Kaunas University of Technology

School of Economics and Business

Auditing Financial Statements of Clients Using High-Risk Artificial Intelligence Systems

Master's Final Degree Project

Abdelmounaim Hadaoui

Project author

Prof. Lina Dagilienė

Supervisor

Kaunas, 2026

Kaunas University of Technology

School of Economics and Business

Auditing Financial Statements of Clients Using High-Risk Artificial Intelligence Systems

Master's Final Degree Project

Accounting and Auditing (6211LX037)

Abdelmounaim Hadaoui

Project author

Prof. Lina Dagilienė

Supervisor

Prof. Practitioner Borisas Seminogovas

Reviewer

Kaunas, 2026

Kaunas University of Technology

School of Economics and Business

Abdelmounaim Hadaoui

Auditing Financial Statements of Clients Using High-Risk Artificial Intelligence Systems

Declaration of Academic Integrity

I confirm the following:

1. I have prepared the final degree project independently and honestly without any violations of the copyrights or other rights of others, following the provisions of the Law on Copyrights and Related Rights of the Republic of Lithuania, the Regulations on the Management and Transfer of Intellectual Property of Kaunas University of Technology (hereinafter – University) and the ethical requirements stipulated by the Code of Academic Ethics of the University;

2. All the data and research results provided in the final degree project are correct and obtained legally; none of the parts of this project are plagiarised from any printed or electronic sources; all the quotations and references provided in the text of the final degree project are indicated in the list of references;

3. I have not paid anyone any monetary funds for the final degree project or the parts thereof unless required by the law;

4. I understand that in the case of any discovery of the fact of dishonesty or violation of any rights of others, the academic penalties will be imposed on me under the procedure applied at the University; I will be expelled from the University and my final degree project can be submitted to the Office of the Ombudsperson for Academic Ethics and Procedures in the examination of a possible violation of academic ethics.

Abdelmounaim Hadaoui *Confirmed electronically*

Abdelmounaim Hadaoui. Auditing Financial Statements of Clients Using High-Risk Artificial Intelligence Systems/ supervisor Prof. Lina Dagilienė; School of Economics and Business, Kaunas University of Technology.

Study field and area (study field group): Accounting, Business and Public Management.

Keywords: High-risk artificial intelligence; financial reporting; audit risk; professional skepticism; AI governance; AI assurance; Big Four audit firms.

Kaunas, 2026. 76 pages.

Summary

The increased adoption of artificial intelligence in organisational processes has significantly changed the circumstances under which financial reporting is prepared, audited and assured.The high-risk categories of AI systems that raise complex and layered challenges to auditors and are not fully addressed in existing professional standards are known as high-risk.Meanwhile regulatory regimes controlling AI, most notably the European Union AI Act, have started to introduce structured accountability requirements on organisations implementing such systems.The combination of these trends makes it timely, as well as necessary, to consider how the audit profession is positioning itself in regards to high-risk AI in the context of financial reporting.This is the main topicality of the current research.

The body of public disclosures produced by the four largest global professional services and audit firms Deloitte, Ernst & Young, KPMG, and PricewaterhouseCoopers, referred to as the Big Four published between 2023 and 2025 and discussing the topic of artificial intelligence in the context of audit practice, financial reporting, and other related governance and assurance issues.

The aim of the study is to examine how the Big Four audit firms publicly disclose AI-related risks, governance, and assurance-related issues in financial reporting audits involving high-risk AI systems.

To achieve the aim of this project, the following objectives were defined:

1. To map the characteristics of high-risk AI systems to the audit risk assessment.

2. To develop an integrated theoritical framework that combines audit risk model, professional skepticism, and AI governance frameworks.

3. To design and conduct a directed content analysis of Big Four documents published between 2023 and 2025 by developing a corpus table and a codebook.

4. To compare cross-firm communication themes and identify their implications for audit planning and professional guidance in relation to high-risk AI in financial reporting.

On this theoretical basis, a directed content analysis is planned and executed with the help of a purpose-designed corpus of Big Four public reports and a systematic codebook comprising five thematic groups: AI Governance and Assurance, AI and Technology Usage in Auditing, Audit Benefits, Audit Risk, and Professional Skepticism.

This analysis has shown that AI Governance and Assurance is the most dominant thematic category in all four firms meaning that AI Governance and Assurance is what the Big Four public discourse

frames the issue of high-risk AI.AI and Technology Use in Auditing and Audit Benefits are secondarily but substantively significant themes, and Audit Risk is comparatively little explicitly addressed.Professional Skepticism comes out as the least expressedly stated theme throughout the whole corpus.The patterns of cross-firm communication are widely similar, implying a common discursive orientation towards government as opposed to an explicit sceptical challenge.

The research paper is a contribution to the growing body of literature on AI auditing by offering an evidence-based systematic analysis of how the Big Four publicly position themselves with regards to high-risk AI in financial reporting.The implications of the findings on standard-setters, regulators and practitioners include developing more robust professional guidance on audit risk assessment and sceptical judgement in AI-intensive environments.

Abdelmounaim Hadaoui. Klientų, naudojančių didelės rizikos dirbtinio intelekto sistemas, finansinės atskaitomybės auditas. Magistro baigiamasis projektas / vadovė Prof. Lina Dagilienė; Kauno technologijos universitetas, Ekonomikos ir verslo fakultetas.

Studijų kryptis ir sritis (studijų krypčių grupė): Apskaita, Verslas ir viešoji vadyba.

Reikšminiai žodžiai: Didelės rizikos dirbtinis intelektas; finansinė atskaitomybė; audito rizika; profesinis skepticizmas; dirbtinio intelekto valdymas; dirbtinio intelekto užtikrinimas; didžiojo ketverto audito įmonės.

Kaunas, 2026. 76 p.

Santrauka

Intensyvėjanti dirbtinio intelekto integracija organizaciniuose procesuose iš esmės pakeitė aplinką, kurioje finansinės ataskaitos yra rengiamos, peržiūrimos ir tikrinamos. Didelės rizikos dirbtinio intelekto sistemos yra tos, kurios daro įtaką reikšmingiems sprendimams, pavyzdžiui, kreditingumo vertinimams, finansiniams prognozavimams ar vidaus kontrolės funkcijoms. Tai kelia sudėtingų iššūkių auditoriams, į kuriuos galiojantys profesiniai audito standartai dar nėra visiškai atsižvelgę. Tuo pačiu reguliavimo sistemos, reglamentuojančios dirbtinį intelektą, ypač Europos Sąjungos dirbtinio intelekto aktas organizacijoms, diegiančioms tokias sistemas, pradeda nustatyti struktūrizuotus atskaitomybės reikalavimus. Šių pokyčių konvergencija suteikia pagrindą ir aktualumą tirti, kaip audito profesija pozicionuoja save didelės rizikos dirbtinio intelekto ir finansinių ataskaitų audito santykyje.

Tyrimo objektas yra viešai prieinamos ataskaitos, kurias 2023–2025 m. laikotarpiu paskelbė keturios didžiausios pasaulinės profesinių paslaugų ir audito bendrovės „Deloitte", „Ernst & Young", „KPMG" ir „PricewaterhouseCoopers", bendrai vadinamos Didžiuoju ketvertu ir kuriuose nagrinėjamas dirbtinis intelektas audito praktikos, finansinių ataskaitų bei susijusių valdymo ir užtikrinimo klausimų kontekste.

Tyrimo tikslas išanalizuoti, kaip Didžiojo ketverto audito bendrovės viešai prieinamose ataskaitose atskleidžia su dirbtiniu intelektu susijusias rizikas, valdymo ir užtikrinimo aspektus finansinių ataskaitų audituose, apimančiuose didelės rizikos DI sistemas.

Siekiant šio projekto tikslo, buvo iškelti šie uždaviniai:

1. Susieti didelės rizikos dirbtinio intelekto sistemų charakteristikas su audito rizikos vertinimu.

2. Sukurti integruotą teorinį modelį, apjungiantį audito rizika modelį, profesinį skepticizmą ir dirbtinio intelekto valdymo sistemas.

3. Parengti ir atlikti „Didžiojo ketverto“ ataskaitų, paskelbtų 2023–2025 m., turinio analizę, sukuriant analitinę kodų knygą.

4. Ištirti įmonių komunikacijos temas ir nustatyti jų reikšmę audito planavimui ir profesiniam gairių teikimui, susijusiam su didelės rizikos dirbtiniu intelektu finansinėse ataskaitose.

Tyrimo rezultatai rodo, kad DI valdymas ir užtikrinimas yra dominuojanti teminė kategorija visose keturiose bendrovėse. Tai liudija, kad Didžiojo ketverto viešasis diskursas didelę DI riziką pirmiausia interpretuoja per valdymo struktūrų, atskaitomybės mechanizmų, vidaus kontrolės stebėsenos ir pasirengimo užtikrinimui prizmę. DI ir technologijų naudojimas audite bei audito nauda yra antrinės, tačiau turinčios reikšmę temos; audito rizika atskleidžiama palyginti ribotai, o profesinis skepticizmas yra silpniausia tiesiogiai atskleista tema visame dokumentų korpuse. Tarporganizaciniai komunikacijos modeliai yra panašūs, atskleidžiantys bendrą diskursinę orientaciją į valdymą, o ne į skeptišką kvestionavimą.

Tyrimas prisideda prie besiformuojančios DI audito literatūros, pateikdamas struktūrizuotą, empiriškai pagrįstą analizę apie tai, kaip Didžiojo ketverto bendrovės viešai pozicionuoja save didelės rizikos DI finansinių ataskaitų audito kontekste. Tyrimo išvados yra aktualios audito standartų leidėjams, reguliuotojams ir praktikams, siekiantiems parengti profesines gaires didelės rizikos DI aplinkoje atliekamų auditų srityje.

Table of contents

List of figures

List of tables

List of abbreviations and terms

Abbreviations:

AI – Artificial Intelligence;

ATTs – Automated Tools and Techniques;

CAATTs – Computer Assisted Audit Techniques and Tools;

COSO – Committee of Sponsoring Organizations of the Treadway Commission ;

DOI – Diffusion of Innovations;

EU – European Union;

IAASB – International Auditing and Assurance Standards Board;

IIA – Institute of Internal Auditors;

ISA – International Standards on Auditing;

ISO/IEC – International Organization for Standardization / International Electrotechnical Commission;

NIST – National Institute of Standards and Technology;

PCAOB – Public Company Accounting Oversight Board;

RMM – Risks of Material Misstatement;

TAM – Technology Acceptance Model;

TOE – Technology Organization Environment;

UTAUT – Unified Theory of Acceptance and Use of Technology;

Prof. – professor.

Introduction

Background of the study: As the use of generative artificial intelligence (AI) is being implemented today to develop financial reports and management appraisals, the rapid integration of AI in the financial reporting and auditing profession is disrupting the sphere. High-risk AI is defined in two ways in this thesis in a complementary way. First regulatory high-risk AI refers to systems classified as high-risk under the EU Artificial Intelligence (Regulation (EU) 2024/1689).These systems are subject to governance requirements throughout their entire lifecycle, including development, deployment, monitoring, and updating. Second, audit-relevant high-risk AI is AI systems that significantly affect financial reporting processes, accounting estimates, or disclosures in a way that they have a plausible likelihood of contributing to material misstatement are referred to as audit-relevant high-risk AI. Nonetheless, there exists a list of what can be considered by some financial applications as a high-risk category under legislation such as the proposed AI Act by the EU, since they can be used to undermine the confidence of stakeholders or cause a severe misstatement in case of a failure (Genovesi, 2024). External auditors face a significant challenge in the evaluation of such complex systems in client organizations (Fedyk, 2022). A lot of AI systems are black box and thus not easily able to accumulate sufficient audit information and conceal their decision-making processes (Kokina et al., 2025). There are also issues with algorithmic bias, accountability gaps, and unforeseen outcomes which add to the audit risk further (Bin-Nashwan et al., 2025; Shahrour, 2022). Unlike non-adaptive systems, adaptive machine learning models can evolve over time, which is a challenge to traditional audit techniques that examine controls simultaneously (Hemati et al., 2021). Such challenges are compounded by the lack of standardized guidelines by professional organizations, which permit auditors to move through this terrain without pre-established guidelines (Murikah et al., 2024). As AI usage becomes widespread, auditors will have to develop with schemes to assess such high-risk systems and ensure the quality of financial reporting.

Problem Statement.

In evaluating high-risk AI systems of clients, auditors cannot always rely on any of the existing structures or procedures. Audit standards may vary depending on the approaches developed by different audit firms. It is not clear, what frameworks, approaches, and tools are recommended when audit professionals encounter the presence of high-risk AI in client firms (Louis, 2025). This creates an important professional and research concern in the context of financial reporting, where AI-related risks, governance, and assurance issues may affect how audit firms frame and communicate their role.

Although the technical issues of AI (opacity, bias, model risk, and accountability) have been present in previous research (Kokina et al., 2025; Murikah et al., 2024; Commerford et al., 2022; Novelli et al., 2024; Mökander et al., 2021), no systematic study has examined how these issues are publicly disclosed by the largest audit firms, who are on the leading edge of developing the practice. To identify new best practices and areas that need more standard-setting, it is necessary to have the knowledge of what these companies publicly declare in relation to the AI-related risk assessment, governance, and assurance (Manogo C. 2025).

Research Question: How do the Big Four audit firms in their public reporting disclose AI-related risks, governance, and assurance-related issues in the context of financial reporting?

The Aim of the research is to examine how the Big Four audit firms publicly disclose AI-related risks, governance, and assurance-related issues in financial reporting audits involving high-risk AI systems.

The Objectives:

1. To map the characteristics of high-risk AI systems to the audit risk assessment.

2. To develop an integrated theoritical framework that combines audit risk model, professional skepticism, and AI governance frameworks.

3. To design and conduct a directed content analysis of Big Four documents published between 2023 and 2025 by developing a corpus table and a codebook.

4. To compare cross-firm communication themes and identify their implications for audit planning and professional guidance in relation to high-risk AI in financial reporting.

The Method used in the Study: This research bases its analysis on secondary data by conducting a content analysis of publicly available materials of Big Four audit firms published in the last couple of years. The research examines white papers, publications, and web-based guidelines discussing governance structures, assurance methods, and AI threats. The documents are categorized according to title, year, company, the number of pages, and theoretical keywords like audit risk, professional skepticism, and AI governance are considered.

1. Problem Analysis of High-Risk AI Challenges for Audit Risk, Evidence, Judgment, Governance, and Assurance

In this chapter, the challenges of the high-risk AI systems with financial reporting are analyzed, and the impact on external auditors is considered. The study identifies significant issues on which the current study is based in the discussion of how the Big Four audit firms communicate their advice on these issues. These interconnected issues are the basis of the document analysis which will be conducted in the following chapters.

Key terms Definitions:

Accountability (in relation to AI) refers the notion that individuals or organizations can control the outcomes and impacts of AI systems that they develop, deploy, or operate. Auditing responsibility concerns the transparency of the party that manages AI-generated financial data and any misreporting that might be caused by errors or malfunctions of AI systems Novelli et al., 2024.

AI System at High Risk is an AI application with the potential to cause severe harm to individuals, organizations, or society in case of failure or malpractice. Under the proposed EU AI Act, algorithmic trading and credit scoring are classified as high-risk applications. In this paper, high-risk AI is defined as a set of systems that can meaningfully misreport financial reporting in case of a failure (EU AI Act, 2024).

Algorithmic bias is the term used to describe the systematic and repeated errors in the output of AI systems that result in unfair outcomes or favor certain groups of people over others. Biased training data, poor algorithm design, or improper usage of models in new situations can all be contributors to bias (Bahangulu, J. K. 2025).

Algorithm Aversion is the behavior of humans to ignore or fail to utilize the recommendations of algorithm systems or output even when the output is more precise than human judgments. This could manifest itself in the auditing process because auditors usually prefer the use of human judgment or manual calculations over trustful AI-based data Commerford et al. (2022).

Black Box (AI) is a term that is applied to refer to artificial intelligence systems, whose inner decision-making processes cannot be understood or are not laid out clearly to human viewers. The auditors that are required to determine the accuracy of AI-generated data are in trouble because the users might have access to the input and output information but cannot understand how the system arrived at its conclusions (Gryz, 2021).

Machine learning is a subfield of artificial intelligence, which relies on data to train the system to execute specific tasks more efficiently without having to write programs. To produce predictions or judgments, machine learning algorithms identify patterns in training data and use them to the new data (Sarker,2021).

1.1. High-Risk AI Systems in Clients' Financial Reporting

At the intersection of technology and principles of auditing, the use of AI in financial reporting raises complex concerns. High-risk AI system as discussed in this paper is an AI application that could materially misstate financial reports or which can significantly decrease the quality of financial reporting (Onyenahazi, 2025). The European Union proposes the AI Act, which provides a

general framework to understand the classification of the high-risk AI. High-risk applications in the financial sector, e.g. automated trading systems that execute financial transactions and credit scoring models that evaluate the creditworthiness of a borrower to take loans are considered high-risk (European Commission, 2021). High-risk AI systems used to create financial reporting applications include applications that have a significant impact on the production of financial information.

Kokina et a1. (2025) field study on the prospects and problems of AI in auditing states that auditors are increasingly encountering larger amounts of AI-generated data, Although no standardized practices currently exist to determine its reliability. On their findings, the audit firms are setting up processes as they go along, a process that may result in inconsistency and quality failures in series of engagements. The current study is directly related to this discrepancy in the analysis of the reception of recommendations given publicly to close such gaps. In a 2024 observation by the Public Company Accounting Oversight Board (PCAOB), companies had already applied generative AI to write sections of financial reports, including Management Discussion and Analysis sections. With the growing pace of the development of AI capabilities and the rise in their availability to businesses of various sizes and industries, this trend is assumed to pick up, and the necessity for the analysis of professional recommendations gains even greater urgency.

High-risk AI systems for financial reporting include a number of application areas that have a significant impact on how financial data is prepared, presented, or disclosed As shown in Figure 1, five main types of such systems can be identified: AI systems generating accounting estimates, AI systems automating revenue recognition, AI-based fraud detection systems, generative AI applications, and AI systems classifying transactions.

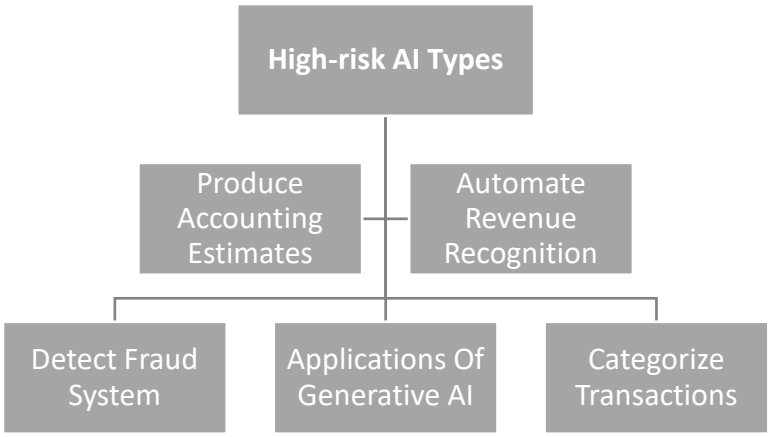


Fig. 1 . Five main types of high-risk AI systems in financial reporting, prepared by the author based on ISA 315, ISA 540, ISA 240, and the PCAOB guidance on generative AI in auditing.

AI systems that generate or provide accounting estimates represent one of the most significant risk areas, especially when machine learning models calculate loan loss provisions,, warranty obligations, insurance reserves or fair value measures. Such estimations directly affect reported profits and financial status and often require a substantial amount of managerial judgment. When opaque or

biased models are used, the resultant financial statement figures can be highly misstated without any discernible source of their error (Hemati, 2021).

AI systems that automate revenue recognition Algorithms to recognize appropriate patterns of revenue recognition can be used under complicated accounting rules such as IFRS 15 or ASC 606, but they are fraught with risk when they utilize the wrong contract terms or presents incorrect recognition rules. The malpractices in this area are of significant importance since revenue is often the largest amount on financial statements and the center of audit interest (Khemka, 2025 & Chun, 2026).

AI Robots that identify fraud. Fraud-detecting systems can identify potentially fraudulent transactions or suspicious patterns in financial information and potentially affect the audit risk evaluation and test procedures. Nonetheless, such technologies can create a false sense of confidence or focus of audit in case they possess some biases or limitations that auditors do not know (Raza, 2025).

Generative AI usages. When systems write narrative disclosures, e.g. management discussion and analysis, financial statement footnotes or other qualitative aspects of financial reporting, this carries the risk of inaccuracy, incompleteness, and inconsistency with the underlying financial data. Specifically, the concerns concerning the ability of generative AI to produce false information that is correct were raised in the 2024 report by the PCAOB.

AI systems classifying or categorizing transactions. When training data has errors or the algorithm faces transactions which are not similar to the ones in the training set, algorithms which automatically classify expenses, revenues or balance sheet items based on learned patterns can misclassify the transactions (Koç. D, 2024).

