

MGI

Mestrado em Gestão de Informação
Master Program in Information Management

A FRAMEWORK FOR LEVERAGING IT AUDIT USING ARTIFICIAL INTELLIGENCE

Ana Rita Oliveira Pinto

Dissertation

presented as a partial requirement to obtain the degree of Master in Information Management

NOVA Information Management School
Instituto Superior de Estatística e Gestão de Informação

Universidade Nova de Lisboa

NOVA Information Management School
Instituto Superior de Estatística e Gestão de Informação
Universidade Nova de Lisboa

A FRAMEWORK FOR LEVERAGING IT AUDIT USING ARTIFICIAL INTELLIGENCE

by

Ana Rita Oliveira Pinto

Dissertation presented as a partial requirement to obtain the degree of Master in information management, with specialization in Information System and Technologies Management.

Supervisor: Professor Doctor Vítor Duarte dos Santos, PhD, NOVA Information Management School

July, 2024

STATEMENT OF INTEGRITY

I declare that I have carried out this academic work with integrity. I confirm that I did not resort to plagiarism or any other form of misuse of information or falsification of results during the process of preparing this work. I further declare that I am aware of the Rules of Conduct and Code of Honor of NOVA Information Management School.

Ana Rita Oliveira Pinto

Oeiras, 15/07/2024

DEDICATION

I dedicate this thesis to all those who share a passion for knowledge and curiosity about audit, may this thesis inspire and contribute to our collective quest for understanding and improvement.

ACKNOWLEDGMENTS

I extend my deepest gratitude to my beloved family, especially my mother and grandparents, namely, Alexandra Oliveira, Rosalina Oliveira e José Alexandre Oliveira, for their unwavering love, support, and encouragement throughout my journey of completing this master's thesis. Your belief in my abilities and your continuous motivation have been my pillars of strength.

To my dear boyfriend, Diogo Encarnação, I am immensely grateful for your unwavering patience, understanding, and unquestionable support throughout this challenging academic endeavour. Your love and encouragement have been a constant source of inspiration and motivation.

I extend my sincere thanks to my friends that I made throughout my master's degree, but also, to my longtime friends for their camaraderie, understanding, and encouragement throughout this academic challenge. Your friendship and support have provided much-needed moments of respite, joy and amazing dinners, during intense periods of study.

Special thanks to my thesis advisor, Professor Vítor Duarte dos Santos, whose invaluable guidance, expertise, and unwavering commitment played a pivotal role in shaping this research. Your insightful feedback, encouragement, and dedication to excellence have significantly contributed to my academic growth and success.

Finally, I am grateful to *NOVA Information Management School* for providing the necessary resources and environment conducive to learning and research, enabling me to embark on this academic journey.

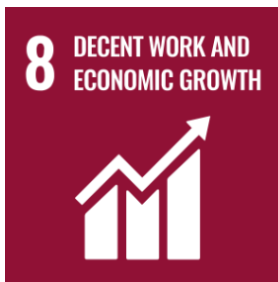
ABSTRACT

The integration of Artificial Intelligence (AI) in IT audit processes represents a transformative advancement in the field, promising enhanced efficiency, accuracy, and strategic insight. This thesis proposes a comprehensive framework designed to leverage AI in IT audit, aiming to streamline audit procedures, mitigate risks, and elevate audit quality. The framework encompasses various AI techniques, including machine learning, natural language processing, and robotic process automation, tailored to automate routine tasks, analyse vast datasets, detect anomalies, and predict risks. Key components of the framework include audit data analytics, AI-powered audit tools, and robotic process automation, facilitating real-time monitoring, proactive risk management, and adaptive audit strategies. Through case studies and theoretical analyses, this thesis explores the practical implementation and potential benefits of AI in IT audit, emphasizing its role in optimizing resource utilization, improving decision-making processes, and ensuring compliance with regulatory standards. The proposed framework serves as a strategic guide for organizations seeking to harness AI's capabilities to enhance IT audit effectiveness and adaptability in the digital age.

KEYWORDS

IT Audit; Artificial Intelligence; Methodologies; Decision support; Framework; Enterprises

Sustainable Development Goal (SDG):



INDEX

1	Introduction	1
1.1	Background and problem identification	1
1.2	Objectives	2
1.3	Importance and Relevance	2
2	Methodology	4
2.1	Design Science Research	4
2.2	Research implementation	6
3	IT Auditing Context	11
3.1	Overview	11
3.2	Local and global Regulation	11
3.3	Main enterprises Issues	13
4	Literature Review	15
4.1	IT Audit	15
4.1.1	Concepts	15
4.1.2	Main proposes	22
4.1.3	General Challenges and Opportunities	23
4.2	Artificial Intelligence	24
4.2.1	Core concepts	25
4.2.2	Key areas and approaches	26
4.2.3	Practical Applications	28
4.3	AI Technology in Auditing	34
4.3.1	PRISMA Methodology	34
4.3.2	PRISMA Execution	34
4.3.3	PRISMA results and analysis	44
5	Application of Artificial Intelligence in expediting IT Audit processes	51
5.1	Assumptions	51
5.2	Framework AROP	52
5.3	Strategy for the implementation of the AROP Framework in IT Audit	55
5.3.1	Strategy and Detailed Process Description	55
5.4	Use case – Demonstration	56
5.5	Evaluation & Discussion	59

6	Conclusions	62
6.1	Synthesis of the developed work	63
6.2	Limitations	64
6.3	Future work	65
	References	66
	APPENDIX A.....	70
	APPENDIX B.....	71
	APPENDIX C.....	73
	APPENDIX D.....	75

FIGURES INDEX

Figure 1: DSR Methodology Process Model (Peppers et al., 2008)	4
Figure 2: Design Science Research Framework (Hevner & Chatterjee, 2010).....	7
Figure 3: Drivers that shape IT audits and influence internal and external auditing.	12
Figure 4: IT audits prioritize internal controls, employing distinct methods.....	17
Figure 5: Examples of Internal Controls Categorized by Type and Purpose	17
Figure 6: IT audits, conducted from technical, operational, business/company viewpoints	19
Figure 7: AI opportunities in SMEs (adapted from Ulrich et al., 2021).	30
Figure 8: Most adopted AI use cases (adapted from Chui et al., 2021).....	31
Figure 9: Unstructured data extracted and formatted to CSV in excel	37
Figure 10: Sequence of data	37
Figure 11: Code for structuring data in sequences of 11.....	38
Figure 12: Code for structuring data in sequences of 9.....	39
Figure 13: PRISMA execution	40
Figure 14: Strategy and process for implementation of AI in IT Audit	56

TABLES INDEX

Table 1: DSR Methodology Process Model in the context of the research question	8
Table 2: Legal audit drivers - impact in organizational compliance and accountability, (Gantz, 2013).	12
Table 3: External and Internal Risks	18
Table 4: Technology-Related subject areas of focus to IT Audit.....	19
Table 5: Definition of Internal & External Audit, according to the international references	20
Table 6: Sources of External IT Audit Requirements in the USA.....	21
Table 7: Sources of External IT Audit Requirements in the European Union.	22
Table 8: General challenges and opportunities in the context of IT Audit.....	24
Table 9: AI Areas and Corresponding Methods & Algorithms, (Russel and Norvig, 2020).....	26
Table 10: Examples of AI Applications throughout the different industries	32
Table 11: Systematic Review's Research Questions	35
Table 12: Systematic Review's Keywords	35
Table 13: Systematic Review's Resource Databases.....	36
Table 14: Systematic Review's inclusion and exclusion criteria	36
Table 15: Summary of the PRISMA Output.....	40
Table 16: Framework	53
Table 17: Background and expertise of the professionals.....	59
Table 18: Expert Summarized Interview and points of view	60

LIST OF ACRONYMS AND ABBREVIATIONS

AGI	Artificial General Intelligence
AI	Artificial Intelligence
AROP	AI-Integrated-Audit and Review Optimization Process
CIS	Center for Internet Security
CNNs	Convolutional Neural Networks
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CSC	Cyber Security Controls
CYK	Cocke-Younger-Kasami algorithm
DSR	Design Science Research
EBA	European Banking Authority
ECPA	Electronic Communications Privacy Act of 1986
ENISA	European Union Agency for Cybersecurity
FISMA	Federal Information Security Management Act of 2002
GAAS	Generally Accepted Auditing Standards
GANs	Generative Adversarial Networks
GDPR	General Data Protection Regulation
GLBA	Graham–Leach–Bliley Act of 1999
HIPAA	Health Insurance Portability and Accountability Act of 1996
HITECH	Health Information Technology for Economic and Clinical Health
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
IS	Information System
ISACA	Information Systems Audit and Control Association
ISAE	International Standard on Assurance Engagements
ISO	International Organization for Standardization
IT	Information Technology
ML	Machine Learning

NER	Named Entity Recognition
NIS	Network and Information Systems
NIST	National Institute of Standards and Technology
NLG	Natural Language Generation
NLP	Natural Language Processing
OMB	Office of Management and Budget.
PCAOB	Public Company Accounting Oversight Board.
PCFG	Probabilistic Context-Free Grammar
PRISMA	Preferred Reporting Items for Systematic Reviews and Meta-Analyses
R&D	Research and Development
RNNs	Recurrent Neural Networks
RPA	Robotic Process Automation
SAP	Systems, Applications, and Products in Data Processing
SDG	Sustainable Development Goal
SEC	Securities and Exchange Commission
SLAM	Simultaneous Localization and Mapping
SMEs	Small and Medium-sized Enterprises
SOX	Sarbanes–Oxley Act of 2002
US	United States
VBA	Visual Basic for Applications

1 Introduction

1.1 Background and problem identification

Nowadays international and multinational companies are looking for ways to integrate Artificial Intelligence within their organization, specially where the volume of data is increasing rapidly, not allowing a possible and complete human analysis, in IT Audit it's the case, (Fedyk, A., Hodson, J., Khimich, N., & Fedyk, T. (2022)). In order to put an end to this paradigm, companies are investing in a transformative approach that integrates advanced technology into the traditional practices of information technology (IT) auditing. This innovation is also driven by the growing complexity and volume of data, coupled with the need to ensure data security, compliance, and operational efficiency. IT audit, traditionally conducted by auditors who review and assess an organization's IT infrastructure, policies, and controls, can greatly benefit from the capabilities of AI, (Bojorque, R., & Pesántez-Avilés, F. (2020).

One critical aspect of AI in IT audit is its ability to automate repetitive tasks and analyze vast datasets at a speed and scale that would be impossible for human auditors. Machine learning algorithms can detect anomalies, identify potential risks, and provide insights into areas of concern or improvement. By automating routine audit procedures, AI frees up auditors to focus on higher-value tasks such as strategy development and addressing complex IT issues. This not only enhances audit efficiency but also allows organizations to allocate resources more strategically, (Cangemi, M. P. (2016)).

Moreover, leveraging AI in IT audit can enhance the accuracy and effectiveness of audits. AI-driven tools can continuously monitor IT systems in real-time, identifying deviations from established norms and flagging potential security breaches or compliance violations promptly, (Karmańska, A. (2022)). This proactive approach helps organizations mitigate risks and respond swiftly to emerging threats.

In addition to this, another important aspect is Data Integration and Governance in the context of AI implementation for IT audit, since is a critical facet that requires meticulous attention. The successful utilization of AI technologies in this domain hinges upon the quality, security, and accessibility of data. Data integration and governance are of paramount importance, namely, *Data Quality*, the foundation of effective AI-driven IT audit lies in high-quality data. Inaccurate or incomplete data can lead to erroneous audit findings, compromising the entire process. Data quality assurance mechanisms, including data cleansing, validation, and verification, are imperative to ensure that auditing is accurate and has reliable information; *Data Security*, since Auditors deal with sensitive and confidential information, and any data breach can have severe consequences; lastly, *Data Accessibility*, accessibility to data, especially in real-time or near-real-time scenarios, is vital nowadays, since companies are constantly changing their processes. Timely access to data enables auditors to detect and respond to potential risks promptly.

Although companies are increasing their knowledge and experience by testing and researching new methods, that may help solve IT Audit paradigm, a critical gap is the need for standardized regulations and frameworks that address AI-specific auditing practices.

AI-driven IT audit methods introduce a level of complexity that differs significantly from traditional audit approaches. These complexities arise from the intricate algorithms, machine learning models, and vast datasets involved.

While many traditional audit frameworks exist, they may not comprehensively cover the unique challenges and opportunities presented by AI technologies. A clear set of industry-specific standards and best practices is essential to ensure that AI-powered audits are conducted uniformly and ethically across different organizations and sectors.

Also, this alignment enables companies to demonstrate compliance, reducing the risk of legal or financial repercussions stemming from non-compliance. Standardized regulations provide a structured approach for auditors to follow, ensuring that AI-based audits meet regulatory expectations.

The absence of such frameworks can lead to inconsistency, confusion, and potential misuse of AI in auditing, which may undermine the credibility and effectiveness of the entire process. These interrogations allow to formulize the following research question:

How to leverage IT Audit using AI?

1.2 Objectives

The main goal of the research is to propose a comprehensive framework for the application of Artificial Intelligence (AI) in expediting IT Audit processes. This framework will be meticulously designed to accommodate diverse methodologies, fostering adaptability and precision throughout the audit lifecycle. The core ambition is to significantly reduce audit duration while concurrently enhancing accuracy and efficiency. By harnessing AI technologies, this research aims to establish a unified approach that streamlines IT Audit procedures, ensuring timely and more reliable outcomes in alignment with industry standards.

In order to achieve this goal, the following intermediate objectives were defined:

- Framework for IT Audit Area;
- Study on Key AI Concepts and Practical Applications;
- Make a comprehensive Literature Review on AI Technology in Auditing
- Build strategy Proposal for the Utilization of Artificial Intelligence in IT Audit
- Validate the Proposed AI Strategy

1.3 Importance and Relevance

A framework for leveraging IT audit using artificial intelligence (AI) can have a profound and far-reaching impact on various aspects of our society, economy, scientific knowledge, and sustainable development goals.

The integration of AI into IT audit processes enhances efficiency and accuracy. This, in turn, can lead to cost savings and reduced operational risks for businesses. In the context of the economy, when organizations can ensure the security and integrity of their IT systems through AI-augmented audits, they are better positioned to attract investors, foster trust among customers, and drive economic growth, (Rodrigues, L., Pereira, J., da Silva, A. F., & Ribeiro, H. (2023)). The application of AI in IT audit can contribute to job creation, economic stability, and overall well-being. People's happiness can also be positively affected as they benefit from more efficient services and data protection measures, resulting in a sense of security and satisfaction, as well as the fact that employee's perform jobs that are more mentally rewarding.

The adoption of AI in IT audit can be a catalyst for scientific advancement and the accumulation of knowledge. As AI systems analyse vast datasets and identify patterns or anomalies, they can uncover insights and trends that human auditors might miss, (Tiwari, R. (2023)). These discoveries can have implications beyond auditing, feeding into broader scientific research and contributing to our understanding of complex systems. Additionally, the continuous refinement of AI algorithms for IT audits necessitates ongoing research and development in the fields of computer science and artificial intelligence. This fosters a virtuous cycle of innovation and knowledge creation, pushing the boundaries of what AI can achieve and expanding our collective scientific understanding.

Furthermore, this research topic also covers an essential part to our society globally, namely the 8th Sustainable Development Goal: *"Decent work and Economic Growth"*, due to the fact that by answering the topic, there's a contribute to: *"higher levels of economic productivity through diversification, technological modernization, and innovation, including a focus on high-value-added sectors"*; *"Sustaining per capita economic growth"*; and *"Promote development-oriented policies that support productive activities, the creation of decent employment, entrepreneurship, creativity, and innovation"*, (United Nations. (n.d.). Goal 8: Decent work and economic growth).

2 Methodology

The chosen methodology is the Design Science Research, since is a research methodology that focuses on the development and creation of innovative artifacts to solve real-world problems, so the primary goal is to create a practical and applicable solution rather than just gaining theoretical knowledge.

In Design Science Research, the creation of an artifact is a central element, and this artifact can often take the form of a framework. A framework, in this context, is a structured and conceptual representation that serves as a foundation for solving a particular problem or addressing a set of related problems. In this case, the framework is going to cover how to leverage IT audit with AI.

2.1 Design Science Research

Design Science Research methodology process model, developed by Peffers and his colleagues, provides a systematic framework for conducting design science research. The DSR methodology has 6 key phases as it can be seen in figure 1, (Peffers, Ken & Tuunanen, Tuure & Rothenberger, Marcus & Chatterjee, S.. (2007)).

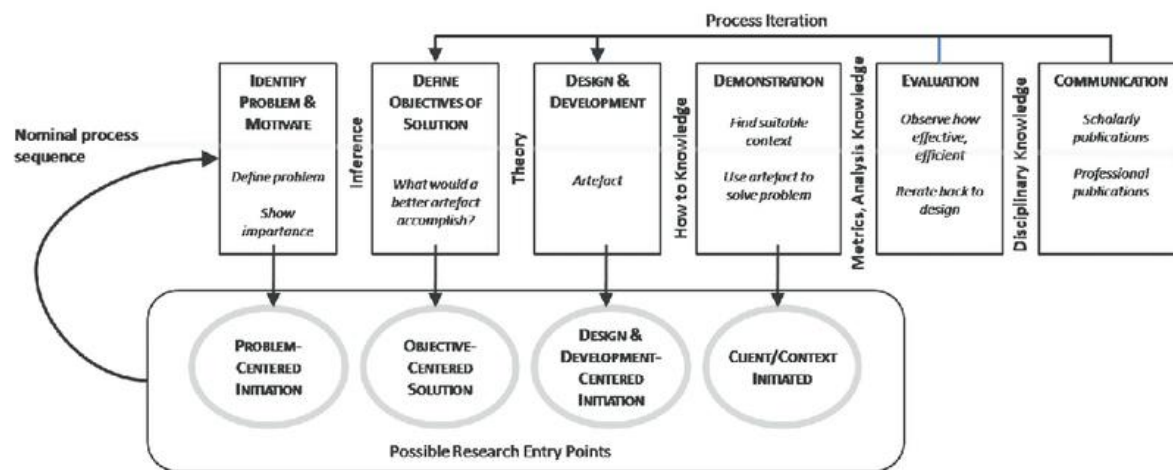


Figure 1: DSR Methodology Process Model (Peffers et al., 2008)

Following the identification of a problem and the formulation of corresponding objectives for a solution, the subsequent phase involves the creation of an artifact. This pivotal step necessitates the utilization of pre-existing theories or the formulation of new theories guiding the development of an artifact specifically tailored to effectively address the defined problem, (Peffers, Ken & Tuunanen, Tuure & Rothenberger, Marcus & Chatterjee, S.. (2007). Subsequently, the crafted artifact undergoes a demonstration within the problem context, where it is rigorously tested to ascertain its proficiency in resolving the given problem. This evaluation phase may encompass various methodologies such as experimental studies, simulations,

or case studies, providing a comprehensive understanding of the artifact's capabilities, (Peppers, Ken & Tuunanen, Tuure & Rothenberger, Marcus & Chatterjee, S.. (2007).

Upon completion of the demonstration and testing, a thorough evaluation is undertaken, drawing insights and lessons from the process. This evaluation serves as a foundation for iterative improvements to the artifact, ensuring its continuous enhancement based on acquired knowledge, (Peppers, Ken & Tuunanen, Tuure & Rothenberger, Marcus & Chatterjee, S.. (2007).

In the final phase, the generated knowledge is communicated to relevant stakeholders and the wider community. This dissemination of insights, findings, and the refined artifact contributes to the collective understanding of the addressed problem and potential solutions, fostering collaboration and advancement in the respective field, (Peppers, Ken & Tuunanen, Tuure & Rothenberger, Marcus & Chatterjee, S.. (2007).

Below, the DSR phases are presented.

Phase 1: Problem Identification and Motivation

- Objective: Clearly identify and understand the problem that the research aims to address. Articulate the significance and motivation for solving this problem.
 - Activities:
 - Identify the problem domain.
 - Assess the relevance and importance of the problem.
 - Understand existing solutions and their limitations.

Within the whole iteration process, which is defined by 5 different phases, its objective is to go through iterative cycles of the DSR process to refine and improve the artifact; while incorporating feedback and lessons learned into the artifact, as well as consider changes based on evolving requirements or new insights.

Phase 2: Define the Objectives for a Solution

- Objective: Establish the goals and objectives for the design and development of a solution (artifact) to address the identified problem.
 - Activities:
 - Formulate specific objectives for the research.
 - Define the scope and boundaries of the solution.

Phase 3: Design and Development

- Objective: Develop the artifact (solution) that can effectively address the identified problem.
 - Activities:
 - Design the conceptual model for the artifact.
 - Develop the actual artifact (e.g., a framework, system, or methodology).
 - Ensure that the artifact aligns with the defined objectives.

Phase 4: Demonstration

- Objective: Present and demonstrate the capabilities and functionalities of the developed artifact.
 - Activities:
 - Showcase how the artifact works.
 - Illustrate its potential in addressing the identified problem.
 - Provide evidence of the artifact's effectiveness.

Phase 5: Evaluation

- Objective: Assess the effectiveness and impact of the developed artifact and reflect on the design and development process, considering what worked well and what could be improved.
 - Activities:
 - Define evaluation criteria and metrics.
 - Evaluate the artifact against these criteria.
 - Gather feedback from stakeholders.
 - Analyze the outcomes of the research.
 - Identify lessons learned.
 - Consider implications for future research or iterations.

Phase 6: Communication

- Objective: Clearly communicate the research process, outcomes, and implications.
 - Activities:
 - Document the research in a comprehensive manner.
 - Publish research findings in academic journals or conferences.
 - Share insights with the academic and practitioner communities.

2.2 Research implementation

Within the context of this master thesis, the identification of the problem is encapsulated in the carefully crafted research question, “*How to leverage IT Audit, using AI?*”, while the corresponding objectives have been delineated in chapter 1.2.

In the initial stages of the research, it became apparent that there were insufficient theoretical frameworks providing a robust foundation for the creation of an innovative artifact. Consequently, a critical step in this master thesis involves the development of theoretical frameworks, forming a solid basis for the subsequent design of the artifact.

