdom of the expert group, resulting in more reliable and impactful findings. Upon collecting responses from the experts, the data will be analysed to determine the rankings of each risk in terms of magnitude and likelihood. The median will be calculated to identify the central tendency of the rankings. The findings from the quantitative assessment will provide valuable insights into the perceived significance of AI risks in financial auditing. By incorporating expert opinions and utilizing a numerical ranking scale, we can quantitatively compare and prioritize the risks. This approach enables us to identify the risks that are considered most severe or likely to occur, allowing auditors and organizations to allocate resources and implement appropriate risk mitigation strategies accordingly. The rankings obtained from this study can inform decision-making processes, policy development, and resource allocation efforts. It is recommended that organizations develop comprehensive risk management frameworks that encompass the identified risks, focusing on data quality, data security, expertise, human agency and algorithmic errors and biases. It is important to acknowledge certain limitations of this study. In the quantitative assessment of the research interviews conducted for this study, it is important to address

the limitations imposed by the relatively small number of interviews. With only nine experts participating in the study, it was deemed inappropriate to calculate certain statistical measures such as the mean and standard deviations. As a result, the analysis focused on calculating the counting and median values of the responses. The decision to exclude the mean and standard deviations was primarily driven by the limited sample size. These statistical measures are more reliable and meaningful when applied to larger datasets, allowing for a more accurate representation of the central tendency and dispersion of the data. With a small sample size, even one extreme response can skew the mean and produce unreliable results. In the case of this study, the small number of interviews would have resulted in a lack of statistical power and the potential for skewed or unreliable results. By focusing on the sums and median values, the analysis aimed to provide a basic understanding of the frequency and central tendency of the responses. It is essential to acknowledge that the decision to exclude the mean and standard deviations might have limited the depth of the statistical analysis. However, it was a necessary choice considering the small number of interviews conducted. By acknowledging this limitation and discussing the rationale behind the chosen statistical measures, the study maintains transparency and ensures the accuracy and reliability of the quantitative assessment given the available data. This study makes a significant contribution to the field of quantifying AI risks by providing valuable insights into the prevalence and importance of specific risks in the context of financial auditing. The quantification of AI risks is an essential aspect that has been relatively underexplored in existing literature, and this study addresses this gap by systematically examining and analysing the expert responses. By utilizing the median scores as a measure of central tendency, this study allows for a meaningful quantification of the perceived magnitude and likelihood of AI risks. This approach enables a comparative assessment of different risk categories, revealing which risks are considered more prevalent and important by the experts. By highlighting the risks with higher median scores, the findings help auditors and risk assurance professionals prioritize their focus and allocate resources effectively. This information can inform the development of risk management strategies and guide decision-making processes in identifying and addressing the most critical AI risks.

Figure 4.2. Rating AI Risk's Magnitude and Likelihood-Median results



Based on the average of the ratings provided by the 9 experts, the following conclusions can be drawn regarding the AI risks presented. The results obtained from the study are presented in terms of median scores for each risk category. The median represents the middle value when the scores are arranged in ascending order.

The risk category of "Data Quality" received a median magnitude score of 85, indicating that experts consider it to be a significant risk in financial auditing. This highlights the importance of ensuring the accuracy and integrity of data used in financial records. The median likelihood score of 55 suggests a moderate level of perceived risk, indicating that while data quality is significant, it may not be perceived as highly likely to occur. Experts ranked the risk of "Data Security" as substantial, with a median magnitude score of 87.5. This underscores the criticality of safeguarding financial data from unauthorized access, breaches, and malicious activities. The median likelihood score of 60 indicates a moderate level of perceived risk, highlighting the need for robust security measures to protect financial information. The risk category of "Lack of Expertise" received a median magnitude score of 75, indicating a moderate level of perceived risk. This suggests that experts recognize the importance of having the necessary knowledge and expertise to effectively address AI-related risks in financial auditing. The median likelihood score of 60 reflects a moderate level of perceived risk associated with the lack of expertise. The risk category of "Lack of Human Agency in AI Processes" received a median magnitude score of 60, indicating a relatively lower perceived magnitude of risk compared to other categories. This suggests that experts may consider the impact of reduced human control and oversight in AI processes to be less significant in the context of financial auditing. The median likelihood score of 60 reflects a moderate level of perceived risk. Experts ranked the risk of "Errors and Biases in Algorithms" as highly significant, with a median magnitude score of 90. This underscores the potential for errors and biases in AI algorithms to have a substantial impact on financial auditing. The median likelihood score of 75 indicates a relatively higher level of perceived risk, emphasizing the need for robust validation and auditing processes to mitigate algorithmic biases and errors.

The findings of this study highlight the varying levels of perceived likelihood and magnitude associated with different AI risks in financial auditing. It is important for auditors and risk assurance professionals to recognize the significance of data quality, data security, expertise, human agency, and algorithmic errors and biases in their audit processes. Overall, the results provide valuable insights into the relative importance and potential impact of different AI risks in the context of financial auditing. The findings of this study underscore the criticality of addressing data security, errors and biases in algorithms, and data quality as high-magnitude risks in the integration of AI in financial auditing. These risks warrant careful attention and proactive risk mitigation strategies. The risks associated with lack of expertise and lack of human agency in AI processes are considered moderately significant, highlighting the need for ongoing skill development and striking a balance between human judgment and AI automation in financial auditing. The level of agreement among the experts varied across the risk categories. Data security exhibited a higher level of consensus, suggesting a shared understanding of its importance. On the other hand, there was more diversity in expert opinions regarding lack of human agency in AI processes and errors and biases in algorithms. These variations emphasize the need for further discussions and research to gain a comprehensive understanding of these risks and develop consensus-based approaches to address them. In summary, the experts consider data security, errors and biases in algorithms, and data quality as the most substantial risks associated with AI, all with high magnitudes. Lack of expertise and lack of human agency in AI processes are seen as moderately significant risks. However, it is important to note that these conclusions are based on the opinions of the 9 experts and may not capture the full spectrum of AI risks or reflect a consensus within the field.

4.4. AI Risks Explored: Assessing Impacts and Mitigating Strategies

This segment presents the results of a comprehensive exploration of AI risks, drawing on the perspectives of the experts in the field. This study answers the second and third research questions by qualitatively analysing the potential consequences of AI risks in financial auditing. It explores how these risks manifest and identifies effective mitigation strategies. The research sought to identify and assess the potential impacts and challenges associated with the deployment of AI systems. The valuable insights obtained from these expert interviews contribute to a more nuanced understanding of the complex landscape of AI risks and serve as a basis for formulating effective strategies and mitigation measures. This study makes a significant contribution to the current literature by addressing a crucial gap in knowledge regarding the specific impacts of AI risks on financial records, particularly in the context of financial auditing. While existing literature recognizes the potential risks associated with AI in various industries, there is limited research that specifically focuses on the impacts of these risks on financial reports and their relevance to financial audits. The experts' responses provide valuable information about how these risks can affect the accuracy, integrity, and reliability of financial reports,

which are fundamental aspects of financial audits. This research goes beyond the general recognition of risks and delves into the nuanced implications that these risks can have on financial reports, which are critical for financial audits. Furthermore, the exploration of mitigation strategies in this study helps fill the gap in knowledge regarding how auditors can proactively respond to the emerging challenges associated with AI risks. By identifying and analysing these strategies, this research offers practical insights and recommendations that can be utilized by auditors and risk assurance professionals to effectively address and mitigate the identified risks in the context of financial audits.

4.4.1. Data Quality Risks

4.4.1.1. Data Quality Risks: Impacts on Financial Integrity and Investor Trust

Based on the answers provided by the audit experts, we can draw that the consequences or impacts of the risk can be as significant as the lack of quality of the data on which AI relies for its projections. If the risk is not addressed, the lack of quality data can significantly affect the accuracy of AI-generated projections. Decisions made based on inaccurate data can be amplified, resulting in possible incorrect financial records. It highlights the importance of monitoring and establishing action plans to mitigate such risks. The experts presented impacts at the following levels regarding the quality of the Data:

-Incomplete or inaccurate transaction records: Ignoring or neglecting the risk can result in incomplete or inaccurate transaction records. This can have a direct impact on the presentation and disclosure of financial statements, potentially leading to misleading or incorrect information.

-Data loss and incorrect information: Neglecting the risk can also result in data loss and the propagation of incorrect information throughout the financial records. This can further exacerbate the potential inaccuracies and misrepresentations within the financial statements.

-Impact on financial projections: If input data is incomplete, inaccurate, or unreliable, it can directly compromise the accuracy of financial projections. This, in turn, can have a cascading effect on the financial statements, potentially distorting the true financial position and performance of the entity.

Neglecting the risk can lead to audit opinions that do not align with the truth. If financial records are compromised, auditors may be unable to provide accurate assessments and opinions, which can undermine the credibility of the entity's financial statements. Experts also pointed to the possible consequence of loss of trust by investors and markets. When the integrity of financial data is compromised, it can result in a loss of trust by investors and markets. Investors rely on accurate financial information to make informed decisions, and if that trust is eroded, it can have detrimental effects on the entity's reputation and financial standing. In summary, if the risk to the integrity of financial records is ignored or not adequately addressed, the consequences can include misleading financial statements, inaccurate projections, misaligned audit opinions, loss of trust by investors, and

potential data loss. It is crucial for entities to recognize and mitigate these risks to ensure the integrity and reliability of their financial records.