AI has brought in a new paradigm to the auditors who are used to auditing manual or predictable processes. Previously, auditors who encountered AI systems at client organizations often approached the audit by going around the controls of the AI systems that examine their audits and checking the system results but not always investigating what the AI model itself is. The reasoning behind this approach is that advanced AI is a black box in that it may not provide auditors with technical capabilities or access rights to view code or algorithms themselves. Rather, they examine whether the inputs and outputs are acceptable and whether there are controls surrounding the use of AI. (Abadi, 2018). However, if AI becomes a key component of financial reporting, this strategy could not be sufficient. Auditors could overlook systematic errors in the AI's underlying logic if they do not examine the AI process itself. This development represents a significant change in the focus of auditing from auditing individuals and basic systems to auditing intricate, self-learning systems (Davarzani, 2025). Nevertheless, this strategy might not be adequate in case AI is an important part of financial reporting. Without investigating the AI process, auditors may fail to identify systematic errors in the logic of the AI. It means a drastic shift in the scope of auditing of individuals and simple systems towards more complex self-learning systems (Davarzani, 2025). This change demands the combination of the old-fashioned audit concepts with the AI governance findings as described in the theoretical framework in Chapter 2. It also brings out the necessity of understanding how the audit firms are assisting practitioners in managing such problems.

1.2. Inter-related Challenges of High-Risk AI Systems in Auditing

There are a number of interrelated issues with auditors when it comes to the use of high-risk AI systems in financial reporting. These difficulties are caused by the complexity of AI systems and their use in the accounting and reporting processes. Specifically, the reliability of AI-generated financial information and the rise of audit risk may be influenced by such factors as lack of accountability, algorithmic bias, model risk, and opacity. These issues are closely related and thus, they cannot be discussed as separate problems. Instead, they are an interdependent combination of challenges that affect the evidence assessment of auditors, professional judgment, and consideration of internal controls.

One of the most discussed problems in all AI fields is called opacity or the lack of transparency regarding the functioning of AI systems and their judgment. Most high-risk AI models, in particular, deep neural networks and other complex machine learning models, operate as a black box where the decision-making procedure and parameters are thousands or millions of interacting non-linear parameters. They cannot even be understood by the developers of these models (Ali, 2024). As shown in Figure 2, transparency is a broader concept that includes intelligibility, interpretability, and explainability. This distinction is important in auditing because auditors may observe AI-generated outputs without fully understanding the internal logic that produced them.

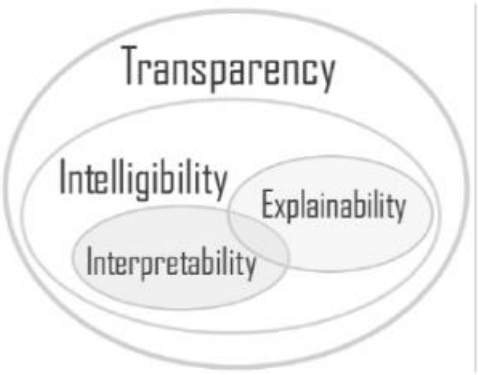


Fig. 2. AI transparency and explainability Ali, I. (2024).

To the external auditors, AI-based financial systems present significant complications in complying with the standards of professionalism. In accordance with the provisions of the International Standard on Auditing 500, the auditors have to provide adequate and relevant evidence, but the oblique AI generated estimates make it difficult to evaluate the accuracy and reasonableness. In the absence of understanding of the way the inputs are converted into outputs, it becomes hard to establish reliability. The study backs this issue Murikah (2024) and colleagues discover that AI transparency compromises the adequacy of evidence since auditors are unable to confirm the logic behind it. Similarly, Kokina and Davenport (2017) state explainability as one of the primary obstacles and state that most algorithms are black boxes. Conventional audit methods rely on the ability to see and follow a data flow, whereas AI systems are often not transparent in this manner. As AI becomes part of reporting, the audit methods should be designed to implement transparency and explainability obligations, to

prevent the reliance on the outputs that cannot be sufficiently justified. Opacity increases audit risk in a number of ways, which are related to one another.

- The first is that it enhances intrinsic risk the vulnerability of a financial statement assertion to material misstatement. In the case of complex and non-interpretable AI systems, such systems might give inaccurate results that go undetected by the management or auditors (Fidyah, 2024).
- Second, the fact that a company is opaque increases the level of detection risk which according to the International Standard on Auditing 200 is the risk that the audit procedures will fail to identify the material misstatement. In case auditors are unable to meaningfully test AI systems beyond the input-output superficially, it is possible that the existence of meaningful errors will not be detected.
- Last, but not the least, the insufficient transparency of the internal controls undermines the performance of the internal controls because the management might not have adequate knowledge to formulate and oversee the right controls over the processes driven by AI (Fidyah, 2024).

Mökander et al. (2021). state that explainability is a major requirement related to meaningful accountability and oversight in their investigation of ethics-based audit of automated decision-making systems. The absence of adequate transparency is a barrier to the auditors assessing the suitability or living up to expectations of the regulatory and ethical professionalism of the behavior of an AI system. In reaction, researchers have advocated the concept of explainable AI (XAI), as a way of making an algorithmic decision more interpretable. Nevertheless, the tools are not consistent and are not standardized in the field of audit. Unless explainability is enhanced, and auditors are properly equipped to evaluate AI outputs, the issue of opacity is going to be a serious challenge to audit quality.

There are systematic errors or unfair consequences that AI systems may bring about due to training data, model design, or deployment settings. These concerns are critical factors that should be known when evaluating the quality and objectivity of AI-generated financial information. Bias takes several forms. In training data, models acquire and strengthen existing biases, which results in historical bias. Representation bias is the result of datasets being unable to represent some groups, scenarios, or edge cases. Measurement bias is a feature that is based on the selection or definitions of variables that bias the representation of events or groups. Aggregation bias is a situation of poor combination of heterogeneous groups of people resulting in none fit outputs. Belenguer, (2021) talks about evaluation bias, which is present when the performance benchmarks are skewed. In their review, Murikah (2024) and colleagues include additional sources homogeneous data, unrepresentative samples, and implicit algorithmic assumptions displaying the way bias may compromise the quality and judgment of auditing. These biases may have a material impact on statements in financial reporting. To illustrate, AI-based property valuation tools can result in systematic misstatements by being trained in a disproportionate way on particular regions or types of property. Likewise, an AI fraud-detection system can either over-flag or miss some transactions in case it is trained with biased historical data, setting the audit priorities in the wrong direction or not identifying high-risk items. Noordin (2022) and the team discover that the issue of AI fairness plays a major role in forming perceptions among the auditors in the data reliability question. According to their survey, the assessment of bias is necessary and difficult, and auditors do not always know that algorithmic bias has harmed the integrity of financial information thus a new methodology of fairness assessment should be introduced different than the old audit methods.

Prejudice in AI systems increases inherent risk since it creates directional and systematic misstatements including understating liabilities or overstating assets that can accumulate cross-account and through time. Such persistence enhances the chances of misstatement of material at the financial statement level. The client control environment highly influences the impact on the audit risk. Rigorous controls, such as model-governance designs, independent verification and management review have the potential to reduce biased results, but lax controls can have distortions pass right into the financial data. As (Johri et al., 2026) remarks, auditors are expected to determine that the clients evaluate AI systems adequately in terms of bias such as development of models, representativeness of training data, and continuous monitoring processes. Bias not dealt with leads to the possibility of undiscovered misstatements. There are also the ethical implications that widen the roles of the auditor. The AI systems can deliver results that disfavor stakeholders or hide unethical actions even when they think that the numerical results appear correct. In that eventuality, integrity and the common good demand that auditors should consider the fairness of the process giving rise to financial figures. According to (Semenova,2023), quality management of auditing processes in technologically developed companies needs independent knowledge to determine the presence of fairness, accountability and non-discrimination. The tendency to produce biased AI results can also reflect poor control and governance and require the auditors to report the same to the individuals in charge of governance to maintain ethical reporting in financial reporting.

The threat that inaccurate outputs are generated by the use of defective or abused models is all the more threatening as AI-driven estimates are used to constitute financial reporting and auditing. There are various sources of model risk. The error in model specification comes about by the use of inappropriate variables, assumptions or even functional forms. Impairment errors involve the mistake of inaccurate coding or implementation of a sound model. Error in application arises when a model is applied to the situations that it was not developed to serve. The error of calibration is due to poor generalization of parameter estimates and concept drift is due to changing economic conditions which worsen the accuracy. According to a study by Commerford et al. (2022), auditors will change the extent to which they depend on AI depending on the rigour of the model development, validation, and monitoring. Reliability indicates the consistency of the results of a model under different conditions. In cases where AI tools are involved in estimating warranty provisions or inventory obsolescence, the auditors should identify whether the results can be relied upon. There are a number of technical threats that compromise reliability. Strong performance on training data, but weak generalization is demonstrated by overfitting; weak performance due to omission of meaningful relationships is demonstrated by underfitting; and high sensitivity to small input variations leading to large output variations is demonstrated by instability. One such issue, which (Aliferis, 2024) describes as brittle, is models that are generically normal, but crash in rare or edge-case situations, a matter of special interest to auditors considering financial estimates.

Audit risk increases with the presence of defective models which augment inherent risk by producing estimations that are not congruent with actual values, which is not discovered until the stressed situations reveal the shortfalls. The traditional methods are independent, the evaluation of the estimation processes by the management, and sensitivity analysis are still applicable, however, AI brings a certain risk of a statistical unsoundness of the estimation method as such. Analytically oriented auditors place greater demands on the model based estimates as demonstrated by the study by Samagaio and Felício (2022) which demonstrates the interaction between auditor and

methodological complexities to create audit effectiveness. Model validation, extensively applied in regulated industries, needs conceptual soundness reviews, performance testing and ongoing monitoring, but similar models with AI-based estimates in corporate reporting are scarce, as De Jongh 2017 observes. Auditors might hence require more validation methods, such as back-testing, benchmarking, sensitivity analysis, documentation inspection and expert consultation to provide reliable and transparent behavior of the model with increasing algorithmic complexity.

1.3. Auditor Responses to High-Risk AI systems

When assessing output of AI, auditors can alternate between algorithm aversion and overreliance, and it is critical to balance judgment. Overreliance is a situation in which auditors put undue reliance on client AI systems based on the lack of technical expertise or the assumption that computerized outcomes are accurate in and of themselves. This compromises professional Skepticism and increases the chances of concealed misstatements, with auditors accepting model-generated numbers without adequate validation. This type of overreliance can weaken professional skepticism, particularly when auditors accept AI-generated outputs without sufficient validation or independent evaluation (Commerford et al., 2022). Regulators express similar concerns. PCAOB (2024) notes that GenAI should augment rather than replace human judgment, that human involvement remains essential, and that auditors remain responsible for reviewing outputs and documenting the work performed.
In this way, the principle is not to trust but verify or rather not to trust before proven. This risk is further increased by automation bias in favor of automated outputs and against conflicting evidence. It occurs when auditors give AI analyses a higher value in comparison to other evidences or professional intuition. As an example, when there are no irregularities detected by AI, an auditor can cut testing short. Chaker (2024) cautions that the bias only jeopardizes the quality of audits but can be mitigated with a policy that forces auditors to explain their reliance on AI outputs to strengthen critical evaluation.

There is a dilemma in auditing in the contemporary world due to algorithm aversion. According to (Commerford et al., 2022), although skepticism demands the questioning of evidence, there is a tendency to reflexively dismiss the correct AI output, which affects the quality of the audit process. This kind of mistrust brings back the biases that are very human, which AI is supposed to eliminate. To illustrate, when AI-admonished high-risk transactions are disregarded, it is possible that major misstatements will remain unnoticed, as the human sampling might not identify the patterns, which are detected by the model. It is a prejudice against non-human evidence and not actual skepticism. It is also a waste of resources because auditors use their time in performing manual tedious procedures rather than concentrating on high-risk areas. With the increased complexity of financial reporting, it becomes critical to have the capacity to trust AI. Good companies will educate auditors to decide on the merits of the AI results separating a reasonable doubt and a mechanical dislike. Achievement of a good balance between Skepticism and trust is one of the primary auditing problems that AI can pose. It involves realizing the capabilities and limitations of AI, using systematic checks, being aware of cognitive bias, and having a clear set of directions on how to properly rely. According to the results of the survey conducted by Abiyyu and Mustafida 2024, the use of AI does not necessarily positively affect the quality of an audit; the benefits of the technique are determined by the ways in which auditors combine technology with judgment and suspicion. Evidence provided by (Wang 2017) suggests that responses of auditors are influenced by institutional and personal characteristics, which means that a corporate culture and training are the keys to minimize overreliance and mistrust.

1.4. Regulatory, Ethical, Governance, and Assurance Implications of High-Risk AI

High-risk AI in financial reporting has significant implications of regulation, governance, and assurance to auditors. With the increasing level of involvement of AI systems in accounting processes, estimates, disclosures, and decision-making activities, auditors cannot only react to technical risks like the ones of opaqueness, bias, and model risks, but also adapt to an evolving institutional environment with its new regulatory demands, ethical issues, and assurance practices. These innovations are not independent of one another. The expectations of governance are affected by the regulatory requirements, and the form of governance determines how the auditors measure the control risk, gather evidence, and decide whether the audit responses are appropriate. This is why the effects of high-risk AI on auditing are to be interpreted as a single large problem instead of the technical or legal ones.

One of the most significant changes in this regard is that AI systems have been placed under more regulatory scrutiny. The EU Artificial Intelligence Act can also serve as a valuable source of information as it introduces requirements to high-risk AI systems in the fields of risk management, data governance, technical documentation, transparency, human control, accuracy, robustness, and cybersecurity (European Union, 2024). Even though not all AI systems deployed in financial reporting are covered by the legal definition of a high-risk system, the Act remains significant to auditors since it indicates the direction about prospective regulatory expectations of a responsible use of AI. Meanwhile, regulators like the Public Company Accounting Oversight Board have also argued about the increased application of generative AI in financial reporting and auditing, particularly in terms of reliability, confidentiality, and adequate audit evidence (PCAOB, 2024). Consequently, auditors have to pay more attention to the possibility of AI-related regulatory requirements and compliance risks as the part of their knowledge of the entity and its environment.

Ethical and professional implications are also formed as a result of these developments. The classic principles of auditing, including integrity, objectivity, due professional care, and professional skepticism are quite applicable, but the utilization of AI comes with new circumstances where they are increasingly challenging to implement. To take the example of client organizations using AI systems to produce accounting estimates, transactions classifications or narrative disclosures, the auditor should determine whether the process being considered is transparent enough, management monitoring significant, and responsibility of AI-related decisions is well defined. Such problems like fairness, accountability, confidentiality and transparency thus enter the greater audit evaluation. Moreover, the growing utilization of AI can cause some stress related to auditor independence, especially when audit firms are simultaneously advisors or implementers of AI systems. Auditors in these environments have to be vigilant of the possibility that complexity in technology can make the ethical vices indistinct or undermine critical thinking (Kokina and Davenport, 2017).

Meanwhile, the emergence of high-risk AI has also led to the development of new expectations of assurance. There is a growing emphasis on both whether the ultimate financial deliverables are materially misstated as well as whether the underlying AI systems and systems of governance are dependable, regulated, and monitored accordingly. Here, assurance is slowly becoming more inclusive of the assurance of the numbers being generated, to the assessment of the systems and controls creating them. According to Farley and Lansang (2025), AI auditing could become more specialized and focus on assessing quality of training data, model design, and validation processes,

monitoring practices and governance structures as well as financial consequences. Even though these methods of assurance are not fully developed yet, it is indicative that the risks associated with AI might force auditors to look beyond the traditional forms of substantive testing and expose the control environment as a whole in which AI is used.

The trend is supported by the increasing applicability of governance standards, including the NIST AI Risk Management Framework, COSO advice on AI, ISO/IEC standards, and the AI auditing framework of the IIA. These models are not the replacements of the auditing standards, but they offer the reference points when the understanding of the way the organizations are supposed to govern, monitor, and control AI systems. To auditors, they can thus act as effective standards when determining whether the client organizations have put sufficient controls, validation, accountability systems, and control systems on AI-informed reporting. Practically, this implies that audit teams might have to seek more and more aid of IT auditors, data professionals, and AI specialists, particularly in cases that involve AI systems that can have a material impact on financial reporting. Therefore, the increasing regulatory and governance demands in respect of AI are also altering the knowledge that auditors are required to have, the evidence that auditors should gather and their plans and execution of work.

All in all, the regulatory, governance, and assurance implications of high-risk AI point to the fact that the auditing profession is going through a transition phase in terms of both institutional and methodological aspects of its performance. The main point is that auditors are not interested in the outputs delivered by the client systems only, but in the regulatory environment, the governance structures, and the assurance methods that contribute towards the reliability of the outputs or not. That is why the issue of professional guidance is particularly critical. The fact that large audit firms are redefining audit evidence, judgment and accountability in the face of high-risk AI suggests that we should consider how the large audit firms are communicating these implications in their third-party guidance and whether their guidance is offering a sufficiently consistent response to the problems that have been uncovered in the literature.

1.5. The Guidance Gap in Connecting Problems to Professional Literature

The earlier sections have determined the key technical, human, regulatory, ethical, governance, and assurance concerns of high-risk AI in financial reporting. These problems are the premise of the main problem that is discussed in this thesis: the disconnection between the risks that are discussed in academic literature and the guidance offered by the Big Four audit firms in a professional context. Even though big audit firms have increasingly made public their thinking leadership, reports, and practice-focused publications on AI, minimal systematic knowledge exists on how their published advice responds to the peculiarities of auditing clients who use high-risk AI systems. This is a significant gap since the Big Four are crucial in responding to audit practice and the debate over regulation as well as establishing how newer technological threats are converted into the professional audit answer.

This loophole is at various levels. Conceptually, it is not clear how companies classify the risk of AI in the current audit procedures. There is still some doubt about whether AI is classified as a different category of risks that needs a new methodology or as a follow-up of the traditional IT risks as a subdivision of the audit risk model. At a more practical level, the question still exists regarding the exact steps that should be suggested to be taken in cases when auditors come across the AI-driven

systems. There is no clear understanding of what the methods that firms suggest to assess AI-based estimates are, testing controls over the model building and data inputs, and record the audit work concerning AI outputs. At the governance tier, it is not clear how firms instruct auditors to evaluate client AI oversight frameworks and policies, whether they cite such frameworks as the Committee of Sponsoring Organizations of the Treadway Commission guidance on AI or the National Institute of Standards and Technology AI Risk Management Framework. Lastly, on the training and capability level, there is no information about what is expected of auditors in terms of competence to analyze AI systems, such as the use of specialists and formal AI training. It is important to know what the Big Four firms report in the market since they audit the majority of big, publicly traded companies in the world and are powerful crafters of influence over regulators, small companies, and standard setters.

2. Theoretical Audit Risk Foundations and Technology Adoption Theories of AI-Enabled Auditing.

This chapter develops the theoretical basis on which the research examines the role of Big Four audit firms in conveying advice in relation to high-risk AI systems in financial reporting. The framework includes three free theoretical positions, including modern AI Governance and Assurance Frameworks, the Audit Risk Model of traditional auditing theory, and the Professional Skepticism principle of audit psychology and ethics. Taken together, these perspectives can provide a comprehensive perspective in which to analyze the challenges to the audit profession posed by client-side AI systems and their responses.

2.1. Theories for AI/technology usage in auditing

With the assistance of technologies, auditing begins to be influenced by technology-assisted analysis, computer-assisted audit techniques and tools (CAATTs) and AI-powered analytics that enable the assessment of risks, substantive testing, and the detection of anomalies. The use of automated tools and techniques (ATTs) in planning and undertaking risk assessment procedures is expressly recognized (and being more expected) by regulators and standard setters, along with the focus on proper documentation, use of professional judgment, and audit evidence. Indicatively, the risk assessment process has been reinforced by ISA 315 (Revised 2019), which has been compatible with ATT usage, and the IAASB has been given material support on the possible use of ATTs in identifying and assessing risks of material misstatement, and the recording of work that has been completed using ATTs. The PCAOB has made regulatory updates in the US setting that are more specific to audit procedures where electronic information will be analyzed with technology-based tools and identified audit quality considerations relating to AI in a more regulatory context.

In order to clarify the reasons why auditors and audit firms embrace (or are unwilling to embrace) AI/advanced analytics, researchers generally rely on families of complementary theories: individual-level acceptance, organizational adoption, and institutional/governance pressures. A review of auditing-technology studies suggests that the use of technology is multi-determined (technology perceptions, organizational readiness, environment/regulation, and task fit) and not predetermined by one factor.

Technology Acceptance Model (TAM) and extensions.
Technology Acceptance Model (TAM) is a theory that suggested that the intention to adopt is mainly influenced by the perceived usefulness (PU) and perceived ease of use (PEOU) (Davis, 1989) . In auditing, uptake of analytics/CAATTs is explained using TAM in which:

- PU is correlated with the anticipated changes in the effectiveness (improved risk targeting, enhanced evidence) and efficiency (improved coverage, automation of repetitive work).
- PEOU captures usability, workflow integration (e.g. with audit platforms) and learning effort.
  Empirical auditing research has been used to apply TAM to technology situations like big data analytics in auditing and its implications on audit quality that TAM is suitable in modelling the adoption decisions of auditors in big data analytics intensive environments.