The importance of theorizing in this context is underscored by its role in facilitating the creation of an artifact that is not only innovative but also rooted in a theoretical underpinning. The absence of pre-existing frameworks necessitates a deliberate effort to conceptualize and develop theories that guide the design process, ensuring that the resulting artifact is both effective and aligned with the objectives set forth.

To shed light on the interplay between the creation of the artifact, the existing knowledge base, and the problem context, Hevner's graphic is referenced in figure 2. This graphic provides a valuable perspective on the Design Science Research (DSR) approach, emphasizing the dynamic interaction between building the artifact, the knowledge base, and the specific requirements highlighted by the problem context. The environment, representing the needs a solution must address, serves as a guiding force, while the knowledge base offers insights into existing foundations and methodologies available for application to the identified problem.

As the research progresses, this integrated approach ensures that the theoretical frameworks developed contribute not only to the creation of the artifact but also to the overall understanding of the problem within its broader context. This iterative process aligns with the principles of DSR, fostering a symbiotic relationship between theory and practice in the pursuit of a comprehensive and effective solution.

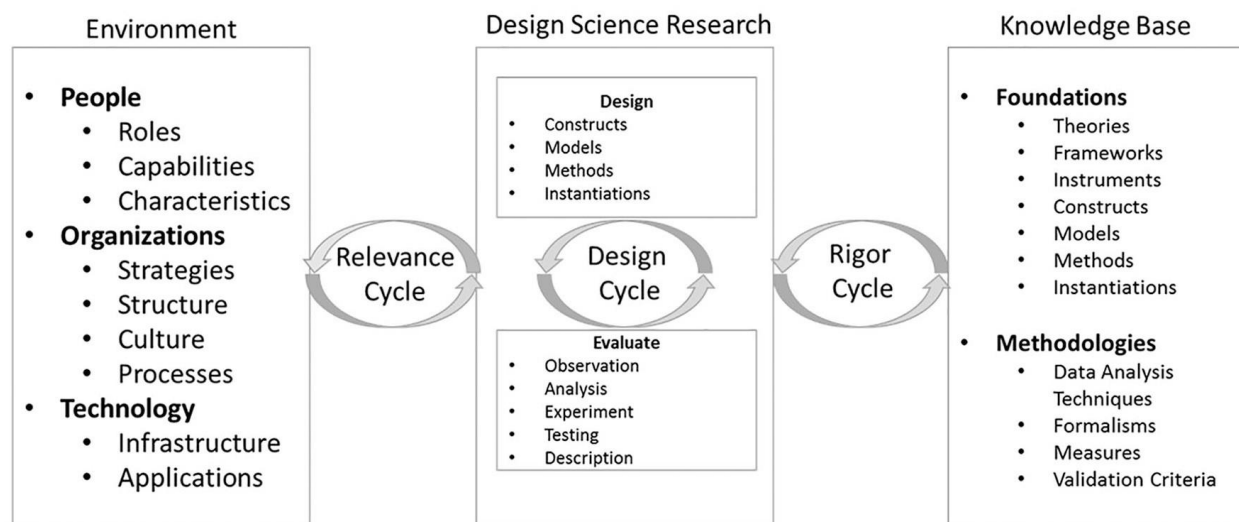


Figure 2: Design Science Research Framework (Hevner & Chatterjee, 2010)

The Design Science Research Framework (DSR) framework by Hevner, (figure 2), provides a structured methodology for creating and evaluating artifacts in the field of Information Systems. The process involves several key steps, and applying the DSR framework to construct an artifact follows a systematic approach, but its main objective is to ensure that the construction of the artifact is a well-grounded, systematic, and iterative process, aligning with the principles of design science research.

Figure 2 illustrates the encompassing influence of the environment, delineating issues within the area of interest. Noteworthy components within this environment include people, organizations, and technology, each mutually impacting the others. The people domain encompasses crucial roles, capabilities, and characteristics; organizations involve strategies, structure & culture, and processes; technology relevance is found in infrastructure, applications, communication architecture, and development capabilities. These interdependencies provide valuable insights for the researcher, guiding considerations for future research endeavours.

The information system (IS) research unfolds in two phases: development/build and justify/evaluate. Behavioural science elucidates through development and justification, while design science progresses

through building and evaluation, aligning with the multifaceted demands of the environment. The overarching goals are the attainment of truth and utility. The knowledge base comprises foundational elements and methodologies. The foundation encompasses theories, frameworks, instruments, constructs, models, and methods, utilized during the development, and build phases. On the other hand, methodologies, including data analysis, techniques, formalisms, measures, and validation criteria, come into play during the justifying and evaluating phases (Hevner et al., 2004).

Table 1: DSR Methodology Process Model in the context of the research question

Phase	Objectives and Activities
Phase 1 – Problem Identification and Motivation	The phase 1, T corresponds to the identified question in the chapter, specifically, "<i>How to Leverage IT Audit using AI.</i>" The primary motivation is to address not only the creation of more sustainable methods for the field, but also the development of a framework that takes into account ongoing technological advancements. Additionally, the framework aims to consider the various aspects of a comprehensive audit that encompasses AI and its facets. The goal is to provide a solution that goes beyond immediate challenges, ensuring adaptability to evolving technologies and encompassing the diverse elements inherent in a thorough AI-integrated audit.
Phase 2 – Define the Objectives for a Solution	In Phase 2, fundamental objectives are outlined for the framework, aiming to address the identified question. In addition to constructing the framework, it is crucial to consider the various aspects of AI and IT audit, the challenges encountered, opportunities for enhancement, and how an innovative framework will be presented to fulfill its purpose. This involves a comprehensive exploration of the intersection between AI and IT audit, a thorough examination of challenges, and an identification of areas for improvement. The overarching goal is to articulate an innovative framework that not only acknowledges the complexities but also effectively addresses the evolving landscape of AI in IT auditing.
Phase 3 – Design and Development	In Phase 3, the spotlight shifts to the framework itself, portraying its development and articulating solutions in alignment with the diverse objectives outlined in Phases 1 and 2. This phase encapsulates the realization and implementation

	of the framework, illustrating how it effectively addresses the identified question and fulfills the fundamental goals set forth in the preceding phases. From the conceptualization and design to the practical application, Phase 3 serves as the narrative of the framework's journey, offering insights into its evolution and the tangible solutions it brings to the fore in response to the challenges and opportunities identified earlier. Additionally, in the design and development of the framework, Hevner's theory will be applied. This entails leveraging Hevner's guidelines and principles to inform and guide the systematic construction and structuring of the framework. By incorporating Hevner's theoretical framework, the development process will be characterized by a methodical and principled approach, ensuring that the resulting framework aligns seamlessly with the overarching goals and objectives established in earlier phases. This application of Hevner's theory contributes not only to the theoretical robustness of the framework but also to its practical effectiveness in addressing the intricate intersection of AI and IT audit challenges.
Phase 4 – Demonstration	Phase 4, the demonstration phase, involves presenting data that substantiates the effectiveness and tests the validity of the created framework. This pivotal stage includes showcasing real-world examples, empirical evidence, and practical applications to validate the framework's ability to address the outlined objectives. Through concrete data, this phase aims to illustrate how the framework performs in diverse scenarios, providing tangible proof of its efficacy in leveraging AI for IT audit purposes. The demonstration serves as a crucial step in establishing the credibility and reliability of the framework in real-world contexts.
Phase 5 – Evaluation	In Phase 5, the proposed metrics for the defined objectives are assessed. This stage involves a comprehensive evaluation of the established metrics to gauge their effectiveness in measuring the success and impact of the framework. Through careful analysis, the chosen metrics are scrutinized against predefined criteria, ensuring they align with the overarching goals set in the earlier phases. The evaluation process in Phase 5

	provides critical insights into the framework's performance, allowing for adjustments and refinements to optimize its ability to meet the established objectives in leveraging AI for IT audit.
Phase 6 – Communication	The final phase is aimed at communicating results and insights that facilitate the evolution of the field. In this conclusive stage, the focus is on effectively disseminating the outcomes achieved through the framework. This involves presenting tangible results, lessons learned, and valuable insights gained during the entire process. By sharing these findings, the aim is not only to demonstrate the impact of the framework but also to contribute to the broader knowledge base of the field, fostering continuous improvement and evolution. The emphasis in this ultimate phase is on transparently communicating the framework's outcomes, with the intent to inspire advancements and further innovation in the intersection of AI and IT audit.

3 IT Auditing Context

In the dynamic landscape of modern business, the critical role of Information Technology (IT) and its security cannot be overstated. As organizations increasingly rely on advanced technological infrastructures and digital processes, the significance of effective IT Auditing has become paramount. In the face of ever-evolving cyber threats, stringent regulatory frameworks, and the rapid pace of technological advancements, businesses find themselves navigating a complex terrain where the assurance of robust IT controls is imperative. This introduction delves into the current needs of companies concerning IT Auditing, exploring the pressing challenges, and emerging opportunities that shape the strategic focus of organizations in safeguarding their digital assets and ensuring the integrity of IT processes.

3.1 Overview

IT audit in Europe and on the international stage plays a pivotal role in ensuring the robustness and security of digital infrastructures. In Europe, as well as globally, the increasing complexity of technology landscapes and the surge in cyber threats have elevated the significance of IT audits. These audits encompass a spectrum of critical areas, including cybersecurity, data privacy compliance, and the governance of emerging technologies such as artificial intelligence.

Key needs in IT audit revolve around adapting to evolving regulatory frameworks, addressing the shortage of skilled professionals with expertise in emerging technologies, and ensuring the resilience of organizations against sophisticated cyber threats. Moreover, with the rise of digital transformation initiatives, there is a growing demand for audits that align IT strategies with overall business objectives, emphasizing the need for continual improvement and adaptability in the face of dynamic technological advancements and regulatory landscapes.

3.2 Local and global Regulation

The regulatory landscape shaping IT audit activities is extensive and varies significantly across sectors, industries, and nations. Generally encompassing financial management, accounting, organizational governance, and information security, laws and regulations necessitate diverse compliance efforts. Organizations navigate this complex framework through centralized compliance programs or internal auditing initiatives.

Key legal and regulatory drivers include requirements for privacy protection, IT management, and financial accountability, as stated in figure 3.

Numerous factors propel the necessity for IT audits, shaping the methodologies in both internal and external auditing for organizations. Evolving technology, regulatory compliance, data security concerns, and the increasing complexity of IT systems are pivotal drivers. Internal audits focus on organizational

governance, risk management, and compliance, while external audits assess financial accuracy and compliance with industry standards. The synergy of these factors compels organizations to continually adapt their audit approaches to ensure the integrity and security of their IT environments, (Arena, Marika & Azzone, Giovanni, 2009).

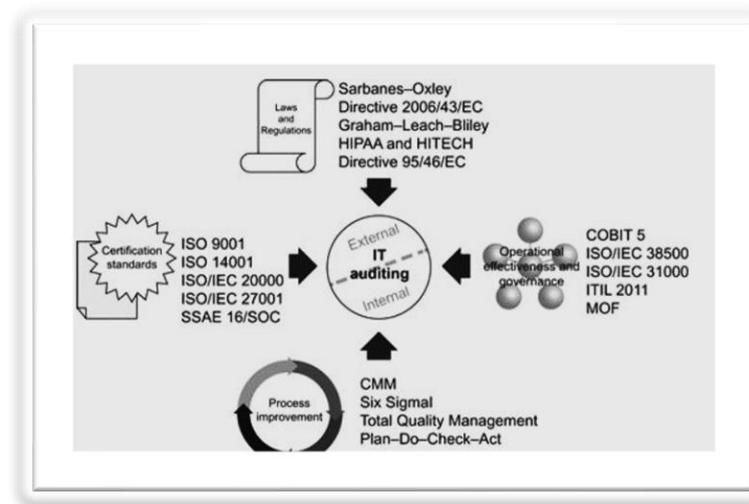


Figure 3: Drivers that shape IT audits and influence internal and external auditing.

While no international laws universally apply, notable commonalities exist in the United States, the European Community, and other industrialized nations like China, Japan, India, Canada, Australia, and Russia.

Table 2, encapsulates major laws, delineating their applicability across sectors and subject matters. This intricate regulatory tapestry underscores the imperative for organizations to maintain awareness and compliance, tailored to their specific operational contexts, (Gantz, 2013).

- United States and Europe:

Table 2: Legal audit drivers - impact in organizational compliance and accountability, (Gantz, 2013).

Law	Applicability
Sarbanes–Oxley Act of 2002 (SOX)	Regulates public companies and their auditors; applies to all issuers of securities exchanged in US markets.
European Council Directive 2006/43/EC	Sets standards for auditors and audits in the public interest; applies to organizations subject to statutory audit requirements.

• Graham–Leach–Bliley Act of 1999 (GLBA)	Enabled consolidation of different types of financial services firms within a single holding company; applies to financial institutions
• Health Insurance Portability and Accountability Act of 1996 (HIPAA)	Protects the privacy and security of health-related personal information; applies to health-care providers, plans, and clearinghouses.
• Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH)	HIPAA-covered entities, business associates, and contractors and subcontractors.
• European Council Directive 95/46/EC	Protects personal data privacy; applies to all organizations in European Union countries.
• Computer Fraud and Abuse Act of 1986	Criminalizes unauthorized access or damage to protected computers; applies to all computing devices used in interstate or international commerce or communications.
• Electronic Communications Privacy Act of 1986 (ECPA)	Protects the content of personal communications; applies to electronic communications service providers, government organizations.
• Federal Information Security Management Act of 2002 (FISMA)	US federal executive agencies; applies to systems and information operated by the government or on the government's behalf.
• The Privacy Act of 1974	US federal executive agencies; protects personally identifiable information for US citizens and legal resident aliens.
• State Privacy and Security Breach Notification Laws	Requires protection of personal information about state residents; in many states laws apply to organizations operating within or outside state borders whose customers include state residents.

3.3 Main enterprises Issues

IT audits play a crucial role in safeguarding enterprises against a myriad of challenges. From cybersecurity vulnerabilities and data privacy concerns to the complexities of managing diverse technology infrastructures, organizations face a host of issues that demand meticulous scrutiny. This introduction sets the stage for exploring the main enterprise issues in IT audit, delving into the intricacies of cybersecurity risks, regulatory compliance, technology complexities, and more. Navigating these challenges requires a proactive and comprehensive approach, ensuring the resilience and security of enterprise IT environments.

Cloud Security is one of the main issues of enterprises, nowadays, since the widespread adoption of cloud computing introduces new complexities in ensuring the security and compliance of data stored in the cloud. IT audits need to expand their focus to include thorough assessments of cloud security measures, data encryption, and adherence to regulatory standards in cloud environments.

Another concern for enterprises is the **security risks in AI Systems**, which includes identifying vulnerabilities and safeguarding against potential security threats in AI algorithms and integrating robust cybersecurity measures within AI development and deployment processes.

Change Management and System Updates, since companies have a hard time implementing and ensuring prompt application of updates and patches to mitigate security risk.

Data Privacy and Compliance, which is transposed to stringent data protection regulations and compliance complexities, due to the emerging technologies and lack of knowledge on how to adhere to data privacy laws and regulatory standards.

Vulnerabilities and insider threats, that emerge in the rapidly evolving technological environment, which can only be solved by continuous assessment of security measures, threat intelligence, and proactive defence mechanisms.

4 Literature Review

This literature review is systematically structured into four key sections to offer a comprehensive examination of the research topic.

The first section addresses IT audit, detailing its processes and practical applications to underscore its role; the second section explores artificial intelligence, focusing on its main purposes and practical applications in various fields; the third section integrates IT audit and AI, examining their synergistic potential and combined practical applications; and the final section discusses the PRISMA methodology, elucidating its importance and implementation in conducting systematic reviews. Each section provides a thorough analysis, supported by relevant academic and practical insights.

4.1 IT Audit

IT Audit is a crucial discipline that ensures the integrity, confidentiality, and availability of an organization's IT systems and data. This chapter delves into the principles and practices of IT auditing, exploring how it assesses the effectiveness of IT controls, compliance with regulations, and the alignment of IT strategies with business objectives, by examining various methodologies, standards, and frameworks, this chapter aims to provide a comprehensive understanding of IT audit processes, including the integration of advanced technologies and their impact on audit efficiency and accuracy. This foundation will set the stage for a deeper exploration of the evolving landscape of IT auditing.

4.1.1 Concepts

- What is IT Audit?

According with the *International Organization for Standardization*, (ISO), guidelines, an Audit is defined as a systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled”, (Durham, NC: American Institute of Certified Public Auditors, 2013).

IT Audits inherently rely on established baselines or standards for comparison against the subject under scrutiny. The comparison has a wide range and determines, whether is an auditing processes, systems, components, software, or entire organizations, the focus remains on explicit comparisons to predetermined standards. The objective is clear: auditors assess whether the subject meets the established criteria, ensuring a systematic evaluation grounded in specific benchmarks, (Gantz, 2013).

Audit determinations exhibit a binary nature distinct from other assessment types. Items within an audit either align with or deviate from specified requirements. Auditors typically express findings in terms of controls' adherence or nonconformity to established criteria, (*ISO 19011:2011. Guidelines for auditing management systems. (n.d.)*). These findings spotlight deficiencies arising when observed actions or

evidence analysis diverge from anticipated or mandated standards, rendering the audit subject incapable of meeting a given requirement. The emphasis lies on the stark contrast between compliance and noncompliance, creating a clear-cut evaluation framework in the audit process.

External audits adhere to rules, legal mandates, or regulatory requirements aligned with the audit's purpose and objectives. In contrast, internal audits afford organizations flexibility, enabling them to define their baselines or adopt standards, frameworks, or requirements set by external entities. This adaptability in internal audit baselines allows organizations to align evaluations with specific needs or industry best practices while maintaining a structured approach to assess and enhance their IT governance and security measures.

- Controls

Controls play a pivotal role in the realm of IT management, serving as a foundational component outlined and cited in various standards, guidance documents, methodologies, and frameworks that encompass diverse facets such as business processes, service delivery, management, information systems design, implementation, operation, information security, and IT governance. These controls collectively form a structured framework for ensuring the effectiveness, efficiency, and security of IT environments, (Institute, 2007).

When approaching the planning and execution of IT audits, internal controls emerge as the essence of auditing endeavours. These controls serve as the main points subjected to examination, testing, analysis, and various evaluative measures. In the context of IT audits, internal controls constitute the pivotal elements that undergo comprehensive assessment to ascertain their effectiveness and adherence to established standards and practices.

In IT audit practices, and legislative guidelines, prevalent categorization schemes organize controls based on their purpose, functional type, or a combination of both. Purpose-driven classifications encompass preventive, detective, and corrective controls, where preventive measures aim to forestall undesired events, detective controls unveil occurrences, and corrective controls respond to and recover from unwanted incidents. Function-based divisions further segregate controls into administrative, technical, and physical types. Administrative controls consist of organizational policies and procedures safeguarding operational integrity. Technical controls involve mechanisms and technologies implemented to achieve control objectives, while physical controls pertain to provisions regulating access to facilities and information assets. This comprehensive structure, illustrated in figure 4, delineates the multifaceted nature of controls within internal control frameworks. Figure 5 offers examples of internal controls, mapping each control type and purpose combination.



Figure 4: IT audits prioritize internal controls, employing distinct methods

	Preventive	Detective	Corrective
Administrative	Acceptable use policy; Security awareness training	Audit log review procedures; IT audit program	Disaster recovery plan; Plan of action and milestones
Technical	Application firewall; Logical access control	Network monitoring; Vulnerability scanning	Incident response center; Data and system backup
Physical	Locked doors and server cabinets; Biometric access control	Video surveillance; Burglar alarm	Alternate processing facility; Sprinkler system

Figure 5: Examples of Internal Controls Categorized by Type and Purpose

- Risk Analysis and Mitigation:

Risk analysis and mitigation is an essential process to the entity's success. It includes identification of the key business processes where potential exposures of some consequence exist, as well as significant changes to those processes. Once the significance and likelihood of risk have been assessed, management considers how the risk should be managed. This involves judgment based on assumptions about the risk, and reasonable analysis of costs associated with reducing the level of risk. Necessary actions are taken to reduce the significance or likelihood of the risk occurring, and identification of the control activities

necessary to mitigate the risk, (Service Trust Portal, n.d.). In table 3, (Service Trust Portal, n.d.) stated below, are some examples of internal and external risk factors:

Table 3: External and Internal Risks

External Risks	Internal Risks
Technological developments.	Significant changes in policies, processes, or personnel.
Changing customer needs or expectations.	Types of fraud.
Competition that could alter marketing or service activities.	Fraud incentives and pressure for employees.
New legislation and regulation that could force changes in policies and strategies.	Employee attitudes and rationalizations for fraud.
Natural catastrophes that could lead to changes in operations or information systems.	A disruption in information systems processing
Economic changes that could have an impact on management decisions	The quality of personnel hired, and methods of training utilized.
Threats from malware including ransomware.	Changes in management responsibilities.

- Main areas or processes within the organization that are subject to audit:

IT audits can have a broad spectrum of evaluations, ranging from comprehensive assessments of entire organizations to in-depth individual business units, functions, business processes, services, systems, infrastructure, or specific technology components. This versatile approach ensures a thorough and professional examination of various facets within the IT landscape, allowing for targeted insights and recommendations to enhance overall efficiency and compliance. IT audits invariably address one or more technology-related subject areas, including controls related to the following, in table 4:

Table 4: Technology-Related subject areas of focus to IT Audit

Technology-Related Subject Areas
• Data Centers and other Physical facilities • Network Infrastructure • Telecommunications • Operating Systems • Databases • Storages/Backups • Application Systems/Tools • Virtualized Servers and environments • Cloud/AI Algorithms, Blockchain/Platforms • Outsourced services and operations • Web and application servers • Software and Package applications • User and application interfaces • Mobile devices

In IT audits, a meticulous focus is placed on internal control processes and functions, encompassing operations and maintenance procedures, business continuity and disaster recovery protocols, incident response mechanisms, network and security monitoring practices, configuration management, system development life cycle, and project management. This comprehensive approach ensures a thorough examination of critical aspects promoting robust governance and risk management, as seen in figure 6.