The results of the study corroborate the findings from the literature review, emphasizing the significant challenges posed by data quality risks in AI systems (CMA Exam Academy, 2023; McKinsey Global Institute, 2018; EY, 2018; Cheatham, Javanmardian, & Samandari, 2019; ICAEW, 2018). Both the study and the literature review highlight the potential consequences of using flawed, biased, incomplete, or inaccurate data for AI training and inference. The experts' responses underscore that neglecting these risks can significantly impact the accuracy of AI-generated projections, potentially leading to incorrect financial records. This aligns with the literature's concern about biased data perpetuating existing biases in AI decision-making processes, as well as the risk of incomplete or insufficient data hindering accurate predictions (McKinsey Global Institute, 2018; EY, 2018; Cheatham, Javanmardian, & Samandari, 2019). The study adds valuable insights by focusing on the implications of data quality risks for the integrity of financial records. The experts' assessment reveals that neglecting these risks can result in incomplete or inaccurate transaction records, which directly affect the presentation and disclosure of financial statements, potentially leading to misleading information (McKinsey Global Institute, 2018). Furthermore, the study highlights the potential impact on financial projections if the input data is incomplete, inaccurate, or unreliable, compromising the accuracy of financial statements and distorting the entity's true financial position and performance (EY, 2018; Cheatham, Javanmardian, & Samandari, 2019). These findings contribute to the literature by shedding light on the specific consequences of data quality risks in the context of financial audits and the importance of addressing these risks to maintain the credibility of financial statements.

4.4.1.2. Mitigating Data Quality Risks: Tactics for Ensuring Integrity in Financial Records

The experts' responses highlighted the importance of analysing relevant systems. Conduct thorough analysis of the systems involved in financial record-keeping to identify potential vulnerabilities, weaknesses, or areas for improvement. This can include system assessments, risk assessments, and security audits. Starting by the implementation of various IT processes and controls to enhance the security and integrity of financial records. This can include the:

-Implementation of monitoring procedures: Establish monitoring procedures to regularly assess the integrity of financial records. This can involve continuous monitoring of data inputs, system logs, and alerts to detect any anomalies or unauthorized activities that may compromise data integrity.

-Data quality improvement procedures: Implement procedures to improve the quality of data used in financial that are subject of AI analysis. This can involve data cleansing, data normalization, and data validation processes to ensure the accuracy and completeness of the data used for financial calculations.

-Confirm data reliability and accuracy: Verify that the data used in financial records comes from reliable sources and undergoes appropriate validation processes. This helps ensure that the data is accurate, complete, and suitable for financial reporting purposes.

-Introduction of Implementation of internal controls mechanisms for information security, policies, and controls on the use of AI across all organizational structures, and a thorough evaluation of each AI technology. To ensure data integrity, the evaluation and assessment of each AI technology's impact are undertaken, followed by the implementation of appropriate controls. These controls include review controls, which involve implementing procedures to review and validate financial data and calculations through independent reviews, cross-checking of data, and verification of calculations. The aim is to ensure accuracy and identify discrepancies or errors. Additionally, compensatory controls are established to validate the completeness and accuracy of input data. This may entail conducting additional checks, reconciliations, or cross-referencing data from multiple sources to ensure consistency and reliability.

By employing these tactics, organizations can strengthen the integrity of their financial records. Establishing IT processes, introducing review controls, implementing monitoring procedures, improving data quality, confirming data reliability, implementing compensatory controls, establishing internal controls, and analysing relevant systems help mitigate risks and ensure the accuracy and integrity of financial records. The study results align well with the literature review on auditing AI systems and mitigating data quality risks. The experts' responses emphasize the importance of analysing relevant systems and conducting thorough assessments to identify vulnerabilities and weaknesses in financial record-keeping (ISACA, 2018; Deloitte, 2023). This aligns with the literature's emphasis on the need for auditors to possess a deep understanding of AI design, architecture, and various technologies, processes, and controls associated with AI (ISACA, 2018). By implementing IT processes and controls to enhance the security and integrity of financial records, organizations can effectively address data quality risks in AI systems (Deloitte, 2023). The study adds to the literature by providing specific tactics for ensuring the integrity of financial records in the context of AI systems. The focus on implementation of monitoring procedures, data quality improvement procedures, and confirmation of data reliability and accuracy underscores the practical steps that organizations can take to address data quality risks (Deloitte, 2023). The emphasis on internal controls mechanisms, review controls, and compensatory controls demonstrates how organizations can establish comprehensive risk management protocols to effectively manage AI-related risks (ISACA, 2018; ICO, 2020). By offering concrete tactics for mitigating data quality risks, the study enriches the literature by providing actionable insights for auditors and organizations grappling with the challenges of auditing AI systems.

4.4.2. Data Security Risks

4.4.2.1. Data Security Risks: Impacts on Financial Integrity and Investor Trust

Based on the answers provided by the audit experts, neglecting or ignoring the risk to the integrity of financial records can lead to several significant consequences and impacts. In the case of a cyber attack, the systems can be compromised as a whole, ranging from the availability of systems being jeopardized to the alteration of specific data. In both situations, AI would either become unavailable (in the first case) or make erroneous decisions based on tampered information (in the second case). The experts mentioned possible consequences that result in the manipulation and destruction of data directly impacting the integrity of financial records. This can lead to misleading financial statements and affect the availability of systems, thereby impacting timely financial reporting. Also the theft and improper disclosure of important data, if the risk is not tackled, important financial data may be stolen and improperly disclosed. This can have severe consequences for the integrity of financial records and may lead to unauthorized access or misuse of sensitive information. All these can lead to the loss of trust by investors and markets. Neglecting the risk can result in a loss of trust by investors and markets regarding an organization's financial data. When the integrity of financial records is compromised, it undermines confidence in the accuracy and reliability of the information presented, potentially leading to negative implications for the organization's reputation and financial standing. In conclusion, neglecting or not addressing the risk to the integrity of financial records can have severe consequences. These include data manipulation and destruction, compromise of systems and data due to cyber-attacks, theft and improper disclosure of important data, impact on financial statements, loss of trust by investors and markets, and the occurrence of cybersecurity attacks. It is crucial for organizations to proactively tackle this risk and implement robust controls to safeguard the integrity and reliability of their financial records.

The study results align with the literature review, both emphasizing the significant concerns and consequences of data security risks in AI systems used for financial and accounting activities (Zhu & Guan, 2022; McKinsey Global Institute, 2018; ICAEW, 2020; Parlak, 2023; Cheatham, Javanmardian, & Samandari, 2019; EY, 2018). The experts' responses in the study highlight the potential impacts of cyber attacks, data manipulation, and unauthorized access, which resonate with the risks mentioned in the literature review. Both the study and the literature emphasize that data breaches, unauthorized access, and data manipulation can compromise the privacy, integrity, and overall trustworthiness of AI systems (McKinsey Global Institute, 2018; ICAEW, 2020; Parlak, 2023). Furthermore, the study adds value to the literature by focusing on the specific consequences of neglecting data security risks for the integrity of financial records. The experts point out that cyber attacks can lead to compromised systems and altered data, resulting in AI making erroneous decisions based on tampered information. This highlights the potential impact on the accuracy and reliability of financial statements, emphasizing

the importance of safeguarding the integrity of financial records through robust controls (Cheatham, Javanmardian, & Samandari, 2019). Moreover, the experts' recognition of the potential loss of trust by investors and markets due to compromised financial data aligns with the literature's emphasis on the severe consequences of data security risks (ICAEW, 2020). By highlighting the possible loss of trust and its negative implications for an organization's reputation and financial standing, the study contributes to the literature by underscoring the importance of addressing data security risks to maintain stakeholders' confidence.

4.4.2.2. Mitigating Data Security Risks: Tactics for Ensuring Integrity in Financial Records

The experts recommend a multi-faceted approach to mitigate the risk, encompassing various measures including deploying defence mechanisms to prevent intrusion attacks starting by identifying and addressing existing vulnerabilities by monitoring security systems to detect and respond to potential threats to improve security protocols. A firm should establishing IT governance and security processes and controls to enhance it´s security robustness, including:

-Implementing firewalls with Intrusion Detection Systems (IDS) to make unauthorized access attempts more difficult.

-Developing action plans that outline the appropriate steps to take based on the severity of an incident.

-Implementing secure backups that are not susceptible to cyber attacks.

- Incorporating internal control mechanisms for information security, including policies and controls on the use of AI across all organizational structures. For example utilizing application controls, such as access restrictions and segregation of duties, to enhance system security. And implement management controls for information security and physical security.

By implementing these tactics, organizations can enhance the security and integrity of their AI systems. It is important to note that risk mitigation is an ongoing process, and organizations should regularly review and update their strategies to adapt to emerging threats and advancements in technology. The study results on mitigating data security risks through various tactics align well with the literature review on auditing AI systems and managing AI-related risks (ISACA, 2018; Deloitte, 2023; ICO, 2020). Both the literature review and the study results emphasize the importance of deploying defense mechanisms, identifying and addressing vulnerabilities, and monitoring security systems to detect and respond to potential threats (ISACA, 2018; Deloitte, 2023; ICO, 2020). The study's focus on implementing firewalls with Intrusion Detection Systems (IDS), developing action plans, and establishing secure backups aligns with the literature's recommendation to enhance security protocols and governance processes (Deloitte, 2023). Both the literature and the study emphasize the importance of internal controls and risk governance processes to effectively manage AI-related risks

(ISACA, 2018; ICO, 2020). The study's emphasis on utilizing application controls, access restrictions, and segregation of duties to enhance system security mirrors the literature's emphasis on having auditors possess a deep understanding of various technologies, processes, and controls associated with AI (ISACA, 2018). The study adds to the literature by providing specific tactics for ensuring the integrity of financial records by mitigating data security risks in AI systems. While the literature review focuses on the broader challenges and principles of auditing AI systems, the study results delve into practical measures that organizations can implement to protect their financial records (ISACA, 2018; Deloitte, 2023; ICO, 2020). By providing a multi-faceted approach that includes deploying defence mechanisms, establishing IT governance and security processes, and implementing internal control mechanisms for information security, the study enriches the literature by offering actionable insights for enhancing the security and integrity of AI systems in the financial domain. Furthermore, the study's emphasis on risk mitigation as an ongoing process and the need for regular review and updates to strategies aligns with the literature's recommendation for auditors to anticipate and address concerns and adapt to emerging threats (Deloitte, 2023).