Unified Theory of Acceptance and Use of Technology (UTAUT).
UTAUT adds the individual acceptance to the performance expectancy, effort expectancy, social

influence, and facilitating conditions (Venkatesh et a1., 2003) . UTAT applies to auditing as it is able to explicitly capture:

- Social influence (partner/manager expectations, peer norms, client expectations),
- Legislative requirements (training, information technology support, data access, audit approach support),that are very salient in service firms. UTAUT-type models have been empirically employed to examine the acceptance of CAATs by auditors and it is argued that it does not simply depend on the usefulness of the tool, but on organizational enabling factors and normative pressure also.

Technology Organisational Environment (TOE) and Diffusion of Innovations (DOI).

Due to the audit being conducted in the firms which have to invest, govern and standardize the methods, the organizational-level structures are required.

- TOE describes adoption through three contexts, including technological (availability, compatibility, complexity), organizational (resources, structure, competence) and environmental (regulation, competition, clients) contexts. TOE fits well in audit environments in terms of firm size, centralized approach, data infrastructure and expectations of the regulators.
- The focus of Diffusion of Innovations (DOI) is on perceived innovation attributes (relative advantage, compatibility, complexity, trialability, observability) and over time adoption within a social system. DOI can be applied in an audit since the innovations are likely to proliferate through pilot engagements, internal communities of practice and observable wins (e.g. improved risk identification on complex engagements).

The institutional theory (isomorphism) and the legitimacy pressures.

Audit firms work under a strictly regulated environment, and legitimacy, audit risk, and reputation among the market are important. Convergence in practices is attributed to institutional theory because:

- Coercive pressures (norms, controls),
- Normative pressures (training norms, professional bodies),
- Mimetic pressures (replicating leading companies in periods of uncertainty).

This rationale is in line with the institutional isomorphism school of thought written by DiMaggio and Powell. It assists in understanding why companies can embrace AI not only because it is efficient, but also as one of the signals of modernity/quality and as a means of keeping pace with the expectations of regulators regarding technology-assisted analysis.

Agency theory and assurance demand for technology-enabled auditing

Agency Theory Focus Agency theory, Auditing minimizes the information asymmetry between principal and agent, Technologies can enhance monitoring, such as by increasing coverage and detection, but can pose new risks (model risk, opacity, bias). Theorizing that AI/analytics are more likely to be invested in, the agency theory suggests (Jensen and Meckling, 1976), is higher assurance demanded by the stakeholders, the stricter the governance and the higher the cost of audit failure (inspection, litigation, reputational damage).

Information Systems (IS) success and quality of system + information.

Impact, even in the case of acceptance, is dependent on the quality of systems and information. As antecedents of use and net benefits, the DeLone and McLean IS Success Model (revised) focuses on the quality of systems, quality of information, and quality of service. Information quality is

particularly acute in terms of auditing due to the fact that AI outputs are determined by the integrity, completeness, and accessibility of client data; the inability to maintain data pipelines might lower trust levels and rework, suppressing long-term usage.

New AI-related acceptance models.

Recent auditing-oriented studies suggested AI-oriented acceptance models (e.g., AIDUA-like models) that directly incorporate technology readiness and AI-related perceptions in the adoption decision of auditors. This stream is useful in the auditing process where explainability, accountability, and perceived risk of overreliance are the key aspect, particularly when a regulator focuses on responsible AI use.

Table 1. Main theories for AI/technology usage in auditing and the approach adopted in this study

Theory / framework	Main focus	Level of analysis	Relevance to this study	Role in this thesis
TAM / UTAUT	Explain acceptance and use of technology through usefulness, ease of use, social influence, and facilitating conditions	Individual / auditor level	Useful for understanding why auditors may accept AI, analytics, and CAATTs	Supporting theory
TOE / DOI	Explain technology adoption through organizational readiness, technological context, and diffusion processes	Organizational / firm level	Useful for explaining how audit firms adopt and spread AI-enabled tools and methods	Supporting theory
Institutional theory	Explains adoption through coercive, normative, and mimetic pressures	Institutional / professional environment	Useful for explaining why audit firms align with regulatory and professional expectations regarding AI	Supporting theory
Agency theory / IS success model	Explain assurance demand and the importance of system and information quality	Governance / system level	Useful for linking AI use with monitoring, assurance expectations, and data quality	Supporting theory
Audit Risk Model	Explains how audit risk is structured through inherent, control, and detection risk	Audit engagement level	Central for analysing how high-risk AI affects audit risk assessment and audit response	Main approach
Professional skepticism	Explains the judgmental discipline needed when evaluating evidence and AI outputs	Auditor / engagement level	Central for analysing how firms frame balanced auditor responses to AI	Main approach
AI governance and assurance frameworks	Explain how AI should be governed, validated, monitored, and assured	Organizational / governance level	Central for evaluating how firms communicate AI controls, oversight, and assurance	Main approach

Table shows that several theories help explain AI and technology usage in auditing from different perspectives. However, the present study does not follow a behavioural adoption approach focused on individual auditor intention. Instead, the main analytical approach adopted in this thesis is the integrative framework centred on the audit risk model, professional skepticism, and AI governance and assurance. Technology adoption theories such as TAM, UTAUT, TOE, DOI, institutional theory, agency theory, and IS success theory are therefore treated as supporting perspectives rather than as the main conceptual model.

2.2. Conventional Audit Risk Model

Audit risk model is one of the most basic ideas in auditing theory and practice. It gives a systematic methodology to auditors of how to deal with the risk of opining wrongfully about financial statements that are materially misstated. This part analyzes the elements of the model, how it can be applied to AI risks, and how it can be used to learn the way audit firms convey advice on high-risk AI systems.
Foundations of the Audit Risk Model
The audit risk model is formally expressed as:

$$Audit\ Risk\ =\ Inherent\ Risk\ \times\ Control\ Risk\ \times\ Detection\ Risk \qquad 2.1$$

Where:
Audit Risk is a risk which is associated with expressing an inappropriate audit opinion by the auditor which occurs when the financial statements are materially misstated (ISA 200).
Inherent Risk Inherent Risk is the vulnerability of an assertion regarding a class of transaction, account balance, or disclosure to a material misstatement, in the absence of related internal controls.
Control Risk refers to the risk of not preventing, or not discovering and fixing material misstatement, timely by the entity internal control.
Detection Risk- this risk is associated with the likelihood that the procedures carried out by the auditor will fail to identify a material misstatement.
This risk-based approach is incorporated in the international auditing guidelines, i.e. ISA 315 (Identifying and Assessing the Risks of Material Misstatement) and ISA 200 (Overall Objectives of the Independent Auditor). The model assists the auditors in planning the audit procedures by considering inherent and control risks of various accounts and claims, and then determining the acceptable level of detection risk to reduce the total audit risk to an acceptable level In cases where clients use complex technologies, auditors should consider how IT-related risks, automated processing, cybersecurity weaknesses, and AI-generated outputs may affect the risks of material misstatement and the reliability of audit evidence (IAASB, 2019; PCAOB, 2024). This observation is particularly relevant with the increased adoption of AI technologies in the financial reporting processes.

AI Systems' Inherent Risk Implications
Before taking controls into account, inherent risk the vulnerability of financial statement statements to substantial misstatement can be greatly impacted by AI systems. High-risk AI systems have a number of traits that increase inherent risk:
Complexity and Opacity: According to Chapter 1, many advanced AI models are black boxes and opaque in how they make decisions. The fact that an AI model is used to compute warranty liabilities or loan loss provisions may be riskier than the more simple and well-known methodologies due to the uncertainty involved in the projections of the algorithm. Kokina et a1. (2025) report that an increasing number of auditors receive AI-generated estimates, and there are no standardized ways of evaluating their reliability. This is an indication that in these areas, inherent risk assessment remains challenging.

Potential of Systematic errors Systems such as AI can also result in systematic errors, unlike random human errors, which come about as a result of biased training data, defective algorithms or improper model specification. These types of systematic errors may occur in a series of transactions or accounts, which would result in material misstatements, which are hard to identify using the old-

fashioned sampling method. Murikah et al. (2024) point out that bias in AI systems may systematically mislead financial information, and this directly raises the risk in itself.
Model Risk: That a model is imperfect or is applied incorrectly is a specific source of inherent risk. As Commerford et al. (2022) show, model risk has a strong impact on auditor decisions regarding the suitability of AI-generated estimates, and auditors change their dependence in accordance with the evaluation of model development rigor and validation procedures.

Estimation Uncertainty AI models can frequently generate point estimates, without necessarily giving clear information about the range of possible outcomes or the confidence level behind predictions. This has the potential to mask the actual estimation uncertainty which results in a feeling of overconfidence on the accurate appearance of numbers which may not be accurate.
Implications of AI Systems for Risk Control.

The way that businesses handle their AI systems and integrate them into internal control systems affect control risk. The traditional internal controls may not be enough to curb AI-specific risks and new oversight, and control processes may need to be created.
AI Governance as a Control Factor: With an increased likelihood that AI-generated data is credible and that errors are detected and removed, effective AI governance structures that encompass AI-development policies, validation policies, monitoring and policies, and a defined allocation of roles can reduce control risk. Conversely, since internal controls have not kept pace with new risks posed by AI, the control risk increases in cases where customers are not governed by AI.
Automated Controls and their Limits: Certain AI systems can themselves be automated controls (e.g. fraud detection algorithms). Nonetheless, such controls must be monitored and checked. A poorly designed AI control or a poorly monitored control can give a false assurance, and it will not identify material misstatements.

Segregation of Duty and Accountability: AI systems have the potential to break the conventional segregation of duties since they can automate the tasks that were performed by more than one person. In the absence of proper accountability designs, the decentralization of responsibility can lead to control loopholes. As Murikah et al. (2024) note, AI can blur the responsibility determination, which, in turn, can become a deficiency in control.

Risk Detection and Auditor Reaction
Detection risk is the aspect that the auditors can influence the most in connection with their audit procedures. To achieve a reasonable total audit risk in case inherent and control risk has increased due to the complexity of AI and poor governance, auditors need to reduce detection risk. This normally involves modifying the nature, the timing, and the direction of the audit processes.
Substantive Procedure Adaptations: The auditors may need to develop new or modified substantive procedures to deal with AI-generated data. They might consist of:
Independent recalculation of values using alternative methods.
Expanded transaction testing to challenge AI classifications.
Engagement of specialists with relevant technical expertise.

Enhanced analytical procedures designed to identify anomalies that AI systems might miss.
Dependency on IT Specialists: Detection risk can be reduced by having IT auditors, data scientists, or AI specialists participate in the audit team. Kokina et a1. (2025) discovered that auditing firms

address the issue of AI through the emergence of the specialist pool and educating auditors on the basic principles of data science.

Testing AI System Controls: In instances where the clients have put in place controls on AI systems, auditors can also test AI system controls with the purpose of minimizing substantive procedures. Nevertheless, this presupposes that the controls should be designed in an effective way and should work in a stable manner as assumptions that can be not true in the case of fast developing AI systems. Application in this study.

The audit risk model provides a systematic approach to the investigation of the effects that AI systems have on audit risk factors and how auditors should respond. The following documents will be investigated according to the model in this study:
How are inherent, control, and detection risks of AI perceived by the Big Four companies?
What are the recommendations companies give to analyzing the intrinsic risk of financial data created by AI? What is the recommendation of companies on how auditors should evaluate the AI governance and control systems of their clients?
What are the auditing changes that companies propose in reaction to threats linked to artificial intelligence?

In case the companies expressly consider the audit risk model in their AI guidelines.
The audit risk model can allow any guidance to be developed or communicated by firms based on the established principles of fundamental auditing, as the AI-related issues are mapped to the established categories of inherent, control, and detection risk.

2.3. Professional Skepticism

The attitude the auditors should have during the engagement is professional skepticism which is a fundamental element of auditing ethics and quality. In this section, the author explores the notion of professional skepticism, its applicability in AI auditing, and its purpose in the theoretical framework. According to the International Standards on Auditing, professional skepticism can be defined as a mindset and it contains a questioning mind, awareness of the situations that can make an error or misstatements prone to fraud and a critical evaluation of its evidence in the audit (ISA 200). Practically, it means that auditors consider the risk of misrepresentation always, and seek to find convincing evidence before making judgment instead of assuming that management is dishonest or is always honest. To define professional skepticism, Nelson (2009) views professional skepticism as the attitude (tendencies towards doubt) and action (inquiry, investigation, and verification). This difference is significant because an auditor might have a skeptical mind, but he might not be able to convert it into productive skeptical behavior.

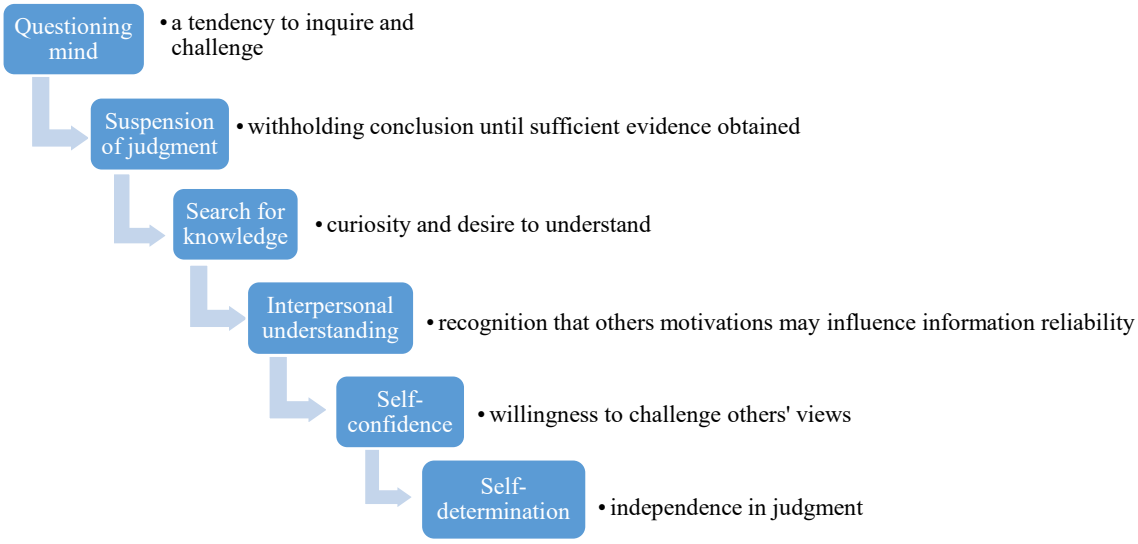


Fig. 3. Hurtt et al. (2013) identified six characteristics of skeptical auditors

A study conducted by Hardies and colleagues at the Foundation of Auditing Research shows that personal differences among auditors such as personality, experience and knowledge have a great impact on the professional skepticism and, by implication, the audit quality. Their results show that social pressure (subjective norms) is the best predictor of skeptical behaviour, and conscientiousness, openness and narcissism have a positive association with skepticism, whilst psychopathy and high agreeableness decrease it. These results highlight the importance of the fact that skepticism is not just a personality issue but that it is conditioned by organizational culture and norms.

Importance of Skepticism in AI

Contexts Professional skepticism is especially imperative with regards to auditing AI-generated information since AI systems have the potential to facilitate along with obstruct skeptical practice in a manner that should be mindfully controlled by auditors.

Threats to Skepticism: Overreliance and Automation

Bias The overuse of AI outputs is one of the potential major risks as auditors can become overly confident in the client AI systems either because they believe that the computer systems would be right or because they do not have enough knowledge to challenge the outputs of AI. This is called automation bias, the human bias to overlook the counter-evidence and give preference to the suggestions by the automated systems (Jackson, 2025). According to the Center of Audit Quality, professional skepticism and professional judgment are exercised by experienced auditors who are required to review the results produced by artificial intelligence in a careful manner and verify them to guarantee their accuracy and fullness. This involves a deliberate attempt to curb the influence of automation bias and keep a critical mind towards AI generated evidence. Chaker (2024) finds that automation bias poses a substantial threat to the quality of the audit, and this issue can be addressed by implementing systematic solutions, including the mandature of auditors to justify why they use AI outputs, as this solution could help to curb the bias.

Threats to Skepticism: Algorithm Aversion

Alternatively, at the other end of the spectrum will be overcaution of AI that is called algorithm aversion, whereby auditors will discard legitimate AI generated information which will be inefficient and thus a human factor can be reintroduced. Commerford et a1. (2022) give evidence that auditors might be hesitant to heed AI systems suggestions or under-use AI output especially when they are doing complex estimates audits. Although doubt is good, dismissing factual information just because it was provided by an AI will be wastage of resources and compromise audit effectiveness. An auditor who will fail to act on AI-identified risk transactions due to lack of trust in the technology might fail to detect issues, which the AI correctly detected.

Skepticism in AI Environment The CAQ indicates that in AI-enhanced auditing, human factors prevail, and the quality, integrity, and commitment to professional ethics of auditors remain always based on experience, judgment, and commitment. This is reflected by the Global Leader of the EY Artificial Intelligence Assurance, who mentions that Objectivity, independence and professional skepticism of the auditors are at the core of responsible AI integration, which auditors apply on their daily work.
Maintaining appropriate skepticism in AI contexts requires:

- Being aware of AI capabilities and limitations in order to comprehend when AI is likely to be reliable and in case the AI might fail.
- Structured verification approaches that explicitly address AI-generated information.
- Awareness of cognitive biases including automation bias and algorithm aversion.
- Clear guidance on appropriate reliance and required verification.

Skepticism and AI Governance

The use of professional skepticism is also applicable to the assessment of the client AI governance. The auditors must be very keen in determining whether the management has put proper controls over the AI systems, whether the AI outputs are properly reviewed, and whether accountability of the AI decisions is clearly defined. The lack of such governance can be in itself a sign of control weaknesses that augment audit risk. The quality of fraud brainstorming according to the research carried out by Hardies indicates that skepticism among the professionals has a direct effect on the quality of fraud identification and response by the audit team. Partner-led engagements that are of high trait skepticism also demonstrate wider discussion, longer preparation, and greater involvement of specialists all conditions that probably benefit risk identification of any AI aspect, too.

Professional skepticism is particularly important when auditing clients that use high-risk AI systems because such systems may generate outputs that appear precise, consistent, and objective while concealing underlying problems related to opacity, bias, weak data quality, or flawed model assumptions. Prior research suggests that auditors may react to AI in two problematic ways: they may over-rely on AI-generated outputs because of automation bias, or they may dismiss useful AI-generated evidence because of algorithm aversion. Both responses can weaken judgment and reduce audit quality. In this context, professional skepticism requires auditors to critically evaluate not only the plausibility of AI outputs, but also the processes through which those outputs are generated, the adequacy of supporting audit evidence, and the reasonableness of management's assumptions. Thus, in audits involving high-risk AI systems, professional skepticism remains an essential safeguard for maintaining audit quality and sound professional judgment.

2.4. AI Assurance and Governance Frameworks

The growing penetration of AI in the business processes especially in the financial reporting presents new and intricate risks. In order to deal with such risks, organizations should have strong governance arrangements. To the auditors, these structures are important to comprehend, since effective AI governance or lack of it is a direct influence on the evaluation of the control risk. Although classic principles of auditing such as the audit risk model and professional skepticism form the basis, modern AI governance models offer critical theoretical tools of assessing how companies are supposed to cope with AI-related risks and how auditors are supposed to ascertain such initiatives. This part is a synthesis of the main frameworks in order to apply them to this research based on the academic sources and professional recommendations.

The Accountability and Governance Imperative

It is important to be aware of the nature of problems that these frameworks are meant to address before analyzing them. The use of AI systems especially in financial reporting inspires deep-seated accountability and governance concerns.

The Accountability Problem is the issue of responsibility diffusion. In the traditional processes, when an accounting estimation turns out to be inaccurate, an auditor can negotiate the issue with an individual concerned in the management. However, once an AI model provides a prediction, which results in a material misstatement, responsibility is unclear. This puts the management at blame, which is wrong to trust the AI, the developer, who created a bad model, or data providers, who provided biased data, as Murikah et al. (2024) point out. Clarity of accountability is needed by auditors since the audit process relies on obtaining viable representations of the concerned parties and assessment of the control environment. The inability of a client to define the accountability of the AI results, as a matter of fact, is a serious weakness of control (Murikah et al., 2024).

The frameworks, policies, and limitations that an organization implements to manage its AI systems are known as AI Governance, which helps it solve this accountability issue. Good AI governance can be a good sign among audit firms that the management is aware of the risks involved in AI, and has put in place measures to control these risks, hence it may result in lowering the control risk. On the other hand, absence of governance as such, using machine learning to render estimates in accounting without management, and without control, validation or records, is of great concern and contributes to high control risk. The major aspects of good governance are:

- Policies and Standards: Defining principles for ethical and responsible AI development and deployment.
- Risk Assessment Processes: Identifying, analyzing, and evaluating AI-specific risks.
- Documentation Requirements: Mandating comprehensive records of AI model development, validation, data lineage, and ongoing monitoring.
- Clear Role Definition: Assigning responsibilities for AI oversight, including model owners, validators, and risk committees.
- Monitoring and Oversight: Establishing processes for the ongoing review of AI outputs and performance against benchmarks.
- Incident Response Plans: Planning and regulating the cases when AI outputs are incorrect or harmful.