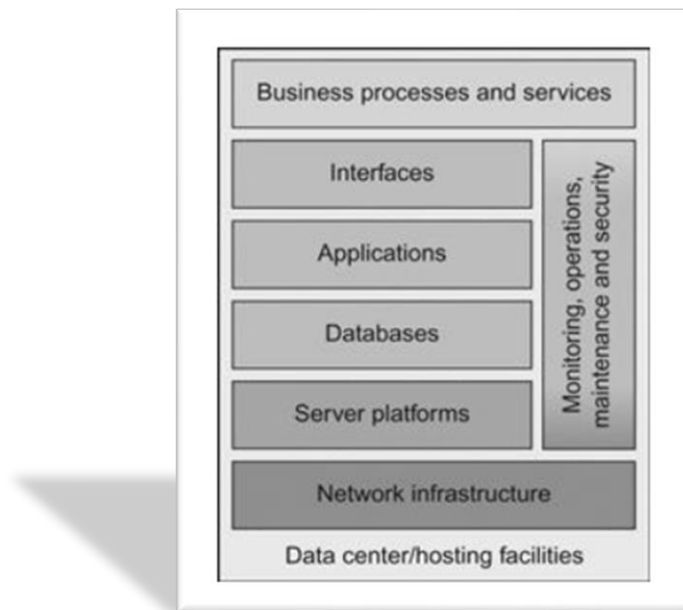


Figure 6: IT audits, conducted from technical, operational, business/company viewpoints

- Internal and External audit:

Table 5: Definition of Internal & External Audit, according to the international references

Internal Audit	External Audit
The Committee of Sponsoring Organizations of the Treadway Commission (COSO) defines internal control as a process “ <i>designed to provide reasonable assurance regarding the achievement of objectives</i> ” including operational effectiveness and efficiency, reliable reporting, and legal and regulatory compliance, (Committee of Sponsoring Organizations of the Treadway Commission. Internal control—Integrated framework. New York (NY): Committee of Sponsoring Organizations of the Treadway Commission; 2013).	External audits are performed by outside auditors and auditing firms; and the standards, requirements, or other audit criteria used in external audits are defined outside the organization being audited. Some standards bodies and professional associations further divide external auditing into second-party and third-party audits, the former conducted by customers or suppliers or others with an interest in the operations of the subject organization and the latter conducted by independent organizations with no direct interest in the organization undergoing the audit, (Gantz, 2013).

- IT Auditing Characteristics:

Definitions, standards, methodologies, and guidance universally align on fundamental characteristics intrinsic to IT audits, rooted in Generally Accepted Auditing Standards (GAAS) and international codes of practice.

These shared principles emphasize the necessity for auditors to possess proficiency and critical thinking relevant to their audit, adhere to ethical and professional codes, and maintain auditor independence, (*American Institute of Certified Public Accountants, Auditing Standards Board, 2001; Gantz, 2013*). Proficiency extends to encompass general principles, procedures, standards, and expectations, applicable across IT auditing. Depending on the complexity of IT controls or the operational context under scrutiny, auditors may necessitate specialized knowledge. Codes of conduct, prevalent in auditing, underscore principles like integrity, objectivity, competency, confidentiality, and adherence to standards, (Code of Ethics, The Institute of Internal Auditors, 2013; Code of Professional Ethics, ISACA, 2013).

The Auditor independence is vital in both internal and external audits, mandates that auditors and their affiliated organizations maintain impartiality, free from financial interests or conflicts of interest concerning the audited entities. This principle, enshrined in GAAS and international standards, holds legal significance in public corporations under the Sarbanes–Oxley Act, enforced by the Securities and Exchange Commission (SEC).

- Importance of IT Auditing in the context of enterprises and entities that are subjected to IT Auditing:

Given the widespread integration of Information Technology (IT) across diverse organizations, ranging in size and industry, the establishment and maintenance of internal IT audit programs are increasingly valuable. Organizations of all types can reap significant benefits from these programs, ensuring the effective management and security of IT resources. Internal IT audits serve as proactive measures,

enabling businesses to enhance their IT governance, identify potential risks, and optimize operational efficiency, (Gantz, 2013).

When it comes to external IT auditing, the landscape may vary. Some organizations might not have the autonomy to decide whether, how, or when to undergo external IT audits, as certain forms of external audits are legally mandated, leaving little room for choice. For instance, regulatory requirements or industry standards may dictate the necessity of external validation. Seeking certification or compliance often compels organizations to subject themselves to external IT audits willingly. (Gantz, 2013).

In specific sectors, legal and regulatory obligations are intrinsic to the nature of business operations. Organizations operating within highly regulated industries must conform to external audit mandates to ensure compliance and maintain the integrity of their operations. Therefore, the value of IT auditing extends beyond optional measures, becoming a crucial component for those aiming to uphold standards, secure certifications, and meet legal requirements in an ever-evolving digital landscape. (Gantz, 2013).

- Sources of External IT Audit Requirements:

Various organizations face external IT audit requirements, driven by different factors, which can be the enterprise industry, business, if it's in the stock market, among others.

Many organizations fall into multiple categories and subject to a range of IT audit regulations, reflecting the intricate landscape of legal and industry-specific demands in the digital era, as seen in table 6 and 7:

Table 6: Sources of External IT Audit Requirements in the USA

USA	
Sector, Industry, Type	Drivers – External IT Audit
Public Corporations	• SEC rules; Sarbanes–Oxley Act rules on internal controls and the PCAOB the law created; • Federal Financial Institutions Examination Council IT Examination Handbook, Audit Booklet; • Revisions to Health Insurance Portability and Accountability Act (HIPAA) Security Rule and Privacy Rule in the Health Information Technology for Economic and Clinical Health (HITECH) Act; • Federal and state audits of internal controls for various types of nonprofits, often tied to sources and amount of funding received; • Government Auditing Standards (the “Yellow Book”); • Single Audit Act of 1984 and OMB Circular A-133, Audits of states, local governments, and nonprofit organizations; • ISAE 3402: Assurance reports on controls at a service organization; • Among other sources.
Financial Institutions	
Healthcare organizations	
Nonprofit organizations	
Government agencies	
Service Providers	
Federal Funding Recipients	

Table 7: Sources of External IT Audit Requirements in the European Union.

EUROPEAN UNION	
Sector, Industry, Type	Drivers – External IT Audit
Public Corporations	• General Data Protection Regulation (GDPR); • National Regulatory Authorities - each EU member state has its own national regulatory authorities that may prescribe specific IT audit requirements, particularly in sectors such as telecommunications, energy, and healthcare;
Financial Institutions	
Healthcare organizations	
Nonprofit organizations	
Government agencies	
Service Providers	
Industry, Energy and Telecom	• ISO Standards; • Network and Information Systems Directive (NIS Directive); • ISAE 3402: Assurance reports on controls at a service organization; • Sarbanes–Oxley Act rules on internal controls and the PCAOB the law created; • European Banking Authority (EBA) Guidelines; • Among other sources.

4.1.2 Main proposes

IT audit, or Information Technology audit, serves several crucial purposes within an organization. These purposes are designed to ensure the effective and secure use of information technology resources and give reliability to the information contained within the different systems, in order to support the financial auditors, to guarantee that the information as well as the systems, aren't corrupted or have any fraudulent information. These are some main purposes of IT audit, namely, (Gantz, 2013):

- **Risk Assessment**, which allows to identify and assess risks associated with the organization's information systems and technology infrastructure; also, those risks take into account the different systems and how are they relevant for the organizations. In risk assessment, auditors also evaluate the potential impact of risks on business operations, data integrity, and confidentiality.
- **Compliance Verification**, that ensures that the organization's IT practices and systems comply with relevant laws, regulations, and industry standards. Additionally, allows to confirm adherence to internal policies and procedures, as well as external compliance requirements. These requirements vary among the different countries, although internationally they can be stipulated by ISO, ISACA, ENISA, NIST, CSC, CIS or even the recommended policies and procedures by the manufacturer of the technology, for instance, Microsoft, Oracle, SAP, among others.
- **Data Integrity and Security**, is one of the most important purposes of IT Audit, because it's crucial to assess the effectiveness of information security measures to protect data from unauthorized access, alteration, or identify vulnerabilities in the IT environment that could compromise the confidentiality, integrity, or availability of data.

- **System Reliability and Availability**, which evaluates the reliability and availability of IT systems and infrastructure to ensure continuous business operations and identifies potential points of failure and recommend measures to enhance system resilience.
- **Operational Efficiency**, that takes into consideration a comprehensive review of IT processes and operations to identify areas for improvement in efficiency and effectiveness and recommend solutions to streamline IT operations and enhance overall productivity.
- **Business Continuity and Disaster Recovery**, that assess the organization's preparedness for unforeseen events or disasters that could impact IT operations and ensures the existence and effectiveness of business continuity and disaster recovery plans.
- **Audit Trail and Accountability**, by verifying the existence and effectiveness of audit trails for monitoring and tracking user activities within IT systems and by validating the accountability for system access and changes through proper authentication and authorization controls.
- **Technology Governance**, to determine the governance structure for IT within the organization, including decision-making processes, oversight, and management of IT resources, which plays an overall alignment between IT and overall organizational objectives.
- **Vendor and Third-Party Risk Management**, by determining the risks associated with third-party vendors providing IT services or products and guarantee compliance with contractual agreements and evaluate the security measures implemented by external partners.
- **Continuous Improvement**, by providing recommendations for ongoing improvement of IT processes, controls, and security measures and facilitate a culture of continuous improvement in managing and utilizing IT resources.

4.1.3 General Challenges and Opportunities

As the digital landscape continues to evolve, the challenges and opportunities in IT audit have become increasingly intricate, requiring a nuanced understanding of cybersecurity, regulatory compliance, and strategic alignment to navigate successfully. In table 8 are represented some of the general challenges and Opportunities in the context of IT Audit.

Table 8: General challenges and opportunities in the context of IT Audit

Challenges	Opportunities
• Increasing Technological Advancements • Increasing Cybersecurity Threats • Evolving Regulatory Compliance Landscape, as well as the technology, such as AI, RPA ML • Data Privacy and Protection Regulations • Complex IT Environments and Infrastructures • Talent Shortage and Skill Gaps • Audit Scope Expansion due to Cloud Adoption • Balancing Speed and Accuracy in Audits • Ensuring Vendor and Third-Party Compliance • Adapting to Remote Work Environments Hall, J. A. (2013).	• Integration of Advanced Analytical Tools • Strengthening Security Protocols and Incident Response • Enhanced Governance and Compliance Frameworks • Implementation of Robust Data Privacy Measures • Improved Automation and Streamlining of Audit Processes • Investing in Continuous Training and Skill Development • Cloud Security Assessment and Compliance Monitoring • Leveraging AI and Machine Learning for Efficient Auditing • Developing Comprehensive Vendor Risk Management Strategies • Strengthening Remote Auditing Capabilities and Security Vasarhelyi, M. A., Alles, M., Kogan, A., & Krishnan, G. (2004).

IT Audit faces challenges such as adapting to rapid technological changes and ensuring compliance with evolving regulations. However, it also presents significant opportunities, including leveraging advanced technologies like AI to enhance audit accuracy and efficiency. Addressing these challenges while capitalizing on new technologies can significantly advance audit practices.

4.2 Artificial Intelligence

In the ever-evolving landscape of technology, the concept of Artificial Intelligence (AI) has emerged as a transformative force, reshaping the way society perceive and interact with machines. Understanding AI is not merely an exploration of sophisticated algorithms and cutting-edge technologies; it is a journey into the realm of creating intelligent entities that can mimic, learn, and adapt in ways reminiscent of human intelligence. As we delve into this intricate field, the multifaceted nature of AI unfolds, encompassing diverse subfields, ethical considerations, and the dynamic interplay between machine capabilities and human aspirations. AI sets the stage for a comprehensive exploration in technology, inviting us to unravel its complexities and grasp the profound impact it holds on to our technological landscape and societal and enterprise fabric.

4.2.1 Core concepts

The contemporary definition of Artificial Intelligence (AI) is encapsulated in the 2020 edition of "Artificial Intelligence: A Modern Approach" by Russell and Norvig, widely regarded as the authoritative compendium in the field. According to the authors, AI is delineated as "the study of intelligent agents" — entities that receive environmental inputs and respond with actions through the application of functions, (Russel and Norvig, 2020). This definition seeks to encompass the multifaceted perspectives presented by various authors in the historical trajectory of AI, emphasizing the four key characteristics of intelligent agents:

- Acting humanly.
- Thinking humanly.
- Thinking rationally.
- Acting rationally.

The inception of the term "Artificial Intelligence" can be traced back to John McCarthy, who coined the expression in the proposal for the seminal 1956 Dartmouth conference, (Muthukrishnan et al., 2020). McCarthy, an Assistant Professor of Mathematics at Dartmouth College, defined AI as any aspect of learning or intelligence that can be simulated by a machine.

However, the influential 1950 article "Computing Machinery and Intelligence" by Alan Turing, (Turing, 2012) holds substantial significance in the development of the AI field. Turing, in his exploration of whether machines can think, proposed the Turing Test as a measure of computational intelligence, encompassing natural language processing, knowledge representation, reasoning automation, and learning capabilities.

Despite Turing's foundational contributions, the term "Artificial Intelligence" was not embraced by him; instead, he favored "Computing Intelligence." The discussion around terminology resurfaced in 2006 during the 50th anniversary of the Dartmouth conference, with considerations of whether "computational intelligence" might have shaped the field differently, (Moor, 2006).

Notably, the British Government's decision to feature Alan Turing on the £50 banknote in 2021 recognized his profound contributions, marking a departure from historical discrediting by the scientific community. Preceding Turing, philosophical inquiries into the essence of humanity, intelligence, and the potential consciousness of machines laid the groundwork for AI, (Alan Turing to Feature on New £50 Banknote | Bank of England | The Guardian, 2019).

The interdisciplinary roots of AI extend from classical Philosophy to diverse fields such as Mathematics, Economics, Neuroscience, Psychology, Computer Engineering, Control Theory, Cybernetics, and Linguistics.

The historical trajectory of AI is a narrative interwoven with intellectual contributions and evolving perspectives across a spectrum of scientific disciplines.

4.2.2 Key areas and approaches

AI encompasses various areas and approaches, each addressing different aspects of intelligence and problem-solving. Within the expansive landscape of artificial intelligence (AI), the classification into subfields, as articulated by Russell and Norvig (2020), encompasses six areas intricately tied to Turing's characteristics of computer intelligence, as represented by table 9:

Table 9: AI Areas and Corresponding Methods & Algorithms, (Russel and Norvig, 2020)

AI Areas	Examples of AI Methods and Algorithms
- Searching	Breadth-first search, depth-first search, Depth limited search, iterative deepening search, iterative lengthening search, bidirectional search.
- Planning	Planning domain definition language, Graph plan algorithm, Boolean satisfiability, first-order logical deduction, constraint satisfaction problem.
- Machine Learning	Classification, linear and logistic regression, decision trees, neural networks, nearest neighbors and locally weighted regression, support vector machines, boosting.
- Natural Language Processing	Probabilistic language models, CYK algorithm, lexicalized PCFG.
- Perception	Early vision image-processing algorithms.
- Robotics	Probabilistic filtering algorithms, configuration space search algorithms, potential field techniques.

However, Andrew Moore's definition of AI as the "science and engineering of making computers behave in ways that, until recently, we thought required human intelligence" highlights the vast, aspirational, and evolving nature of the term. Moore's perspective suggests that the dynamic essence of AI may give rise to unforeseen subfields in the future, mirroring yet unexplored dimensions of human intelligence, (High. Peter, 2017). The classification thus remains open to continual expansion and refinement.

Below are key AI areas and approaches, along with brief explanations of each:

Machine Learning is a subset of AI that focuses on developing algorithms and models that enable machines to learn from data and improve their performance over time.

Approaches:

- **Supervised Learning:** The algorithm is trained on labeled data, learning the mapping between input and output.

- Unsupervised Learning: The algorithm discovers patterns and relationships within unlabeled data.
- Reinforcement Learning: Agents learn to make decisions by receiving feedback in the form of rewards or penalties.
- Semi-Supervised Learning: Combines elements of supervised and unsupervised learning, using both labeled and unlabeled data for training.

Natural Language Processing, involves the interaction between computers and human language, enabling machines to understand, interpret, and generate human language.

Approaches:

- Text Classification: Assigning predefined categories to text data.
- Named Entity Recognition (NER): Identifying and classifying entities (e.g., names, locations) in text.
- Machine Translation: Translating text from one language to another.
- Sentiment Analysis: Determining the sentiment expressed in a piece of text.

Computer Vision enables machines to interpret and understand visual information from the world, similar to how humans perceive and interpret visual data.

Approaches:

- Image Classification: Assigning labels or categories to images.
- Object Detection: Identifying and locating objects within images or videos.
- Facial Recognition: Recognizing and verifying faces in images or videos.
- Image Generation: Creating new images using generative models.

Expert Systems, mimic the decision-making abilities of a human expert in a specific domain by leveraging a knowledge base and an inference engine.

Approaches:

- Rule-Based Systems: Utilizing a set of predefined rules to make decisions.
- Knowledge Graphs: Representing knowledge in a structured format to facilitate reasoning.

Robotics, integrates AI with physical systems, enabling machines to perceive, act, and interact in the physical world.

Approaches:

- Simultaneous Localization and Mapping (SLAM): Mapping an environment while simultaneously keeping track of the robot's location within that environment.
- Motion Planning: Determining a sequence of actions for a robot to achieve a specific goal.

Evolutionary Algorithms are inspired by the process of natural selection and evolution. They are used for optimization and search problems.

Approaches:

- Genetic Algorithms: Population-based search algorithms that mimic the process of natural selection.
- Genetic Programming: Evolving computer programs or solutions.

Knowledge Representation and Reasoning, focuses on representing knowledge in a form that machines can utilize for reasoning and decision-making.

Approaches:

- Semantic Networks: Representing knowledge using nodes and edges to denote relationships.
- First-Order Logic: Expressing relationships and constraints using logical statements.

Deep Learning involves neural networks with multiple layers (deep neural networks) to model and solve complex problems.

Main Approaches:

- Convolutional Neural Networks (CNNs): Particularly effective for image-related tasks.
- Recurrent Neural Networks (RNNs): Suited for sequential data and natural language processing.
- Generative Adversarial Networks (GANs): Used for generating new, realistic data.

These AI areas and approaches are not mutually exclusive, and many AI applications leverage a combination of them to address complex challenges. Additionally, ongoing research and advancements continuously expand and refine these approaches within the field of AI.

Additionally, a fundamental distinction exists between two main types of AI concepts: Strong AI, also known as Artificial General Intelligence (AGI), and Weak AI.

Strong AI refers to a scenario where machines attain self-awareness and possess cognitive capabilities akin to human intelligence. In this context, machines with Strong AI would not be limited to specific tasks but would exhibit a broad range of intellectual abilities, potentially mirroring the complexities of human thought, (Searle, 1980). Conversely, Weak AI, also referred to as Narrow or Applied AI, pertains to systems designed for specialized tasks or domains. These systems excel in performing specific functions but lack the overarching cognitive breadth associated with Strong AI. Weak AI is tailored to address well-defined objectives, making it adept in areas such as natural language processing, image recognition, or game playing, without transcending the boundaries of its designated scope, (Searle, 1980).

This distinction underscores the current state of AI development, where most practical applications fall within the domain of Weak AI—solving targeted problems efficiently but without imbuing machines with a comprehensive understanding or self-awareness. Strong AI remains an aspirational goal, representing the potential for machines to achieve a level of intelligence and consciousness akin to human beings. The differentiation between Strong and Weak AI serves as a crucial delineation in understanding the scope and capabilities of artificial intelligence systems.

4.2.3 Practical Applications

In the contemporary era, Artificial Intelligence (AI) has transcended the theoretical concepts, manifesting its transformative potential through a myriad of practical applications across diverse industries.

The integration of intelligent algorithms, machine learning models, and advanced data analytics has ushered in a new era of efficiency, innovation, and enhanced decision-making. From revolutionizing

healthcare diagnostics to optimizing financial transactions, and from streamlining customer interactions to driving autonomous vehicles, AI has become an indispensable tool in addressing complex challenges and elevating various facets of our daily lives. This exploration into the practical applications of AI unveils a tapestry of innovation, where intelligent systems navigate the intricate landscape of real-world scenarios, promising advancements that resonate across sectors and shape the future of technological evolution.

The big question persists: "*Should we embrace or not AI?*".

The advantages are manifold, heralding automation, enhanced efficiency, and increased productivity. Yet, the other questions remain, "What are the latent risks accompanying this technological paradigm shift?". From lethal autonomous weapons to pervasive surveillance, biased decision-making to employment impacts, safety-critical applications to cybersecurity concerns—each merits careful consideration.

As posited by Russell and Norvig (2021), while AI promises transformative benefits, a judicious evaluation of its potential risks is essential to navigate a future where innovation aligns seamlessly with ethical and societal considerations.

- **AI Applications:**

The discourse on Artificial Intelligence (AI) leaders potentially supplanting human leaders is addressed in research by Grotenhermen et al. (2020), focusing on trust and transparency as pivotal in leadership. The study reveals that employees may struggle to comprehend AI-based decisions, leading to a deficit in trust. In complex decision-making, both AI and humans possess merits and demerits, where AI excels in processing vast information, while humans leverage intuition and holistic features. Globally, scientists integrate AI capabilities into everyday work through cognitive services, encompassing Vision, Speech, Language, and Decision capabilities (Yakubu, 2022). These facets empower applications, facilitating tasks like creating Chatbots with multi-faceted functionalities for seamless integration into daily business operations.

Another practical application is illustrated in Figure 6, Ulrich et al.'s (2021) research underscores the burgeoning prospects of Artificial Intelligence (AI) in Small and Medium Enterprises (SMEs). As a foundational step, organizations recognize the potential of AI and its applications.