4.4.3. Lack of Expertise Risks

4.4.3.1. Lack of Expertise Risks: Impacts on Financial Integrity and Investor Trust

According to the experts the lack of experienced programmers in AI applications can lead to inadequate maintenance of these applications since constant updates are necessary, whether due to business evolution or changes in legislation. Potential impacts could include tasks being performed incorrectly or not performed at all, resulting in incorrect data in the systems. Ignoring the risk can compromise the accuracy of the data within the financial records. If the systems are not properly maintained and updated, errors can occur in the data, leading to incorrect financial calculations and reporting. Some examples include:

-Lack of knowledge in analysing AI results: Untrained employees who lack the necessary knowledge to interpret and analyse AI-generated results may struggle to identify anomalies or errors within the financial records. This can lead to the acceptance of inaccurate information and decisions based on flawed data.

-Non-compliance with accounting rules: If the system is not based on properly defined accounting rules established by accounting experts and implemented by IT specialists who understand the technology, the entity may be relying on incorrect information. This can result in non-compliance with accounting standards and regulations, potentially leading to legal and regulatory issues.

-Failure to identify flaws and vulnerabilities: Ignoring the risk can prevent the identification and resolution of potential flaws and vulnerabilities in the system. This leaves the financial records

susceptible to manipulation, unauthorized access, or cyber-attacks, which can compromise the integrity and confidentiality of the data.

In conclusion, ignoring or neglecting the risk can have severe consequences. These include inaccurate data, non-compliance with accounting rules, lack of data reliability, and vulnerabilities that can be exploited by threat actors. It is crucial to address the risk effectively through appropriate measures and controls to maintain the integrity and accuracy of financial records. The study results are aligned with the literature review, both highlighting the significant risks associated with the lack of expertise in AI systems for financial and accounting activities (Parlak, 2023; CMA Exam Academy, 2023; Luo, Meng, & Cai, 2018; Rao, 2020; Cheatham, Javanmardian, & Samandari, 2019; McKinsey Global Institute, 2018). The experts' responses emphasize that the lack of experienced programmers in AI applications can lead to inadequate maintenance and updates of these systems, potentially resulting in incorrect data within financial records. This aligns with the literature's concerns about poor model development, inadequate data governance, and limited interpretability and explainability due to insufficient expertise in AI technologies (Rao, 2020; Cheatham, Javanmardian, & Samandari, 2019; Parlak, 2023). Furthermore, the study adds value to the literature by focusing on the specific impacts of the lack of expertise on financial integrity and investor trust. The experts' mentions of untrained employees struggling to interpret and analyze AI-generated results and non-compliance with accounting rules highlight the potential consequences of inadequate knowledge in AI technologies for financial recordkeeping (Cheatham, Javanmardian, & Samandari, 2019). Additionally, the study's emphasis on the failure to identify flaws and vulnerabilities in AI systems due to neglecting the risk aligns with the literature's concerns about compromised data integrity and susceptibility to unauthorized access or cyber-attacks (McKinsey Global Institute, 2018). Moreover, the study highlights the need for organizations to effectively address the risk through appropriate measures and controls to maintain the integrity and accuracy of financial records. By providing concrete examples of the potential impacts of the lack of expertise in AI systems, the study adds practical insights to the literature, emphasizing the importance of ensuring adequate training and expertise for those involved in AI-related financial activities.

4.4.3.2. Mitigating Lack of Expertise Risks: Tactics for Ensuring Integrity in Financial Records

Mapping key controls during the financial statement preparation process helps ensure that appropriate checks and balances are in place. These controls can help detect and prevent errors, anomalies, or fraudulent activities that may compromise the integrity of financial records. When implementing AI applications, it is important for the entity to have application maintenance contracts with clearly defined Service Level Agreements (SLAs) and penalties for non-compliance. This ensures

that the applications are regularly maintained and updated to prevent errors and inaccuracies in the financial records. Ensuring that IT staff members have specialized training in areas such as AI monitoring and security can enhance the entity's capability to identify and address potential risks. Implementing comprehensive training and awareness programs throughout the organization raises awareness about the importance of data integrity and the potential risks associated with AI applications. This promotes a culture of data accuracy and security. Regular training sessions on the use and regulation of AI, coupled with periodic audits, can help ensure that AI applications are being used in compliance with relevant laws, regulations, and internal policies. This helps maintain data integrity and mitigates the risk of non-compliance. Also, providing specialized training to employees involved in the financial record-keeping process equips them with the necessary skills and knowledge to handle AI-generated data and results, will help reduce the likelihood of misinterpretation or incorrect analysis of AI outputs. Alternatively, the entity can consider hiring a service provider with expertise in monitoring and securing AI systems. Before selecting a supplier for AI applications, it is crucial to evaluate their expertise and knowledge in the relevant areas. This ensures that the supplier has the necessary capabilities to provide reliable and secure AI solutions that support the integrity of financial records. Transferring knowledge from the supplier to the entity and providing training to members of the organization can enhance their understanding of the AI applications. This empowers employees to effectively maintain and utilize the applications, reducing the risk of errors and incorrect data. By employing these tactics, organizations can effectively mitigate the risk to the integrity of financial records and maintain accurate and reliable financial information.

The study's results on mitigating the lack of expertise risks in financial records align well with the literature review on auditing AI systems and managing AI-related risks (ISACA, 2018; Deloitte, 2023; ICO, 2020). Both the literature review and the study emphasize the importance of auditors possessing a deep understanding of various technologies, processes, and controls associated with AI to ensure a successful audit and reliable financial reports (ISACA, 2018; Deloitte, 2023). The study's focus on mapping key controls during the financial statement preparation process, having application maintenance contracts, and providing specialized training to employees involved in financial record-keeping aligns with the literature's emphasis on promoting transparency, continuous improvement, and expertise in AI design and architecture (ISACA, 2018; Deloitte, 2023). Both the literature and the study highlight the significance of collaboration with internal engineering and security teams, as well as business leaders responsible for the AI strategy, to effectively manage AI-related risks and ensure data integrity (ISACA, 2018; ICO, 2020). The study adds to the literature by providing specific tactics to address the lack of expertise risks in financial records and how to effectively manage AI applications in this context. While the literature review focuses on the challenges and principles of auditing AI systems, the study results delve into practical measures that organizations can implement to ensure

the accuracy and reliability of financial records when using AI (ISACA, 2018; Deloitte, 2023; ICO, 2020). By offering actionable insights on mapping key controls, implementing application maintenance contracts, and providing specialized training, the study enriches the literature by providing practical solutions for mitigating risks related to AI applications in financial record-keeping. Furthermore, the study's emphasis on evaluating and transferring knowledge from service providers to the entity aligns with the literature's focus on flexibility and adaptability in implementing AI risk-management techniques (Deloitte, 2023). Both the literature and the study highlight the iterative nature of AI development and the importance of continuous improvement and ongoing vigilance to ensure the effectiveness and reliability of the auditing process and AI applications (ISACA, 2018; Deloitte, 2023).

4.4.4. Lack of human agency in AI processes and accountability Risks

4.4.4.1. Lack of human agency in AI processes and accountability Risks: Impacts on Financial Integrity and Investor Trust

AI implementation often involves multiple areas beyond computer science, such as electrical engineering and automation. If these areas are not aligned and synchronized during the development process, issues can arise. This can result in software development not keeping pace with automation or vice versa, leading to impacts on data processing and updates. This can affect both financial and business-related data. Ignoring the risk can undermine the accuracy and completeness of the financial records. Incorrect or incomplete data may also be generated due to AI not being programmed correctly or not following the company's guidelines and best practices. This can result in unreliable financial information and decision-making. If the AI systems are not properly programmed or maintained, unauthorized changes can occur. These changes may impact the controls and automated calculations used as the basis for financial data. This can introduce errors or manipulate the data, compromising the integrity of financial records. Ignoring the risk of inadequate AI implementation can lead to the dispersal of AI technologies throughout the organization without proper controls and oversight. This dispersal can compromise the components that contribute to the trustworthiness of organizations and their data. Trust in the financial records may erode, affecting stakeholders' confidence and potentially leading to legal and reputational consequences. In conclusion, ignoring or not tackling the risk related to the integrity of financial records can have significant negative consequences. These include issues arising from lack of alignment and synchronization, data inaccuracy and incompleteness, unauthorized changes impacting controls, and a compromised trustworthiness of organizations and their data. It is essential to address the risk effectively to ensure the integrity and reliability of financial records, maintain data accuracy, and uphold stakeholder trust.

The study results are in alignment with the literature review, as both highlight the significant risks associated with the lack of human agency in AI processes and the potential impacts on financial integrity and investor trust (Zhu & Guan, 2022; Parlak, 2023; Rao, 2020; Cheatham, Javanmardian, & Samandari, 2019; Marr, 2018). The experts' responses emphasize the potential consequences of inadequate AI implementation, such as data inaccuracies and incomplete data, which align with the concerns raised in the literature review about lack of transparency and explainability in AI systems (Rao, 2020; Cheatham, Javanmardian, & Samandari, 2019). Additionally, the study's findings regarding unauthorized changes impacting controls and compromising the integrity of financial records are consistent with the literature's emphasis on the potential risks arising from limited control and decision-making when humans are excluded from key AI processes (Parlak, 2023; Marr, 2018). Moreover, the study adds value to the literature by focusing on the specific impacts of the lack of human agency in AI processes on financial integrity and investor trust. The experts' mention of issues arising from lack of alignment and synchronization during AI development, impacting data processing and updates, provides practical insights into the potential consequences for financial and business-related data (Zhu & Guan, 2022). The study further highlights the dispersal of AI technologies throughout the organization without proper controls and oversight, potentially compromising the trustworthiness of organizations and their data, a concern not only for financial integrity but also for overall data reliability (Parlak, 2023).