Key AI Governance and Assurance Frameworks

Several frameworks have recently emerged to provide structured guidance for organizations and their auditors. These frameworks, while not formal auditing standards, offer critical reference points for evaluating the design and operating effectiveness of an organization's AI governance.
The NIST AI Risk Management Framework (AI RMF 1.0) Released The NIST AI RMF is a multi-stakeholder framework (voluntary) that provides a comprehensive view of AI risk management released by the U.S. National Institute of Standards and Technology in January 2023. It is intended to be universal in nature and suitable in all types of organizations and sector, and is therefore very applicable to a wide variety of audit clients. The framework is organized on four core functions:

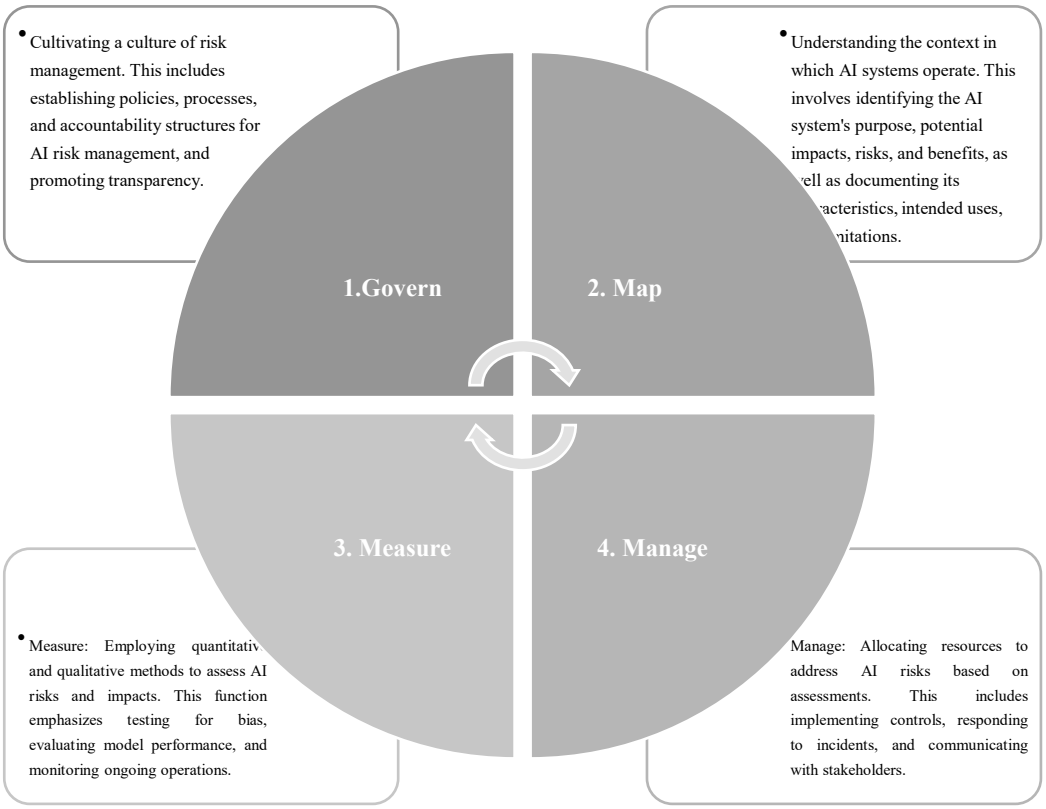


Fig. 4. The NIST AI Risk Management Framework (AI RMF 1.0)

To the auditors, the NIST AI RMF offers a beneficial scale of reference. An auditor, conversant with this guidance, may therefore make appropriate inquiries through whether the client has in place oversight structures (Govern), AI systems and the risk documented (Map), has tested its systems and accuracy of the tests (Measure), and has the controls in place to counter risks (Manage). The centrality of the framework as analyzed by Forrester can be observed since all controls in their AEGIS framework refer to NIST (Pollard et al., 2025).

COSO Guidance on AI Governance and GenAI Internal Control

For this thesis, two key sources for AI governance literature are publications by the Committee of Sponsoring Organizations of the Treadway Commission (COSO). First, the Committee of Sponsoring Organizations of the Treadway Commission (COSO, 2021) provides a top-level governance and enterprise risk management (ERM) view of AI. This 2021 publication applies COSO's ERM

framework to the implementation of AI and highlights governance and culture, strategy and objective-setting, performance, review and revision, and information, communication, and reporting. In this sense, AI is not a technical problem, but an institutional one that requires governance, risk management and objectives. This is significant for auditing research because it positions AI risk within governance structures rather than outside of control and accountability.

This governance perspective was further developed by COSO in 2026 with its publication, Achieving Effective Internal Control Over Generative AI (GenAI). COSO notes that this document is an extension of the previous thought piece on AI, and operationalises enterprise risk management principles through internal-control practices. The 2026 guidance is more specific than the 2021 thought piece as it deals specifically with generative AI and states it does not cover all types of AI. It is however, particularly relevant to this thesis because it extends the earlier document's governance principles to operational control design, monitoring, traceability and auditability. It is also highly relevant to assurance, as the target audiences include controllers, financial reporting groups, internal audit, and external auditors who will investigate GenAI controls.

The two COSO publications form a consistent theoretical framework for this thesis. The 2021 publication provides the governance and risk-management context needed for a discussion of high-risk AI in financial reporting, and the 2026 publication provides a more operational supplement to the discussion in the situation where generative AI is used to influence financial reporting processes, documents, or control systems. So, using both sources makes it possible for the thesis to provide a broad view in the theoretical chapter and support the more specific control-oriented discussion in the empirical chapter.

ISO/IEC AI Standards

The International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) have developed key standards for AI governance:

- ISO/IEC 23894: Guides AI risk management, which gives principles and processes to identify, measure, and treat risks that are related to AI.
- ISO/IEC 42001: Provides guidelines on how to set up, execute, sustain, and constantly evolve an AI management system in a company. This is a certifiable standard.

According to Forrester (2025), ISO/IEC 42001 serves as the “certifiable, audit-ready” complement to the more flexible NIST framework. Whereas NIST assists organizations to develop internal capabilities, ISO 42001 provides a formal standard with which they can pursue external certification, and therefore have their AI governance practices vetted independently. To auditors, such ISO standards represent possible guidelines on how to assess client AI systems, a trend that is already being taken by such companies as KPMG in their AI assurance services (KPMG, 2025).

The IIA AI Auditing Framework

This framework, which is available in 2024, was released by the Institute of Internal Auditors (IIA) and targets auditors who are to examine AI systems. It offers a sensible direction on how to scope AI audits, the most significant areas of assessment (data, algorithms, models, outcomes, and controls) and how to report. Although it is targeted at internal auditors, its principles can be very flexible to

external auditors to review AI systems influencing financial reporting. The major aspects are that management should have listed its AI systems, control structures to AI development and usage, and reasonableness of results.

The Forrester AEGIS Framework

Published in 2025, AEGIS (Agentic Governance, Integrity, and Security) Framework by Forrester is the attempt at the synthesis of the available frameworks into a unified blueprint of governance (Forrester, 2025). AEGIS classifies 39 substantive controls in significant frameworks, such as NIST AI RMF, ISO/IEC 42001, the EU AI Act, and OWASP Top 10 in LLM. Key insights include:

- Framework Integration: 80% of AEGIS controls map to four or more major frameworks, demonstrating significant convergence in AI governance expectations.
- Foundational Frameworks: NIST AI RMF and ISO/IEC 42001 form the "backbone" of AI governance, with every AEGIS control referencing both.
- Control Density: The EU AI Act has an 80 number of references within AEGIS controls, which means that it has high operational imperatives.
- High-Density Controls: Controls addressing governance oversight (GRC-01), data integrity (DATA-01), development practices (DEV-01), and monitoring serve as the essential “scaffolding” for trust in AI systems.

In the case of auditors, AEGIS proves that several governance frameworks can be combined into a unified platform and outlines a way of assessing the AI governance of a client holistically.

The EU AI Act

The AI Act of the European Union is a historic regulatory instrument that has significant consequences on AI regulation. In the case of the high-risk AI systems including numerous financial applications the Act requires that the requirements be adhered to in the following aspects:

- Risk management systems
- Data governance
- Technical documentation
- Record-keeping
- Transparency and information provision
- Human oversight Accuracy, robustness, and cybersecurity

In case the AI systems of a client are within the boundaries of the EU AI Act, compliance should be taken into account by auditors when understanding the entity and its environment. The emphasis on human control and responsibility in the Act offers more, legally binding standards of assessing the client governance.

The Emergence of AI Assurance Services

Alongside governance frameworks, the idea of AI assurance or independent verification or certification of AI systems is fast-growing in popularity. Major audit companies are coming up with new service offerings that directly relate to the AI risks. An announcement of the AI Assurance services suite made by KPMG depicts this trend (KPMG, 2024) and it involves:

- AI Model Risk Assessments: Organized evaluation of risk risk and control effectiveness works.

- AI Model validation: Checking or testing the models in terms of accuracy, assumptions, and regulatory compliance.
- Real-Time Systems Assessments: The review of AI-related updates on financial reporting controls.
- AI Assurance and Attestation: Independent verification against recognized standards like ISO/IEC 42001.

On the same note, EY has also declared substantial investments to incorporate AI-powered capabilities into its primary audit platform and at the same time, formulate its own and its clientele even use of the technology via its so-called Responsible AI principles (Abu-Shakra, 2025; EY, 2024). These advances are an indication that the profession is not simply modifying the current methods of audit but rather developing alternative new and distinct practices of AI. This directly affects financial statement audit work since engagement teams are likely to have to work with, or rely on the efforts of, AI assurance specialists more and more.

Application to this Subject

Such frameworks set the standards of the assessment of AI governance that directly affects audit risk. Strong AI governance, with clear accountability and alignment with reference frameworks such as the NIST AI RMF, COSO's broad AI governance guidance, and relevant ISO/IEC standards, may reduce control risk. In this context, COSO's later GenAI internal-control guidance provides a more operational extension of this broader governance logic, especially for control design, monitoring, and audit-readiness considerations. This study will use these frameworks to analyze Big Four guidance, examining: 1) which frameworks are referenced, 2) how firms conceptualize AI governance expectations, 3) recommended controls, 4) use of framework concepts in risk assessment, and 5) consensus or divergence among firms. This grounds the analysis in established theory.

2.5. Integrative Conceptual Framework for Auditing Clients Using High-Risk AI Systems

Relying on the theoretical discussion of the foregoing sections, this study formulates a single integrative conceptual framework for analysing how Big Four audit firms address the auditing of clients that use high-risk AI systems in financial reporting. The purpose of this framework is to synthesise the key theoretical perspectives discussed in this chapter into one coherent analytical structure. Instead of keeping separate and possibly overlapping models, the study adopts a consolidated framework in which the audit risk model serves as the central analytical component, while professional skepticism, AI governance and assurance, AI/technology usage in auditing, and audit benefits are treated as complementary elements. Together, these elements shape how AI-related audit issues are interpreted and addressed in financial reporting contexts.

The framework is centred on the assumption that the implications of high-risk AI for auditing can be understood most clearly through the logic of audit risk. At the same time, it recognises that audit responses to high-risk AI are shaped not only by risk assessment, but also by professional skepticism, governance and assurance structures, and the practical use of AI-related technologies in auditing. Accordingly, technology-usage theories are incorporated as supporting elements within the broader audit-focused framework rather than treated as a separate behavioural model. When these elements are properly aligned in audit practice and professional guidance, they may contribute to stronger audit outcomes, including improved risk identification, enhanced audit evidence, better documentation, and higher overall audit quality.

The audit risk model is the main focus of the model since most implications of high risk AI on auditing eventually reflect in inherent risk, control risk and detection risk. The inherent risk is the disposition of financial statement assertions to material misstatement without taking into account the related controls. Under high-risk AI, opacities, bias in algorithms, model risk, complexity, uncertainty in estimation, and adaptive behaviour or model drift are characteristics that exacerbate the inherent risk. All these characteristics render AI-generated outputs less comprehensible, to be tested and evaluated, and consequently, there are more chances that financial information can be prepared in material misstatement. In this sense, high-risk AI alters the nature of the underlying audit object and forces firms to realise that AI-specific characteristics can become the sources of audit risk themselves.

Control risk is a possibility that the internal control mechanism of a client will not avoid, detect, and correct material misstatements timely. When AI is of high-risk, the control risk is largely reliant on AI governance structures and associated control arrangements. In this regard, the framework outlines controller risk using factors like control framework governance, human supervision, model validation, data governance, documentation and audit trail, monitoring and change supervision, and accountability and responsibility. These aspects indicate the notion that technically sophisticated AIs are risky in terms of auditing when companies do not develop proper governance, auditing, validation and documentation. In this way, the framework approaches the control risk as a highly important sphere where the governance and assurance procedures directly impact the determination made by the auditor whether the AI-driven processes are controlled enough.

Detection risk is the risk that the material misstatements that exist in the financial reporting in relation to AI will not be detected during the audit procedures. Detection risk, in this case, is associated with quality and suitability of audit response. That is why the framework describes the detection risk by using modified audit procedures, substantive testing of AI outputs, benchmarking and back-testing, the application of computer-assisted audit technique and data analytics, participation of the IT or AI experts, and increased audit documentation. This is an indication of the argument that auditing clients with high-risk AI does not only demand awareness of new risks, but also alterations in the execution of the audit. In cases where the audit firms prescribe the appropriate processes, expert assistance, and sound documentation strategies, the risk of detection is minimized, in cases where the advice is weak or nonexistent, the probability of AI-related misstatements going undetected increases.

Professional skepticism is treated as an element of the framework rather than as a component associated with only one part of the audit risk model. The reason behind this is that skepticism affects the inherent risk interpretation by auditors, control evaluation by auditors, and the design or execution of audit procedures. Professional skepticism in the aspect of high-risk AI deals with having a questioning mind, critical evaluation of AI results, not depending on automated systems excessively, not developing aversion to algorithms and practicing professional judgment. The fact that skepticism is integrated as a cross-cutting category supports the argument that the reaction of the auditor to AI will not be a blind following of the technologically generated outputs and/or reflexive avoidance of them. Rather, companies must convey a moderate stance, whereby AI-made information will be evaluated strictly by the professional standards. Skepticism, in this case, serves as both a behavioural and judgmental anchor, to the entire audit risk framework.

The second element of the framework is AI governance and assurance. Relevant reference points for the governance and assurance dimension include the NIST AI RMF, COSO's broader AI governance guidance together with its later GenAI internal-control extension, ISO/IEC standards, and the IIA AI

auditing framework. Although governance and assurance mechanisms are particularly pertinent in controlling risk, they also determine the interpretation of inherent and detection risks. Their place in the model is evaluative: they are one of the criteria to which the sufficiency of AI-related oversight, controls, validation procedures, accountability systems, and assurance schemes can be measured. This category is especially relevant in the context of the current study since it will enable the analysis to investigate whether Big Four firms resort to recognised governance and assurance frameworks to discuss about high-risk AI, and whether they frame such frameworks into audit quality and risk management.

The third element of the framework is AI/technology usage in auditing. This dimension describes the practical and organizational aspect of technology in the audit work. It features the implementation of CAATs, data analytics, AI-guided processes, technology-assisted risk assessment, digital audit tools, and specialist assistance. The addition of this category enables this framework to capture the key findings of technology-usage theories to avoid transforming them into a behavioural model. That is, the model recognises that the use of technology in auditing is conditioned by the readiness of organizations, expectations of the profession and pressures of the institutions, but it considers those concerns as a part of the overall audit response environment and not the phenomenon that is to be explained. This element therefore reflects the role of technology as part of the broader audit response to high-risk AI rather than as an independent behavioural phenomenon.

The last area of the framework is audit benefits that give the anticipated results in case the former areas are properly tackled in practice and guidance in the field of the profession and the audit. The advantages of audit in this model are characterized by an enhanced risk of material misstatement identification, quality of audit evidence, quality of documentation, enhanced high-risk areas focus, increased efficiency and coverage of the audit and the quality of the overall audit. These results cannot be perceived as the automatic effects of using technologies only. Instead, the framework presupposes that the positive effects of audit will be attained when a mix of proper risk assessment, efficient governance and assurance systems, reasonable use of technologies, and long-term professional Skepticism will be discovered. In that way, the model does not show AI as something intrinsically bad or good, but as a source of a risk and an opportunity that needs to be mediated using audit-relevant structures and responses.

The integrative conceptual framework created in this paper is shown in Figure 5. The broader contextual condition is that the client had used the systems of high-risk AI in financial reporting. It then puts the audit risk model at the middle of the framework organized in inherent risk, control risk and detection risk. The complementary elements that affect the interpretation and management of all three risk components are professional skepticism, AI governance and assurance, and AI/technology usage in auditing. Lastly, the framework connects these dimensions with the audit benefits as the most probable expected results of good audit-firm guidance and suitable audit responses. By doing so, the figure summarises the theoretical reasoning of the study and presents a structured representation of the relationships developed in this chapter.

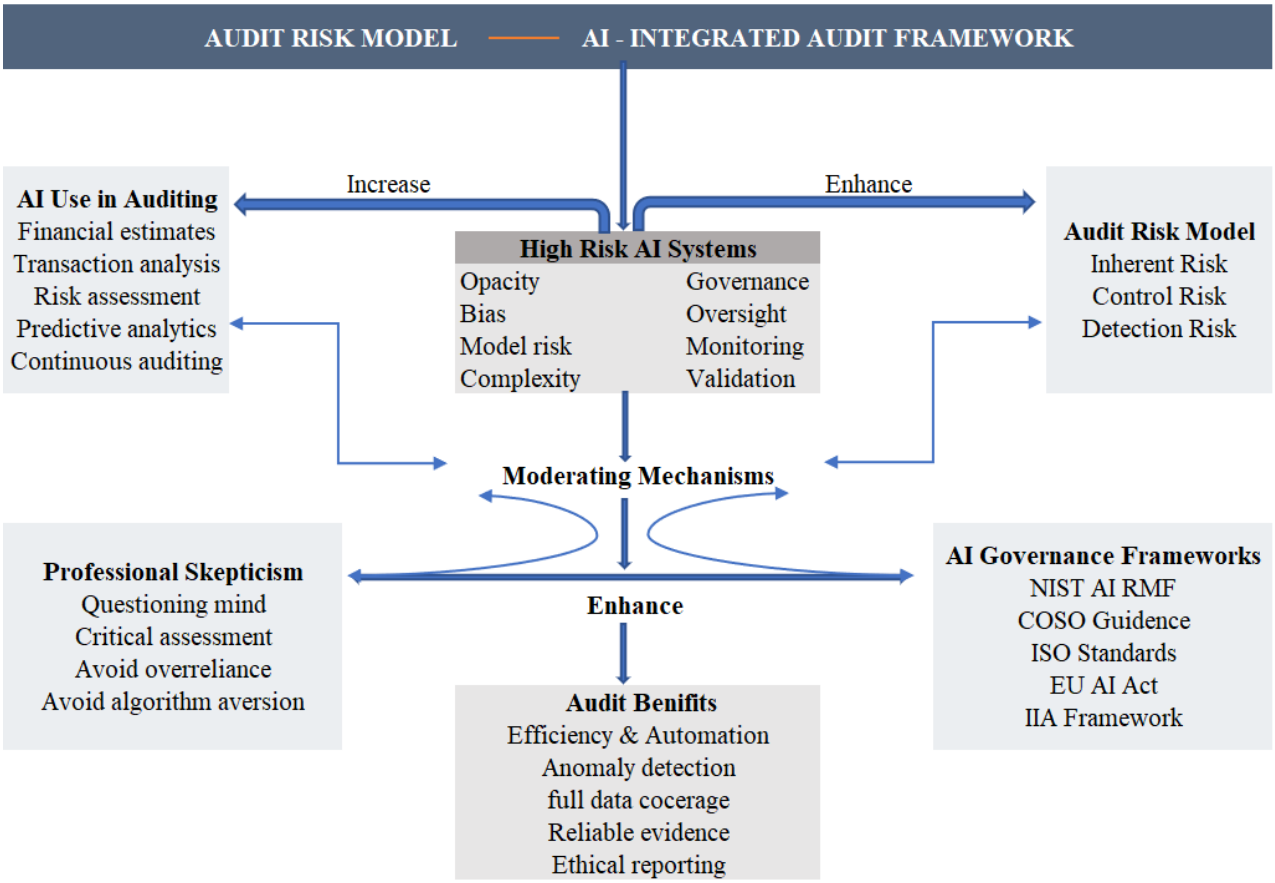


Fig. 5. AI integrated audit framework

Figure 5 summarises the integrative conceptual framework developed in this chapter. It shows that the use of high-risk AI systems in financial reporting forms the broader context of the model, while the audit risk model occupies the central position through inherent risk, control risk, and detection risk. Professional skepticism, AI governance and assurance, and AI/technology usage in auditing operate as complementary elements that shape how these risks are interpreted and addressed. The framework also links these elements to audit benefits as the expected outcomes of appropriate audit responses and strong professional guidance.

The framework is intentionally audit-focused and does not treat technology adoption theories as a separate behavioural model centred on individual auditor intention. Instead, these theories are incorporated only insofar as they help explain how technology is positioned and embedded in audit practice. In this way, the framework remains focused on audit risk, professional skepticism, governance and assurance, technology usage, and audit-related outcomes.