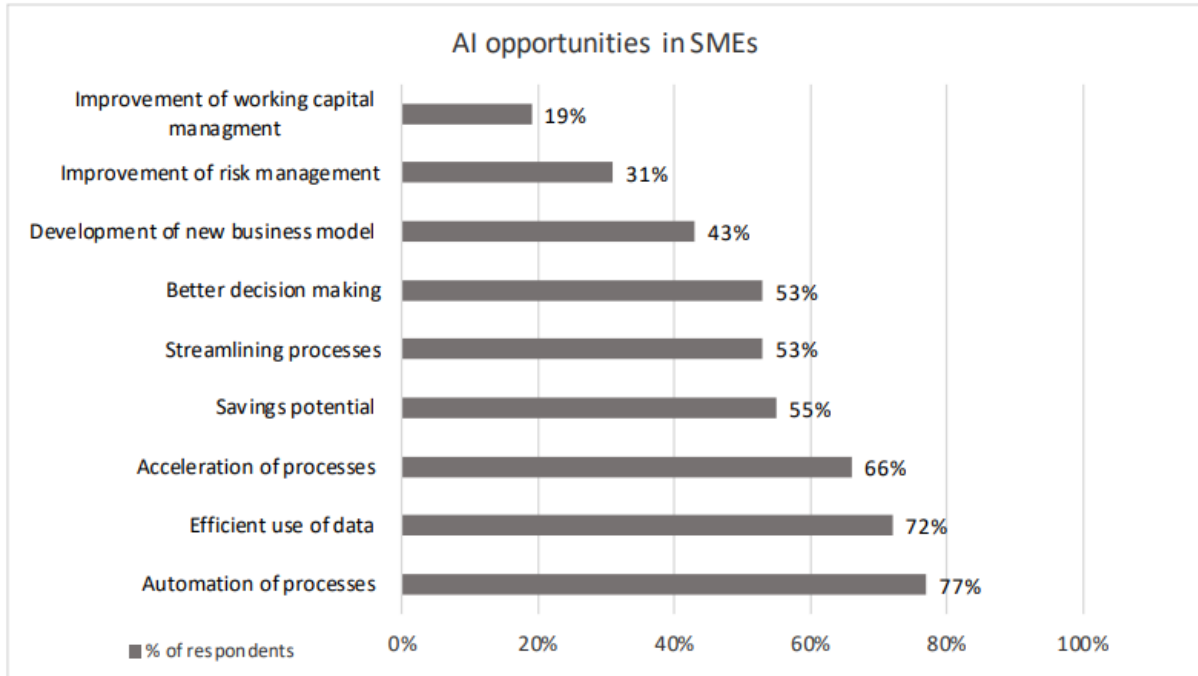


Figure 7: AI opportunities in SMEs (adapted from Ulrich et al., 2021).

The integration of Artificial Intelligence is advancing steadily. In 2018, (Chui & Malhorta, 2018) reported that forty-seven percent of surveyed companies had incorporated at least one AI capability. Fast forward to 2021, and (Chui et al., 2021), findings reveal an uptick, with fifty-six percent of respondents having embraced at least one AI function. This progression signifies a notable increase in AI adoption within companies over the years, reflecting a growing acknowledgment of the transformative potential and practical applications of artificial intelligence in various business domains.

In the research by (Chui et al., 2021) represents that the most adopted use-cases are service-operation, optimization, chatbots and data analytics do new AI-based product enhancements and contact-center automation.

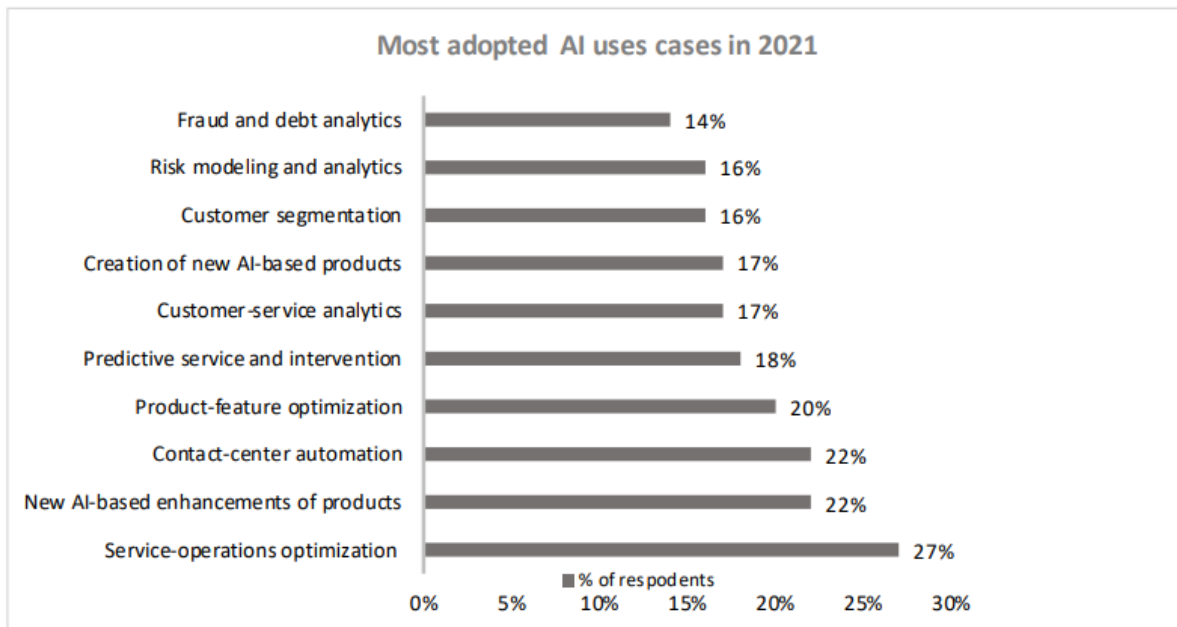


Figure 8: Most adopted AI use cases (adapted from Chui et al., 2021).

Additionally, in the dynamic landscape of modern enterprises, the strategic integration of Artificial Intelligence (AI) has emerged as a transformative force, ushering in a new era of efficiency, innovation, and competitiveness. The benefits of leveraging AI technologies within organizational frameworks are profound and multifaceted. By harnessing the power of machine learning algorithms, predictive analytics, and automation, enterprises can unlock unparalleled insights from vast datasets, empowering data-driven decision-making processes. This not only enhances operational agility but also fosters a culture of adaptability in the face of rapidly evolving business environments, (Microsoft, 2021).

Beyond operational efficiency, AI presents a compelling case for cost reduction through the automation of routine tasks and optimized resource allocation. Furthermore, the deployment of AI strengthens cybersecurity measures, safeguarding enterprises against sophisticated threats. From a customer-centric perspective, AI enables personalized experiences, leveraging advanced recommendation systems and responsive virtual assistants to elevate customer engagement and satisfaction. As enterprises navigate the complexities of the digital age, embracing AI becomes not merely a choice but a strategic imperative, positioning organizations at the forefront of innovation and resilience., (Microsoft, 2021).

Some of the benefits of using AI in the enterprises, (Microsoft, 2021):

- Free up time by automating complex business processes;
- Improve product quality through defect detection;
- Increase uptime with predictive maintenance;
- Enhance customer service with an intelligent chatbot;
- Prevent fraud and compliance risk;

- Forecast revenue more accurately;
- Drive customer loyalty by personalizing experiences;
- Close more deals through advanced lead scoring;
- Ensure product availability by optimizing supply chains.

- **Examples of AI applications in the different industries:**

Artificial Intelligence is reshaping industries, enhancing efficiency and innovation. From healthcare diagnostics to financial fraud detection and manufacturing automation, AI applications are diverse and transformative. Table 10 offers a glimpse into the wide-ranging impact of AI across industries, showcasing its versatile applications and real-world significance.

Table 10: Examples of AI Applications throughout the different industries

Industries	Examples of AI Applications
<u>Healthcare</u>	• Disease Diagnosis: AI algorithms analyze medical images and patient data to assist in diagnosing diseases. • Personalized Treatment Plans: AI helps in developing personalized treatment plans based on patient data. Shen, D., Wu, G., & Suk, H. I. (2017).
<u>Finance</u>	• Fraud Detection: AI algorithms analyze transaction data to identify and prevent fraudulent activities. • Algorithmic Trading: AI is used for analyzing market trends and executing trades at high speeds. Phua, C., Lee, V., Smith, K., & Gayler, R. (2005).
<u>Retail</u>	• Recommendation Systems: AI powers personalized product recommendations for customers. • Inventory Management: AI optimizes inventory levels and predicts demand patterns. Ricci, F., Rokach, L., & Shapira, B. (2011).
<u>Customer Service</u>	• Chatbots: AI-driven chatbots provide instant responses to customer queries. • Voice Assistants: Virtual assistants use natural language processing for voice-based interactions. Ricci, F., Rokach, L., & Shapira, B. (2011).
<u>Education</u>	• Personalized Learning: AI tailors educational content based on individual student performance.

	• Automated Grading: AI automates the grading process for assessments. Zaiane, O. R., & HersHKovitz, A. (2019). Luckin, R. (2017). Holmes, W., Bialik, M., & Fadel, C. (2019).
<u>Manufacturing</u>	• Predictive Maintenance: AI analyzes equipment data to predict maintenance needs, minimizing downtime. • Quality Control: AI-powered systems detect defects in real-time during the manufacturing process. Siciliano, B., Sciavicco, L., Villani, L., & Oriolo, G. (2008)
<u>Autonomous Vehicles</u>	• Self-Driving Cars: AI algorithms process sensor data to navigate and make real-time driving decisions. • Traffic Management: AI optimizes traffic flow and enhances transportation systems. Russell, S. J., & Norvig, P. (2021).
<u>Cybersecurity</u>	• Anomaly Detection: AI identifies unusual patterns in network traffic to detect and prevent cyber threats. • Behavioral Analysis: AI analyzes user behavior to identify potential security breaches. Shackleford, D. (2018).
<u>Human Resources</u>	• Recruitment: AI streamlines the hiring process by analysing resumes and assessing candidate suitability. • Employee Engagement: AI tools analyse employee data to provide insights into satisfaction and retention. Davenport, T. H. (2019). Srinivasan, A., & Davenport, T. H. (2018).
<u>Agriculture</u>	• Precision Farming: AI analyzes data from sensors, satellites, and drones to optimize crop management. • Crop Disease Detection: AI-powered image recognition identifies diseases in crops. Bochtis, D., & Sørensen, C. G. (2020). Mohanty, S. P., Hughes, D. P., & Salathé, M. (2016).

4.3 AI Technology in Auditing

This section provides an in-depth examination of AI technology in auditing, and by analyzing AI's role in enhancing audit practices alongside a meticulous review of relevant literature using PRISMA, it aims to offer comprehensive insights into the evolving landscape of auditing and its methodologies.

4.3.1 PRISMA Methodology

The methodology adopted for conducting the systematic literature review is PRISMA, an acronym for "Preferred Reporting Items for Systematic Reviews and Meta-Analysis" as outlined by Moher (2009). PRISMA offers a comprehensive set of guidelines aimed at facilitating the execution of systematic literature reviews, critical analyses of literature, and meta-analyses (Moher, 2009).

The PRISMA methodology employs a systematic approach to comb through scientific papers and other literature for review-based studies. Central to its operation are inclusion and exclusion criteria, which determine the suitability of each study under review (Liberati et al., 2009).

Initiated in 2005 by a consortium of 29 experts spanning diverse scientific domains, PRISMA culminated in a 27-item checklist and a comprehensive four-phase flow diagram following extensive consensus building (Liberati et al., 2009). This consensus yielded a robust template, empowering researchers with a structured framework.

The workflow of PRISMA revolves around four distinct phases:

- **Identification:** This phase involves the systematic search for relevant articles, papers, and scientific literature using predefined search strategies across commonly used databases.
- **Screening:** Rigorous criteria are applied in this phase to sift through the gathered literature, ensuring the inclusion of pertinent materials and the exclusion of irrelevant ones, thus streamlining the research process.
- **Eligibility:** Included articles undergo thorough assessment to determine their suitability based on predefined criteria, with well-justified exclusions made for those that do not meet the requirements.
- **Inclusion:** The culmination of the PRISMA process results in a curated list of included papers that serve as the primary source material for the research endeavor.

4.3.2 PRISMA Execution

The Sections 4.1 and 4.2 of this these were dedicated to presenting the theoretical underpinnings relevant to the two primary areas of inquiry. These sections provided a thorough grounding in foundational concepts and theories essential for grasping the subject matter. Keywords gleaned from this theoretical framework were subsequently utilized in constructing the search string aimed at retrieving scientifically pertinent literature. The overarching objective is to foster a comprehensive comprehension of the contemporary landscape surrounding the utilization of artificial intelligence within the IT Audit domain.

The proposed research endeavors to address the following fundamental inquiries:

Table 11: Systematic Review's Research Questions

RQ1	What is the present state of research within this domain?
RQ2	What are the primary concerns/issues regarding the utilization of artificial intelligence in auditing processes for both businesses and governmental entities?
RQ3	Which artificial intelligence techniques are currently deemed efficacious in addressing the challenges within this area?
RQ4	What are the advantages and disadvantages of applying AI techniques in this field?

To answer these questions, and following the PRISMA guidelines, the most relevant studies in this field have been selected. A set of keywords deemed most pertinent based on the theoretical background has been chosen to conduct the search. Only English keywords were used, resulting in a search outcome predominantly composed of articles written in English. Articles written in other languages were excluded according to the criteria established in the PRISMA methodology. The keywords utilized are:

Table 12: Systematic Review's Keywords

Keywords	Auditing	Artificial Intelligence
	Audit	Artificial Intelligence
		Deep Learning
		Machine learning
		AI Applications
		Intelligent tools

A specific search string was constructed to include the aforementioned words or terms, with the objective of finding them in abstracts, titles, or keywords of articles and other scientific papers. This careful selection of words ensured that the search results were highly relevant to the topics under study. The focus was exclusively on recent scientific documents, given the rapid evolution of technology in this field. Consequently, only the most recent articles could provide up-to-date and pertinent information. A filter was applied to show only articles published between 2021 and 2024, to ensure the acquisition of accurate information about the current state of the art in the utilization of AI in the cybersecurity domain.

The search string used was: (**"Artificial intelligence" OR "Machine Learning" OR "Deep Learning" OR "AI Applications" OR "Intelligent tools"**) AND (**"Audit"**).

The search was conducted in May 2024 on the following scientific information resource databases:

Table 13: Systematic Review's Resource Databases

Resource Database	Resource URL
Scopus	https://www.scopus.com/home.uri
Science Direct	https://www.sciencedirect.com/

Following the PRISMA methodology, the next step was to define the inclusion and exclusion criteria for the articles resulting from the mentioned search.

Table 14: Systematic Review's inclusion and exclusion criteria

Inclusion Criteria	Exclusion Criteria
Any scientific article showing evidence of AI utilization in Auditing	Papers focusing on Auditing but without focusing on AI techniques utilization
Paper must be a peered research article, recognized book chapter or approved conference paper written in English	Articles not in English and duplicate papers
Research articles belong to the fields of economics, management, information technology, and computer science.	Articles published before 2021
Paper is published between 2021 and 2024	Non-academic or non-scientific papers (e.g., websites, magazines reports, newspapers, consulting articles, books, citations)
	Papers with titles outside the scope of this work

After inserting the search string in the sources websites, the output is all the identified articles through database searches, which resulted in a total of n=5565 articles.

After extracting the data from the databases, it was found that the data were not formatted, even though they were extracted in txt, Bibtex, or CSV formats (Figure 9). Therefore, it was necessary to use VBA programming to format the data for analysis.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
578	A	trust	transitivity	model	of	small	and	medium-sized	manufacturing	enterprises	under	blockchain-based	supply	chain	finance,								
579	International	Journal	of	Production	Economics,																		
580	Volume	247,																					
581	2022																						
582	108469																						
583	ISSN	0925-5273,																					
584	https://doi.org/10.1016/j.jpe.2022.108469 ,																						
585	https://www.sciencedirect.com/science/article/pii/S0925527322000627)																						
586	Abstract: Small and medium-sized manufacturing enterprises (SMEs) have been facing the financing contradiction of a strong demand for and a weak trust for a long time, and financing constraints are closely related to the production efficiency of manufac																						
587	Keywords: Blockchain; Trust trans; Small and ; Intuitionistic fuzzy set																						
588																							
589	Cristina I. Fernandes, Pedro M. Veiga, João J. Ferreira, Hussain G. Rammal, Vijay Pereira,																						
590	Assessing strategic leadership in organizations: Using bibliometric data to develop a holistic model,																						
591	Journal of Business Research,																						
592	Volume 141,																						
593	2022																						
594	Pages 646-655,																						
595	ISSN 0148-2963,																						
596	https://doi.org/10.1016/j.jbusres.2021.11.067 ,																						
597	https://www.sciencedirect.com/science/article/pii/S0148296321008742)																						
598	Abstract: The role of organizational leaders has transitioned over time, from being supervisory to strategic. This trend has been reflected in the literature, with research related to strategic leadership has risen swiftly in quantity but distributed across divergent acade																						
599	Keywords: Bibliometr; Research agenda																						
600																							
601	Stephen Kastoryano, Ben Vollaard,																						
602	Unseen annihilation: Illegal fishing practices and nautical patrol,																						
603	Journal of Environmental Economics and Management,																						
604	Volume 120,																						

Figure 9: Unstructured data extracted and formatted to CSV in excel

A careful analysis of the extracted data revealed that the data were in a single column; however, most of them followed a sequence of 11 lines per article or 9 lines. Therefore, the files were organized according to these sequences, with fields lacking information marked as "N/A". The code for the macro in excel, is displayed in figure 11 – sequence of 11 lines and figure 12 – sequence of 9 lines.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
606	102881																						
607	ISSN 0095-0696,																						
608	https://doi.org/10.1016/j.jeem.2023.102881 ,																						
609	https://www.sciencedirect.com/science/article/pii/S0095069623000992)																						
610	Abstract: A host of regulations should protect fish, a common-pool resource, from overexploitation, but detecting violations of these regulations is challenging, both at sea and in port. We present a novel approach to uncover a supposedly widespread and particular																						
611	Keywords: Regulator; Environme; Fisheries																						
612																							
613	Sweta Sinha, Agnata Pandey,																						
614	My job is to hide it! A role strain perspective,																						
615	Development and Learning in Organizations: An International Journal,																						
616	Volume 36, Issue 5,																						
617	2022																						
618	Pages 13-15,																						
619	ISSN 1477-7282,																						
620	https://doi.org/10.1108/DLO-10-2021-0186 ,																						
621	https://www.sciencedirect.com/science/article/pii/S1477728222000260)																						
622	Abstract: Purpose																						
623	The study presents a framework of knowledge hiding (KH) driven by positive and negative intentions. The study also highlights the impact of KH on the employee's role-related responsibility to engage in KH.																						
624	Design/methodology/approach																						
625	We review the literature on KH from the perspective of role strain theory and propose a conceptual framework.																						
626	Findings																						
627	The study proposes a conceptual framework of KH practices driven by positive and negative intent, further segregated into organizational and personal causes of KH. The framework also depicts the positive and negative impact of KH on the employees and highlights																						
628	Originality/value																						
629	This paper provides a framework to understand how role-related KH responsibilities (organization driven) and personal motives map to employee outcomes.																						
630	Keywords: Knowledge; Role strain																						
631																							

Figure 10: Sequence of data

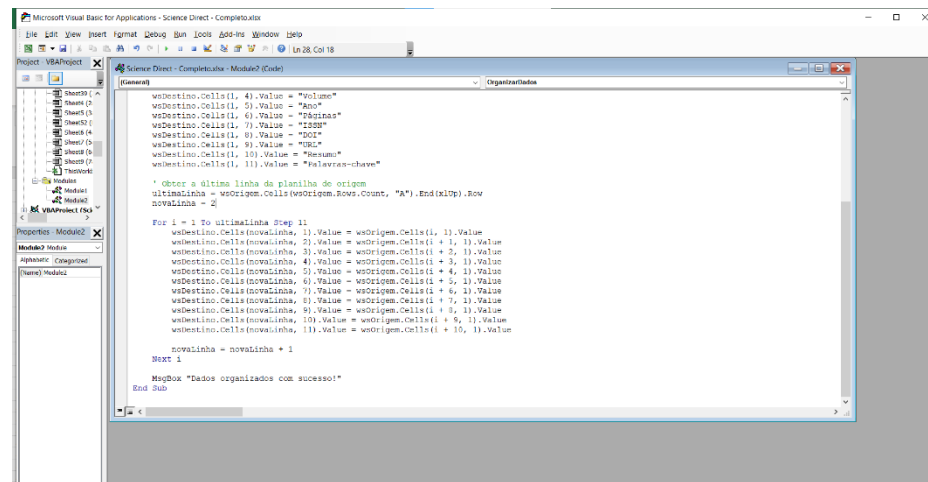
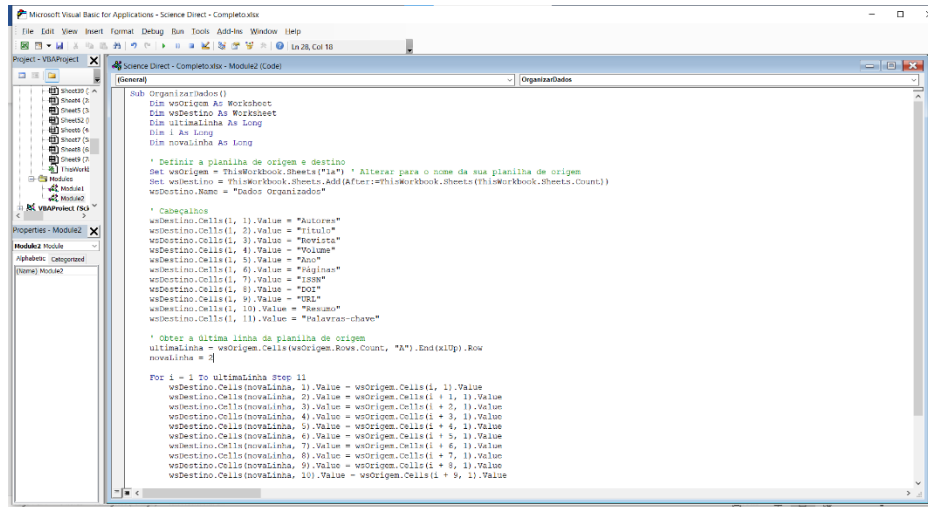