4.4.4.2. Mitigating Lack of Human Agency in AI processes and accountability Risks: Tactics for Ensuring Integrity in Financial Records

The development cycle of an application should consider various aspects and controls. Establishing well-defined development procedures is crucial to mitigate risks associated with uncontrolled development. These procedures should outline how development should be carried out, involve relevant areas, and specify the controls to be implemented. This includes incorporating testing, approvals, and transitioning to production after successful testing. Following such procedures ensures that development activities align with established controls and reduces the likelihood of errors or inconsistencies. The entity must identify and map key controls throughout the business process to ensure that appropriate checks and balances are in place. By understanding the critical points within the process, organizations can implement targeted controls to prevent errors, detect anomalies, and enhance the integrity of financial records. For example introduce controls that require pre-production approval before implementing any changes to AI systems or processes that impact financial records. This control ensures that changes undergo proper review, testing, and validation before they are applied in production. It helps mitigate the risk of unauthorized or untested modifications that could

compromise the integrity of financial data. The firm should also conduct periodic audits and engage specialists. Regular audits, both internal and external, help evaluate the effectiveness of controls and identify areas for improvement. Engaging specialists who possess expertise in risk assurance and financial record integrity can provide valuable insights and recommendations for mitigating risks. Their expertise can help uncover potential vulnerabilities and suggest appropriate control measures to address them. It was also highlighted by the experts, the importance to develop comprehensive training and awareness programs for employees involved in AI implementation and financial record management. These programs should cover topics such as data integrity, controls, compliance, and best practices. By equipping employees with the necessary knowledge and awareness, organizations can foster a culture of data integrity and ensure that individuals understand their roles in maintaining the integrity of financial records. In conclusion, organizations can mitigate the risk related to the integrity of financial records by implementing tactics such as developing clear development procedures, mapping key controls, conducting periodic audits, implementing pre-production approval controls, and providing training and awareness programs. These tactics promote a structured and controlled approach to AI implementation and financial record management, reducing the likelihood of errors, inconsistencies, and unauthorized changes.

The literature review emphasizes the importance of auditors being well-prepared to audit AI systems and ensure reliable financial reporting (ISACA, 2018). The study's results shed light on the risks related to the lack of human agency in AI processes and its potential impact on financial integrity and investor trust (Zhu & Guan, 2022; Parlak, 2023). Both the literature review and the study highlight the significance of understanding AI design, architecture, and various technologies to conduct successful AI audits (ISACA, 2018; Deloitte, 2023). They underscore the need for auditors to collaborate with internal engineering and security teams, as well as business leaders responsible for AI strategy, to ensure comprehensive audits of AI systems (Deloitte, 2023). The study adds valuable insights by focusing on the implications of inadequate AI implementation on data accuracy, completeness, and trustworthiness of organizations (Zhu & Guan, 2022). It identifies the potential risks associated with AI systems not being properly programmed, maintained, or aligned with other development areas, leading to errors in financial data and undermining stakeholder trust (Parlak, 2023). Both the literature review and the study highlight the importance of transparency, continuous improvement, and documentation in AI auditing to ensure the effectiveness and reliability of the process (ISACA, 2018; ICO, 2020). The study's findings further align with the literature review by emphasizing the risks of unauthorized changes in AI systems impacting controls and compromising financial record integrity (Zhu & Guan, 2022). This adds evidence to the concerns raised in the literature about the potential consequences of limited human agency in key AI processes (Rao, 2020; Cheatham, Javanmardian, & Samandari, 2019). Both the literature and the study stress the need for organizations to adopt risk-

specific controls and protocols throughout the AI development process to manage AI-related risks effectively (ISACA, 2018; ICO, 2020).

4.4.5. Errors and biases in algorithms Risks

4.4.5.1. Errors and biases in algorithms Risks: Impacts on Financial Integrity and Investor Trust

The consequences may vary depending on the specific process involved. For example, if errors or miscalculations occur in the payroll process, it can lead to inaccurate remuneration for employees, incorrect calculation of taxes and deductions, and non-compliance with laws and regulations. This emphasizes the importance of addressing the risk in each specific process to ensure accurate financial record-keeping and compliance with legal requirements. Errors in algorithms, regardless of their nature, can significantly impact the calculation of financial data, compromising the integrity of the information. Many controls that ensure financial data integrity rely on algorithms themselves. If these algorithms are incorrect or flawed, it can lead to widespread inaccuracies and errors in financial records. This highlights the critical role algorithms play in maintaining data integrity and the need for rigorous testing and validation to mitigate algorithmic risks. Ignoring the risk can result in compromised accuracy of financial records. Inaccurate calculations, errors in data processing, and improper handling of information can result in financial records that do not reflect the true financial position and performance of the entity. Leading to the use of information and data that do not align with the truth. This can result in the dissemination of misleading financial information, potentially leading to misguided business decisions, financial misrepresentation, and reputational damage. This can hinder decision-making processes and undermine the trust of stakeholders in the organization's financial reporting.

The study results are in alignment with the literature review, as both emphasize the significant risks posed by errors and biases in algorithms in AI systems (CMA Exam Academy, 2023; EY, 2018; McKinsey Global Institute, 2018; Information Systems Audit and Control Association, 2018; Cheatham, Javanmardian, & Samandari, 2019; Rao, 2020; Parlak, 2023). The experts' responses highlight the potential consequences of errors and biases in algorithms in various financial processes, such as inaccurate remuneration, incorrect tax calculations, and non-compliance with regulations. This is consistent with the literature's concerns about algorithmic bias leading to biased decisions or actions (Cheatham, Javanmardian, & Samandari, 2019; Rao, 2020). Additionally, both the literature review and the study results emphasize the critical role of algorithms in maintaining data integrity and the need for rigorous testing and validation to mitigate algorithmic risks (McKinsey Global Institute, 2018; Parlak, 2023). The study adds to the literature by providing specific examples of how errors and biases in algorithms can impact financial integrity and investor trust. The emphasis on errors in the payroll

process leading to incorrect remuneration and tax calculations highlights the practical implications of algorithmic risks for financial record-keeping and compliance (CMA Exam Academy, 2023). Moreover, the study underlines the importance of addressing the risk in each specific financial process to ensure accurate data and compliance with legal requirements, shedding light on the need for targeted risk mitigation strategies for different aspects of financial operations.

4.4.5.2. Mitigating Errors and Biases in Algorithms Risks: Tactics for Ensuring Integrity in Financial Records

The experts proposed the identification and implementation of key controls at critical points within the financial record-keeping processes. These controls should address areas such as data entry, validation, reconciliation, and reporting to ensure accuracy, completeness, and compliance with regulations. A firm must establish controls and processes that regularly review the configurations, calculations, and overall functioning of the systems and applications involved in financial record-keeping. This ensures that the desired outcomes are achieved and helps detect and rectify errors or anomalies promptly. A firm should also develop and follow procedures that ensure a structured and controlled development and change cycle for applications and systems. This includes monitoring the development process to identify any potential errors or issues that may arise during implementation or updates. Experts also advised regular audits and engagement of AI experts. Conduct periodic audits to assess the effectiveness of controls and identify areas for improvement. Considering hiring experts in AI programming and development who can provide specialized knowledge and insights to mitigate risks associated with AI-based financial record-keeping. By employing these tactics, organizations can enhance the integrity of their financial records. Implementing controls and review processes, following structured development cycles, implementing key controls, conducting regular audits, and engaging AI experts help identify and address potential errors, ensure accuracy, and promote compliance with regulations and best practices.

The literature review emphasizes the crucial role of financial auditors in providing assurance to society through reliable and trustworthy financial reports that audit AI systems (ISACA, 2018). It highlights the unique challenges that auditing AI presents and the need for auditors to have a deep understanding of AI design and architecture, as well as expertise in various AI-related technologies (ISACA, 2018). The study's results align with the literature review by focusing on the importance of mitigating errors and biases in AI algorithms to ensure the integrity of financial records (ICO, 2020). The experts' recommendations in the study support the notion of implementing controls and processes to review the configurations, calculations, and overall functioning of systems involved in financial record-keeping (ICO, 2020). This aligns with the literature review's emphasis on promoting

transparency, continuous improvement, and explicit documentation in the auditing process (ISACA, 2018). The literature review stresses the significance of addressing risks associated with third-party control over infrastructure, especially with the use of cloud computing in AI deployments (Deloitte, 2023). The study's results do not directly address this specific concern, as it mainly focuses on mitigating errors and biases in AI algorithms within the organization's financial record-keeping processes. However, the study does propose the engagement of AI experts, which could potentially include experts in cloud computing security and infrastructure to address the third-party control risks indirectly. One aspect that the study adds to the literature is its focus on mitigating errors and biases in AI algorithms to ensure the integrity of financial records (ICO, 2020). By exploring tactics for addressing algorithmic risks, the study provides practical insights into enhancing the reliability and accuracy of financial data in the context of AI technology. This specific focus on algorithms and their impact on financial records adds valuable knowledge to the existing literature on auditing AI systems. Additionally, the study's emphasis on regular audits and engagement of AI experts offers a proactive approach to managing AI-related risks in financial record-keeping, providing organizations with concrete steps to implement safeguards effectively. Overall, the study contributes to the literature by providing actionable strategies for organizations to ensure the integrity of financial records in the rapidly evolving AI landscape.

4.4.6. Detecting Rogue AI Risks

4.4.6.1. Detecting Rogue AI Risks: Impacts on Financial Integrity and Investor Trust

The experts' responses shed light on the potential consequences and impacts that can arise if the risks related to the integrity of financial records are ignored or left unaddressed, including unauthorized code leading to potential fraud. Ignoring or neglecting the risk can result in the development and implementation of unauthorized code, which has been known to cause significant fraud incidents. Such fraudulent activities not only impact the financial aspects of the entity but also tarnish its reputation. This emphasizes the importance of addressing the risk to prevent unauthorized access and fraudulent manipulation of financial records. If the risk is ignored, there is also a possibility that AI systems may generate false or inaccurate information that does not comply with regulations. This can have detrimental effects on the integrity of financial records, as incorrect or misleading data can lead to incorrect financial reporting, non-compliance with legal requirements, and reputational damage. Neglecting to tackle the risk can also result in inadequate access controls, leaving financial records vulnerable to unauthorized access. Insufficient access controls can lead to unauthorized modifications, unauthorized data creation, and potential breaches that compromise the integrity of financial records. In conclusion, if the risk related to the integrity of financial records is ignored or not properly tackled,

the consequences can be severe. Unauthorized code can lead to fraud and reputation damage, false information generated by AI can result in non-compliance and inaccurate financial reporting, and inadequate access controls can leave financial records vulnerable to unauthorized access and manipulation. It is crucial for organizations to implement robust controls, adhere to regulations, and maintain strict access controls to safeguard the integrity of their financial records and protect their reputation.