3. Research methodology

3.1. Directed content analysis

The research employs the directed content analysis as the principal empirical research methodology. The approach is suitable since the research analyzes open textual records that are issued by the Big Four audit companies and attempts to read how these companies are communicating with regards to AI risks, governance frameworks, implications of the assurance, and reaction of the auditors in the financial reporting. Such an analysis is not aimed to be confined to determining whether certain issues are mentioned or not, but anyway, to analyzing how these issues are put across, the amount of focus they get, and the degree to which they are elaborated in various reports. This is consistent with the logic of content analysis as a technique of extracting meaning out of text data and to learn communication in a contextual form.

Directed content analysis seems to be the best approach especially in situations where the researcher has a given theoretical framework to start on and utilizes it to direct the preliminary coding. Hsieh and Shannon (2005) make a difference between a directed content analysis and the traditional content analysis by stating that in the former, the analysis begins with theory or previous research results that offer guidelines to initial categories of coding. Elo and Kyngas (2008) also define deductive content analysis as a suitable method in cases when previous theoretical knowledge is applied to organize the analysis beforehand. Assarroudi et al. (2018) also go on to explain that the directed qualitative content analysis is particularly effective under the conditions that a study is intended to validate, extend or conceptually elaborate an existing theoretical framework by conducting systematic text analysis.

This reasoning is aligned with the structure of the current thesis. The empirical analysis is based not on open-ended themes, but a conceptual structure, which has been predefined in Chapter 2. The lens of analysis is clearly developed in the thesis draft with the audit risk model, professional skepticism, AI governance and assurance, and AI/technology usage in auditing. Later these ideas are operationalized into thematic categories and subcodes of analysis of Big Four documents. Since the theory-directed empirical coding is not created inductively by itself but based on the reports, a guided sort of content analysis is more appropriate methodologically in comparison with a concerningly inductive or traditional one.

The approach is also suitable due to the fact that the empirical data is in the form of reports, frameworks, disclosure of transparency and policy texts and is not numerical data; it is a professional communication. Krippendorff also considers content analysis as a mechanism of providing replicable and valid inferences to texts that are considered to be meaningful communications in context. This interpretation is especially applicable in this case, since the purpose of the study is to examine how Big Four audit firms communicate the risks, governance structures, and assurance implications of high-risk AI systems in financial reporting.

There is a substantive and methodological justification of directed content analysis. Substantively, it enables the study to examine how Big Four companies position high-risk AI as auditing and financial reporting issues. In terms of its structure it is methodologically equivalent to the deductive structure of the thesis, as the empirical analysis is not formed by the purely induction manner, but by the pre-determined theoretical categories. It is due to this fact that directed content analysis can give the best coherent connection between the problem analysis in Chapter 1, the theoretical background in

Chapter 2 and the findings that will be made later in the thesis. This study is made up of secondary textual data as the empirical material. To be more precise, the information will be retrieved using publicly accessible reports published by the Big Four audit firms, namely, Deloitte, EY, KPMG, and PwC, via their web pages, transparency platforms, insights centers, and PDF archives. These documents consist of audit quality reports, transparency reports, responsible AI principles, AI governance frameworks and AI-related thought leadership reports. The thesis paper has already characterized the research as an analysis of public Big Four materials and claims that the materials are sorted by title, year, company, pages and theoretical keywords.

3.2. Sample and data source

Chosen texts and conclusive sample.

The empirical data of the present study is based on the secondary written material presented in publicly-available reports issued by the Big Four audit firms: Deloitte, EY, KPMG and PwC. The choice of these documents is due to the fact that they address the research question directly and include clear professional communication on the implications of AI-related audit risk, governance, audit quality, transparency, and assurance. The chosen materials are audit quality report, transparency report, governance framework, and AI related thought leadership report. This option aligns with the study objective that is to investigate how the Big Four report high-risk AI concerns on financial reporting and auditing.

The sample was developed purposely. The final corpus only kept documents which provided substantive discussion of AI in audit, responsible AI, governance mechanisms or audit-quality implications. The last document table shows the chosen reports by the firm, document title, type, year, source link, the number of pages, and the inclusion reason. The final corpus currently is made up of 12 documents spread among Deloitte, EY, KPMG, and pwC.

Table 2. The final sample

Firm	Document title	Type	Year	URL	Pages	Inclusion reason
Deloitte	Audit Quality Report (GlobaL)	Audit quality report	2024	2024-audit-quality-report.pdf	41 pages	Contains AI references and tech.
Deloitte	UK Audit Transparency Report	Transparency report	2024	deloitte-uk-annual-review-2024-audit-transparency-report.pdf	155 pages	Focus on audit quality, AI mention
Deloitte	UK Audit Transparency Report	Transparency report	2025	2025 UK Transparency Report	191 pages	Audit quality and technology

Firm	Document title	Type	Year	URL	Pages	Inclusion reason
EY	UK Audit Quality Report	Audit quality report	2024	ey-uk-2024-audit-quality-report.pdf	30 pages	Comprehensive QA report
EY	Gibraltar Transparency Report	Transparency report	2025	ey-gi-transparency-report-gibraltar-2025.pdf	52 pages	Firm governance/innovation
EY	Responsible AI Principles (Global)	Governance framework	2024	ey-gl-responsible-ai-principles-09-2024.pdf	11 pages	Official AI governance stance
KPMG	AI in Audit (Global insights)	Thought leadership	2024	AI in financial reporting and audit: Navigating the new era	28 pages	Directly on AI+audit topic
KPMG	US Transparency Report	Transparency report	2024	2024-transparency-report-jan-2025.pdf	37 pages	QA reporting, tech mention
KPMG	Asia Audit and Assurance Quality Report	Quality report	2023	2023 KPMG HK Audit Quality Report	28 pages	Tech adoption in audit
PwC	NL Transparency Report 2024/25	Transparency report	2025	pwc-transparency-report-2024-2025.pdf	41 pages	Mentions “AI agents” in audit
PwC	Global Audit Quality Report	Audit quality report	2024	Audit Quality Report 2024	51 pages	Global QA (US+UK present)
PwC	Responsible AI: Putting Ethics to Work	Governance framework	2023	Responsible AI - Maturing from theory to practice	34 pages	Official AI ethics/guidance

As shown in Table, the final sample includes 12 publicly available Big Four documents that form the empirical basis for the directed content analysis.

Inclusion and exclusion criteria

In order to convert the chosen documents into a consistent and analytical measure, inclusion and exclusion criteria were pre-established to screen the selected documents. These criteria aided in

determining what sources will and will not be included in the analysis and what materials need to be left out. The criteria also enhance the transparency of the sampling process by demonstrating how the end corpus was reduced to the most pertinent official documents in the Big Four. Both tables and the criteria of firm, source type, time period, content relevance, analytical value, language and exclusion criteria (insufficient content, topic, unofficial source and incompleteness).

Table 3 Inclusion criteria

Criterion	**Description**	**Relevance to this study**
Firm	The document must be published by one of the Big Four firms: Deloitte, EY, KPMG, or PwC.	Ensures that the study focuses only on the leading global audit firms relevant to the research question.
Source type	The document must be publicly available on an official firm website, official PDF repository, transparency hub, or insights page.	Ensures the authenticity and reliability of the data source.
Time period	The document must be published between 2023 and 2025.	Matches the study scope defined in the thesis draft.
Content relevance	The document must address at least one of the following: AI in audit, high-risk AI, audit quality, transparency, AI governance, responsible AI, assurance implications, audit innovation, or digital audit.	Ensures direct alignment with the research problem and conceptual model.
Analytical value	The document must contain enough substantive text for coding and interpretation.	Allows meaningful use in directed content analysis.
Language	The document must be available in English.	Supports consistency in analysis and writing of the thesis.

Table 4. Exclusion criteria

Criterion	Description	Reason for exclusion
Insufficient content	The item is only a short webpage, news post, or promotional note with no substantial guidance.	Such material cannot support systematic coding.
Topic mismatch	The document does not meaningfully address AI, auditing, governance, assurance, or financial reporting.	Keeps the corpus focused on the research question.
Unofficial source	The file is reposted on a third-party website and not directly issued by the firm.	Reduces reliability and traceability of the source.
Inaccessible / incomplete	The document cannot be accessed fully or lacks essential information.	Prevents accurate screening and coding.
Purely marketing-oriented	The document mainly promotes services without discussing frameworks, risks, controls, or audit implications.	Limits analytical usefulness for academic comparison.
Balanced firm representation	An additional document was excluded when one Big Four firm was overrepresented in the preliminary sample and the document was less directly focused on auditing than the other selected reports..	Ensures equal representation of the four Big Four firms in the final corpus and improves cross-firm comparability while preserving stronger alignment with the study's audit-focused analytical scope.

The inclusion criteria were used so that official, relevant, and substantive enough (sufficient) Big Four documents only were included in the analysis. The exclusion criteria was applied to eliminate the materials that did not have analytical interest, were not directly connected to the subject of the

research or were not likely to be coded effectively. These criteria, together with each other, formed the narrow and clear document corpus of the guided content analysis.

The initial screened sample contained 13 reports. One Deloitte document, the 2023 AI Survey report, was excluded from the final sample to ensure equal representation across the four Big Four firms. In addition, the report primarily provided cross-industry survey evidence on AI use rather than direct discussion of audit quality, transparency, AI governance in auditing, or assurance implications. For this reason, its exclusion improved the comparability and audit-specific relevance of the final 12-document corpus.

3.3. Data analysis procedure

A well-organized, theoretically based analysis process using the Maxqda software is used to carry out the analysis of the chosen reports. The analytical structure is based on Chapter 2 and adheres to the reasoning of directed content analysis where preconceived notions dictate the identification and interpretation of pertinent pieces of text. The analysis process is structured based on thematic issues, preliminary key word categories and a coding scheme that will be subsequently used on the chosen Big Four reports in this study. According to the thesis, the empirical analysis will rely on an integrated lens incorporating such aspects as audit risk, professional skepticism, AI governance and assurance, and AI or technology usage in auditing.

Thematic areas and preliminary keywords.

The initial part of the analysis is the definition of the key thematic areas according to which the reports are reviewed. These thematic areas are deductively based on the theoretical construction as presented in Chapter 2. They assist in organizing the empirical material and keeping the analysis within direct connection with the research problem and conceptual model.
Five major thematic areas are the focus of the analysis:

- Audit risk
- Professional skepticism
- AI governance and assurance
- Use of AI/technology in auditing.
- Audit benifits.

These areas of thematization represent the significant conceptual dimensions that have already been identified in the thesis and form the point of finding the relevant text in the documents.
A preliminary set of keyword families are employed in supporting the preliminary review of the reports. These keywords are not the final results of the analysis, these keywords are the starting points of searching in the documents possible passages that may be relevant. The keywords families were chosen based on the key ideas that were discussed in Chapter 2 and the terms that are often employed in Big Four reports. These are: audit risk, inherent risk, control risk, detection risk, opacity, bias, model risk, data quality, governance, accountability, validation, monitoring, human oversight, professional skepticism, automation bias, audit evidence, assurance, responsible AI, training, innovation, audit quality, documentation and specialists. This step of the study can be substantiated by the guidelines used in the methodology of KTU, which suggests an identification of core keywords, related expressions, narrower and broader terms, and synonyms and then performing the analysis.This subsection is thus aimed at establishing the analysis focus of the study prior to the actual

coding process. Through this, the thematic areas and keywords bring a systematic transition between the theoretical framework and the chosen empirical material.

Coding framework

Reports are then analyzed using a coding framework after the identification of the thematic areas and the initial keywords. The coding scheme will be based on the combined theoretical lens of the research and will be created to provide the abstract theoretical terms into the analytical operational categories. This method would be aligned with directed content analysis in which the coding categories are predefined by theory.

In the current research, coding frame comprises parent categories, and corresponding subcodes on the five main areas of thematic focus. Appendix 1 contains the entire codebook, and this chapter contains merely an example extract to demonstrate how the coding system works, but not to excessively fill up the text of the main methodology.

Table 5. Example of the coding framework used in the analysis

Parent category	**Purpose in the analysis**	**Example subcodes**
AI related audit risk	To identify how Big Four documents describe AI-related inherent, control, and detection risks in financial reporting and audit work.	IR_OPACITY, IR_BIAS, CR_MONITORING, CR_GOVERNANCE, DR_PROCEDURES, DR_EVIDENCE_LIMITS
Professional Skepticism	To identify how documents describe the auditor's mindset, judgment, challenge, and the risks of overreliance or algorithm aversion.	SKEP_QUESTIONING, SKEP_CORROBORATE, SKEP_AUTOMATION_BIAS, SKEP_AUTOMATION_BIAS, SKEP_ANOMALY_INVEST
AI Governance and Assurance	To identify governance expectations, validation mechanisms, transparency requirements, and AI assurance practices.	GOV_ACCOUNTABILITY, GOV_VALIDATION, GOV_HUMAN_OVERSIGHT, GOV_POLICY_FRAMEWORK ASSURANCE_SERVICE
AI / Technology Usage in Auditing	To identify how documents frame the use, usefulness, adoption conditions, and implementation of AI tools in audit practice.	USE_USEFULNESS, USE_TRAINING, USE_METHOD_INTEGRATION, USE_PERCEIVED_RISK
AI Benifits	To identify how documents connect AI use with audit quality, evidence, efficiency, and contextual factors such as data quality or auditor expertise.	OUT_AUDIT_QUALITY, OUT_EVIDENCE_QUALITY, MOD_DATA_QUALITY, OUT_RISK_ASSESSMENT

The full coding framework, including all parent categories and subcodes, is provided in Appendix 1

The primary software tool applied in the arrangement and analysis of the chosen reports is the use of the software called MAXQDA. The software will be suitable to this study as it will enable importation of PDF documents, group them with a firm and document type, code them systematically and compare them under thematic categories. In the MAXQDA-supported analysis, a code is understood as a conceptual label assigned to a meaningful portion of text that reflects a specific idea relevant to the analytical framework. Subcodes are more specific categories placed under a broader parent code in order to capture finer distinctions within the same thematic area. A segment refers to the selected textual passage to which a code or subcode is assigned; depending on the context, a segment may consist of a phrase, sentence, or short paragraph. The codebook serves as the operational guide for

the analysis by listing the parent codes, subcodes, and their analytical meanings in a consistent way. The tools of MAXQDA help to generate a structured codebook, get access to coded passages and compare coded work across documents visually as well.

The selected reports were imported into MAXQDA and organised according to the four Big Four firms. The organization of the Big Four report corpus in MAXQDA is presented in Appendix 2. These predefined codes are then inputted into the software in form of hierarchical coding system. The MAXQDA coding system, including the main thematic categories, subcodes and coded segment frequencies, is presented in Appendix 3. The passages are identified and coded based on the thematic areas and subcodes identified in the coding framework. Coded segments are also retrieved using the software and compared with the distribution of the code across the firms and illustrative quotations are extracted to use in the findings chapter. Also, the summaries of codes and coded material can be exported and used by MAXQDA in tables, appendices and comparative analysis.

The analysis is thus made more transparent and organized with the help of MAXQDA. It is not in place of the interpretation on the part of the researcher, as it aids systematic use of the coding framework and help compare the negotiated Big Four documents across firms.

4. Research results and discussion

4.1. Descriptive analysis of Big Four firms' reports

This section presents a descriptive analysis of the 12 documents that were included in the final sample that is provided in Chapter 3 (see Table 2). It is meant to present the empirical foundation of the study and then proceed with the detailed results of the guided qualitative content analysis. To be more precise, this section is going to detail the document corpus composition, the time dynamics of the reports, how the documents are distributed among the Big Four audit firms, and the key AI- and technology-related tools or platforms that have been mentioned in these publications. Table 6 presents the descriptive profile of the final document corpus, including the distribution of report types, page volume, and named AI/digital audit tools across the Big Four firms.

Table 6. Descriptive profile of the final document corpus by firm

Descriptive indicator	Deloitte	EY	KPMG	PwC	Overall
Number of documents, n	3	3	3	3	12
Share of corpus, %	25.0	25.0	25.0	25.0	100.0
Audit quality reports, n (% within firm)	1 (33.3)	1 (33.3)	1 (33.3)	1 (33.3)	4 (33.3 of corpus)
Transparency reports, n (% within firm)	2 (66.7)	1 (33.3)	1 (33.3)	1 (33.3)	5 (41.7 of corpus)
AI-related publications, n (% within firm)	0 (0.0)	1 (33.3)	1 (33.3)	1 (33.3)	3 (25.0 of corpus)
Total pages, n	387	93	93	126	699
Average pages per document	129.0	31.0	31.0	42.0	58.3
Named AI/digital audit tools disclosed, n*	3	3	1	2	9

Note. Percentages in the report-type rows are calculated within each firm; the overall column shows the proportion out of the full corpus (n = 12). Named tools/platforms explicitly mentioned in the analysed documents include Deloitte's Omnia, PairD, and Levvia; EY's Canvas, Helix, and Atlas; KPMG Clara; and PwC Aura and Halo.

The sample includes documents from the Big Four audit firms - Deloitte, KPMG, EY and PwC. First, as a descriptive finding, the empirical data is not confined to one type of report. Instead, it includes a range of reporting types through which Big Four convey audit quality, transparency, governance, digital transformation and the increasing integration of artificial intelligence in audit and assurance. In particular, there are three types of reports in the sample: audit quality reports, transparency reports, and AI- or responsible AI-related publications. This is important because these documents are generally issued at the level of national member firms, regional offices or global networks, rather than through a single global annual report. Thus, they differ in terms of structure, detail and communicative logic based on regulatory, jurisdictional and strategic considerations.

In terms of inter-firm comparison, the final corpus is representative of the Big Four networks, with three documents from each firm. This allows a reasonably comparable descriptive foundation for the analysis and shows Big Four reporting is not completely consistent. While the four firms are equally represented in terms of numbers, the nature of the corpus varies in terms of type of report and number of pages (see Table 6). The corpus, then, should not be seen as a collection of uniform reports, but rather a collection of complementary public reports through which the firms communicate audit quality, governance and technology.

These report types also differ in their primary focus. Audit quality reports usually explain how firms define, maintain, and improve audit quality through governance, methodology, people development, monitoring, inspection, and technology. Transparency reports are generally more formal and more directly linked to regulatory or code-based disclosure requirements, with stronger emphasis on governance systems, independence safeguards, quality management systems, and accountability. AI- and responsible AI-related publications are particularly relevant to this thesis because they place AI within the broader context of governance, risk, assurance, ethics, and digital transformation. Taken together, these report types provide a more complete picture of how the Big Four communicate the role of AI in contemporary auditing.

The analysed documents differ in title, structure, jurisdiction, and level of detail; however, thematic overlap across the sample is substantial. Recurring themes include quality management, governance, transparency, accountability, ethics, people capability, monitoring, digital transformation, and the use of technology in auditing. This suggests that the Big Four increasingly position AI not as an isolated technical innovation, but as part of a broader transformation of audit infrastructure and assurance practice.

The time dynamics of the reports is another descriptive dimension that is important. The analysed documents show that the reporting year and the publication date do not always coincide. In most instances, a report is described as having one reporting period but published in the next calendar year. It is implied that the interpretation of the corpus must be based on at least two temporal indicators, including the period, to which the information is associated, and a date when the report was publicly published. This difference is practical as it demonstrates that Big Four reporting has a more widely annual cycle, yet, not a completely standardised one among companies and jurisdictions. Transparency reports usually have a specified year-end date but audit quality reports are more likely to be based upon a reporting year or annual review cycle.

One of the most significant descriptive results is related to the visibility of AI and digital audit devices. Throughout the last sample, technology is not only introduced as a support feature, but also as a significant part of audit process, workflow integration, analytical capacity, and quality improvement. The materials analysed in the case of Deloitte include the Omnia platform, the in-house generative AI system PairD, and the digital platform Levvia, which demonstrates that the company publicly associates the delivery of audit services with named digital and GenAI-enabled solutions. Innovation, data connectivity, anomaly detection, and AI-enabled auditing are heavily emphasized in the reporting of KPMG, and this further technological trend is often related to the audit platform of KPMG Clara. According to the reports and other materials provided by EY, audit transformation is linked to next-generation assurance technology and responsible AI governance and the digital audit environment developed by the company is often defined by EY Canvas, EY Helix, and EY Atlas. The publications of PwC also appear to correspond with an environment of technology- and AI-focused auditing and are commonly linked to the fundamental audit platforms, like Aura and Halo. The fact that these named tools are included in the descriptive analysis is significant in that it demonstrates that the Big Four do not talk about AI in abstract or strategic terms; they also relate it to tangible digital infrastructures involved in practice of audit and assurance.

Another descriptive trend is the growing trend of quantified disclosures in these documents. Some of the reports contain indicators concerning the results of inspections, training, use of technology, employee development, governance, or quality of audit performance. Even though this part is not yet

statistical but descriptive, this is nonetheless quite important since this indicates that the Big Four are starting to back their stories with quantifiable deliverables and dashboard-like displays. That is, these publications do not simply convey ideals and promises, but also strive to illustrate progress and responsibility with the help of chosen indicators.

As shown in Table 6 the corpus is balanced at the firm level, with three documents from each Big Four network, but not fully symmetrical in terms of report type. Transparency reports form the largest category in the sample (41.7%), followed by audit quality reports (33.3%) and AI-related publications (25.0%). The page distribution is also uneven: Deloitte contributes the largest page volume, while EY and KPMG provide more compact document sets. Finally, the table confirms that named AI or digital audit platforms are disclosed across all firms, although with different levels of specificity, which supports the interpretation that technological infrastructure is an increasingly visible part of Big Four public communication.