Figure 11: Code for structuring data in sequences of 11

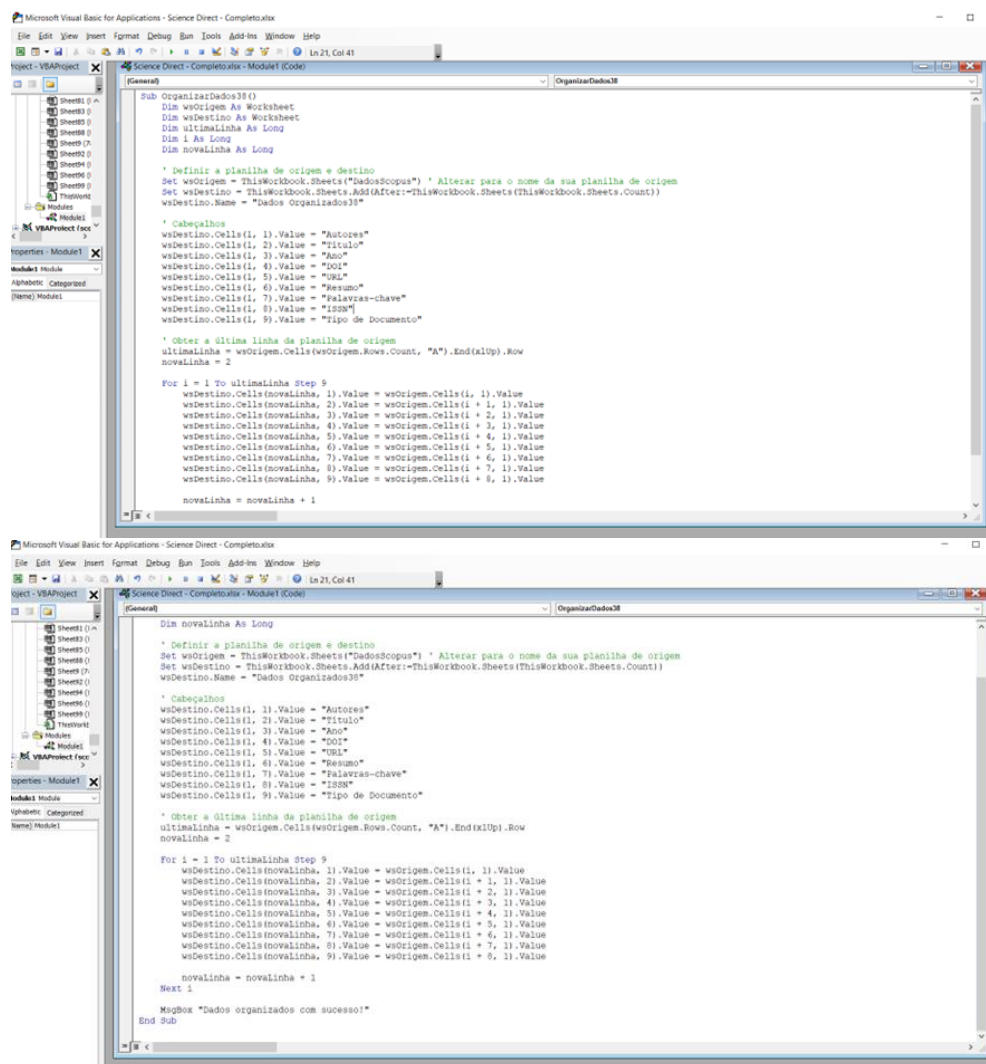


Figure 12: Code for structuring data in sequences of 9

A pre-formatting was done after the selection of $n=5565$ articles, specifically excluding those that did not match the previously defined string but were initially selected. Consequently, the analysis continued with $n=4173$ articles.

Next, duplicate research articles found across different databases are removed to obtain a concrete result for applying exclusion criteria, with the following articles being retained, $n=3736$.

At this stage, the analysis follows the PRISMA flow, defined by inclusion and exclusion criteria. Research articles that did not fall within the topics of computer science, engineering, business, management and accounting, social sciences, and economics were excluded, resulting in $n=3518$. Next, a filter was applied to include only articles published between 2021 and 2024, resulting in $n=3078$. Subsequently, a criterion was applied to exclude articles whose abstracts and titles did not contain essential keywords, specifically "does not contain = Audit"; "does not contain = Auditing"; "does not contain = AI"; "does not contain = Artificial Intelligence," leading to $n=254$. Finally, a detailed analysis was conducted on the titles and

research articles that contained the keywords "audit," "auditing," "AI," and "Artificial Intelligence," but whose context was not relevant to the research question, resulting in n=24.

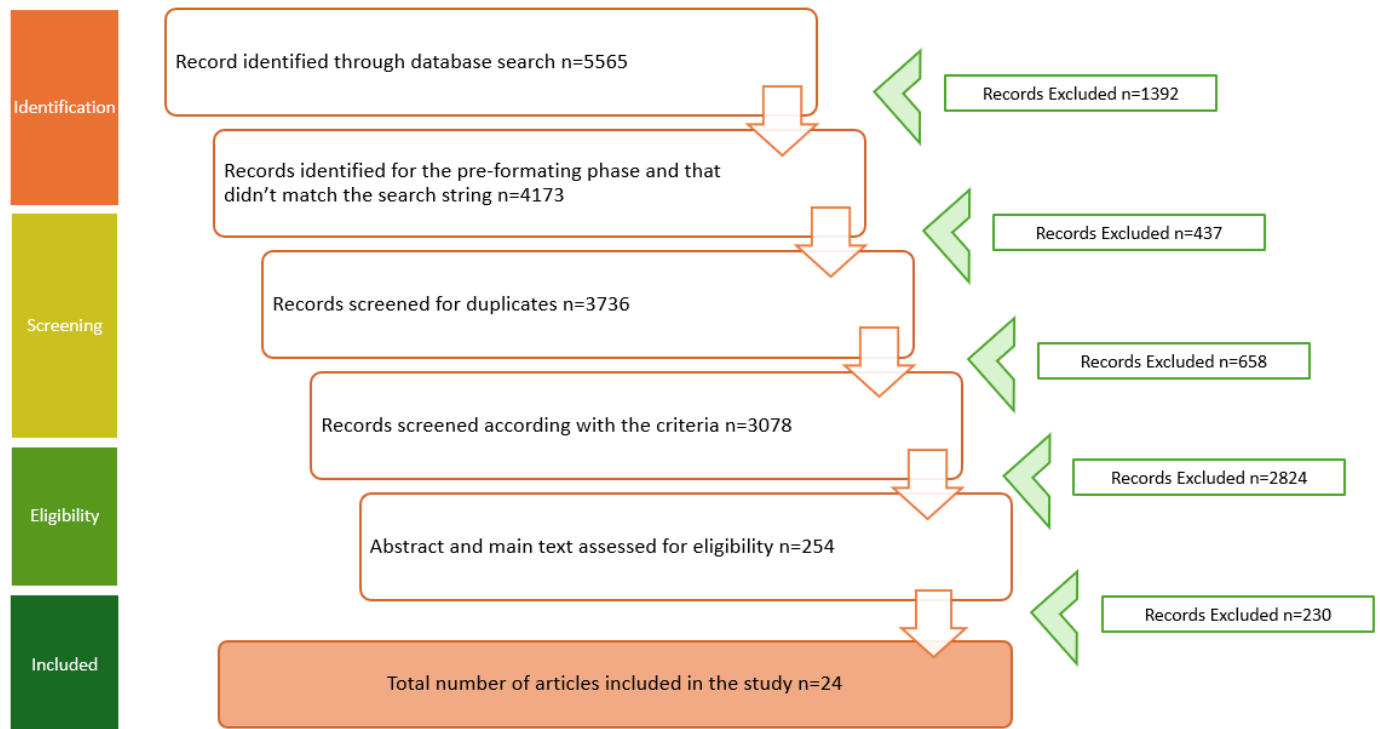


Figure 13: PRISMA execution

The output of the PRISMA execution, resulted in 24 research articles, including articles, conference papers and journal articles, which are listed in the following table 15, along with a brief description of its contribution, conclusions, and gaps/future work suggestions.

Table 15: Summary of the PRISMA Output

#	Authors	Article	Contribution
[1]	Feiqi Huang, Won Gyun No, Miklos A. Vasarhelyi, Zhaokai Yan;	Audit data analytics, machine learning, and full population testing;	Emerging technologies like data analytics and machine learning are transforming the accounting profession, especially audit and assurance procedures. Traditional audit sampling, which examines only a subset of transactions, is becoming less relevant in the big data era. A viable solution is using audit data analytics and machine learning to analyze entire populations of transactions. This paper presents an approach for applying these technologies to full population testing, enhancing audit accuracy and efficiency, and discusses the challenges associated with integrating these advanced methods into auditing practices.

[2]	Chanyuan (Abigail) Zhang, Soohyun Cho, Miklos Vasarhelyi;	Explainable Artificial Intelligence (XAI) in auditing;	This paper introduces Explainable Artificial Intelligence (XAI) techniques to enhance the transparency of AI and Machine Learning (ML) in auditing. It addresses the challenge of explainability and demonstrates how XAI methods, such as Local Interpretable Model-agnostic Explanations (LIME) and Shapley Additive exPlanations (SHAP), can meet audit documentation and evidence standards. Using an example of assessing the risk of material misstatement, the paper contributes to accounting information systems research and practice by improving the interpretability of AI applications in auditing tasks.
[3]	Masashi Goto;	Anticipatory innovation of professional services: The case of auditing and artificial intelligence;	This case study explores how professional services firms (PSFs) can utilize service R&D to innovate and adapt to AI. Focusing on the Big Four audit firms in Japan during the 2010s, it reveals the critical role of service R&D in advancing AI adoption, overcoming traditional innovation limitations. The study constructs a three-phase model for service R&D evolution and highlights the importance of innovation process design for legitimizing new technologies in PSFs.
[4]	Yogesh K. Dwivedi, Laurie Hughes, Elvira Ismagilova, Gert Aarts, Crispin Coombs, Tom Crick, Yanqing Duan, Rohita Dwivedi, John Edwards, Aled Eirug, Vassilis Galanos, P. Vigneswara Ilavarasan, Marijn Janssen, Paul Jones, Arpan Kumar Kar, Hatice Kizgin, Bianca Kronemann, Banita Lal, Biagio Lucini, Rony Medaglia, Kenneth Le Meunier-FitzHugh, Leslie Caroline Le Meunier-FitzHugh, Santosh Misra, Emmanuel Mogaji, Sujeet Kumar Sharma, Jang Bahadur Singh, Vishnupriya Raghavan, Ramakrishnan Raman, Nripendra P. Rana, Spyridon Samothrakis, Jak Spencer, Kuttimani Tamilmani, Annie Tubadji, Paul Walton, Michael D. Williams;	Artificial Intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy;	This study explores the transformative potential of Artificial Intelligence (AI) in augmenting and potentially replacing human tasks across various sectors, akin to the impact of the industrial revolution. It highlights the rapid advancements in machine learning and autonomous decision-making, which offer significant opportunities and challenges for industries such as finance, healthcare, manufacturing, and logistics. By gathering insights from experts, the research assesses AI's impact on business, government, public sector, and technology, providing timely insights into AI's future influence on industry and society.
[5]	Sonia Vitali, Marco Giuliani;	Emerging digital technologies and auditing firms: Opportunities and challenges;	This article examines the impact of robotic process automation (RPA) and artificial intelligence (AI) on auditing firms, focusing on daily activities, organizational structure, hiring practices, and the competitive gap between Big4 and non-Big4 firms. Based on a study of 14 auditing companies, the findings highlight differing opinions on the future of auditing. Key points include potential positive impacts, unchanged traditional structures, the need for IT and data analytics skills, and the varying effects on the competitive gap between large and smaller firms. Despite limited current use, significant changes are anticipated.
[6]	Bernd Carsten Stahl, Rowena Rodrigues, Nicole Santiago, Kevin Macnish,	A European Agency for Artificial Intelligence: Protecting fundamental rights and ethical values	This article reviews the ethical and human rights challenges of AI and proposes a regulatory framework, focusing on a potential European Agency for AI. It outlines the agency's terms of reference and necessary characteristics to address these challenges, contrasting it with the proposed European Artificial Intelligence Board in the AI Act.
[7]	Samiolo R., Spence C., Toh D.	Auditor judgment in the fourth industrial revolution	This paper challenges the notion that technological advancements will primarily automate low-level tasks in auditing. Based on 44 interviews with auditors, regulators, and AI providers, it argues that automating seemingly straightforward tasks risks

			undermining critical aspects of judgment, sensemaking, and professional development in auditing. While technology can augment higher-level audit processes, it introduces new complexities that require auditors to navigate unfamiliar territories of judgment. The study underscores the evolving nature of auditor skills amidst technological changes and the potential risks to practical knowledge acquisition.
[8]	Pereira L., Résio M., da Costa R.L., Dias Á., Gonçalves R.	Artificial intelligence in strategic business management: the case of auditing	This study explores the discrepancy between the potential benefits of AI adoption in audit processes and its current low utilization. Based on a survey of approximately 200 employees in Portuguese companies, it identifies tasks suitable for AI automation and outlines technological challenges that need addressing in this transformation.
[9]	Yao L.	Application of Artificial Intelligence Technology in Enterprise Financial Audit	This paper underscores the necessity for financial audits to evolve into data-centric practices in the era of big data. It advocates for leveraging artificial intelligence (AI) to enhance audit efficiency and effectiveness. Highlighting stagnation in current approaches, the paper calls for widespread adoption of AI to propel the audit sector into a digitally networked and intelligent management framework, promising enhanced quality and industry advancement.
[10]	Musa A.M.H., Lefkir H.	The role of artificial intelligence in achieving auditing quality for small and medium enterprises in the Kingdom of Saudi Arabia	This study investigates AI adoption by SMEs in Saudi Arabia and its impact on audit quality, comparing perspectives of accountants and external auditors. Findings suggest both groups believe AI enhances audit quality, with no significant differences in their evaluations of AI's contribution.
[11]	Wassie F.A., Lakatos L.P.	Artificial intelligence and the future of the internal audit function	This review addresses research gaps in AI adoption in the Internal Audit Function (IAF), proposing a comprehensive framework (CACS) for effective implementation. It emphasizes the need for more studies on AI's role in IAF, offers insights for scholars and industry experts, and outlines implications for auditing practices. The paper aims to guide future research, assist internal auditors in assessing AI benefits and risks, and inform regulators and organizations on updating practices.
[12]	Seethamraju R., Hecimovic A.	Adoption of artificial intelligence in auditing: An exploratory study	This study explores factors influencing AI adoption in auditing using the TOE framework and semi-structured interviews. It identifies technological, organizational, and environmental factors impacting AI adoption. While AI promises to enhance audit quality and client services, concerns over transparency and control in AI systems necessitate a reassessment of audit practices.
[13]	Aljaaidi K.S., Alwadani N.F., Adow A.H.	The impact of artificial intelligence applications on the performance of accountants and audit firms in Saudi Arabia	This study investigates the impact of artificial intelligence (AI) applications on accountants and audit firms in Saudi Arabia. Based on a survey of 38 audit firms, findings from multiple regression analysis indicate that AI tools enhance audit performance by reducing costs, time, and effort. They also improve audit quality, aid in materiality determination, enable efficient sample selection, and enhance control procedures for electronic transactions. These insights are crucial for advancing understanding and adoption of AI in accounting and auditing practices.
[14]	Adamyk O., Benson V., Adamyk B., Al-Khateeb H., Chinnaswamy A.	Does Artificial Intelligence Help Reduce Audit Risks?	This article explores how AI-powered systems enhance auditing, while also identifying emerging risks. AI's self-learning capability improves efficiency and accuracy but introduces new security concerns. The study highlights limitations and proposes a security model to mitigate risks, offering insights for future research in AI-enabled audit practices.
[15]	Dambe S., Gochhait S., Ray S.	The Role of Artificial Intelligence in Enhancing	This paper explores how AI enhances cybersecurity and internal audit practices by automating processes, detecting threats in real-time, and improving operational visibility. It emphasizes AI's role in

		Cybersecurity and Internal Audit	enhancing accuracy, compliance with regulations, and overall security posture, underscoring its potential as a critical technology in safeguarding organizations from cyber threats.
[16]	Adeoye I.O., Akintoye R.I., Theophilus A.A., Olagunju O.A.	Artificial intelligence and audit quality: Implications for practicing accountants	This study investigates the impact of artificial intelligence (AI) on audit quality through surveys administered to accountants and staff from Big Four firms. Findings indicate widespread support for AI's utility, with regression analysis confirming its positive effect on audit quality. The study recommends embracing AI across private, corporate, and accounting sectors for its economic benefits and enhancement of audit precision, reliability, and timeliness in financial reporting.
[17]	Priya V.L., Aghanaashaa A., Chahar A., Alisha A.	Artificial Intelligence as a Tool for Enhanced Data Integrity and Data Security	The article discusses the critical importance of data integrity and security in the era of big data analytics. It emphasizes the role of Artificial Intelligence (AI) tools in ensuring robust data management across various sectors, while also highlighting challenges that need addressing to optimize AI's effectiveness in safeguarding data integrity and security.
[18]	Dennis, Anita;Jenkins, J. Gregory	Using technology to boost audit quality: With tools such as artificial intelligence, auditors can implement new processes that enhance effectiveness and efficiency	The article identifies the benefits of using technology in audit and presents findings from a survey by the American Institute of Certified Public Accountants (AICPA) Auditing Standards Board on the impediments to technology use in audits. Benefits of technology use include risk identification and assessment, improved planning and processes and staff support. Technologies used in audit include cloud computing, data analytics and visualization, artificial intelligence (AI) and textual analysis.
[19]	Rodrigues L., Pereira J., da Silva A.F., Ribeiro H.	The impact of artificial intelligence on audit profession	The study surveys certified auditors in two Portuguese districts to gauge their perceptions on AI's impact on auditing. Results indicate that auditors foresee AI enhancing efficiency, effectiveness, sampling techniques, cost-benefit ratios, and the identification of material distortions in financial statement analysis.
[20]	Ahmet Efe	The Future of the Audit Related Professions in the Light of Risk and Benefits of Artificial Intelligence Advancements	This study examines the impact of super AI on auditing and investigative practices, highlighting benefits and risks like automation, ethical issues, and security concerns. It stresses the need for careful assessment and strategic measures to mitigate risks and maximize AI benefits, offering recommendations for audit professionals in Türkiye.
[21]	Markert T., Langer F., Danos V.	GAFAI: Proposal of a Generalized Audit Framework for AI	This paper introduces the Generalized Audit Framework for ML-based AI Applications (GAFAI), addressing the challenges of robustness, explainability, and transparency in AI systems. It proposes a risk-driven approach with generalized and application-specific requirements to enhance auditability, aiming to bridge existing gaps in auditing ML technologies.
[22]	Fedyk A., Hodson J., Khimich N., Fedyk T.	Is artificial intelligence improving the audit process?	This study investigates the impact of artificial intelligence (AI) on audit quality and efficiency using a dataset of over 310,000 resumes from major audit firms. It reveals that AI investments correlate with improved audit quality, reduced audit fees, and eventual displacement of human auditors over several years. Centralized AI functions within firms focus on enhancing audit quality and efficiency, as confirmed by interviews with audit partners from top U.S. firms
[23]	Nur Muslihatun F.A., Sunarfri Hantono B., Fauziati S.	Using Artificial Intelligence Technology for Decision Support System in Audit Risk Assessment: A Review Paper	This paper explores the integration of Artificial Intelligence (AI) in internal audits, emphasizing risk assessment improvements amidst the COVID-19 pandemic. It highlights AI's role in enhancing audit efficiency through advanced models like logistic regression, decision trees, neural networks, and support vector machines, alongside expert systems and fuzzy theory for comprehensive risk management.

[24]	Zhu S.	Audit and technology	This research explores the impact of the Fourth Industrial Revolution on auditing and accountancy, focusing on the adoption of Data Analytics, Machine Learning, and Distributed Ledger Technology. It identifies key drivers behind the demand for these technologies in auditing while highlighting challenges and implications for auditors adapting to these advancements.
------	--------	----------------------	--

4.3.3 PRISMA results and analysis

Following the comprehensive research conducted for this study, adhering to the PRISMA methodology as previously outlined, let's proceed to the critical phase of results analysis. This involves a detailed examination of each included article to extract their primary contributions and address the research questions posed.

Each selected study will be systematically reviewed to identify key findings, methodologies, and implications relevant to our investigation of AI's impact on traditional auditing and investigative practices. The aim is to synthesize the data to discern patterns, correlations, and gaps within the existing literature.

By rigorously analyzing these contributions, we seek to provide a coherent and comprehensive understanding of how AI is transforming the audit profession, including ethical considerations and evolving roles. This analytical process will enable us to formulate evidence-based conclusions and recommendations, thus contributing to the broader academic and professional discourse on AI integration in auditing and investigative fields.

The references indicated by #[number] are not traditional bibliographic references but serve to facilitate easier reading of the text. They reference the table above (table 15), which lists selected articles pertinent to addressing the research questions. This approach ensures that readers can quickly identify and locate the relevant studies supporting the research findings, thereby enhancing comprehension and engagement with the material; by linking the narrative to specific entries in the table, the text maintains a clear and organized structure, aiding in the systematic exploration of the chosen literature.

RQ1 - What is the present state of research within this domain?

Before analyzing the current context and the state of the art from different perspectives, it is important to highlight that for the topic of "IT Audit" there has not been a significant amount of research, indicating a need for further investigation and development of more comprehensive studies in this area. Considering that the field of IT Audit emerges as a guarantee and support for financial auditing, ensuring that the information from the systems is reliable and can be used for financial auditing, the collected articles are mostly applied in the more traditional context of financial auditing. However, AI applications can be used and transferred to the context of IT Audit, since auditing an entity is conducted as a whole and not as a division of processes between the financial and IT areas. With this in mind, we proceed with the analysis.

When evaluating the state-of-the-art research in this area, the primary focus is on the current research in AI and its relationship with auditing, as well as the ontologies present in the literature. The aim is to understand how the industry and researchers are addressing this thematic area, rather than delving into specific AI techniques and their applications to particular problems. This approach allows for a broader

understanding of the overarching trends and implications of AI in auditing, facilitating a comprehensive assessment of the field's development and identifying potential areas for future research and application.