The literature review emphasizes the risks associated with rogue AI and the potential loss of control when AI systems become autonomous and exceed human understanding (Cheatham, Javanmardian, & Samandari, 2019). It highlights the importance of human supervision and transparency in the AI design framework to ensure that the AI's decisions align with the entity's intentions (Marr, 2018). The study's results align with the literature review by focusing on detecting rogue AI risks and their impacts on financial integrity and investor trust (Rao, 2020). The experts' responses in the study highlight the potential consequences of ignoring or neglecting the risks related to the integrity of financial records, such as unauthorized code leading to potential fraud and the generation of false or inaccurate information (Rao, 2020). This supports the literature's concerns about the misalignment between human goals and machine decisions when AI operates without proper human supervision (Marr, 2018). The literature review mentions the risks of unauthorized access and modification by rogue AI, which can lead to data breaches or unauthorized changes to financial records (Rao, 2020). The study's results complement this by emphasizing the potential consequences of inadequate access controls, leaving financial records vulnerable to unauthorized access and manipulation (Rao, 2020). Both the literature review and the study highlight the importance of addressing access control risks to safeguard the integrity of financial records. Moreover, the literature review discusses the lack of transparency in rogue AI, making it challenging for auditors to verify the accuracy of accounting data (Rao, 2020). The study's results align with this concern by emphasizing the potential impacts of false or inaccurate information generated by AI on financial reporting and compliance (Rao, 2020). This reinforces the significance of transparency and the need for auditors to be able to understand and explain the AI system's decisions. One contribution of the study to the literature is its focus on detecting rogue AI risks specifically in the context of financial integrity and investor trust (Rao, 2020). By exploring the potential consequences of ignoring or neglecting these risks, the study provides practical insights into the specific impacts on financial records and reputation.

4.4.6.2. Mitigating Detecting Rogue AI Risks: Tactics for Ensuring Integrity in Financial Records

Conduct regular audits and implement code review controls specifically for AI systems. This helps identify any potential issues or vulnerabilities in the AI algorithms or models used in financial record-

keeping. Code reviews can help detect errors, ensure compliance with regulations and best practices, and enhance the accuracy and integrity of AI-generated financial information. A company must also ensure that all code developed within the scope of new implementations or changes follows a set of controls. These controls include obtaining approval for the entire development/change process, carrying out development/changes in a segregated environment by experienced professionals, conducting testing in a segregated quality environment by key users, and transitioning to production with the involvement of a different person. No further changes should be allowed after testing, and the code should be retested after transitioning to production to ensure alignment with expected behaviour. By employing these tactics, organizations can mitigate the risk related to the integrity of financial records. Adhering to development controls, conducting regular audits and code reviews for AI systems, and performing system analysis help ensure that code is developed and implemented correctly, vulnerabilities are identified and addressed, and appropriate controls are in place to maintain the integrity of financial records.

The study results propose tactics for mitigating rogue AI risks specifically in the context of ensuring the integrity of financial records. One of the key strategies suggested is conducting regular audits and implementing code review controls for AI systems. This aligns with the literature review's emphasis on the importance of auditing AI systems to ensure reliable and trustworthy financial reports (ISACA, 2018). Auditing AI is highlighted as a critical process that requires a deep understanding of AI design, architecture, and various technologies, including machine learning and software testing (ISACA, 2018). The study's recommendation for code reviews aims to detect errors and vulnerabilities in AI algorithms or models used in financial record-keeping, which corresponds to the need for ongoing vigilance and documentation throughout the AI life cycle mentioned in the literature review (ISACA, 2018). The study's focus on code development controls and the involvement of key users aligns with the literature's emphasis on the involvement of all stakeholders, including internal engineering and security teams and business leaders responsible for AI strategy (ISACA, 2018). Another key tactic proposed by the study is implementing a set of controls for the development and change process of AI systems in financial record-keeping. This includes obtaining approvals, conducting development and testing in segregated environments, and ensuring code retesting after transitioning to production. The study's approach to establishing protocols for adherence to controls throughout the AI development process resonates with the literature review's recommendation of adopting risk-specific controls to effectively manage AI-related risks (ICO, 2020). The study's focus on transitioning to production with the involvement of different personnel aligns with the literature review's emphasis on the involvement of various stakeholders in auditing AI systems (ISACA, 2018). One notable contribution of the study to the literature is its specific focus on mitigating rogue AI risks in financial record-keeping. While the literature review discusses the importance of auditing AI systems and implementing risk-specific

controls, the study delves deeper into practical tactics to address integrity-related risks unique to financial records (ISACA, 2018; ICO, 2020). By proposing code review controls and development process controls, the study adds specific strategies that financial auditors can employ to ensure the accuracy, completeness, and compliance of AI-generated financial information (ISACA, 2018; ICO, 2020). The study's emphasis on regular audits and code reviews for AI systems also aligns with the literature's emphasis on the iterative nature of AI development and the need for ongoing vigilance and documentation (ISACA, 2018). Overall, the study's results contribute to the literature by providing actionable tactics to enhance the integrity of financial records in the context of AI implementation.

4.4.7. Excessive reliance on AI Risks

4.4.7.1. Excessive reliance on AI Risks: Impacts on Financial Integrity and Investor Trust

Based on the provided expert responses ignoring or neglecting the risk can lead to inaccuracies and incompleteness in financial records. This can result in incorrect financial reporting, misinterpretation of financial data, and potential financial losses for the entity. If the risk is not tackled, there is also a possibility of information theft and its subsequent misuse. Unauthorized individuals or malicious actors may gain access to financial records, leading to data breaches, identity theft, or fraudulent activities. This increases the risk of cybersecurity breaches, unauthorized modifications, or data manipulation. Such incidents can compromise the integrity of financial records and expose the entity to legal and regulatory consequences. In conclusion, ignoring or not addressing the risk related to the integrity of financial records can have significant consequences for an entity. It can lead to inaccuracies and incompleteness in financial records, theft of information with potential misuse, and heightened cybersecurity risks due to inadequate access controls. It is crucial for organizations to implement appropriate measures and controls to safeguard the accuracy, completeness, and security of their financial records, protecting both their financial interests and their reputation.

These findings align with the literature review's emphasis on the importance of striking a balance between the autonomy of AI systems and the need for human oversight and control (Bose, Dey, & Bhattacharjee, 2022). The literature review highlights that excessive reliance on AI can transform it from an asset into a liability for the organization and can lead to severe consequences such as data breaches and compromised sensitive information (Cheatham, Javanmardian, & Samandari, 2019). Both the study results and the literature review emphasize the significance of maintaining a symbiotic relationship between AI and human oversight to ensure the integrity and security of financial records. The study's specific focus on the risks related to excessive reliance on AI in financial record-keeping adds to the literature by providing practical insights and potential impacts on financial integrity and investor trust. While the literature review discusses the risks of excessive reliance on AI in general

terms, the study delves deeper into the implications for financial record-keeping, such as incorrect financial reporting and unauthorized data breaches (Cheatham, Javanmardian, & Samandari, 2019; Bose, Dey, & Bhattacharjee, 2022). The study's identification of potential financial losses for the entity highlights the importance of addressing these risks to safeguard the organization's financial interests (Bose, Dey, & Bhattacharjee, 2022). Additionally, the study's emphasis on implementing appropriate measures and controls aligns with the literature review's recommendation of incorporating proper safeguards and human oversight to mitigate the risks associated with AI (Zhu & Guan, 2022). Furthermore, the study results accentuate the necessity of proactive monitoring and continuous assessment of AI systems to detect and mitigate cyber threats or system malfunctions. It underscores the role of human experts in analysing complex patterns, identifying anomalies, and implementing countermeasures, all of which contribute to maintaining the integrity and security of financial records (Zhu & Guan, 2022). The literature review emphasizes the vulnerability of AI systems to hacking or cyber-attacks and the importance of human involvement in addressing these issues (EY, 2018; Petkov, 2020). Thus, the study's emphasis on human oversight and involvement in AI operations adds to the literature by reiterating the significance of maintaining a balanced and collaborative approach between AI and human experts to optimize the benefits of AI while minimizing potential risks (Petkov, 2020).

4.4.7.2. Mitigating Excessive Reliance on AI Risks: Tactics for Ensuring Integrity in Financial Records

To mitigate the related risks, experts advise to implement defence mechanisms to protect financial records from external attacks and unauthorized access. This can include the use of firewalls, intrusion detection systems, encryption, and other cybersecurity measures to safeguard the integrity of financial data. Additionally, establish controls to limit AI's access to certain sensitive information, ensuring that AI systems are only granted access to authorized data and functionalities. The firm must also identify and map key controls throughout the business processes involved in financial record-keeping. This includes understanding the critical checkpoints, data inputs, and outputs, as well as implementing appropriate controls at each stage to ensure the integrity of financial records. Mapping key controls helps identify potential vulnerabilities and areas for improvement. By employing these tactics, organizations can mitigate the risk related to the integrity of financial records. Mapping key controls, implementing defence mechanisms and access controls, and conducting system analysis contribute to strengthening the overall security and integrity of financial records, reducing the likelihood of data breaches, unauthorized access, and other risks that could compromise the accuracy and trustworthiness of financial information. The experts' recommendations align with the literature

review's emphasis on the importance of implementing robust risk-specific controls and cybersecurity measures to safeguard the integrity of financial records (ISACA, 2018; Deloitte, 2023). Both the study and the literature review stress the significance of establishing controls and protocols to address the unique challenges posed by auditing AI systems. The literature review recommends flexibility in adapting existing frameworks and regulations until more specific AI standards are established, which resonates with the study's emphasis on implementing defence mechanisms and access controls to protect financial records from external attacks and unauthorized access (Deloitte, 2023). Moreover, the study results add practical tactics, such as mapping key controls throughout the financial record-keeping processes, to identify vulnerabilities and improve the overall security of financial information. This detailed approach complements the literature review's focus on promoting transparency, continuous improvement, and explicit documentation to ensure the effectiveness and reliability of the auditing process for AI systems (ISACA, 2018). Furthermore, the study's emphasis on limiting AI's access to certain sensitive information aligns with the literature review's concern about the risks associated with third-party control over infrastructure when using cloud computing in AI deployments (Deloitte, 2023). Both the study and the literature review highlight the importance of collaboration among auditors, internal engineering and security teams, and business leaders to effectively manage AI-related risks (ISACA, 2018). The study's specific tactics for addressing excessive reliance on AI, such as using firewalls, intrusion detection systems, and encryption, provide practical ways to protect financial records and mitigate cybersecurity risks.