4.2. AI-related thematic disclosures

This section will present a general overview of the distribution of the coded material across the five major categories of analysis before discussing each category in more detail. Figure 6 is a summary of the distribution of coded segments and, consequently, indicates what themes were given the most coverage in the analysed Big Four reports.

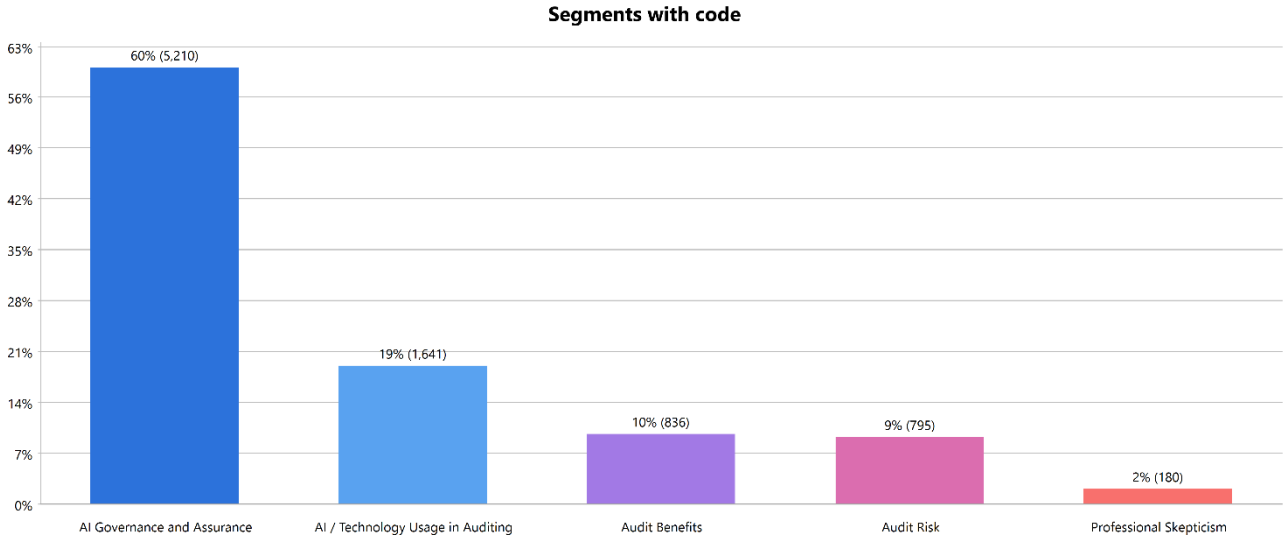


Fig. 6 distribution of thematic areas

The prevalent category in the corpus analysed, as illustrated in Figure 6, was that of AI Governance and Assurance, which made 60% of all the coded segments (5,210 segments). It means that the greatest overall focus, in the chosen reports, was on governance models, monitoring systems, accountability, transparency, policy models, ethical standards, monitoring, and assurance-related disclosures around AI and technology application in auditing. The overwhelming prevalence of this category indicates that the popular discourse of the Big Four represents AI as a sphere that needs to be regulated, managed, and adjusted to the expectations of the wider assurance and quality management.

The second most notable thematic area was AI / Technology Usage in Auditing, which was 19 percent of all coded segments (1,641 segments). This demonstrates that the practical use of AI, digital platforms, data analytics, automation, and technology-supported audit procedures are also significantly covered in the reports that are analysed. Descriptively, this finding implies that the Big Four are not talking about technology at the level of strategic principles or issues of governance. They also introduce it as a working component of modern audit practice that is part of audit processes, gathering evidence, analysis, and more extensive digital transformation activities.

The other three thematic categories were significantly less addressed in text. Accounts with audit benefits took up 10 percent of all coded segments (836 segments), and Audit Risk took 9 percent (795 segments). According to these findings, the reports under analysis contain the discussion of both the positive potential of AI and the risks of its application, although these debates are less extensive than the prevalent focus on governance and practical implementation of technology. The category of the Audit Benefits implies that the issues of increased efficiency, increased ability to analyze, expanded coverage of the audit, and facilitation of the quality of the audit are also paid certain attention. Simultaneously, the Audit Risk category indicates that the reports also consider issues connected with the use of AI, such as the necessity to control, ensure reliability, responsibility, and be careful with the implementation. Nonetheless, none of these categories is placed in the center of the whole discussion.

Professional Skepticism was the least represented category with a representation of only 2 percent of all coded segments (180 segments). This implies that despite the fact that professional skepticism is a significant principle of auditing, it has a relatively small role in the external reporting that was part of the ultimate sample. That is, the sceptical judgement, the critical challenge, and the auditor vigilance can be found in the documents, but are not addressed in the same vein as governance, assurance, or technology-related topics. This could imply that professional skepticism is handled more as an internal of professional expectation than the topic of professional skepticism that is explicitly expounded in open disclosures.

In general, the frequency of coded segments shows a definite thematic hierarchy throughout the final sample. The analysed Big Four reports are mainly focused on AI Governance and Assurance, then on AI / Technology Usage in Auditing, and on Audit Benefits, Audit Risk, and on Professional Skepticism in particular, much less emphasis is devoted. This trend implies that the hegemonic discourse in the chosen reports represents AI primarily in the terms of governance, accountability, assurance readiness and organised control, but not in the terms of a strictly promotional or innovation-based view. Simultaneously, the large portion of AI / Technology Usage in Auditing proves that digital tools and AI-driven systems become more offered as an operational reality in the audit practice.

Combined, these results demonstrate that the public reporting of the Big Four portrays AI in the field of auditing most of all as a governance issue and regulated enforcement. According to the reports, the adoption of AI is strongly linked to the quality of assurance, institutional control, and organizational technological integration. This general thematic outline is the foundation of the next subsections where each major category is considered in more detail, with its background codes and particular thematic patterns.

4.3. Cross-firm comparison of AI-related thematic disclosures

To complement the aggregate thematic distribution presented in Section 4.2, this subsection compares how the four Big Four firms emphasise the five main thematic categories in their public disclosures. This comparison is important because the study is not limited to identifying the dominant themes across the full sample, but also seeks to compare how the firms communicate high-risk AI issues in relation to governance, technology use, audit risk, professional skepticism, and audit benefits. The cross-firm perspective therefore adds an important analytical layer to the findings by showing whether the overall thematic hierarchy is shared across firms or whether some firms place greater emphasis on specific themes.

	KPMG	PwC	EY	Deloitte
Audit Risk	9.01%	13.01%	9.06%	7.79%
Audit Benefits	0.00%	0.00%	0.00%	17.61%
AI / Technology Usage in Auditing	16.09%	34.95%	19.71%	13.27%
AI Governance and Assurance	69.31%	49.02%	69.80%	60.12%
Professional Skepticism	5.58%	3.02%	1.43%	1.20%

Fig. 7 Cross-firm distribution of the five main thematic categories in Big Four AI-related disclosures

The cross-firm matrix shows that AI Governance and Assurance is the dominant category for all four firms, although the degree of emphasis varies. Governance-related disclosures account for 69.31% of coded segments for KPMG, 49.02% for PwC, 69.80% for EY, and 60.12% for Deloitte. This indicates that all four firms frame AI primarily as a governance and assurance issue, but EY and KPMG do so more strongly than PwC. Deloitte also shows a high governance share, although lower than EY and KPMG. Taken together, this pattern suggests that governance, accountability, oversight, and assurance readiness form the central discourse through which the Big Four publicly position high-risk AI in auditing.

The second most visible area of variation concerns AI / Technology Usage in Auditing. PwC shows the highest relative emphasis in this category at 34.95%, compared with 19.71% for EY, 16.09% for KPMG, and 13.27% for Deloitte. This makes PwC stand out as the firm whose disclosures are comparatively more oriented toward practical adoption, implementation, and operational use of AI tools in audit work. By contrast, EY and KPMG appear to allocate proportionally more space to governance than to practical technology-usage themes. Deloitte also discusses AI usage, but with a lower relative share than PwC and EY. This pattern suggests that, within the same overall Big Four discourse, firms differ in the balance they strike between governance-oriented and implementation-oriented communication.

The Audit Risk disclosures are present across all firms, but at a much lower level than governance and technology usage. PwC has the highest relative share of audit-risk-related disclosures at 13.01%, followed by EY at 9.06%, KPMG at 9.01%, and Deloitte at 7.79%. These differences are not large, but they suggest that PwC frames AI somewhat more explicitly in terms of risk implications than the other firms in this sample. KPMG and EY display almost identical proportions, while Deloitte allocates slightly less emphasis to audit risk. Analytically, this indicates that all firms acknowledge AI-related audit risk, but this theme remains secondary compared with governance and practical technology use.

Professional Skepticism is the least emphasised thematic disclosure for all four firms. It accounts for 5.58% of coded segments for KPMG, 3.02% for PwC, 1.43% for EY, and 1.20% for Deloitte. This pattern is consistent with the aggregate result reported earlier, where professional skepticism was the weakest of the five major categories. The cross-firm comparison shows that this is not merely a sample-wide average, but a relatively consistent tendency across firms. KPMG gives somewhat more visible attention to skepticism-related issues than the other firms, but even there the relative share remains small. This suggests that, in public disclosures, the Big Four discuss AI more often through governance, systems, and implementation language than through explicit references to skeptical judgement, challenge, or auditor mindset.

A particularly notable result is the distribution of Audit Benefits disclosures. In this matrix, Deloitte is the only firm with a visible coded share in this category (17.61%), while KPMG, PwC, and EY display 0.00%. This does not necessarily mean that the other firms never refer to benefits in any broader sense, but within the coded sample and category structure used in this study, explicit benefit-oriented discussion appears concentrated in Deloitte's disclosures. This makes Deloitte distinctive in the way it presents AI not only as a governance or implementation issue, but also as a source of positive audit outcomes. Because this difference is pronounced, it should be interpreted carefully and linked to the specific composition of the sampled documents rather than generalised beyond the analysed corpus.

Overall, the cross-firm comparison shows that the four audit firms share a common high-level thematic hierarchy, but differ in relative emphasis. Governance and assurance dominate the discourse across all firms, confirming that AI is framed chiefly as a matter of structured oversight and responsible control. At the same time, PwC places comparatively greater emphasis on practical AI usage, Deloitte stands out in its explicit discussion of audit benefits, and KPMG gives relatively more space to professional skepticism than the others. These differences suggest that, although the Big Four operate within a shared professional discourse on high-risk AI, they do not communicate the issue in exactly the same way. Thus, the cross-firm analysis strengthens the findings chapter by showing that the public reporting of high-risk AI combines both common institutional patterns and firm-specific thematic emphases.

4.4. Cross-Category Analysis of AI-Related Audit Disclosures

This section builds on the descriptive analyses in Sections 4.1 and 4.2 by examining how the coded themes interact within and across the categories of audit risk, professional Skepticism, AI governance and assurance, AI/technology usage in auditing and audit benefits. Using MAXQDA's Code Relations Browser, the analysis below identifies the strongest co-occurrences and interprets their significance for the development of AI-integrated auditing.

Code relations were examined using MAXQDA's Code Relations Browser under the Intersection setting. The reported frequencies therefore represent the number of overlapping coded text segments to which both codes were assigned. In this thesis, thematic co-occurrence is thus understood as intersection-based code relation rather than simple proximity or same-document association. All documents in the final sample were activated, and the matrices were used to identify patterns of thematic linkage only; they do not imply causal relationships.

4.4.1. Within-category relationships

Audit Risk

The code-relations matrix of the Audit Risk category reveals that the AI-related audit risk does not exist in an even distribution across all sub-codes, but is rather clustered in a few stronger relationships. CR_HUMAN_OVERSIGHT and IR_ESTIMATION (12) exhibit the strongest visible co-occurrence, indicating that audit-risk implications of AI are most closely related to areas that require estimation and are, hence, most intensive in human review and judgement. The analytical significance of this finding is that it demonstrates that despite the application of AI in financial-reporting, the interpretation and validation of complex estimates remain based on human supervision instead of only on automated outputs.

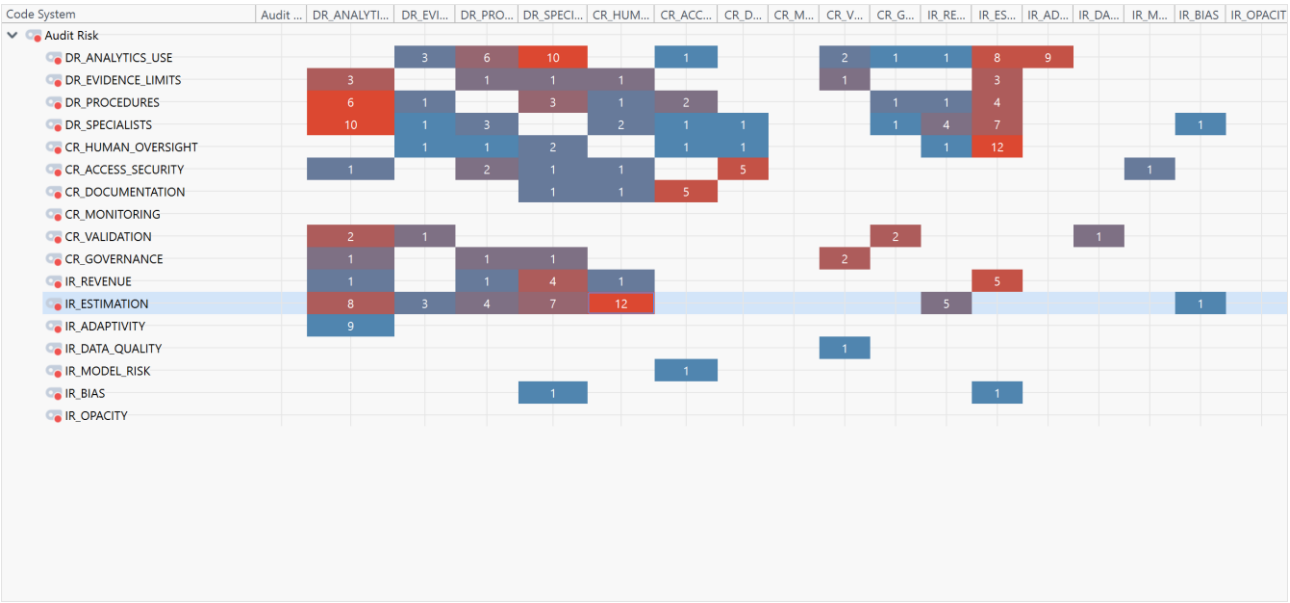


Fig. 8 Code-relations matrix of the Audit Risk category

The second pattern of interest is the detection-risk cluster which connects DR_ANALYTICS_USE, DR_SPECIALISTS and DR_PROCEDURES. The highest correlation in this cluster is between DR_ANALYTICS_USE and DR_SPECIALISTS (10), then between DR_ANALYTICS use and DR_ Procedures (6). Moreover, IR_ESTIMATION goes hand in hand with DR_ SPECIALISTS (7) and DR_ PROCEDURES (4). These links imply that documents present AI-related audit risk in the form of an operation response with the application of improved analytics, expert assistance, and modified audit practices. That is, AI-related risks are not introduced as being manageable by traditional audit procedures only, but seem to need supplementary technical skills and procedural modification.

Another clear relationship that is shown in the matrix is between the detection-risk themes and the inherent-risk themes. Specifically, DR_ANALYTICS_USE is strongly co-occurring with IR_ADAPTIVITY (9) and IR_ESTIMATION (8). According to this pattern, AI-related inherent risk is particularly salient in cases where the systems are adaptive or have an impact on the accounting estimates. Audit wise this is important as adaptive systems are not as stable as they can evolve over a period of time hence their outputs are more challenging to audit using the traditional or purely fixed audit methods. In this way, the research results suggest that the audit-risk issue is both related to the existence of AI and associated with the dynamic and judgement-sensitive character of reporting activities under the influence of AI.

The most visible relationship is that between CR_ACCESS_SECURITY and CR_DOCUMENTATION (5), within the control-risk dimension. The control-risk relationships are weaker and more fractured, in comparison to the detection-risk and estimation-related clusters, however. It indicates that the issues related to access, documentation, validation, and governance are recognised in the analysed documents, but they are not highlighted as intensively as the operational audit response to AI-related risks. Based on this, the control-risk discourse seems to have been supportive of the larger risk structure and not to take over it.

The next interesting aspect of the matrix is that the presence of several AI-specific risk themes that are theoretically relevant is rather weak, i.e., IR_MODEL_RISK, IR_BIAS, and IR_OPACITY. The codes are found in distributed or low frequency co-occurrences and do not constitute a thick interpretive cluster. It does not mean that these issues are not covered in the wider discussion; instead, in the Audit Risk category, they are seen as less key as estimation, analytics usage, specialist engagement, and human controls. This implies that the Big Four documents put AI-related risk in a more solid framework of risks that can be mitigated under familiar audit frameworks, rather than a complete developed discourse on algorithmic obscurity or model failure.

In general, the Audit Risk matrix indicates a set of three key conclusions of analysis. To start with, AI audit risk is concentrated in those areas that have high estimates, and human oversight is especially significant in them. Second, the most widespread reaction to AI-related risk is put in the context of analytics utilization, expert assistance, and procedural modification, which means that there is a distinct detection-risk orientation. Third, even though control-focused issues are also involved they are more secondary compared to the operational issue of auditing AI-influenced estimates and adaptive systems. Put collectively, these results indicate that AI does not automatically mitigate audit risk, but rather transforms audit risk by heightening the dependency on analytical processes, expert knowledge and human judgement in auditing the AI-influenced financial reporting.

Professional Skepticism

The matrix of code-relations in the category of Professional Skepticism is significantly more sparse than that of Audit Risk, which implies that the sub-codes of Skepticism are not as densely interrelated. Instead of creating a large and very integrated cluster, the relationships are focused on a small number of visible pairings. The highest co-occurrence is between SKEP_ANOMALY_INVEST and SKEP_CORROBORATE (6), then there is an association between SKEP_ANOMALY_INVEST and SKEP_QUESTIONING (3). This tendency indicates that, in the documents under analysis, professional skepticism is manifested mainly in the form of a specific reaction to suspiciousness or

other abnormalities, in particular, in the form of corroborative verification and, to a smaller extent, questioning.

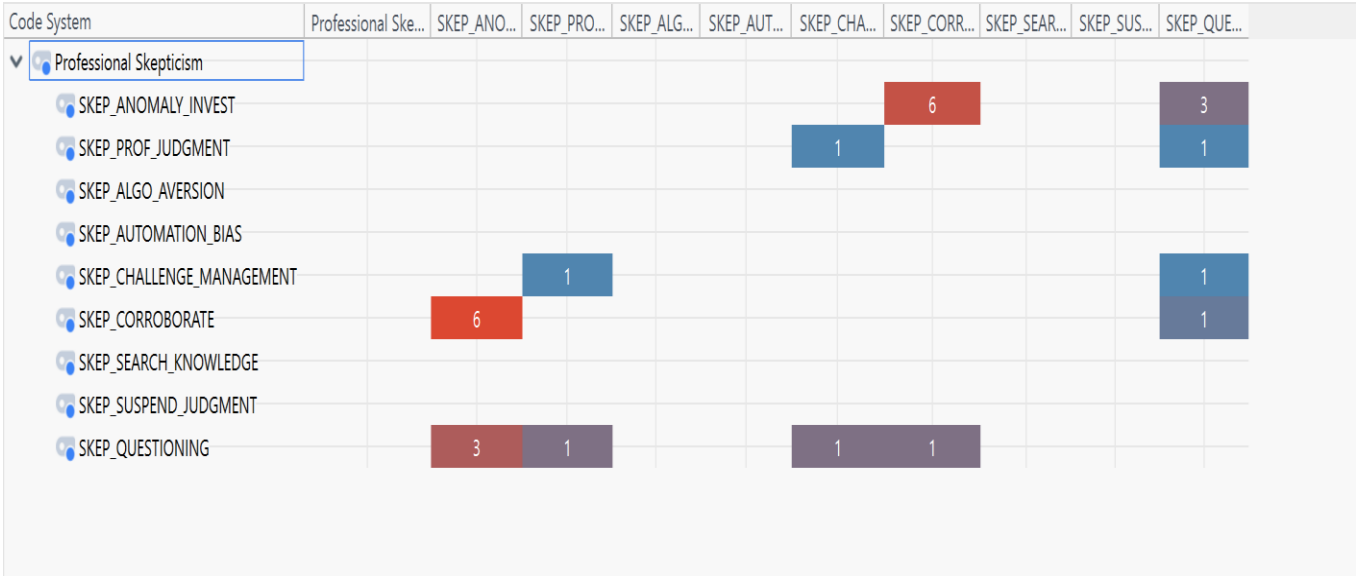


Fig. 9 Code-relations matrix of the Professional Skepticism category

The most obvious visible link, between corroboration and anomaly investigation, suggests that skepticism is operationalised primarily as a verification-oriented practice. That is, an identification of anomalies does not lead to the sceptical response outlined in the documents being merely a doubt in an abstract sense, but an attempt to validate, verify or prove the problem by means of further evidence or verification processes. It is analytically important as it demonstrates that professional skepticism is positioned as an evidence-seeking mechanism that becomes especially pertinent when AI-related processes or products are suspicious, inconsistent, or require additional verification.