Currently, several factors influence the investment in AI within the auditing sector. Economic and technological contexts are particularly crucial, as they dictate that companies, especially professional service firms, must increasingly invest in research and development (R&D) to achieve technological advancement, [#3]. This investment is vital for enhancing efficiency and maintaining competitiveness. Furthermore, with the rapid pace of digitalization, companies that fail to keep up with these advancements risk becoming obsolete, [#3]. Therefore, the integration of AI in auditing is not only a means to improve operational effectiveness but also a strategic imperative for sustaining relevance in the evolving digital landscape, [#3, #19].

In 2017, the Chief Innovation Officer at Deloitte, New York, stated that the adoption of technologies has significantly transformed audit processes towards greater digitalization [#5]. This trend is underscored by forecasts indicating a 94% likelihood that automation will supplant accountants and auditors by mechanizing a wide spectrum of both routine and non-routine cognitive tasks, [#5]. Moreover, industry analysts suggest that artificial intelligence (AI) is anticipated to conduct approximately 30% of corporate audits by 2025, [#5]. Consequently, these emerging digital technologies are poised to introduce novel opportunities and challenges within the realms of accounting and auditing, shaping the future landscape of these professions, having Big-Fours currently investing 9 billion dollars, to integrate AI in the audit profession [#12]. However, despite the transformation of the audit workforce and processes, it is expected that only lower-value tasks will be replaced, thereby enabling the evolution of the field and profession towards more sophisticated analyses, [#7, #12]. This shift is anticipated to enhance the professional judgment of auditors, emphasizing their critical role in interpreting complex data and making informed decisions, [#7].

In recent years, there has been an increasing trend of integrating AI, particularly Machine Learning (ML), into accounting and auditing. ML, a computational technique capable of identifying hidden patterns in data and making predictions or classifications, has been at the forefront of research and application in these fields, [#2, #10]. The primary focus has been on enhancing predictive performance. However, a significant challenge remains: the lack of explainability in complex AI models, [#2, #10]. While AI can identify outlier transactions in audit settings, it struggles to elucidate why these transactions are flagged and what specific aspects auditors should investigate, thereby impeding auditors' ability to explain the model's output and reliability, [#2]. However, there are other AI techniques and tools that have been explored, [#10]. According to the study "Modernization of IT: from critical to digital transformation," conducted by Vanson Bourne [#8], a technology research company, the most sought-after tools include process automation using robots (63%), intelligent automation (61%), and cognitive automation (59%). Increased productivity (85%) and cost savings (62%) are identified as the primary factors influencing organizations to adopt AI. These findings underscore the strategic importance of AI technologies in enhancing operational efficiencies and reducing operational costs across various sectors, [#8].

Another significant topic concerning the implementation of AI in audit is the risks associated with auditing processes, [#9]. Given the impracticality of analyzing all information within an entity, audits typically rely on sampling rather than full entity data review, [#9]. This sampling approach inherently increases the risk of fraud due to potential oversights in substantive testing, [#9]. Therefore, the application of AI in this context has the potential to enhance fraud detection by enabling comprehensive analysis of larger

datasets and identification of anomalous patterns more effectively than traditional methods, [#9]. The study highlighted a positive correlation between increased AI utilization in audit processes and improved fraud detection rates, [#9].

Furthermore, companies are investing in key audit processes and areas, specifically by adopting fully integrated, knowledge-driven approaches enabled through AI, [#18]. These investments result in improved data quality, reduced time consumption and overall audit duration, personalized audit procedures, and enhanced auditor productivity, [#19]. This technological integration not only streamlines audit activities but also elevates the effectiveness and efficiency of the auditing process, [#22, #24].

In terms of the application of AI in internal audits not only enhances assurance on sampled data but also extends the capability to audit the entire population, [#11]. This advancement promises heightened stakeholder satisfaction with organizational operations and governance, as internal audits become more comprehensive, systematic, proactive, predictive, and adept at detecting fraud, [#11]. Stakeholders can consequently take prompt action on potential fraud issues, [#11]. Moreover, investing in AI within the internal audit function enables organizations to identify and cultivate new skills necessary for the effective adoption of AI in audit tasks, emphasizing the importance of training and skill development initiatives, [#11].

Despite substantial investment in R&D, companies increasing their investment in AI for auditing processes become more vulnerable to cyberattacks, [#15]. This heightened risk necessitates careful consideration when restructuring and incorporating technology into auditing. To summarize, proper safeguards and cybersecurity measures must be integrated to protect the integrity and security of the auditing processes, [#15].

RQ2 - What are the primary concerns/issues regarding the utilization of artificial intelligence in auditing processes for both businesses and governmental entities?

When examining the primary issues associated with the utilization of AI in organizations and governmental entities, it is evident that several previously identified disadvantages are also relevant in this context. However, the research literature emphasizes certain aspects that have a more profound impact on these entities. Notably, concerns regarding data security, privacy, and the ethical implications of AI-driven decisions are paramount. Furthermore, the transparency and explainability of AI algorithms, potential job displacement, and the need for comprehensive regulatory frameworks are critical considerations. These factors underscore the necessity for a balanced approach to AI integration, ensuring that its benefits are maximized while addressing the inherent challenges and risks, [#20].

The application of AI in organizations, particularly in auditing, has significant impacts and presents complex challenges. These challenges extend beyond organizational boundaries to encompass broader macro-level contexts, including social, economic, ethical, data-related, political, and legal dimensions, [#4, #6, #19].

In the macro context related to auditing practice, several ethical challenges need to be considered, including responsibility and the explanation of decisions made by AI, the interaction between AI processes and human behavior, the compatibility of machine versus human value judgments, moral dilemmas, and AI-induced discrimination, [#4, #6, #17].

From a technological and data perspective, the integrity of AI algorithms and systems becomes crucial for auditors' analyses and professional judgment, [#21]. Key challenges include the quantity and quality of input data, transparency and reproducibility, lack of data integration and continuity, absence of data standards, vulnerability to adversarial attacks, lack of transparency and interpretability, AI safety, the specialization and expertise of the workforce, and complexities in interpreting unstructured data, [#4, #6, #17]. For instance, the reliability of AI algorithms and systems is contingent upon the integrity of the algorithms they utilize, [#17, #20]. Should these algorithms exhibit biases or inherent flaws, the resultant analyses may be erroneous or misleading. Such inaccuracies can precipitate unwarranted allegations of fraud or other malfeasance, engendering significant repercussions for both individuals and organizations, [#20].

Another significant risk associated with the automation of auditing and investigative processes by advanced AI systems pertains to ethical considerations. AI systems may not inherently incorporate ethical principles in their decision-making processes, potentially resulting in actions that do not align with the best interests of individuals or society at large, [#20, #24]. For instance, an AI system programmed to optimize profits may disregard the adverse environmental or societal impacts of its actions, [#20]. Moreover, the escalating deployment of AI in auditing and investigative processes has substantial implications for the roles of auditors and investigators, [#12, #20]. As automation increases, these professionals may transition from traditional auditing and investigative tasks to roles that demand greater judgment and interpretive skills, [#20, #21]. This shift necessitates the acquisition of new competencies and knowledge to adapt to the evolving demands of their profession, [#12, #20].

In the political-legal and socio-economic contexts, there are multifaceted challenges at both macro and micro levels, including issues such as copyright, governance of autonomous intelligence systems, responsibility and accountability, privacy and safety, national security threats, and the absence of clear accountability rules for AI use, [#4, #11, #20]. Furthermore, there are significant costs associated with human resources legally required to oversee AI-based decisions, a lack of official industry standards for AI use and performance evaluation, questions about the realism of AI applications, and a need for a better understanding of audit process requirements, [#4, #20]. Additionally, organizations face resistance to data sharing, a scarcity of in-house AI talent, concerns about the potential replacement of the human workforce, and a lack of comprehensive strategies for AI development, [#4].

The implementation of AI systems in auditing and its processes presents several additional challenges. First, there is a growing dependence on AI systems, which can be compromised through hacking, leading to data manipulation and erroneous conclusions, [#20]. Moreover, AI systems might fail to detect anomalies that human auditors can identify, resulting in the incorrect classification of data, [#20]. Second, there is a notable lack of technical expertise, which could lead to a shortage of skilled professionals in the field, thereby affecting the quality of services provided, [#20]. Lastly, significant security concerns arise as hackers may exploit system vulnerabilities to access sensitive data, potentially causing substantial financial losses and reputational damage for both audit and investigation professionals and their clients, [#20].

Lastly, while audit sampling is a well-established practice that enhances audit efficiency, it exhibits limitations that are increasingly pronounced in the era of big data, [#1]. Audit sampling provides only a limited view of the entire population, making it challenging to obtain a sample that accurately reflects the characteristics of the vast population, [#1]. Consequently, there exists a sampling risk—the likelihood that

auditors might reach different conclusions if the entire population were audited rather than just a sample. This risk is particularly pronounced as the sample size decreases, [#1]. Therefore, the ratio between the sample size and the population size serves as a proxy for assessing sampling risk, [#1]. This inherent limitation underscores the necessity of exploring more comprehensive approaches in the context of big data to ensure audit reliability and accuracy, [#1].

RQ3 - Which artificial intelligence techniques are currently deemed efficacious in addressing the challenges within this area?

The application of audit data analytics significantly enhances the effectiveness of internal audits. A growing body of literature in accounting demonstrates the application of machine learning (ML) to discern data patterns and predict financial statement fraud and future earnings, [#1]. When artificial intelligence (AI) and machine learning (ML) are incorporated into audit procedures, the sufficiency of audit evidence is improved, as AI/ML can automate specific audit procedures, such as full-population testing, [#1]

When AI/ML supports audit procedures by detecting anomalies or making predictions, auditors must consider which assertions are most relevant to the AI/ML outputs and assess the reliability of these outcomes, [#1, #2, #5]. Robotic Process Automation (RPA) further enables auditors to automate structured, repetitive, and rule-based audit tasks, including reconciliations, internal control testing, and detailed testing, [#5]. RPA is particularly effective for automating tasks characterized by the following attributes: stable environment, which leads to processes that have reached a mature state and undergo infrequent changes; rules-based that adhere to predetermined steps and do not rely on human judgment; low complexity with few exceptions and data sources; high volume of transactions that occur frequently; structured data based on organized text and numbers rather than unstructured data such as images and videos; accessing multiple systems that require interaction with multiple distinct software programs; and high error rate processes that are susceptible to human errors, [#5]. These technological techniques, particularly AI/ML and RPA, present a transformative potential for audit processes by improving accuracy, efficiency, and scope.

Another relevant topic is the fact that with advancements in audit data analytics and machine learning, full population testing has become a viable solution to address the limitations associated with traditional audit sampling, [#1]. Full population testing employs the concepts of "audit-by-exception" and "exceptional exceptions," enabling auditors to utilize audit data analytics to identify and prioritize anomalous or suspicious transactions, [#1]. By focusing on these prioritized transactions, auditors can significantly enhance both the effectiveness and efficiency of the audit process, [#1]. This approach ensures a more comprehensive examination of the entire data set, reducing the risks associated with sampling and improving the overall reliability of the audit outcomes, [#1].

The application of AI in predictive analysis for auditing significantly enhances the accuracy, reliability, and overall effectiveness of audit processes, [#15, #16]. By leveraging smaller data sets, incorporating non-conventional data streams, and generating synthetic data, AI provides robust solutions to modern auditing challenges. Additionally, AI's role in patch management, system state analysis, and security control identification underscores its potential to reduce errors and improve the integrity of audit outcomes, [#15].

Artificial intelligence possesses the capability to perform semi-structured and unstructured tasks, traditionally necessitating human intelligence, [#5] since encompasses a suite of technologies such as

natural language processing (NLP), natural language generation (NLG), computer vision, machine learning, virtual agents, and cognitive computing, [#5, #16]. These technologies have the potential to automate all phases of the auditing process, effectively transforming it into an assembly line where the output from one phase serves as the input for the subsequent phase, while additionally, supports the enhancement of professional judgment capabilities, facilitates the attainment of fair audit conclusions, and aids in the detection of misstatements. [#5, #16, #23].

Additionally other techniques such as NLP, can be utilized to review extensive volumes of contracts, while NLG facilitates the generation of text or speech from structured data, including analysis reports and company performance statistics or even systems, [#5, #16].

Modern tools such as machine learning and text/data mining have further enabled the analysis of unstructured and non-financial data, including emails, newspaper articles, and even big data. This advancement is poised to significantly transform the way auditors make decisions and gather audit evidence, [#5]. The integration of AI technologies represents a paradigm shift, enhancing the precision and efficiency of the auditing process, [#5].

According to a study conducted in [#13], in which 38 audit firms were included, the findings indicate that the majority of the respondents perceive artificial intelligence as a tool that enhances the performance of accountants and audit firms, [#13]. The results of this study further demonstrate that the implementation of artificial intelligence applications facilitates the making of unbiased decisions with high accuracy, [#13]. Additionally, AI offers auditors multiple solutions and alternatives during the decision-making process, thereby reducing the likelihood of errors in the audit process when issuing professional opinions, [#13]. The use of AI also increases the speed of issuing professional opinions and various reports, ensuring accuracy and confidence in their content, [#13]. Moreover, the integration of AI in auditing processes leads to better compliance with international accounting and auditing standards by audit firms, [#13].

In the study referenced in article [#20], significant advancements are observed in the development of in-house tools by the Big Four firms and software solutions created by other companies across various areas of internal and external audit processes.

Specifically for internal audit, the following technologies are notable: *Audit Management Software* automates internal audit procedures, allowing auditors to monitor, manage, and communicate audit progress, [#20]. In terms of leading software in this category includes *ProAuditor*, *KPMG Audit Intelligence*, and *Certify*; while in terms of Artificial Intelligence Audit Tools there are *Deloitte Analytics Studio*, *KPMG Audit Intelligence*, and *PwC's AI-powered audit software* enable auditors to analyze extensive datasets swiftly, detect potential risks, and automate repetitive tasks, [#20].

For external audit processes, distinct techniques and tools are utilized, including Robotic Process Automation (RPA) to automate manual tasks like data collection, analysis, and report generation, [#20]. Similarly to internal audit, there are artificial intelligence audit tools such as *PwC's AI-powered audit software*, *KPMG Audit Intelligence*, and *Deloitte Analytics Studio* facilitate large-scale data analysis, risk identification, and task automation, [#20]. In terms of software services, *Audit Management Software* streamlines the management of external audit operations, allowing external auditors to track audit progress, manage documentation, and communicate effectively with stakeholders, [#20].

Finally, for possible findings, conclusions and observations, that the auditors may have, there are *Fraud Detection Software* which utilizes advanced AI algorithms to enhance fraud prevention by analyzing extensive datasets, detecting patterns, anomalies, and issuing real-time alerts; and artificial intelligence audit tools such as *KPMG Audit Intelligence*, *Deloitte Analytics Studio*, and *PwC's AI technology-enabled audit software* are designed to streamline auditing processes through automated data analysis, risk identification, and task automation capabilities, [#20].

RQ4 - What are the advantages and disadvantages of applying AI techniques in this field?

Advantages:

- **Enhanced Efficiency:** AI automates repetitive tasks such as data collection, analysis, and reporting, thereby reducing the time and effort required for audits, [#15, #16, #18].
- **Improved Accuracy:** AI algorithms can process large volumes of data with high accuracy, minimizing human error and increasing the reliability of audit findings, [#15, #16, #19].
- **Real-time Monitoring and Detection:** AI enables continuous monitoring of IT systems, promptly detecting anomalies, security breaches, or irregular activities, [#5, #18, #20].
- **Advanced Data Analytics:** AI-driven analytics can uncover patterns, trends, and correlations in data that may not be easily identified using traditional methods, providing deeper insights into IT operations, [#5, #19, #20].
- **Risk Prediction and Prevention:** AI can predict potential risks based on historical data analysis, enabling auditors to proactively mitigate risks and strengthen cybersecurity measures, [#5, #19, #20].

Disadvantages:

- **High Initial Costs:** Implementing AI technologies in IT auditing requires substantial investment in infrastructure, software, and skilled personnel, which may be financially burdensome for organizations, [#12].
- **Complexity:** AI algorithms are complex and may require specialized knowledge and expertise to develop, deploy, and maintain effectively within audit processes, [#1].
- **Data Dependency:** AI's effectiveness heavily relies on the quality, completeness, and availability of data. Inaccurate or insufficient data can lead to biased results or inaccurate audit findings, [#1].
- **Ethical and Legal Issues:** The use of AI in auditing raises ethical concerns related to data privacy, transparency, accountability, and the potential impact on human auditing jobs. Ensuring compliance with legal regulations and standards is critical, [#6, #17].
- **Resistance to Change:** Organizations may face resistance from auditors or stakeholders accustomed to traditional audit methods, hindering the adoption and acceptance of AI-driven auditing practices, [#3, #19].

5 Application of Artificial Intelligence in expediting IT Audit processes

This chapter introduces a framework aimed at optimizing IT audit processes through the application of Artificial Intelligence (AI). The framework is meticulously crafted to enhance the efficiency and effectiveness of audits by integrating various AI methodologies. Its design prioritizes flexibility and accuracy, catering to the dynamic requirements of the audit lifecycle. By leveraging AI, the framework seeks to streamline audit procedures, from initial risk assessment to comprehensive analysis and reporting. This approach not only aims to expedite audit tasks but also aims to enhance the reliability and depth of audit outcomes. The framework's adaptability ensures it can accommodate diverse audit environments and technological landscapes, thereby offering a robust foundation for advancing audit practices in alignment with contemporary technological advancements.

5.1 Assumptions

Based on the findings from the literature review, it has been determined that a framework for the application of Artificial Intelligence in IT audit processes should encompass several critical assumptions.

These assumptions provide a foundational basis for implementing AI in both internal and external audit processes, ensuring that the integration is feasible, effective, and aligned with organizational goals and regulatory frameworks.

- **Technological Readiness:** It is assumed that the organization has the necessary technological infrastructure and capabilities to implement AI techniques such as Machine Learning, Natural Language Processing (NLP), Predictive Analytics, Robotic Process Automation (RPA), Data Mining, and AI-driven Dashboards.
- **Data Availability:** The availability of structured and unstructured data necessary for AI techniques to perform effectively is assumed. This includes data related to risk assessment, compliance, controls, audits, cybersecurity, governance, system integrity, third-party risks, regulatory compliance, supplier audits, IT infrastructure, data privacy, cloud security, and disaster recovery.
- **Integration Feasibility:** The framework assumes that AI techniques can be seamlessly integrated into existing IT audit processes without significant disruption to operational workflows or compromising audit quality.
- **Skill and Expertise:** It is assumed that the organization possesses or can acquire the necessary expertise in AI technologies and methodologies to effectively deploy and utilize them in audit processes.

- **Regulatory and Ethical Compliance:** The framework operates under the assumption that AI applications in auditing comply with relevant regulatory requirements and ethical standards, particularly concerning data privacy, confidentiality, and the ethical use of AI.
- **Continuous Improvement:** The organization is committed to continuous improvement and adaptation of AI techniques in audit processes, based on feedback, advancements in AI technologies, and evolving audit requirements.

5.2 Framework AROP

The AROP (AI-Integrated-Audit and Review Optimization Process) framework represents a new approach that integrates advanced AI techniques with IT audit's internal and external processes.

This framework aims to enhance the efficiency, accuracy, and comprehensiveness of audits by leveraging AI capabilities such as machine learning, natural language processing, and data analytics.

AROP framework systematically incorporates these technologies into various audit stages, from planning and execution to reporting and follow-up, ensuring a more robust and dynamic audit process, by addressing both internal controls and external regulatory requirements, AROP provides a holistic and adaptive model for modern IT auditing practices, see below in table 16.

Table 16: Framework

		Artificial Intelligence Techniques					
		T1	T2	T3	T4	T5	T6
Audit Processes	Internal	P1		c)			
		P2	a)		d)		f)
		P3	a)	b)	d)		f)
		P4	a)	c)			f)
		P5		b)		e)	f)
		P6	a)	c)		e)	
		P7				e)	
	External	P8		b)			
		P9	a)	b)			
		P10	a)	b)	d)		f)
		P11	a)	b)	d)	e)	f)
		P12		b)	d)	e)	
		P13			d)		f)

Explanation of Techniques (T1 to T6):

T1: Machine Learning

T2: Natural Language Processing

T3: Predictive analytics

T4: Robotic Process Automation (RPA)

T5: Data mining

T6: AI-driven dashboards

Explanation of the Audit Processes Internal and External, (P1 to P13):

Internal Processes:

P1: Planning and Risk identification and assessment

P2: Compliance monitoring

P3: Control testing and documentation of deficiencies

P4: Continuous auditing and evidence assessment

P5: Fraud detection

P6: IT governance evaluation

P7: System and data integrity checks

External Processes:

P8: Third-party risk management, suppliers and service organizations

P9: Regulatory compliance

P10: IT infrastructure which includes databases, operating systems and domain/network audits

P11: Cloud security assessments

P12: Disaster recovery planning, Backups and IDS/IPS

P13: Findings, conclusions, recommendations and reporting

Key:

a): Machine Learning for anomaly detection in compliance monitoring and cybersecurity.

b): Natural Language Processing for document analysis in control testing.

c): Predictive analytics for risk assessment in systems, data and continuous auditing.

d): Robotic Process Automation (RPA) for automating routine tasks.

e): Data mining for identifying patterns and trends in IT governance evaluation and system integrity checks.

f): AI-driven dashboards for real-time monitoring and reporting in audits.

5.3 Strategy for the implementation of the AROP Framework in IT Audit

The strategy for integrating Artificial Intelligence (AI) into IT audit processes aims to enhance efficiency, accuracy, and compliance. By leveraging AI techniques such as Machine Learning, Natural Language Processing, Predictive Analytics, Robotic Process Automation, Data Mining, and AI-driven Dashboards, organizations can streamline audit tasks, detect anomalies, and automate routine procedures. This strategy involves thorough planning, skill development, pilot projects, phased implementation, strict adherence to regulatory and ethical standards, and continuous improvement. Ensuring the necessary technological readiness, data availability, and integration feasibility are crucial for seamless AI adoption in auditing.