4.4.8. Deepfakes risks

4.4.8.1. Deepfakes Risks: Impacts on Financial Integrity and Investor Trust

Ignoring or neglecting the risk can result in a deepfake of an administrator with elevated access privileges subverting the behaviour of the AI system. They can manipulate the AI's tendencies, alter data, delete records, or introduce false information to make the AI exhibit a specific behaviour. This can lead to skewed financial data, incorrect predictions, or decisions, and ultimately impact the integrity of financial records. If the risk is not addressed, the impact on financial data can be substantial. Manipulation or introduction of false data by an administrator can lead to inaccurate financial reporting, misleading analysis, and incorrect decision-making based on compromised information. This can have financial ramifications, potentially resulting in financial losses or misinformed business strategies. When an administrator is knowledgeable about covering up their activities, the impact on the integrity of financial records may not be easily detectable. Unauthorized alterations or introduction of false data may go unnoticed, potentially leading to prolonged inaccuracies in financial records and increasing the risk of fraudulent activities or data manipulation.

In conclusion, ignoring or not tackling the risk related to the integrity of financial records can have severe consequences for an entity. Administrator-level access can be exploited to manipulate AI behaviour, resulting in compromised financial data. The impact on financial records may not be easily detectable, and the ability to cover up such activities further exacerbates the risk. It is crucial for organizations to implement appropriate access controls, monitor AI behaviour, and conduct regular audits to mitigate the risk and safeguard the integrity of financial records. The study's results are in line with the literature review's concerns about the risks posed by deepfakes in the context of financial audits (Floridi, 2021; Rao, 2020; Kietzmann et al., 2020). Both the study and the literature review highlight the potential for deepfake technology to manipulate financial records and create false evidence, leading to inaccurate audit results and potential financial fraud. The literature review emphasizes the use of AI deepfakes to pretend to be someone with elevated access privileges within a system, such as a system administrator, to perform critical tasks (Floridi, 2021). The study's results echo this concern by pointing out that ignoring or neglecting the risk of deepfake manipulation can lead to an administrator with elevated access privileges subverting the AI system's behavior, altering data, or introducing false information, ultimately impacting the integrity of financial records. Furthermore, the study underlines the difficulty in detecting deepfake manipulations, particularly when administrators are knowledgeable about covering up their activities, which can lead to prolonged inaccuracies in financial records and increase the risk of fraudulent activities (Rao, 2020). This emphasis on the challenges of detecting and mitigating deepfakes in financial records adds valuable contributions to the existing literature.

4.4.8.2. Mitigating Deepfake's Risks: Tactics for Ensuring Integrity in Financial Records

Starting by restrict administrator-level access to a small number of individuals within the IT department, ideally one or two individuals. By limiting the number of individuals with this level of access, the organization reduces the potential for unauthorized alterations or manipulation of financial records. It also helps in maintaining accountability and traceability of activities performed with administrator-level access. When administrator-level access is used, it is important to have controls in place to monitor and regulate its usage. Some control measures that can be implemented include:

-Logging activities: Keep a detailed log of all activities performed using administrator-level access. This helps in tracking and auditing the actions taken by administrators, providing an additional layer of transparency and accountability.

-Authorization for specific tasks: Require authorization from multiple individuals or designated approvers for specific tasks performed with administrator-level access. This ensures that there is

oversight and awareness of the tasks being carried out, reducing the risk of unauthorized or malicious activities going unnoticed.

-Recording justification: Establish a process for recording the justification or business reason behind the use of administrator-level access. This helps in documenting the purpose and necessity of such access, providing a trail of evidence, and ensuring that its usage is justified and properly authorized.

By implementing these tactics, organizations can mitigate the risk associated with the integrity of financial records. Limiting and controlling administrator-level access, along with analysing systems, helps reduce the potential for unauthorized alterations, enhances accountability, and strengthens the overall security and integrity of financial records. The study's results on mitigating deepfake risks align with the concerns raised in the literature review about auditing AI systems and the challenges auditors face in ensuring reliable and trustworthy financial reports (ISACA, 2018; Deloitte, 2023; ICO, 2020). Both the literature review and the study emphasize the importance of transparency, vigilance, and documentation throughout the AI life cycle to effectively manage AI-related risks (ISACA, 2018). The study's tactics for mitigating deepfake risks in financial records complement the literature's focus on the need for auditors to possess a deep understanding of AI design and architecture and to collaborate with various stakeholders in the auditing process (Deloitte, 2023). The study's emphasis on restricting administrator-level access to a small number of individuals and implementing control measures, such as logging activities and requiring authorization for specific tasks, aligns with the literature's recommendation for implementing robust risk-governance processes to manage AI risks effectively (ICO, 2020).

4.5. The Critical Need for IT Experts in Auditing and Analysing AI Controls

This section presents the analysis and discussion of the experts' opinions regarding the need for special IT expertise and IT auditors in assessing and mitigating the relevant risks associated with AI in financial audits. The objective of this part of the study is to explore whether specialized IT knowledge and dedicated IT auditors are required to effectively identify and manage the risks arising from the use of AI technology in financial audit processes or if this can be done solely by the financial audit team. As auditors and accounting professionals navigate an evolving landscape, it becomes crucial to determine the requisite expertise and resources needed to address AI-related risks adequately. In this analysis, the responses of the experts have been carefully synthesized. The findings presented here will shed light on whether specialized IT knowledge is deemed necessary for assessing AI risks, and if dedicated IT auditors are essential in implementing the necessary controls to mitigate those risks effectively. The findings presented here will inform the development of strategies and best practices for auditors and accounting professionals in leveraging IT knowledge and expertise to mitigate the unique risks associated with AI technology in financial audits. This study is relevant for answering the research

questions because the findings provide valuable insights on maximizing the effectiveness of mitigation strategies in this context.

Based on the unanimous responses of the audit experts, it can be concluded that the involvement of special IT expertise, such as IT auditors, is necessary to provide maximum assurance when identifying and testing the controls required to mitigate the risks to the integrity of financial records. The experts agree that the complexity of IT systems and the potential impact on financial records necessitate the expertise of IT auditors. These specialists possess the knowledge and skills required to comprehensively assess and test the controls in place to mitigate the risk. Their understanding of IT processes, systems, and security allows them to identify vulnerabilities, evaluate the effectiveness of controls, and recommend improvements. While financial audit teams can play a role in assessing and testing controls related to financial recordkeeping, the involvement of IT auditors is essential to ensure a thorough and specialized examination of the IT infrastructure. IT auditors bring a deep understanding of technology-related risks and control frameworks, enabling them to provide maximum assurance regarding the effectiveness of controls in mitigating the risks to the integrity of financial records. The consensus among the experts is that the engagement of IT auditors is necessary to supplement the efforts of financial audit teams and provide maximum assurance when identifying and testing controls to mitigate the risk. Their specialized expertise enhances the ability to comprehensively assess the IT systems and controls involved, thereby strengthening the overall integrity and reliability of financial records.

The results of the study align with the literature review, confirming the critical role of IT auditors in financial audit projects due to their specialized skills and knowledge. The unanimous responses from the audit experts highlight the necessity of involving IT auditors to effectively identify and manage the risks associated with AI in financial audits. The findings of the study resonate with the literature, which emphasizes that financial auditors alone may not possess the necessary expertise to navigate, access, and test the controls within complex IT systems that support finance and accounting functions (Otero, 2015). Instead, skilled and qualified IT auditors are specifically trained to perform these tasks and provide valuable insights to enhance the effectiveness of controls and mitigate risks (Davis, Schiller, & Wheeler, 2016). The literature review and the study both emphasize that IT auditors play a vital role in assessing IT risks and controls, identifying vulnerabilities, and recommending improvements (IAASB, 2019). Their understanding of IT systems and controls allows them to bridge the gap between financial audit teams and IT systems, thereby enhancing the overall assurance process (Davis, Schiller, & Wheeler, 2016). This is crucial as AI technology introduces complexities and potential risks that require specialized IT knowledge to address adequately. The involvement of IT auditors is considered necessary to provide maximum assurance when identifying and testing the controls required to mitigate the risks to the integrity of financial records. The literature review supports this notion by

showing that IT auditors' inclusion in financial audits has been associated with successful detection of financial misstatements and manipulation of financial information (Otero, 2015). Their expertise in selecting and implementing appropriate digital controls tailored to the organization's needs effectively mitigates the risk of information manipulation or abuse (Borges et al., 2021). Embracing the role of IT auditors will strengthen the effectiveness of financial audits, leading to more reliable and trustworthy financial information within organizations (Borges et al., 2021). The consensus among the experts in the study supports this idea, emphasizing that the engagement of IT auditors is necessary to supplement the efforts of financial audit teams and provide maximum assurance when identifying and testing controls to mitigate the risks (IAASB, 2019). In short, the results of the study are in alignment with the literature review, which emphasizes the critical role of IT auditors in financial audit projects. The study reinforces the need for specialized IT knowledge and dedicated IT auditors to effectively identify and manage the risks associated with AI in financial audits. By leveraging their expertise, IT auditors contribute to the overall assurance process, ensuring that financial audits adequately address the complexities and risks associated with IT dependencies. Organizations that recognize the value of IT auditors and overcome the challenges of their involvement can strengthen the integrity and reliability of financial records and enhance the effectiveness of financial audits.