This interpretation is supported by the second strongest relation, between anomaly investigation and questioning (3). It implies that questioning exists as a sceptical behaviour, which is more restricted compared to corroboration. This can be taken to mean that the Big Four reports are more focused on testing and verification of anomalies than on long-term scrutiny of assumptions, model logic, or decision processes. In the context of the AI-based auditing, this matters to the extent that it shows that the process of Skepticism is primarily triggered once a marker of irregularity has been noticed, and not engraved in a more general attitude to AI-based products.

Other visible co-occurrences in the matrix are feeble and desolate. The correlation between SKEP_PROF_JUDGMENT and SKEP_CHALLENGE_MANAGEMENT only at a low frequency (1), and the same can be said of low-frequency relationships between SKEP_QUESTIONING and SKEP_PROF_JUDGMENT, SKEP_CHALLENGE_MANAGEMENT and SKEP_CORROBORATE (1 each). These less strong connections suggest that the discourse of Skepticism contains the judgement, questioning, and management challenge, but they are not a strong and dense analytical group. Thus, even though the category does include some elements of traditional audit Skepticism, these are not quite as systematically combined as would be the case in a more developed or more fully developed AI-Skepticism.

The other significant aspect of the matrix is that there is almost no significant co-occurrence between SKEP_ALGO_AVERSION, SKEP_AUTOMATION_BIAS, SKEP_SEARCH_KNOWLEDGE and SKEP_SUSPEND_JUDGMENT. These sub-codes lack visible relationships of equivalent strength and seem to be isolated or of a minimum relationship. This implies that in the material under analysis, there is no intense framing of professional Skepticism in terms of overreliance on algorithms, refusal of algorithmic decision-making, or the intentional lack of judgment. Rather, the Skepticism discourse seems more constrained and procedural and it mainly deals with the detection of anomalies, the corroboration of evidence and the selective questioning.

In general, the Professional Skepticism matrix identifies three primary conclusions of analysis. To begin with, professional skepticism is manifested in a selective and narrow rather than an inclusive form. Second, the prevailing sceptical reaction is focused on anomaly investigation and corroborative verification, which implies that the Skepticism is primarily aroused by anomalies that have to be verified. Third, less reflective or AI-specific sceptical issues, e.g., automation bias, aversion to algorithms, or suspension of judgement are loosely related in the category. Collectively, these results indicate that, within the examined documents, professional skepticism serves more as a problem-specific control reaction to problematic cues than as a well-developed interpretive system that can be used to assess AI critically in auditing.

AI Governance and Assurance

The code-relations matrix in the category of AI Governance and Assurance has very high density compared to the Audit Risk and Professional Skepticism, which implies that the themes concerning governance constitute a very strong interpretive network. The category has multiple robust clusters of co-occurring themes, as opposed to being organised in terms of isolated pairings. GOV_EXPLAINABILITY and GOV_TRANSPARENCY (511), GOV_Compliance and GOV_POLICY_FRAMEWORK (359), GOV_HUMAN_OVERSIGHT and GOV_OVERSIGHT (280), GOV_FAIRNESS_ETHICS and GOV_POLICY_FRAMEWORK (259) have the strongest visible co-occurrence. These tendencies indicate that in the examined documents, AI governance is built not as one control mechanism but as a multidimensional construct consisting of interpretability, regulatory structure, ethical principles, and human supervision.

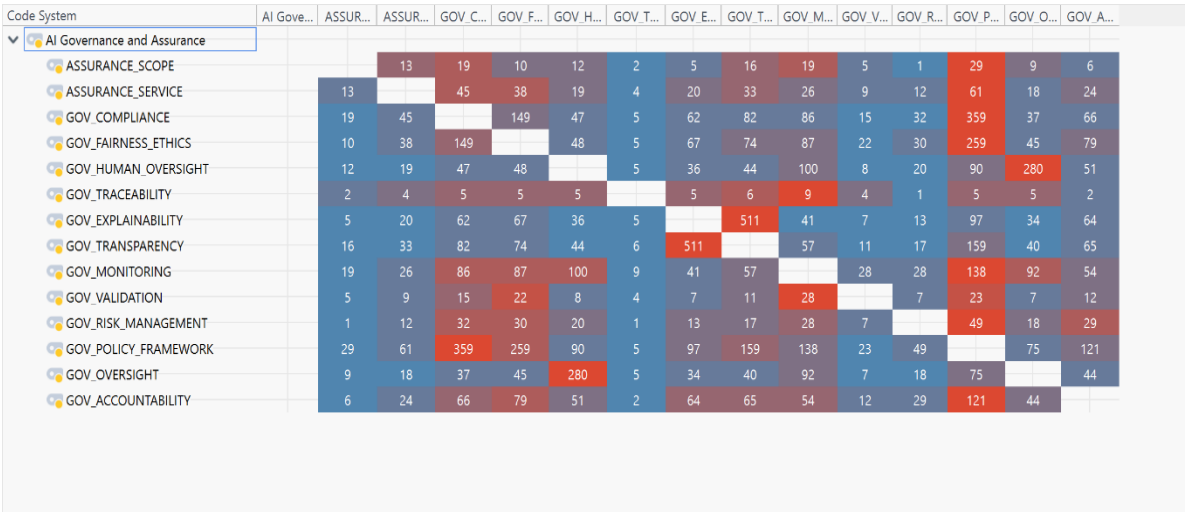


Fig. 10 Code-relations matrix of the AI Governance and Assurance category

The most robust related to explainability and transparency, which means that these two themes are addressed as the conceptual centre of AI governance. This analytic significance is important in that it may imply that the Big Four documents do not perceive transparency as a robust undertaking in its own right; instead, transparency is most significant when it is in the company of explainability. When auditing involves AI, this means that the visibility into the processes or outputs of the system should be accompanied by the possibility to interpret and explain the production of the outputs. Therefore, governance is not presented as the disclosure of technical information only, but as the establishment of circumstances, in which AI can be intelligibly perceived, examined, and trusted.

The second large cluster is that of policy and compliance. The relationship between GOV_COMPLIANCE and GOV_POLICY_FRAMEWORK (359) is the strongest in the whole matrix, and between GOV_FAIRNESS_ETHICS and GOV_POLICY_FRAMEWORK (259) is also a very noticeable one. Besides, GOV_POLICY_FRAMEWORK is co-occurring with GOV_TRANSPARENCY (159), GOV_MONITORING (138), and GOV_ACCOUNTABILITY (121). A combination of these relations indicates that policy frameworks serve as a structural anchor in the discourse of governance. That is, the documents suggest that compliance, fairness, transparency, monitoring, and accountability are not considered as a set of independent governance factors, but they are components of wider organisational and regulatory frameworks, on which the application of AI in audit-related situations is based.

Another powerful cluster of human oversight and operational control is visible in the matrix as well. The most noticeable of these co-occurrences is GOV_HUMAN_OVERSIGHT, GOV_OVERSIGHT (280), followed by GOV_HUMAN_OVERSIGHT and GOV_MONITORING (100) and then GOV_POLICY_FRAMEWORK (90). This tendency shows that the regulation of AI is not viewed solely as an issue of formal policy, but as an issue of continuous human oversight and organisational control. This is of particular importance to auditing since it indicates that AI governance will not become an entirely automated process and that it will still be reviewed by humans to be implemented in the future.

Another interesting trend is the interdependence of compliance, fairness, and monitoring. The GOV_COMPLIANCE and GOV_MONITORING (86), GOV_FAIRNESS_ETHICS and GOV_MONITORING (87), GOV_COMPLIANCE and GOV_TRANSPARENCY (82) demonstrate that the ethical and regulatory aspects are associated not only with the formal rules, but also with the ongoing control. This implies that the governance in the reports under analysis is operational and not declarative. In other words, fairness and compliance seem to need active monitoring and visibility and not just official commitments at the policy level.

Otherwise, certain governance themes are relatively weak. GOV_TRACEABILITY exists, but the co-occurrences are comparatively low throughout the matrix, with the majority falling between 4 and 9. Likewise, GOV_VALIDATION has moderate relationships, with the most obvious observable correlation being with GOV_MONITORING (28) and GOV_POLICY_FRAMEWORK (23). The assurance-related codes, ASSURANCE_SCOPE and ASSURANCE_SERVICE are also not central as compared to the wider governance codes, but ASSURANCE_SERVICE can be seen to have visible relationships with GOV_POLICY_FRAMEWORK (61), GOV_COMPLIANCE (45) and GOV_FAIRNESS_ETHICS (38). This implies that formal assurance is included in the discourse of

governance, although it is not the overriding organising principle. Rather, internal control logic, policy design, oversight, and interpretability are more significant drivers of governance.

Altogether, three key analytical conclusions are indicated in the AI Governance and Assurance matrix. First, the concept of governance is reflected as a highly integrated and structurally central category, far more closely related than the other thematic categories explored to date. Second, governance discussion is constituted by three prevailing pillars such as interpretability (explainability and transparency), regulatory framework (policy frameworks and compliance), and human control (oversight and monitoring). Third, despite the presence of assurance, traceability and validation, they are more of secondary roles to the wider governance architecture. Collectively, all these findings indicate that AI-integrated auditing should be presented as acceptable and manageable only when integrated into a strong system of governance that renders AI explainable, policy-constrained, ethics-driven, and under to continuous human control.

AI / Technology Usage in Auditing

The matrix of code-relations in the AI / Technology Usage in Auditing category has a moderately connected structure which is structured around a clear central cluster instead of relationships which are distributed evenly. The most significant visible co-occurrence is between USE_EASE and USE_USEFULNESS (196), then there are significant co-occurrences between USE_TRUST and USE_INNOVATION_POSITIONING (16), USE_TRUST and USE_USEFULNESS (15), USE_METHOD_INTEGRATION and USE_USEFULNESS (13), and USE-TRUST and USE_PERCEIVED_RISK These patterns indicate that the application of AI in auditing is oriented more towards practical value, usability, trust, and integration of audit work instead of external pressure.

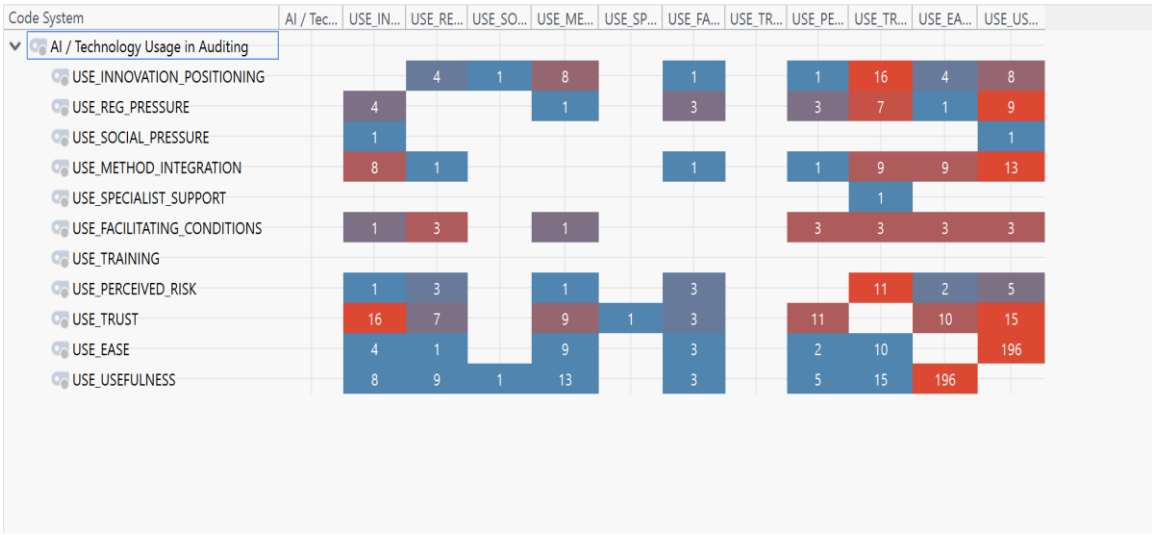


Fig. 11 Code-relations matrix of the AI / Technology Usage in Auditing category

The correlation with the most strong is the linkage of ease of use and usefulness, meaning that usability is the focus of the AI-usage discourse. This analytical significance in that it implies that AI tools are presented as more relevant to auditing when not only functionally advantageous, but also convenient to implement in practice. When applied to auditing, this means that technological value is not talked about in abstract or more innovative terms; usefulness seems more directly related to the

ability of the tools to be integrated into the routine audit operations without undue operational complexity. The matrix thus shows that practical applicability is closely related to adoption.

The second large cluster is focused on trust. USE_TRUST is related to USE_INNOVATION_POSITIONING (16) with the strength of the relationship being one of the highest in the given matrix, and the relationships of USE_TRUST with USE_USEFULNESS (15), USE_PERCEIVED_RISK (11), USE_ease (10), and USE_METHOD_INTEGRATION (9) are also significant. This trend can be interpreted as the trust being a connector concept between the strategic framing of AI, its practical value, and what concerns the usage of AI. Stated differently, the documents that have been analysed suggest that the use of AI in auditing does not hinge on just functionality, but also on whether the auditors or companies consider such tools as reliable enough, usable, and compatible with audit operations. Simultaneously, the presence of trust and perceived risk co-occurrence implies that the concept of trust is being talked about in the very same place where the apprehension about AI is still apparent, which means that the confidence towards AI does not erase the fear of its potential constraints.

The method-integration cluster is also quite evident in the matrix. USE_METHOD_INTEGRATION is a co-occurring factor with USE_USEFULNESS (13), USE_TRUST (9), USE_EASE (9) and USE_INNOVATION_POSITIONING (8). This implies that the application of AI is not merely described as the use of isolated tools, but as the adoption of technological potentials into the current audit procedures. This is of analytical importance since it suggests that AI is framed as a valuable, though not external or supplementary technology when integrated into the audit practice. The apparent connection between method integration and usefulness also facilitates the conclusion that practical audit relevance is conditioned by the extent to which AI can be effectively included in the current audit procedures and judgement processes.

Another interesting trend is related to the regulatory and organisational factors, but it seems not to be core in comparison with the usability and trust cluster. USE_REG_PRESSURE is used together with USE_USEFULNESS (9), USE_TRUST (7), USE_INNOVATION_POSITIONING (4), and USE_FACILITATING_CONDITIONS (3). These connections imply that regulatory pressure exists as a situational force, although it does not take over the adoption discourse. Rather, it seems to be working together with strategic positioning and perceived value. On the same note, USE_FACILITATING_CONDITIONS demonstrates a number of low-level relationships, most of them at the frequency of 3, which implies that enabling organisational conditions are recognised but not the primary organising principle of the category.

In comparison, some of the sub-codes are relatively weak or remote. USE_SOCIAL_PRESSURE and USE_SPECIALIST_SUPPORT only have weak visible relationships, whereas USE_SOCIAL_PRESSURE and USE_SPECIALIST_SUPPORT have weak relationships. Most conspicuously, the USE_TRAINING does not establish any intensive noticeable co-occurrence cluster in the table. This implies that there is no strong framing of the use of technology in the analysed documents based on peer influence, structured training, and huge dependence on specialists. Rather, perceived usefulness, ease of use, trust, and integration into audit methods have a stronger influence on the discourse. This trend can be a sign that the use of AI is being introduced as a more normalised aspect of the audit practice, rather than a special ability that needs a great deal of social validation or focus on training.

All in all, the AI / Technology Usage in Auditing matrix leads to three general analytical findings. First, the category is characterized by strong usability-value core, where ease of use and usefulness are the foundational components of the adoption of AI. Second, a connecting role is played by trust which connects innovation positioning, method integration, usefulness, and perceived risk. Third, regulatory pressure and enabling conditions exist, but they are less crucial than the practical and perceptual aspects of AI application. Combined, these results indicate that the adoption of AI in auditing is being cast as an issue of operational utility, usability, and trust in the application of technology in audit practices, as opposed to a reaction to social or training pressure or external compliance pressures.

Audit Benefits

The code-relations matrix of the category Audit Benefits indicates a rather tight and well-organized network of relationships. As compared to the denser matrices of AI Governance and Assurance and AI / Technology Usage in Auditing, the benefits category has a narrower scope, but a few visible and meaningful co-occurrences. The highest visible relationship is between OUT_AUDIT_QUALITY and OUT_RISK_ASSESSMENT (24) then between OUT_AUDIT_QUALITY and OUT_DOCUMENTATION (14) and between OUT_AUDIT_QUALITY and both OUT_EVIDENCE_QUALITY (9) and OUT_EFFICIENCY (9). These trends indicate that the benefits that AI has brought to the field of auditing are structured around better audit quality, with the other benefit dimensions being associated with the core outcome.

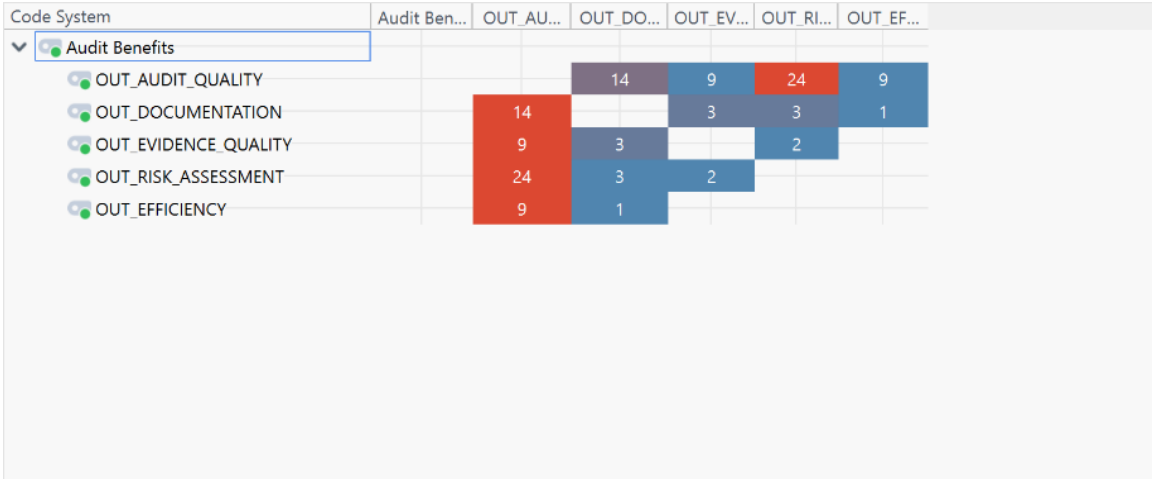


Fig. 12 Code-relations matrix of the Audit Benefits category

The highest dependency, between audit quality and risk assessment, shows that the perceived value of AI is best related to the increase of the ability of the auditors to identify, assess and respond to the risk. This is analytically significant since it implies that the advantages of AI are not being presented as benefits of speed and automation per se, but as benefits of enhancing the quality of audit judgement through improved risk-oriented analysis. This means that enhanced risk assessment is viewed as a fundamental mechanism where AI can be used to enhance the quality of the overall audit in the context of auditing.

A second interesting cluster is the focus on audit quality and documentation. The correlation between OUT_AUDIT_QUALITY and OUT_DOCUMENTATION (14) implies that documentation is

regarded as the significant supportive dimension of quality improvement. It could be a sign that AI is viewed as helpful not only due to its ability to assist auditors in identifying and evaluating problems more efficiently, but also due to the possible enhancement of the consistency, traceability, or completeness of the audit documentation. This analytical relationship is important in that it is a relationship between the perceived performance value of AI and one of the defining procedural aspects of audit work.

It is also indicated in the matrix that the quality of evidence and efficiency are also associated with audit quality, albeit at a moderate level. The co-occurrence of OUT_AUDIT_QUALITY and OUT_EVIDENCEQUALITY (9) and the co-occurrence of OUT_AUDIT_QUALITY and OUT_EFFICENCY (9) indicate that both of the dimensions are used in the discourse of benefits, but neither seems to be in the middle of focus as risk assessment or documentation. This tendency suggests that the documents are not immune to the efficiency gains and evidence-related improvements being addressed as components of the value proposition of AI; though, these are viewed as the supporting benefits rather than as the primary result. That is, AI does not seem to be valued merely due to the fact that it allows making the auditing process faster, but it is related to high-quality audit processes and final products.

In comparison, the connections between the secondary benefit dimensions themselves are not very strong. OUT_DOCUMENTATION is only modestly co-occurring with OUT_EVIDENCE_QUALITY (3) and OUT_RISK_ASSESSMENT (3), whereas OUT_EVIDENCE_QUALITY and OUT_RISK_ASSESSMENT co-occur at a low level (2). Out documentation and out efficacy have a specific restriction, especially without documentation (1). This shows that the category of benefits does not have a loose and closely knit internal structure. Instead, the benefits are grouped around a central anchor, that is, audit quality of which the other good outcomes are linked. Therefore, the matrix indicates that the discourse does not show various benefit dimensions, which have the same weight, but it forms audit quality as the key integrative benefit of AI use in auditing.