5.3.1 Strategy and Detailed Process Description

1. Assessment and Planning

Technological Readiness: Assess the current technological infrastructure to ensure it supports AI implementation. Additionally, identify gaps, and plan upgrades, if necessary.

Data Availability: Identify and prepare structured and unstructured data necessary for AI applications, as well as compile and cleanse the respective data.

Integration Feasibility: Conduct feasibility studies to identify potential integration challenges and solutions.

2. Skill Development

Training Programs: Design and develop training programs for current employees on AI techniques that are relevant for the IT audit processes such as: Machine Learning, NLP, Predictive Analytics, RPA, Data Mining, and AI-driven Dashboards.

Hiring Expertise: Recruit or contract AI specialists to supplement existing skills within the organization.

3. Pilot Projects

Internal Processes: Start with internal audit processes such as P1-P7 while applying the respective T1-T6.

External Processes: Initiate pilots in external audit processes from P8-P13, with the AI techniques associated (T1-T6).

4. Implementation Phases

Phase 1: Implement AI in high-priority areas identified in pilot projects. Example: Implement AI-driven dashboards (T6) for real-time monitoring and reporting in high-priority areas like Continuous Auditing (P4).

Phase 2: Scale AI techniques to other processes gradually, ensuring minimal disruption. Example: Expand AI integration to other processes such as Fraud Detection (P5) and Disaster Recovery Planning (P12), ensuring staff adaptation and process stability.

Phase 3: Continuous monitoring and adaptation based on feedback and advancements in AI technology.
Example: Refine processes to improve effectiveness and efficiency.

5. Regulatory and Ethical Compliance

Compliance Checks: Regularly review audit AI implementations for compliance with regulatory, ethical and industry standards.

Ethical Guidelines: Develop and enforce guidelines for ethical AI use, particularly around data privacy and confidentiality.

6. Continuous Improvement

Feedback Mechanism: Create channels for regular feedback from users and stakeholders on AI effectiveness and areas for improvement.

Technology Updates: Stay updated with the latest advancements in AI and integrate them into the audit processes.

Below is a summary chart of the strategy and process for integrating AI into audit processes.

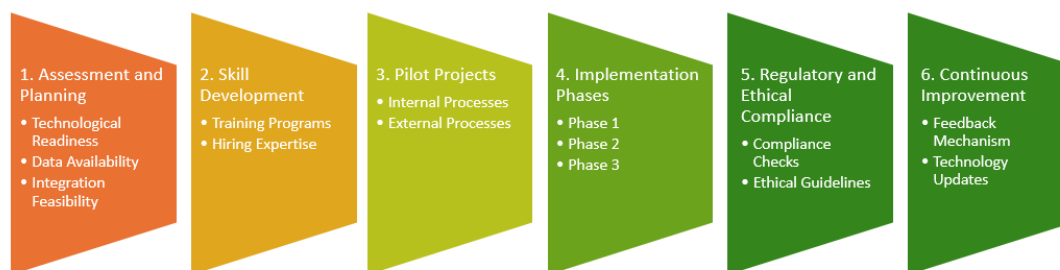


Figure 14: Strategy and process for implementation of AI in IT Audit

5.4 Use case – Demonstration

This subchapter will demonstrate the application of the framework introduced in the preceding section through a fictional case study. The case study is designed to illustrate how the framework can be utilized in practice. Given that this scenario is purely hypothetical, the examples of tools and models provided are illustrative and do not constitute exhaustive or real-world inputs. The objective is to showcase the framework's potential application and effectiveness, rather than to provide a comprehensive or accurate representation of actual tools and methods used in practice.

Case Study: Application of the AROP Framework in an IT Audit Project

Background and Company Overview:

TechSolutions Inc., a leading provider of IT consulting and audit services, has been contracted by *Innovatech Solutions*, a multinational technology company specializing in cloud-based solutions and enterprise software. *Innovatech Solutions* has recently expanded its operations globally and has encountered several challenges related to its IT infrastructure, including compliance with new regulations, data security concerns, and efficient management of its growing network of third-party vendors.

Additionally, given that *Innovatech Solutions* is a multinational company operating in various countries, the need for compliance and transparency has become even more critical. The company hired *TechSolutions Inc.* to conduct a comprehensive audit of its systems, with the aim of providing its investors with robust validation of its internal control practices and regulatory compliance. The audit seeks to ensure that all processes and controls are aligned with international standards and local regulations, safeguarding data integrity and system security. This detailed validation is essential for enhancing investor confidence and maintaining *Innovatech Solutions'* global reputation.

In light of these challenges, *Innovatech Solutions* has engaged *TechSolutions Inc.* to perform a comprehensive IT audit using the AROP (AI-Integrated Audit and Review Optimization Process) framework to enhance their audit processes and address these issues effectively.

Practical Application of the AROP Framework:

In this case study, *TechSolutions Inc.* applies the AROP framework to *Innovatech Solutions'* IT audit project. The project encompasses both internal and external audit processes, leveraging a suite of AI techniques to streamline operations, improve accuracy, and provide actionable insights.

- **Internal Processes**

The audit project begins with the **planning and risk identification** phase, where *TechSolutions Inc.* utilizes *Predictive Analytics* (T3) to assess potential risks and forecast future issues based on *Innovatech's* historical data and current operational metrics. This predictive approach allows the audit team to focus on high-risk areas and allocate resources more efficiently. After this assessment, *AI-Driven Dashboards* (T6) are used to visualize the risk assessment results in real time, providing the audit team with an intuitive interface to monitor evolving risk profiles and adjust their strategies accordingly.

During the **compliance monitoring** phase, *Machine Learning* (T1) algorithms are deployed to detect anomalies and deviations from regulatory requirements. This AI-driven approach enhances the efficiency of compliance checks by identifying patterns that may indicate non-compliance. The *Robotic Process Automation* (T4) is also utilized to automate routine compliance monitoring tasks, reducing the manual workload and ensuring consistent application of compliance criteria, while the *AI-Driven Dashboards* (T6) further support this phase by offering real-time insights into compliance status and trend analysis.

For **control testing and documentation of deficiencies**, the audit team employs *Machine Learning* (T1) to identify deviations in control mechanisms. In order to have a more precise and accurate documentation of the controls and deficiencies, *Natural Language Processing* (T2) is used to analyze control-related documentation and communications, extracting relevant information and assessing control effectiveness.

Taking into consideration last audits information, *Predictive Analytics* (T3) helps evaluate the potential impact of identified deficiencies, while *Robotic Process Automation* (T4) automates repetitive control

testing procedures and in order to present a consolidated overview of the IT Audit process, *AI-Driven Dashboards* (T6) provide a comprehensive view of control testing results, highlighting areas of concern and progress.

The phase of **continuous auditing and evidence** assessment involves the use of *Machine Learning* (T1) to continuously analyze audit evidence for anomalies, enabling the team to detect issues in near real time and *Predictive Analytics* (T3) is employed to forecast future evidence needs and adjust audit procedures dynamically, while *AI-Driven Dashboards* (T6) support ongoing assessment and decision-making.

Fraud detection is a critical component of the audit project, *Natural Language Processing* (T2) is used to analyze textual data, such as emails and reports, for signs of fraudulent activity and at the same time, *Data Mining* (T5) techniques are applied to identify unusual patterns and trends that may indicate fraud and *AI-Driven Dashboards* (T6) offer real-time monitoring and reporting of suspicious activities, allowing the audit team to respond promptly.

In evaluating **IT governance**, *Machine Learning* (T1) is applied to assess governance practices and identify areas for improvement while *Predictive Analytics* (T3) helps evaluate potential governance risks and their impact on the organization and additionally *Data Mining* (T5) is utilized to extract insights from governance-related data, supporting more informed decision-making.

For the last process, **system and data integrity checks** involve *Data Mining* (T5) to detect patterns and anomalies in system operations and data integrity, as well as *AI-Driven Dashboards* (T6) are used to visualize integrity check results and monitor system performance, providing actionable insights into system and data reliability.

- **External Processes**

For external audit processes, *TechSolutions Inc.* applies *Natural Language Processing* (T2) to analyze **third-party contracts and communications** for risk indicators related to third-party risk management. The utilization of *Machine Learning* (T1) ensures **regulatory compliance** by automating the review of compliance data, while *Natural Language Processing* (T2) extracts and validates information from regulatory documents.

In auditing **IT infrastructure**, *Machine Learning* (T1) assesses security and performance issues, *Natural Language Processing* (T2) reviews related documentation, *Predictive Analytics* (T3) forecasts potential vulnerabilities, *Robotic Process Automation* (T4) automates routine tasks, and *AI-Driven Dashboards* (T6) provide real-time insights.

For **cloud security assessments**, *Machine Learning* (T1) evaluates cloud security configurations, *Natural Language Processing* (T2) reviews documentation, *Predictive Analytics* (T3) forecasts threats, *Robotic Process Automation* (T4) automates assessments, *Data Mining* (T5) identifies patterns, and *AI-Driven Dashboards* (T6) visualize cloud security metrics.

Disaster recovery planning, backups, and IDS/IPS evaluations benefit from *Natural Language Processing* (T2) to review disaster recovery plans, *Robotic Process Automation* (T4) to verify backup processes, *Data Mining* (T5) to analyze historical data for recovery improvements, and *AI-Driven Dashboards* (T6) to monitor recovery status and backup integrity.

Finally, for **findings, conclusions, recommendations, and reporting**, *Robotic Process Automation* (T4) is used to generate audit reports and recommendations efficiently and *AI-Driven Dashboards* (T6) offer visual tools for presenting findings and recommendations, ensuring clear and actionable reporting.

5.5 Evaluation & Discussion

To validate the proposed framework, semi-structured interviews were conducted with three experts from diverse yet relevant backgrounds within the IT Audit and IT Advisory sectors.

The interviewees included one expert is an IT Senior Manager with a background in IT Advisory specializing in AI and cloud implementations at a major Big Four firm, and two professionals with a background in IT Audit—specifically, an IT Manager and a Senior Consultant—at the same firm, (see table 17, for more detail). These IT Audit professionals not only engage in auditing practices but also participate in assurance projects for various audit clients. The diverse expertise of these participants provided a comprehensive evaluation of the framework from both IT Audit and Advisory perspectives.

Table 17: Background and expertise of the professionals

Expert	Knowledge & Experience	Current Domain
E1	IT Advisory Senior Manager: • Applications, cloud, DevOps; • Implementation of cloud and AI processes.	Salesforce, SAP, Azure, OutSystems and in-house applications.
E2	IT Audit Manager: • Technology, Media & Telecommunications; • Consumer, retail and automotive; • Energy, resources & industrials; • Financial Services (Assurance); • Government & Public Services; • Life Sciences & Health Care.	Audit and Assurance in PCAOB and ISA.
E3	IT Audit Senior Consultant: • Technology, Media & Telecommunications; • Consumer, retail and automotive; • Energy, resources & industrials; • Financial Services (Assurance); • Government & Public Services; • Life Sciences & Health Care.	Audit and Assurance in ISA.

The interviews were individually conducted with each expert in July, utilizing video conferencing platforms such as Zoom and Microsoft Teams. Each participant consented to audio recording to facilitate accurate transcription of the conversations, which are included as appendices (Appendix B to Appendix D) in the master's thesis.

The names of the interviewed professionals were kept anonymous at their request. Additionally, the transcription of the recordings was limited to excerpts necessary for the discussion and evaluation of the subject matter addressed during the interviews.

Prior to conducting the interviews, a comprehensive interview guide was prepared outlining the research objectives, the AROP implementation framework, and the associated strategy. Additionally, four specific questions were formulated and disseminated to each participant in advance. These questions, (APPENDIX A), were as follows:

Q1: Do you consider the proposed framework as useful and why? If not, why do you believe it is not?

Q2: Do you have any criticism towards the proposed framework? Please explain.

Q3: Would you consider implementing the proposed framework? Please clarify why/ why not.

Q4: Do you have any recommendation or suggestions for further improvements of the proposed framework?

The questions were carefully designed to guide and encourage the experts to critically evaluate the framework, ensuring a predetermined thematic frame and structure for the interviews. By providing a consistent theoretical framework, the methodology facilitated the comparison of responses, enabling the identification of both positive similarities and areas for improvement.

The interviews provided a platform to investigate diverse perspectives and extract the unique expertise of each participant. This structured approach ensured that the discussions remained focused on the evaluation of the framework while allowing for a comprehensive analysis of varying viewpoints. The consistency in questioning also allowed for the systematic identification of recurrent themes, facilitating a deeper understanding of the framework's strengths and limitations.

By eliciting detailed feedback from professionals with different backgrounds within IT audit and advisory domains, the study was able to capture a wide range of insights. This approach not only highlighted common areas of agreement but also uncovered specific criticisms and suggestions for enhancement. Consequently, the interviews contributed significantly to the assessment of the AROP framework, providing valuable input for its refinement and further development.

Below in table 18, it's possible to find the different interviews summarized, (for the complete interviews see appendix B-D).

Table 18: Expert Summarized Interview and points of view

Expert	Summarized Interview and points of view
E1	E1, an IT Advisory Senior Manager with extensive experience in cloud and AI implementations, recognized the framework's potential to enhance audit efficiency and accuracy. E1 particularly noted the value of machine learning for anomaly detection and predictive analytics for risk assessment. However, E1 highlighted the need for industry-

	specific adaptations and expressed concerns about the significant training and infrastructure requirements necessary for successful implementation.
E2	E2, an IT Audit Manager with a broad background in multiple industries, offered a more cautious perspective. E2 acknowledged the framework's utility but stressed that it appeared overly optimistic about the ease of integrating AI into existing audit processes. Moreover, E2 pointed out that the framework should consider the practical aspects of implementation, such as the need for substantial change management and the potential disruption to current practices.
E3	E3, an IT Audit Senior Consultant, provided a balanced view, acknowledging both the strengths and limitations of the AROP framework. E3 appreciated the framework's structured approach to incorporating AI and its potential to enhance audit processes. Nonetheless, E3 voiced concerns about the impact on employment, noting that AI integration could reduce the need for certain audit roles, thereby creating resistance among staff. E3 also underscored the necessity of a robust change management plan to support the workforce transition.

- **Feedback and Opportunities for enhancement and development**

The feedback from experts E1, E2, and E3 reveals favorable attributes and opportunities for refining the AROP framework.

All three experts acknowledged the framework's robust structure and its potential to enhance audit processes through the integration of advanced technologies. Expert 1 appreciated the framework's comprehensive approach to incorporating machine learning and predictive analytics, which are instrumental in improving anomaly detection and risk assessment. Similarly, Expert 3 recognized the structured methodology as a significant strength, noting its ability to systematically integrate AI into audit processes.

Expert 2, despite a more cautious perspective on the ease of integration, agreed that the framework offers valuable insights into leveraging AI for audit improvements. The consensus among the experts highlighted the framework's potential to drive efficiency and accuracy in audits. The structured approach to incorporating AI, as outlined by the framework, was particularly praised for its emphasis on enhancing audit quality and process effectiveness.

Additionally, the experts commended the framework's focus on incorporating cutting-edge technologies and providing a clear, systematic methodology. This structured approach facilitates a thorough understanding of how AI can be integrated into audit processes, thereby offering a strong foundation for future developments and refinements.

In terms of the opportunities, expert 1 and expert 2 emphasized the necessity for industry-specific adaptations, suggesting that the framework could benefit from modular components that allow customization according to sector-specific requirements. This adaptation would enhance the framework's relevance and applicability across diverse industries, ensuring that its recommendations are tailored to the unique needs of various sectors.

Expert 2 advised on the framework's potentially overly optimistic view regarding the ease of AI integration into existing audit processes. This feedback underscores the need for a more nuanced approach that

includes practical guidelines for managing change and mitigating potential disruptions to established practices and possible future iterations of the framework should incorporate detailed strategies for implementing AI technologies, including robust change management protocols and actionable steps to address operational challenges.

Expert 3 highlighted concerns about the potential impact of AI on employment within the audit profession. To address these concerns, the framework should integrate strategies for workforce transition, including reskilling and redeployment initiatives. By considering the human element and providing support mechanisms for affected employees, the framework can facilitate a smoother transition to AI-enhanced audit practices.

In conclusion, the expert feedback highlights the AROP framework's strong potential for enhancing audit processes through AI integration. While its structured approach is commendable, improvements are needed in industry-specific adaptations, practical implementation, and workforce transition strategies. Addressing these areas will optimize the framework's effectiveness and relevance in modern audit environments.

6 Conclusions

This master's thesis has explored the development and evaluation of the AROP framework, aimed at integrating advanced technologies into audit processes. The framework's potential to enhance audit efficiency and accuracy through AI and machine learning was critically assessed. Through expert feedback, we gained valuable insights into the framework's strengths and areas for improvement. This conclusion synthesizes these findings, highlighting the framework's promising aspects and addressing the identified

challenges. By reflecting on the expert evaluations and the proposed refinements, this thesis provides a comprehensive overview of the framework's current capabilities and its potential for future advancements in audit practices.

6.1 Synthesis of the developed work

The primary objective of this research is to streamline IT audit procedures by leveraging AI technologies, with a dual focus on reducing audit duration and enhancing accuracy and efficiency. By integrating AI into the audit framework, the study aims to establish a cohesive and standardized approach that aligns with industry standards, thereby ensuring more reliable and timely audit outcomes. The synthesis of this work revolves around harnessing AI's capabilities to automate routine tasks, such as data collection, analysis, and risk identification, which traditionally require substantial time and effort. This automation not only accelerates the audit process but also minimizes human error, thereby improving the overall quality of audit findings. Moreover, the adoption of AI facilitates continuous auditing practices, enabling auditors to monitor transactions and systems in real-time, enhancing responsiveness to potential risks or anomalies. Ultimately, this synthesis underscores the transformative potential of AI in revolutionizing IT audit practices, emphasizing its role in optimizing resource allocation and bolstering audit effectiveness in contemporary organizational settings.

Since, this master's thesis focused on developing and evaluating the AROP framework, designed to integrate advanced technologies, such as AI and machine learning, into audit processes, it aimed to enhance audit efficiency, accuracy, and overall effectiveness by systematically incorporating these technologies.

The feedback from the expert interviews provided valuable insights into the framework's strengths and areas for improvement. Experts praised the framework's structured approach and its potential to advance audit practices through technological innovation. They specifically highlighted the merits of incorporating machine learning and predictive analytics for improved anomaly detection and risk assessment.

However, several critical areas for refinement emerged. Experts noted the need for industry-specific adaptations to ensure the framework's relevance across diverse sectors. There was also concern about the practical challenges of AI integration, including the need for detailed implementation guidelines and change management strategies. Additionally, the potential impact of AI on employment within the audit profession was identified, emphasizing the need for strategies to support workforce transitions.

In summary, while the AROP framework offers a promising foundation for enhancing audit processes through technology, its effectiveness will be significantly improved by addressing the identified areas of improvement. Future work should focus on tailoring the framework to specific industry needs, providing practical guidance for implementation, and supporting workforce adaptation to ensure its successful application in real-world audit environments.

6.2 Limitations

The limitations of a framework designed to enhance IT audit through AI involves identifying potential constraints that may affect its applicability and effectiveness in real-world scenarios. While frameworks are essential tools for guiding and standardizing practices, they are not without limitations that warrant consideration. Understanding these limitations is crucial for organizations seeking to adopt such frameworks to improve their audit processes.

Several notable limitations impact the effective deployment of AI in enhancing IT audit processes. Primarily, challenges arise in the domain of Data Quality and Availability, where AI models heavily depend on high-quality, comprehensive data to ensure accurate outcomes. Inadequate or incomplete data sets may introduce biases or lead to unreliable insights, compromising the efficacy of AI-driven auditing.

Some of the observed limitations are: integration challenges pose another significant hurdle, as integrating AI tools into existing IT audit frameworks can be intricate and time-consuming, as well as compatibility issues between diverse technologies and platforms further complicate seamless integration efforts, requiring careful planning and resource allocation; the skills and expertise Gaps represent a critical limitation, as the implementation and maintenance of AI technologies demand specialized technical knowledge and organizations often face difficulties in recruiting and retaining professionals proficient in AI, hindering the full realization of AI's potential in auditing practices; ethical and legal concerns also loom large, with AI's use in auditing raising profound ethical considerations related to data privacy, decision-making transparency, and accountability for AI-driven decisions; compliance with stringent legal regulations, especially in sensitive areas like data protection, presents additional complexities and risks; costs and resource Allocation present financial challenges, as the initial investment in AI infrastructure, software, and training can be substantial and ongoing expenses for maintenance and updates further strain financial resources, necessitating careful budgeting and justification; the complexity of AI algorithms poses significant interpretative challenges, particularly for auditors lacking deep expertise in AI principles, since ensuring the explainability and transparency of AI-generated audit decisions becomes crucial to maintain audit quality and foster stakeholder trust; the risk of over-reliance on AI underscores the importance of maintaining human oversight and critical judgment in audit processes; dependence on AI without adequate human scrutiny may lead to complacency or undue trust in automated outputs, potentially compromising audit integrity; resistance to change within organizational cultures presents a formidable barrier to AI adoption in audit practices; and lastly, overcoming internal resistance and fostering stakeholder buy-in are essential for successful AI integration and acceptance within auditing frameworks. Addressing these multifaceted limitations is imperative to harness AI's transformative potential while ensuring robust, ethical, and effective audit practices in the digital age.

Furthermore, this evaluation has been conducted solely from a theoretical standpoint, lacking practical implementation in real-world scenarios. Given that the framework aims to serve organizational needs, obtaining a definitive conclusion regarding its efficacy necessitates practical testing under real conditions. Such empirical validation is crucial to gaining a more realistic assessment of the framework's functionality, identifying areas of success, and pinpointing aspects requiring further refinement. Practical application enables organizations to ascertain the framework's operational feasibility, adaptability to varying contexts, and alignment with specific audit objectives. Only through empirical testing can the framework's

effectiveness in enhancing audit processes and delivering actionable insights be comprehensively evaluated.

6.3 Future work

In future endeavors, a pivotal aspect involves the practical implementation of the proposed framework within organizational settings. This step aims to empirically assess its efficacy and gather tangible outcomes.