4.6. Expanding the Risk Horizon: Uncovering Additional Threats in the Ethical Realm of AI

This section presents the analysis and discussion of the final study conducted as part of the research interviews with experts. The objective was to explore whether the list of AI risks presented to the experts in the preceding questions captured the complete range of risks or if there were additional AI risks that they recognized as relevant for financial auditing. As AI technology continues to evolve, new risks and challenges emerge, and it is essential to stay abreast of the latest developments to ensure comprehensive risk assessment and mitigation strategies. By soliciting the insights and perspectives of the experts, this study aims to uncover any additional AI risks that may have been overlooked in the initial list, thereby enhancing our understanding of the complex landscape of AI risks in financial auditing. The subsequent discussion will delve into the key themes and perspectives identified, highlighting the additional AI risks deemed relevant for financial auditing by the experts. By incorporating the insights of the experts, this section aims to provide a more comprehensive and up-to-date assessment of the risks associated with AI technology, enabling auditors, accounting professionals, and policymakers to proactively address emerging threats and implement robust risk management strategies. Based on the answers provided by the experts, it can be concluded that the list of risks posed by AI that was presented to them is considered complete by the experts. They confirmed that all the risks listed are pertinent and should be taken into consideration when assessing

the impact of AI technologies. Additionally, one expert highlighted an additional risk that involves the lack of ethics and responsibility among individuals or programmers who intentionally develop AI programs to cause harm, mistrust, and spread false information. This highlights the importance of considering not only technical risks, but also ethical risks associated with AI development and deployment. The acknowledgement of this additional risk emphasizes the need for ethical considerations and responsible practices in the development and implementation of AI systems. It highlights the potential for malicious intent or unethical behaviour that can undermine the trust and reliability of AI technologies. In short, the list of risks presented to the experts was deemed complete and relevant. The inclusion of the risk related to the lack of ethics and responsibility underscores the importance of considering ethical considerations alongside technical aspects when working with AI. It serves as a reminder that the responsible development, deployment, and use of AI technologies are crucial to ensure the integrity, trustworthiness, and positive impact of AI systems in various domains.

Chapter 5 - Conclusions

In this chapter, the main findings of the research study are summarized, and the research objectives and questions are revisited. The chapter discusses the theoretical and practical implications of the research, emphasizing the contributions to the field of risk and IT auditing. Furthermore, it offers recommendations for future research in this area, acknowledging the potential for further exploration and development of the topic. This dissertation aimed to investigate the emerging risks of artificial intelligence in the context of financial auditing and develop mitigation strategies to address these risks. Through an analysis of relevant literature and interviews with experts in the field of risk assurance, the study successfully achieved its objectives and shed light on the implications of AI risks in financial auditing projects. The research conducted in this dissertation highlights the growing relevance and importance of AI auditing in the present and future. While AI auditing practices are not yet widely adopted, there is an increasing recognition of the need to address the unique challenges posed by AI systems. The research identified several AI risks that are relevant in the context of financial auditing, including data quality, data security, lack of expertise in AI, lack of human agency in AI processes, errors and biases in algorithms. Organizations need to proactively consider the implementation of AI auditing to ensure the integrity, accountability, and ethical use of AI systems. Addressing these risks is crucial for enhancing the accuracy, reliability, and trustworthiness of financial audit procedures in the AI era. The quantitative assessment of AI risks in financial auditing provides valuable insights into the perceived significance of different risks. By understanding the severity and frequency of these risks, financial auditors can better assess their impact on the reliability and trustworthiness of financial reports. Data security, errors and biases in algorithms, and data quality emerged as the most substantial risks. Experts' opinions underscore the significance of addressing these AI risks to safeguard

the accuracy and reliability of financial records while maintaining investor trust. AI risks encompass a range of challenges. Neglecting these risks can lead to severe consequences, directly impacting the integrity of financial data. Inaccurate or incomplete data used for AI projections can result in misleading financial statements and distorted financial performance representations. Additionally, data security risks pose a significant threat, with the potential for cyber attacks compromising AI systems and altering financial data. Such incidents can lead to the dissemination of incorrect information, unauthorized data access, and a loss of trust by investors and markets. Moreover, errors and biases in algorithms can introduce inaccuracies in financial calculations, potentially causing financial misrepresentations and misguided business decisions. Furthermore, the study explored various techniques that can be applied to mitigate these AI risks. These techniques encompassed robust data governance practices, rigorous testing and validation of AI algorithms, continuous monitoring and auditing of AI systems, and the adoption of frameworks in AI development and deployment. It is evident that mitigating AI risks in financial record-keeping requires a multi-faceted approach. Several tactics and strategies have been suggested to enhance the security, integrity, and accuracy of financial records. Firstly, organizations should analyse relevant systems through thorough assessments, risk evaluations, and security audits. This helps identify vulnerabilities, weaknesses, and areas for improvement. Implementation of various IT processes and controls is crucial to enhance data security and integrity. Monitoring procedures should be established to regularly assess the integrity of financial records. This involves continuous monitoring of data inputs, system logs, and alerts to detect anomalies or unauthorized activities. Data quality improvement procedures, such as data cleansing, normalization, and validation, should be implemented to ensure accurate and complete data for financial calculations. The reliability and accuracy of data used in financial records must be confirmed, including verifying its sources and conducting appropriate validation processes. Internal controls mechanisms, information security policies, and controls on the use of AI should be implemented across organizational structures. Each AI technology should be evaluated for its impact on data integrity, and appropriate controls should be implemented to mitigate risks. Review controls and compensatory controls are essential to validate financial data, calculations, and input data. Independent reviews, cross-checking, and verification of calculations help ensure accuracy and identify discrepancies or errors. Compensatory controls involve additional checks, reconciliations, or cross-referencing of data from multiple sources for consistency and reliability. To mitigate intrusion attacks, organizations should deploy defence mechanisms such as firewalls with Intrusion Detection Systems (IDS) and secure backups that are not susceptible to cyber-attacks. Action plans should be developed to respond to incidents based on severity. IT governance and security processes and controls should be established to enhance security robustness. Regular audits are recommended to assess the effectiveness of controls and identify areas for improvement. Engaging AI experts and specialists in programming and

development can provide specialized knowledge and insights to mitigate AI-related risks in financial record-keeping. Overall, organizations should establish key controls, review processes, structured development cycles, and engage in continuous improvement to enhance the integrity, accuracy, and compliance of financial records and mitigate AI risks effectively. Importantly, the research highlighted the growing importance of IT auditing in financial auditing projects. It emphasized that addressing AI risks is not solely a technical concern but also involves ethical considerations and responsible practices. The inclusion of an additional risk, as highlighted by experts, regarding malicious intent and unethical behaviour in AI development, underscores the need for vigilance and comprehensive risk management approaches. The findings of this study contribute to the field of financial auditing by raising awareness of the emerging risks posed by AI and providing practical insights into their mitigation. By implementing the recommended strategies, auditors can enhance their ability to detect and mitigate AI risks, ensuring the reliability and integrity of financial information. The involvement of IT auditors, with specialized IT knowledge, is critical in effectively auditing and analysing AI controls in financial audits. IT auditors bring a deep understanding of IT systems, processes, and security, allowing them to comprehensively assess controls and identify vulnerabilities. Their involvement is essential for a thorough examination of the IT infrastructure and ensuring maximum assurance in mitigating risks to the integrity of financial records. The research also emphasizes the need to expand the risk horizon and consider additional threats in the ethical realm of AI. Beyond technical risks, ethical considerations and responsible practices in AI development and deployment are crucial. This includes addressing risks associated with malicious intent and unethical behaviour. Responsible development, deployment, and use of AI technologies are essential for maintaining integrity, trustworthiness, and positive impact. The results of the studies presented in this research significantly contribute to the existing body of knowledge on AI risks in financial auditing. They shed light on specific aspects of AI adoption and its implications on financial integrity and investor trust, providing valuable insights for both academia and professionals in the field. Let's discuss how the results align with previous research and whether they confirm, contradict, or extend previous findings. Regarding the stage of AI adoption in companies, the findings align with the points highlighted in the literature review that AI adoption in the accounting industry is still in its infancy, and the current technologies being used do not fully represent the potential of AI. The results of the studies confirm this notion, as experts indicated that the use of AI technology in auditing is not yet widespread, and there is limited adoption of AI auditing practices within companies. In terms of specific AI risks relevant to financial audits, the studies contribute to the existing body of knowledge by addressing a gap in understanding. While previous research identified AI risks that could potentially impact accounting and finance, there was limited research specifically focusing on their implications on financial records and their relevance to financial audits. The studies' results confirm and extend previous findings by providing a comprehensive understanding of AI risks

that could affect the accuracy and integrity of financial records in the context of financial audits. The findings also extend previous research by exploring mitigation strategies for AI risks. Previous literature recognized the importance of addressing AI risks, but there was limited research on practical strategies to mitigate these risks in the context of financial audits. The studies' results contribute valuable insights and recommendations that can be utilized by auditors and risk professionals to effectively address and mitigate identified risks. Looking ahead, future research could focus on further exploring the ethical risks associated with AI development and deployment. This could involve investigating the impact of human bias and unfairness in AI decision-making processes, as well as exploring the development of ethical guidelines and regulatory frameworks specific to AI auditing. In summary, this dissertation underscores the importance of AI auditing, the identification of relevant risks, the quantification of risk significance, the implementation of mitigation strategies, the involvement of IT auditors, and the consideration of ethical dimensions. These findings contribute to the understanding of emerging AI risks in the context of financial audits and provide valuable insights for auditors, accounting professionals, and policymakers to develop robust risk management strategies in an AI-driven landscape.

Bibliography

Abduljabbar, R., Dia, H., Liyanage, S., & Bagloee, S. A. (2019). Applications of artificial intelligence in transport: An overview. Sustainability, 11(1), 189.

Accounting Today. (2020). What AI Does for Accountants. Retrieved May,2023 from https://www.accountingtoday.com/opinion/what-ai-does-for-accountants

Allen, R. D., Hermanson, D. R., Kozloski, T. M., & Ramsay, R. J. (2006). Auditor risk assessment: Insights from the academic literature. Accounting Horizons, 20(2), 157-177.