The framework advocates for the integration of AI techniques in IT auditing, an area traditionally perceived as theoretical but increasingly supported by empirical evidence in the literature. Real-world application will provide clarity on these perceptions. Additionally, staying abreast of industry advancements is imperative to track technological evolution and the utilization of AI methodologies in IT audit practices. Some organizations may contemplate developing proprietary AI solutions where existing vendor offerings fall short. Future research should prioritize refining and adapting the framework based on empirical findings to address identified gaps effectively. This iterative process ensures alignment with emerging needs and advancements in the field of AI-driven IT auditing.

Building on the insights gained from expert feedback, future work should focus on refining the AROP framework to enhance its applicability and effectiveness. Key areas for development include customizing the framework for industry-specific needs to increase its relevance across various sectors. Practical implementation guidelines and comprehensive change management strategies are essential to address the challenges of integrating AI into existing audit processes. Additionally, strategies to mitigate the impact of AI on employment should be incorporated, ensuring a balanced transition for audit professionals. Future research should also explore case studies and pilot implementations to validate and further optimize the framework in real-world scenarios.

References

- The Guardian. (2019, July 15). Alan Turing to feature on new £50 note. The Guardian. <https://www.theguardian.com/business/2019/jul/15/alan-turing-to-feature-on-new-50-note>
- American Institute of Certified Public Accountants. *Reporting on controls at a service organization relevant to security, availability, processing integrity, confidentiality, or privacy* Durham, NC: American Institute of Certified Public Accountants; 2012. <http://www.aicpa.org/About/Pages/About.aspx>
- Arena, Marika & Azzone, Giovanni. (2009). INTERNAL AUDIT EFFECTIVENESS: RELEVANT DRIVERS OF AUDITEES SATISFACTION. <https://doi.org/10.1111/j.1099-1123.2008.00392>.
- Bochtis, D., & Sørensen, C. G. (2020). "Artificial Intelligence in Agriculture."
- Bojorque, R., & Pesántez-Avilés, F. (2020). Academic Quality Management System Audit Using Artificial Intelligence Techniques. In *Advances in Intelligent Systems and Computing* (Vol. 965, pp. 275–283). Springer Verlag. https://doi.org/10.1007/978-3-030-20454-9_28
- Cangemi, M. P. (2016). Views on internal audit, internal controls, and internal audit's use of technology. *EDPACS*, 53(1), 1–9. <https://doi.org/10.1080/07366981.2015.1128186>
- Chui, M., & Malhorta, S. (2018). Adoption of AI advances, but foundational barriers remain. McKinsey. <https://www.mckinsey.com/featured-insights/artificial-intelligence/ai-adoption-advances-butfoundational-barriers-remain>
- Chui, M., Hall, B., Singla, A., & Sukharevsky, A. (2021). Global survey: The state of AI in 2021. McKinsey. <https://www.mckinsey.com/business-functions/mckinsey-analytics/our-insights/global-surveythe-state-of-ai-in-2021>
- Code of Ethics, The Institute of Internal Auditors, (2013). <https://na.theiia.org/standards-guidance/mandatory-guidance/Pages/Code-of-Ethics.aspx>
- Code of Professional Ethics, ISACA, (2013). <http://www.isaca.org/Certification/Code-of-Professional-Ethics/Pages/default.aspx>
- Committee of Sponsoring Organizations of the Treadway Commission. Internal control—Integrated framework. New York (NY): Committee of Sponsoring Organizations of the Treadway Commission; 2013.*
- Davenport, T. H. (2019). "The Potential for Using AI in Hiring."
- Fedyk, A., Hodson, J., Khimich, N., & Fedyk, T. (2022). Is artificial intelligence improving the audit process? *Review of Accounting Studies*. <https://doi.org/10.1007/s11142-022-09697-x>
- Gantz, S. D. (2013, October 31). *The Basics of IT Audit*. Elsevier. http://books.google.ie/books?id=DW6tAAAAQBAJ&printsec=frontcover&dq=The+Basics+of+IT+Audit:+Purposes,+Processes,+and+Practical+Information+By+Stephen+D.+Gantz&hl=&cd=1&source=gbs_api
- Generally accepted auditing standards. New York (NY): American Institute of Certified Public Accountants, Auditing Standards Board; 2001 December. Statement on Auditing Standards 95.*

- Grotenhermen, J.-G., Bruckes, M., & Schewe, G. (2020). Are we Ready for Artificially Intelligent Leaders? A Comparative Analysis of Employee Perceptions Regarding Artificially Intelligent and Human Supervisors. AMCI, Proceedings. https://aisel.aisnet.org/amcis2020/ai_semantic_for_intelligent_info_systems/ai_semantic_for_intelligent_info_systems/12
- Hall, J. A. (2013). "Information Technology Auditing and Assurance."
- Hevner, A., Ram, S., March, S. T., & Park, J. (2004). Design Science in Information System Research. MIS Quarterly, 28(1), 75–105
- High, Peter. (2017, October 30). Carnegie Mellon Dean Of Computer Science On The Future Of AI. <https://www.forbes.com/sites/peterhigh/2017/10/30/carnegie-mellon-dean-of-computerscience-on-the-future-of-ai/?sh=2db2b26f2197>
- Holmes, W., Bialik, M., & Fadel, C. (2019). "Artificial Intelligence in Education: Promises and Implications for Teaching and Learning."
- Institute, I. G. (2007, January 1). COBIT® 4.1. Isaca. http://books.google.ie/books?id=vdC3wAEACAAJ&dq=IT+Governance+Institute.+COBIT+4.1.+IT+Governance+Institute%3B+2007.&hl=&cd=1&source=gbp_api
- ISO 19011:2011. *Guidelines for auditing management systems*. (n.d.).
- Karmańska, A. (2022). Artificial Intelligence in audit. Prace Naukowe Uniwersytetu Ekonomicznego We Wrocławiu, 66(4), 87–99. <https://doi.org/10.15611/pn.2022.4.06>
- Liberati, A., Altman, D. G., Tetzlaff, J., Mulrow, C., Gøtzsche, P. C., Ioannidis, J. P. A., Clarke, M., Devereaux, P. J., Kleijnen, J., & Moher, D. (2009). The PRISMA statement for reporting systematic reviews and meta-analyses of studies that evaluate health care interventions: explanation and elaboration. In Journal of clinical epidemiology (Vol. 62, Issue 10). <https://doi.org/10.1016/j.jclinepi.2009.06.006>
- Luckin, R. (2017). "Artificial Intelligence in Education: Promises and Implications for Teaching and Learning."
- Microsoft. (2021). AI Business Basics. 17.
- Mohanty, S. P., Hughes, D. P., & Salathé, M. (2016). "Using Deep Learning for Image-Based Plant Disease Detection."
- Moher, D. (2009). Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement. Journal of Clinical Epidemiology, 62(10), 1006–1012. <https://doi.org/10.1016/j.jclinepi.2009.06.005>
- Moor, J. (2006). Artificial Intelligence Conference: The Next Fifty Years. AI Magazine, January 2006.
- Muthukrishnan, N., Maleki, F., Ovens, K., Reinhold, C., Forghani, B., & Forghani, R. (2020). Brief History of Artificial Intelligence. Neuroimaging Clinics of North America, 30(4), 393–399. <https://doi.org/10.1016/j.nic.2020.07.004>
- Peppers, Ken & Tuunanen, Tuure & Rothenberger, Marcus & Chatterjee, S.. (2007). A design science research methodology for information systems research. Journal of Management Information Systems.

24. 45-77.
https://www.researchgate.net/publication/284503626_A_design_science_research_methodology_for_information_systems_research
- Phua, C., Lee, V., Smith, K., & Gayler, R. (2005). A Comprehensive Survey of Data Mining-based Fraud Detection Research. CoRR. abs/1009.6119.
https://www.researchgate.net/publication/46887451_A_Comprehensive_Survey_of_Data_Mining-based_Fraud_Detection_Research
- Ricci, F., Rokach, L., & Shapira, B. (2011). Introduction to Recommender Systems Handbook. Recommender Systems Handbook. Springer. https://doi.org/10.1007/978-0-387-85820-3_1
- Rikhardsson, P., Thórisson, K. R., Bergthorsson, G., & Batt, C. (2022). Artificial intelligence and auditing in small- and medium-sized firms: Expectations and applications. AI Magazine, 43(3), 323–336. <https://doi.org/10.1002/aaai.12066>
- Rodrigues, L., Pereira, J., da Silva, A. F., & Ribeiro, H. (2023). The impact of artificial intelligence on audit profession. Journal of Information Systems Engineering and Management, 8(1). <https://doi.org/10.55267/iadt.07.12743>
- Russell, S. J., & Norvig, P. (2021). "Artificial Intelligence: A Modern Approach."
- Russell, S., & Norvig, P. (2020). Artificial Intelligence - A modern approach (S. Russell & P. Norvig, Eds.; 4th ed.). Pearson.
- Russell, S., & Norvig, P. (2021). Artificial Intelligence: a Modern Approach, EBook, Global Edition. Pearson Education, Limited. <http://ebookcentral.proquest.com/lib/novaims/detail.action?docID=6563568>
- Searle, J. R. (1980). Minds, brains, and programs. Behavioral and Brain Sciences, 3, 417– 457.
- Service Trust Portal. (n.d.). <https://servicetrust.microsoft.com/viewpage/SOC>
- Shackleford, D. (2018). "AI in Cybersecurity: A Comprehensive Guide."
- Shen, D., Wu, G., & Suk, H. I. (2017). "Deep Learning in Medical Image Analysis."
- Siciliano, B., Sciavicco, L., Villani, L., & Oriolo, G. (2008). "Robotics: Modelling, Planning and Control."
- Srinivasan, A., & Davenport, T. H. (2018). "Artificial Intelligence for the Real World: Building a Performance Management System."
- Tiwari, R. (2023). The Application of AI And Machine Learning in the Financial Industry and its Effects on Risk Management and Fraud Detection. INTERANTIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT, 07(01). <https://doi.org/10.55041/ijsrem17595>
- Turing, A. M. (2012). Computing machinery and intelligence. Machine Intelligence: Perspectives on the Computational Model, 59(236), 1–28. <https://doi.org/10.1093/mind/lix.236.433>
- Ulrich, P., Frank, V., & Kratt, M. (2021). Adoption of artificial intelligence technologies in German SMEs — Results from an empirical study. 76–84. <https://doi.org/10.22495/cgsetpt13>

United Nations. (n.d.). Goal 8: Decent work and economic growth. United Nations Sustainable Development Goals. <https://sdgs.un.org/goals/goal8>

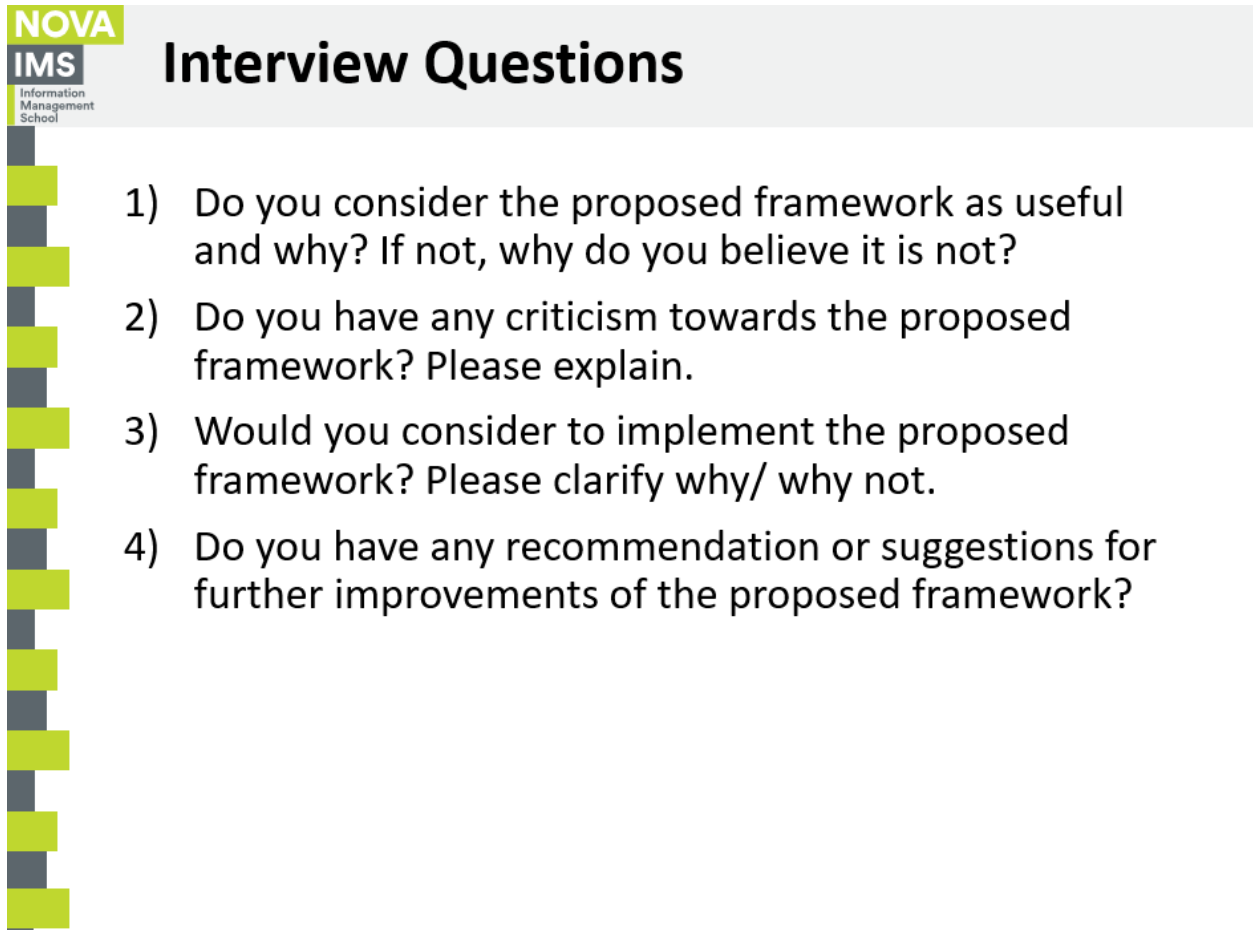
Vasarhelyi, M. A., Alles, M., Kogan, A., & Krishnan, G. (2004). "The Future of IT Auditing."

Yakubu, R. (2022). The Power of AI in Business. In R. Yakubu (Ed.), Conference Building the Future.

Zaïane, O. R., & HersHKovitz, A. (2019). "Artificial Intelligence in Education: Shaping the Future of Learning Through Intelligent Technologies."

APPENDIX A

In following image shows the prepared questions sent to the participants in the interviews:



NOVA
IMS
Information
Management
School

Interview Questions

- 1) Do you consider the proposed framework as useful and why? If not, why do you believe it is not?
- 2) Do you have any criticism towards the proposed framework? Please explain.
- 3) Would you consider to implement the proposed framework? Please clarify why/ why not.
- 4) Do you have any recommendation or suggestions for further improvements of the proposed framework?

APPENDIX B

Interview with Expert 1 on the 11th of July 2024:

Interviewer: Thank you for taking the time to speak with me today. Besides you, I'm going to interview two more people, but they are from audit and given your extensive background in IT advisory and AI, I thought you were the right fit into answering a few questions, regarding this framework and seeing this into a more practical sense of advisory.

Interviewer: Do you consider the proposed AROP framework as useful? If so, why? If not, why do you believe it may not be?

Expert 1: Well, thank you very much, my pleasure. Yes, after the presentation you made, I find the AROP framework to be quite useful. The integration of AI techniques into IT audit processes is very timely and relevant, especially in the context of modern IT environments where systems are increasingly complex and interconnected.

Given my experience with platforms like Salesforce or SAP, that is commonly the ERP in every company nowadays, I see the potential for this framework to enhance the efficiency and accuracy of IT audits, because if you can incorporate real-time monitoring and address key pain points in managing and auditing large-scale IT systems, because let's face it, if you audit big company's you are going to automatically have many relevant information systems, and that can be a problem at some point in terms of human resources. It's simply the future, AI has come to stay, and it makes sense that either you catch the ride or loose it to someone competitor that saw the potential.

Interviewer: Do you have any criticism towards the proposed framework? Please explain.

Expert 1: One potential criticism I have is that while the framework is comprehensive, it may be somewhat generic in its current form. The implementation of AI models and techniques often requires significant customization to align with the specific needs and contexts of different organizations. For instance, integrating AI-driven insights with the data structures and workflows specific to applications like Salesforce or SAP may involve additional complexity. I think it could benefit from more detailed guidelines or case studies illustrating how to adapt its components to various IT environments and specific application scenarios.

Interviewer: Would you consider implementing the proposed framework? Please clarify why or why not.

Expert 1: I would consider implementing the AROP framework, primarily because it offers a structured approach to integrating AI into IT auditing, which is something we are actively looking to enhance in our advisory services and even I imagine all big four's want to improve and solve this problem.

Since your framework's focus on AI techniques that aligns with the increasing demand for more sophisticated and data-driven audit methodologies, which I think is the future.

However, once again, the implementation would need to be tailored to fit the specific IT landscape of the organization. We would need to carefully assess how the framework's components can be adapted to our

existing processes and technologies, such as our cloud-based and on-premises applications, to ensure its effectiveness and efficiency.

Interviewer: Do you have any recommendations or suggestions for further improvements of the proposed framework?

Expert 1: Besides of the previous one I gave, I would include more detailed implementation guidelines and best practices for integrating the framework with specific technologies and platforms, because it hasn't been done, so it needs validation on the market to see how the framework actually works and what we can do to improve it, something like a beta phase before the release.

Lastly, incorporating a feedback mechanism or iterative review process within the framework could help organizations continuously refine their use of AI in auditing based on practical experiences and evolving needs.

Interviewer: Thank you very much for your insightful feedback. Your recommendations will be crucial in refining and enhancing the framework.

Expert 1: You're welcome. I'm glad to contribute and look forward to seeing how the framework evolves.

APPENDIX C

Interview with Expert 2 on the 12th of July 2024:

Interviewer: Thank you for taking the time to join me today. With your experience in auditing across different sectors, I hope to obtain your insights on this new framework, I'm working on my thesis, so let's start with our questions.

Interviewer: Do you consider the proposed AROP framework useful? If so, why? If not, why do you believe it may not be?

Expert E2: Yes, I do find the AROP framework useful and honestly, it's a trending theme, so it actually interested me a lot this framework. I've worked across different industries in all my career in audit and I've seen how complex and varied audit needs can be. The framework's focus on integrating AI, like machine learning for anomaly detection and predictive analytics for risk assessment, which is a big plus, less hours lost on meetings with clients and more critical and professional judgmental being applied, which in fact is what is important in audit, or at least to be a successful auditor.

So, these tools can really sharpen our audit processes and help us meet standards more effectively. Plus, AI it's just a game-changer, especially in fast-paced sectors like financial services.

Interviewer: That's great to hear. Do you have any criticisms of the proposed framework?

Expert E2: One thing that stands out is that the framework is quite high-level. It doesn't dive into the specifics for different industries, and each sector has its own unique challenges. For instance, the energy sector has different regulatory and operational issues compared to financial services. Adding more detailed, industry-specific guidance would make the framework even more practical. Also, it would help to have examples or case studies showing successful implementation in different sectors.

Interviewer: Understood. Would you consider implementing the proposed framework in your audits? Why or why not?

Expert E2: I would consider it, definitely. The AROP framework offers a structured way to integrate AI into our audit processes, which aligns with where we're heading. However, I'd start with a pilot phase. We'd test the framework in specific audit scenarios relevant to our clients. This would help us tweak it as needed and ensure it's tailored to our diverse needs and compliance requirements.

Interviewer: That makes sense. Finally, do you have any recommendations or suggestions for improving the proposed framework?

Expert E2: I'd recommend adding more detailed implementation guides that address the specifics of different industries. Including best practices and lessons learned from actual implementations would be very useful. Also, providing tools or templates that can be adapted for different regulatory environments would make the framework more user-friendly. And having a component for continuous improvement would help organizations keep up with evolving technologies and regulatory changes.

Interviewer: Thank you very much for your valuable insights and suggestions. Your feedback will be crucial in refining and improving the framework.

Expert E2: You're welcome, I'm here to help out and any more questions you may have, I'm available.

APPENDIX D

Interview with Expert 3 on the 12th of July 2024:

Interviewer: Thank you for taking the time to speak with me today, because as a senior, I believe that you can have a more insightful way on you can actually implement this into your projects, so I'm excited in hearing you feedback. So, let's start on the first question.

Interviewer: Do you consider the proposed AROP framework useful? If so, why? If not, why do you believe it may not be?

Expert E3: I do find the AROP framework useful. For instance, using machine learning can help us identify issues that might be missed through traditional methods and AI can indeed allow for more dynamic and responsive auditing practices. However, it's essential to recognize the impact this will have on the workforce.

Interviewer: Yes, I understand your perspective and concerns. Do you have any specific criticisms of the proposed framework?

Expert E3: While I appreciate the potential benefits, I do have some concerns. One major issue is the potential impact on jobs. The integration of AI could lead to a significant reduction in the need for certain audit roles, especially those that involve routine tasks. This could create anxiety among staff and resistance to adopting the new framework.

Interviewer: Would you consider implementing the proposed framework in your audits? Why or why not?

Expert E3: I would consider implementing it, but with a cautious approach. The framework has great potential to improve audit quality and efficiency, which is a significant advantage. However, we need to balance this with the impact on our employees. Training and upskilling will be critical to ensure that our staff can work alongside AI tools rather than be replaced by them. Also, starting with a pilot program to test the framework in a controlled environment would be prudent. This would help us understand its practical implications and make necessary adjustments before a full-scale rollout.

Interviewer: That sounds like a thoughtful approach. Finally, do you have any recommendations or suggestions for improving the proposed framework?

Expert E3: My main recommendation is to include a robust change management plan within the framework. This should address training, upskilling, and the transition process to ensure that our workforce is ready for the changes.

Interviewer: Thank you very much for your thoughtful and insightful feedback. I think I gather that your input will be crucial in refining and enhancing the framework.

Expert E3: You're welcome. I'm glad to contribute and hope these insights help make the framework more practical and inclusive.