Arens, A. A., Elder, R. J., Beasley, M. S., & Hogan, C. E. (2017). Auditing and Assurance Services. Pearson.

Barta, G. (2018). The increasing role of IT auditors in financial audit: risks and intelligent answers. Business, Management and Education, 16(1), 81-93.

Borges, A. F., Laurindo, F. J., Spínola, M. M., Gonçalves, R. F., & Mattos, C. A. (2021). The strategic use of artificial intelligence in the digital era: Systematic literature review and future research directions. International Journal of Information Management, 57, 102225.

Bose, S., Dey, S. K. & Bhattacharjee, S. (2022). "Big Data, Data Analytics and Artificial Intelligence in Accounting: An Overview" in S. Akter and S. F.Wamba (Eds.) Handbook of Big Data Methods (pp.1-34). Edward Elgar Publishing

Brynjolfsson, E., & Mitchell, T. (2017). What can machine learning do? Workforce implications. Science, 358(6370), 1530-1534.

C. Zhu and Y. Guan, "The Risks and Countermeasures of Accounting Artificial Intelligence," 2022 3rd International Conference on Electronic Communication and Artificial Intelligence (IWECAI), Zhuhai, China, 2022, pp. 358-361, doi: 10.1109/IWECAI55315.2022.00076.

CMA Exam Academy. (2023). Artificial Intelligence in Accounting. Retrieved June,2023 from https://cmaexamacademy.com/artificial-intelligence-in-accounting/

Center for Internet Security. (2020). CIS Critical Security Controls Version 8.

Chang, S. I., Tsai, C. F., Shih, D. H., & Hwang, C. L. (2008). The development of audit detection risk assessment system: Using the fuzzy theory and audit risk model. Expert Systems with Applications, 35(3), 1053-1067.

Champlain, J. J. (2003). Auditing information systems. John Wiley & Sons.

Cheatham, B., Javanmardian, K., & Samandari, H. (2019). Confronting the risks of artificial intelligence. McKinsey Quarterly, 2(38), 1-9.

Davis, C., Schiller, M., & Wheeler, K. (2016). IT Auditing: Using Controls to Protect Information Assets. McGraw-Hill Education.

Deloitte. (2023). Riding the wave: Hot Topics for IT Internal Audit. Retrieved July ,2023 from https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/financial-services/deloitte-uk-deloitte-itia-hot-topic-report-digital.pdf

Esteva, A., Robicquet, A., Ramsundar, B., Kuleshov, V., DePristo, M., Chou, K., ... & Dean, J. (2019). A guide to deep learning in healthcare. Nature Medicine, 25(1), 24-29.

EY. (2018). Why AI is both a risk and a way to manage risk. Retrieved May,2023 from https://www.ey.com/en_gl/assurance/why-ai-is-both-a-risk-and-a-way-to-manage-risk

Floridi, L., & Cowls, J. (2019). A unified framework of five principles for AI in society. Harvard Data Science Review, 1(1).

Floridi, L. (2021). Artificial intelligence, deepfakes and a future of ectypes. Ethics, Governance, and Policies in Artificial Intelligence, 307-312.

Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep learning. MIT Press.

Gregory, P. H. (2019). CISA Certified Information Systems Auditor All-in-One Exam Guide (4th ed.). McGraw Hill Professional.

Hasan, A. R. (2021). Artificial Intelligence (AI) in accounting & auditing: A Literature review. Open Journal of Business and Management, 10(1), 440-465.

Hayes, R., Dassen, R., Schilder, A., & Wallage, P. (2019). Principles of Auditing: An Introduction to International Standards on Auditing. Pearson.

HunterSure. (2021). The Impacts of AI in Modern Accounting. Retrieved May,2023 from https://www.huntersure.com/the-impacts-of-ai-in-modern-accounting/

ICAEW. (2018). Artificial intelligence and the future of accountancy. Retrieved June, 2023 from https://www.icaew.com/-/media/corporate/files/technical/technology/thought-leadership/artificial-intelligence-report.ashx

ICAEW. (2020, March). The Risks of AI and How to Mitigate Them. Retrieved June,2023 from https://www.icaew.com/insights/features/2020/mar-2020/the-risks-of-ai-and-how-to-mitigate-them

ICO, U. (2020). Guidance on the AI auditing framework: Draft guidance for consultation.

Information Systems Audit and Control Association. (2018). COBIT® 2019 Framework: Introduction and Methodology. ISACA.

International Auditing and Assurance Standards Board (IAASB). (2018). ISA 220: Quality Control for an Audit of Financial Statements.

International Auditing and Assurance Standards Board (IAASB). (2019). ISA 315 (Revised 2019): Identifying and Assessing the Risks of Material Misstatement

ISACA.(2018).AuditingArtificialIntelligence.RetrievedApril,2023from https://ec.europa.eu/futurium/en/system/files/ged/auditing-artificial-intelligence.pdf

Johnstone, K. M., Gramling, A. A., & Rittenberg, L. E. (2017). Auditing: A Risk-Based Approach to Conducting a Quality Audit. Cengage Learning.

Kietzmann, J., Lee, L. W., McCarthy, I. P., & Kietzmann, T. C. (2020). Deepfakes: Trick or treat?. Business Horizons, 63(2), 135-146.

Leitner-Hanetseder, S., Lehner, O. M., Eisl, C., & Forstenlechner, C. (2021). A profession in transition: Actors, tasks and roles in AI-based accounting. Journal of Applied Accounting Research.

Luo, J., Meng, Q., & Cai, Y. (2018). Analysis of the impact of artificial intelligence application on the development of accounting industry. Open Journal of Business and Management, 6(4), 850-856.

Marr, B. (2018, November 19). Is Artificial Intelligence Dangerous? 6 AI Risks Everyone Should Know About. Forbes. Retrieved May, 2023 from

https://www.forbes.com/sites/bernardmarr/2018/11/19/is-artificial-intelligence-dangerous-6-ai-risks-everyone-should-know-about/

McKinsey Global Institute. (2018, September). Notes from the AI frontier: Modeling the impact of AI on the world economy. Retrieved May, 2023 from

https://www.mckinsey.com/~/media/McKinsey/Industries/Advanced%20Electronics/Our%20Insights/Notes%20from%20the%20AI%20frontier%20Modeling%20the%20impact%20of%20AI%20on%20the%20world%20economy/Notes-from-the-AI-frontier-Modeling-the-impact-of-AI-on-the-world-economy.pdf.

McKinsey & Company. (2019). Confronting the risks of artificial intelligence. Retrieved April, 2023 from https://www.mckinsey.com/capabilities/quantumblack/our-insights/confronting-the-risks-of-artificial-intelligence

Messier Jr., W. F., Glover, S. M., & Prawitt, D. F. (2017). Auditing and Assurance Services: A Systematic Approach. McGraw-Hill Education.

Nadimpalli, M. (2017). Artificial intelligence risks and benefits. International Journal of Innovative Research in Science, Engineering and Technology, 6(6).

Otero, A. (2015). Impact of IT auditors' involvement in financial audits. International Journal of Research in Business and Technology (ISSN: 2291-2118), 6(3), 841-848.

Otero, A. R. (2018). Information technology control and audit. CRC Press.

Parlak, K. (2023). Artificial Intelligence Auditing: Pros and Cons Reviewed [LinkedIn post]. Retrieved April, 2023 from https://www.linkedin.com/pulse/artificial-intelligence-auditing-pros-cons-reviewed-koray-parlak/

Petkov, R. (2020). Artificial intelligence (AI) and the accounting function—A revisit and a new perspective for developing framework. Journal of emerging technologies in accounting, 17(1), 99-105.

Radu, L. D. (2009). Qualitative, semi-quantitative and, quantitative methods for risk assessment: case of the financial audit. Analele Ştiinţifice ale Universităţii» Alexandru Ioan Cuza «din Iaşi. Ştiinţe economice, 56(1), 643-657.

Raewf, M. B., & Jasim, Y. A. (2020). Information technology's impact on the accounting system. Cihan University-Erbil Journal of Humanities and Social Sciences, 4(1), 50-57.

Rao, A. (2020). Five Views of AI Risk [Blog post]. Retrieved April,2023 from https://towardsdatascience.com/five-views-of-ai-risk-eddb2fcea3c2

Russell, S. J., & Norvig, P. (2010). Artificial intelligence: A modern approach. Prentice Hall.

Sage.(2018). The Practice of Now 2018 report . Retrieved June,2023 from https://www.sage.com/en-gb/-/media/files/company/documents/pdf/business%20builders/latest%20news/practice-of-now-report-2018.pdf

Sage.(2019). The Practice of Now 2019 report . Retrieved June,2023 from https://www.sage.com/en-gb/blog/practice-of-now/

Sage.(2020). The Practice of Now 2020 report . Retrieved May, 2023 from https://www.sage.com/en-us/blog/practice-of-now/

Senft, S., & Gallegos, F. (2008). Information technology control and audit. CRC Press.

Senft, S., & Gallegos, F. (2016). Information Technology Control and Audit. McGraw-Hill Education.

Tarantino, A. (2015). Audit Risk Model Handbook: Risk Assessment and Internal Control. Wiley.

Tegmark, M. (2017). Life 3.0: Being human in the age of artificial intelligence. Vintage.

Tsolakis, N., Schumacher, R., Dora, M., & Kumar, M. (2022). Artificial intelligence and blockchain implementation in supply chains: a pathway to sustainability and data monetisation?. Annals of Operations Research, 1-54.

Vasarhelyi, M. A., & Kogan, A. (1998). Artificial Intelligence in Accounting and Auditing: Towards New Paradigms, Volume 4.

Weber, R. A. (1998). Information systems control and audit. Pearson Education.

Weiss, M., & Solomon, M. G. (2015). Auditing IT Infrastructures for Compliance. Jones & Bartlett Publishers.

Wood, J., Brown, W., & Howe, H. (2013). IT Auditing and Application Controls for Small and Mid-Sized Enterprises: Revenue, Expenditure, Inventory, Payroll, and More.