In general, the Audit Benefits matrix suggests three primary analytical conclusions. To begin with, the category has a high focus on the quality of the audit as the prevailing product of the use of AI. Second, the greatest benefit that accompanies it is enhanced risk assessment, and the second and third benefits are enhanced documentation, with the quality of evidence and efficiency being present but secondary. Third, the discourse of benefits seems to be comparatively narrow and hierarchical and not widely spread to numerous equally strong themes. Combined, these results indicate that the analysed documents perceive the advantages of AI in the auditing process mainly through the lens of its role in making the audit work more effective, risk-focused, and better-documented, but not only through the prism of efficiency advantages.

4.4.2. Cross-category relations

Audit Risk × AI/Technology Usage

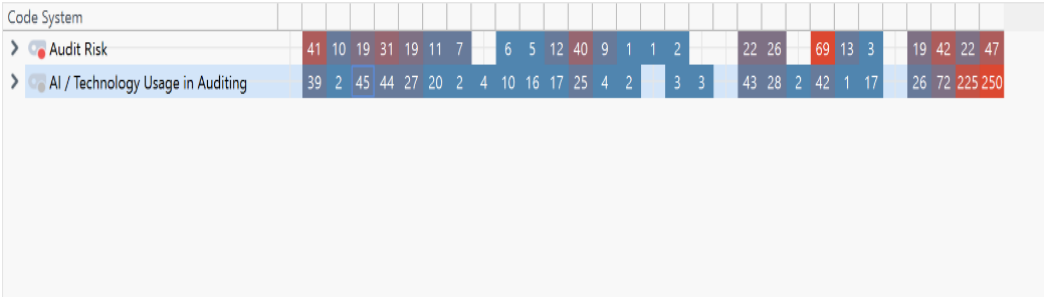


Fig. 13 Cross-Category Relations between Audit Risk and AI/Technology Usage

There are a few high-frequency co-occurrences in the cross-category count between audit risk and AI usage (e.g. counts >200). . The biggest overlaps are found between detection-risk codes and adoption drivers that relate to ease of use, usefulness and integration of methods. These figures suggest that big 4 reports, when they talk about using AI analytics, do so at the same time underlining the ease of use and usefulness of the tools in risk assessment. In the same vein, inherent-risk codes, specifically those related to estimation and revenue recognition, are often used together with USE_Trust and USE_Training, which points to trust and capacity-building as being modeled as enabling to deal with complex risks. These cross-relationships imply that the adoption of AI is not a technological activity but a direct answer to the risk issues.

Audit Risk × AI Governance and Assurance

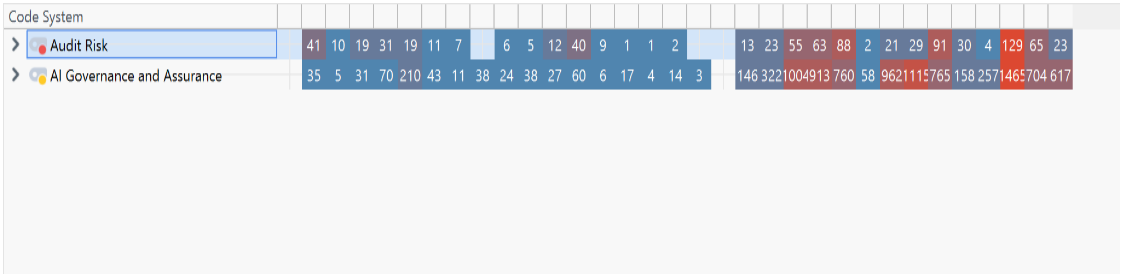


Fig. 14 Cross-Category Relations between Audit Risk and AI Governance & Assurance

Among the cross-category matrices, Audit Risk shows its highest raw co-occurrence with AI Governance and Assurance. The matrix contains several very large intersection counts, with some cells exceeding 900 and one reaching 1 465. These large values are associated in particular with links between control-risk codes and governance subcodes such as GOV_TRANSPARENCY, GOV_EXPLAINABILITY, GOV_TRACEABILITY, GOV_FAIRNESS_ETHICS, and GOV_POLICY_FRAMEWORK. However, these results should be interpreted cautiously, because AI Governance and Assurance is also the largest category overall in the corpus. Accordingly, the matrix does not suggest that Audit Risk is a dominant theme in Big Four disclosures; rather, it indicates that when AI-related audit risk is discussed, it is most often framed through governance, oversight, accountability, and assurance-related language. In the sampled materials, Big Four firms frequently associate AI-related risk reduction with policy frameworks, compliance structures, fairness principles, and ongoing control mechanisms. The observed co-occurrences therefore suggest a strong thematic overlap between audit-risk concerns and governance-oriented responses, rather than evidence that Audit Risk itself occupies a leading position in the overall corpus.

Audit Risk × Professional Skepticism

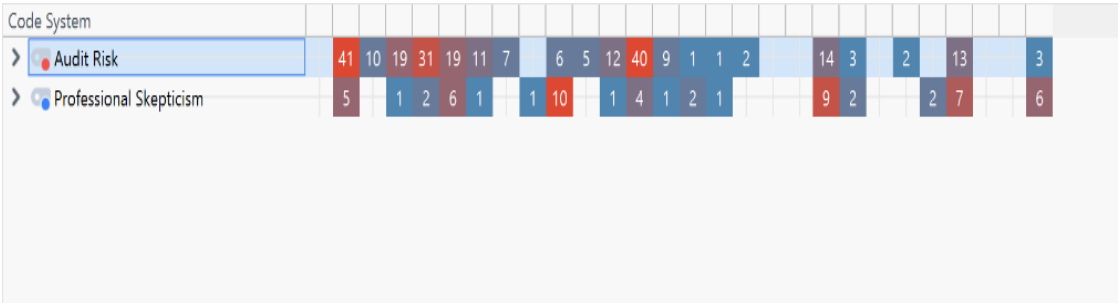


Fig. 15 Cross-Category Relations between Audit Risk and Professional Skepticism

There are moderate but informative cross-relations between audit risk and professional Skepticism. Numbers of co-occurrence are between 1 and 10. The strongest associations were found between DR_PROCEDURES and DR_SPECIALISTS and SKEP_PROF_JUDGMENT and SKEP_MANAGE_CHALLENGE. These connections show that, when companies speak about procedural protection and expert participation, they also focus on the fact that auditors are to practice professional judgment and confront management statements. Nonetheless, most inherent-risk codes do not co-occur with Skepticism codes, indicating that the discourse of AI model risk and bias is not always connected to sceptical behaviours. This loophole indicates that future audit directions might focus on strengthening the need to be sceptical with AI outputs.

AI Governance and Assurance × Professional Skepticism

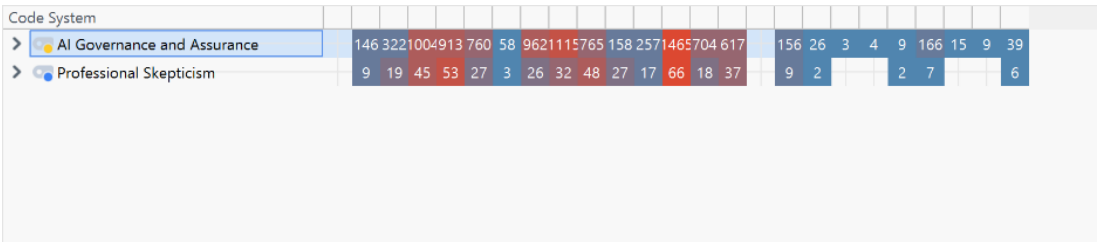


Fig. 16 Cross-Category Relations between AI Governance and Professional Skepticism

The cross-category table of governance vs Skepticism indicates that some of the governance themes-especially fairness and ethics, accountability and human control, co-occur with Skepticism behaviours in moderate counts (about 45-66 counts). These intersections imply that professional Skepticism is understood to be an inherent part of AI governance, particularly within the ethical considerations and supervision. However, the quality of such relationships is not high in comparison with the connection between governance and risk, which means that the discourse of governance remains more concerned with structural than with the mindsets of auditors.

AI Governance and Assurance × Audit Benefits

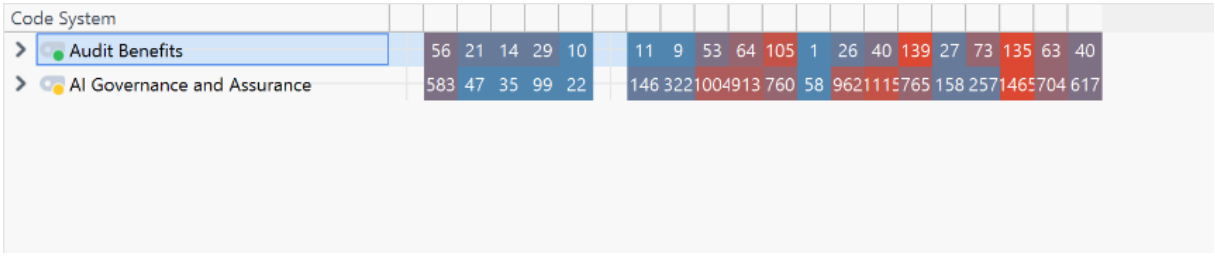


Fig. 17 Cross Category Relations between AI Governance & Assurance and Audit Benefits

There are also significant interrelations between audit advantages and AI governance. The risk assessment, audit quality and documentation benefits relate 105-139 times with the following governance themes: transparency, explainability and risk management. This trend shows that organisations not only conceptualise governance as a risk-reduction mechanism, but also as a source of better audit results. Indicatively, transparency and explainability are described as facilitating the improvement of documentation and audit quality, whereas risk-management frameworks help to conduct stricter risk assessments. This observation confirms the idea that effective AI governance can generate value beyond compliance.

AI/Technology Usage × Audit Benefits

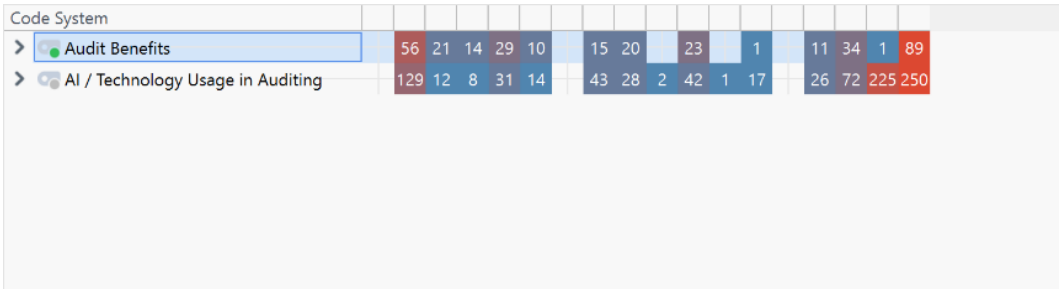


Fig. 18 Cross Category Relations between Audit and AI/Technology Usage

There are clear and meaningful cross-relations between AI / Technology Usage in Auditing and Audit Benefits. The strongest visible associations are found between Audit Benefits and USE_USEFULNESS (89), followed by USE_TRUST (34) and USE_METHOD_INTEGRATION (23). From the opposite direction, AI / Technology Usage in Auditing is linked most strongly with OUT_AUDIT_QUALITY (129), followed by OUT_RISK_ASSESSMENT (31), OUT_EFFICIENCY (14), OUT_DOCUMENTATION (12), and OUT_EVIDENCE_QUALITY (8). These connections show that companies discuss AI benefits mainly when AI tools are seen as useful, trustworthy, and compatible with audit methods. The pattern also suggests that AI is valued less for efficiency alone and more for its contribution to audit quality and risk assessment. Therefore, the adoption of AI in auditing appears to be justified primarily through its practical benefits for audit performance.

4.5. Synthesis of Empirical Findings in Relation to Prior Research

The empirical results of this thesis demonstrate a consistent ranking of Big Four public reporting about AI in auditing. AI Governance and Assurance is the most prominent theme, but AI / Technology Usage in Auditing and Audit Benefits are secondary themes, Audit Risk is a minor theme, and Professional Skepticism is only marginally present. This trend holds for most firms and indicates that, at the level of public discourse, Big Four firms do not position AI primarily in terms of being a productivity tool or an innovation in itself. Instead, when the topic is clients using risky AI in their financial reporting, AI is publicly framed primarily as a governance, control, accountability, monitoring and assurance-readiness object. The comparison below is interpretive, not symmetrical, because this thesis considers public Big Four disclosures while COSO offers normative guidance on governance, Kokina et al. (2025) provide evidence from audit practitioners, and Commerford et al. (2022) examine auditor behavior experimentally.

The strongest alignment is with COSO. At the enterprise level, COSO's 2021 guidance highlights that AI is first and foremost an enterprise risk management (ERM) and governance issue, and insists on integrated governance, risk management, and performance across the five ERM components, rather than a technical issue. At the more operational level, COSO's 2026 guidance applies this to internal-control design for generative AI by identifying risks such as hallucinations, prompt injection, lack of information about how the system works, model drift, and frequent configuration changes, and translates them into audit-ready control mapping, traceability, monitoring, and reliance-based control measures. Specifically relevant for this thesis, the 2026 publication is aimed not only at risk and control practitioners, but also controllers, financial reporting teams, internal audit and external audit of GenAI control practices. In terms of audits of clients with high-risk AI systems in financial reporting this makes COSO a good fit: the results of this thesis similarly suggest that AI is publicly legitimated primarily in cases where it is integrated into governance arrangements that support reliability, accountability and assurance. That said, this agreement should not be overemphasized. The Big Four corpus examined in this thesis is public, and not engagement or internal documents. As such, the current results indicate high consistency with the governance direction of previous research, but not evidence of full standardisation. (COSO, 2021; COSO, 2026).

The second place of prominence of AI / Technology Usage in Auditing and Audit Benefits offers a nuance here. AI is publicly described as beneficial in the empirical data when it helps achieve typical audit goals related to risk management, documentation and evidence management rather than when it is described as substituting audit judgment. This is broadly in line with Kokina et al. (2025), who report that simpler AI applications are already in widespread use in large public accounting firms while more advanced AI applications are still in development. Their empirical evidence is valuable for explaining the predominance of governance vocabulary in public communication. If basic applications are being produced and more complex uses are not, then public discourse is likely to focus on managed integration, explainability and governance rather than the transformative promises of autonomous auditing. In this regard, the current findings should not be read as an indication that the profession has overcome the practical difficulties of AI auditing. Instead, they indicate that governance is the public language that firms are now using to make AI appear manageable, safe and audit-friendly. This is an important point for a thesis on high-risk AI in financial reporting, because the latter requires that the public accept oversight even when underlying methodological problems have not been resolved. (Kokina et al., 2025).

This also presents a negative contrast. While the thesis focuses on auditing clients that use high-risk AI systems, Audit Risk is not the explicit category that is the most common in the public discourse. Rather, risk is subsumed under references to governance, controls, transparency and assurance readiness. This doesn't mean that risk isn't important. On the contrary, it implies that Big Four firms use more indirect phrases, such as controls, governance, and oversight, to describe the challenges of auditing AI, rather than the public articulation of audit risks of material misstatement (and audit responses) in relation to the material use of AI for accounting estimates, transaction classification, disclosures, or internal reporting. This rhetorical approach is not surprising for public documents. But for the audit of risky AI in financial reporting, it is a constraint: governance is brought to the surface, but how governance concerns translate into audit responses at the engagement level is less clear. The bad news is therefore not a lack of concern, but the relative lack of specificity in translating public governance concerns to audit procedures, evidence and risk responses when clients' use of AI systems impacts financial reporting in potentially material ways. This interpretation also aligns with Kokina et al. (2025), whose findings show that more complex AI applications are hard to audit directly and that companies are still somewhat cautious about their status as an audit object. (Kokina et al., 2025; COSO, 2026).

The weakest empirical category, Professional Skepticism, is best understood in the context of Commerford et al. (2022). They demonstrate that if contradictory evidence is presented by an AI system rather than a human expert, auditors are more likely to suggest smaller revisions to management's complex estimates, particularly when the inputs to management's estimates are relatively objective. This matters for the current thesis in that it suggests auditor reactions to AI-generated (or even AI-moderated) evidence is behaviorally dependent on source credibility and objectivity. In other words, professional skepticism remains relevant in the audit context when using AI, but it becomes more challenging and more complex. In this context, the scant explicit mention of skepticism in Big Four documents should not be regarded as a professional irrelevance. It is more likely a characteristic of public communication. Public documents are more comfortable with language of governance, oversight, transparency, control, and assurance, than with language of skeptical challenge, avoidance of overreliance, trust setting and dealing with conflicting machine-generated evidence. This is a second notable negative result: language of governance assurance is well developed while language of challenge is not, even though previous auditing research indicates that it remains highly relevant. In audits of high-risk AI-based estimates and disclosures in financial reporting, this makes a big difference because the reliability of AI-based estimates and disclosures depends not only on the quality of governance arrangements, but also on the skeptically challenging attitude of the auditor toward outputs that might appear systematic, objective, or technically impressive. (Commerford et al., 2022).

Overall, the results support a socio-technical model of AI in auditing. The Big Four's public reporting does not legitimate AI based on technology. Rather, it legitimates AI when technological utility is combined with governance, human oversight, control, and assurance-readiness. This finding is in line with COSO's governance perspective, and Kokina et al.'s evidence that implementation issues are significant. Simultaneously, however, the study also highlights a mismatch between public discourse and the complexity highlighted in previous studies. The public narrative is more governance-focused, more control-focused, and less procedurally specific about how audit risk assessment, evidence evaluation, and sceptical challenge at the engagement level change in response to high-risk AI. This is an important finding for a thesis on auditing the financial reporting of clients that use high-risk AI.

It suggests the public discourse is best suited where AI can be discussed as a matter of governance, accountability and readiness for assurance, but less so where the discussion would require more specific articulation of the implications for auditors of how they challenge, test, and rely on AI-influenced financial reporting processes. (COSO, 2021; COSO, 2026; Kokina et al., 2025; Commerford et al., 2022).

These findings also suggest some lines for future research. One might be to compare Big Four annual reports with proprietary methodologies or interview evidence to investigate whether the governance-focused external communication mirrors internal practice. A second would be to directly study professional skepticism in AI-assisted audits, particularly to the extent that auditors need to evaluate AI-based estimates, classification decisions, or narrative disclosures that technically seem plausible. A third would be to examine particular risky applications of AI in financial reporting, such as AI-supported accounting estimates or GenAI-assisted financial disclosure drafting, to better understand how governance standards are interpreted in audit procedures and evidence gathering. A fourth would be to compare Big Four statements with those of regulators, other firms, or engagement-level audit practitioners to determine whether the current focus on governance and assurance readiness is representative of the profession as a whole or primarily a public reporting strategy. These avenues follow from the current findings, as the thesis identifies both where public discourse is already relatively advanced, and where there are still significant interpretive and procedural gaps.

Conclusions and Recommendations

1. **Mapping high-risk AI characteristics to audit risk.** The thesis maps the salient characteristics of high-risk AI systems (model opacity, algorithmic bias, data quality limitations, overreliance and automation bias, adaptive model behaviour and accountability gaps) in the three components of audit risk model. These features can increase inherent risk when AI systems influence accounting estimates, transaction classification or narrative disclosures. They can increase control risk when AI-supported processes weaken segregation of duties, change-management controls, monitoring controls, or accountability mechanisms. They can increase the risk of detection if the audit team blindly trusts and accepts AI outputs without a proper understanding of the models and data used. The Big Four's public reporting indicates that auditors should not consider AI-related financial reporting risks to be the same as a general technology risk but should treat them as a specific audit-related risk.

2. **Integrating audit risk, professional skepticism and AI governance frameworks.** An integrated theoretical framework has been developed which combining the Audit risk model, professional skepticism and AI governance/assurance frameworks. The audit risk model was used to identify the risks of misstatements arising from the characteristics of AI; professional skepticism highlighted the auditor's critical evaluation of AI -generated evidence and management representations; and AI governance frameworks were used to evaluate the control adequacy, control accountability, monitoring, and assurance readiness. The integrated framework enabled the thesis to examine the relationship between the public discourse of AI governance concerns and audit risk assessment and to demonstrate a need for skeptical vigilance on the part of the auditor when evaluating AI-related evidence.

3. **Directed content analysis of Big Four public documents.** The empirical part of the thesis designed and conducted a directed content analysis on a corpus of publicly available Big Four documents published between 2023 and 2025. The documents were organised through a corpus table and analysed using a codebook. AI Governance and Assurance is the dominant category in the analysed corpus in the public reports of the Big Four, with particular focus on control frameworks, accountability, monitoring and preparedness for assurance. There are traces of AI/technology application in auditing and audit benefits but these are secondary. The discussion of audit risk is more present, but not as strong, and expression or articulations of professional skepticism are the least prominent. The results suggest that in the discourse of the ‘Big Four’, the conversation about AI is largely concerned with governance and control rather than overt Skepticism.

4. **Cross-firm communication themes and implications for audit planning.** The cross-firm comparison showed comparisons across the Big Four were broadly similar. Every firm identifies AI governance and assurance themes as priorities, while none offer specific advice on how to incorporate engagement-level risk assessment, control testing or substantive procedures with regard to high-risk AI systems. Auditors might also be expected to convert the high-level governance discussion into specific audit planning considerations, including the identification of assertions affected by AI, the evaluation of the design and operating effectiveness of AI-related controls, the engagement of specialists to assess model risk and data integrity, and documentation of the application of professional skepticism to AI outputs. The message is that public communications are currently more about governance and

assurance readiness, instead of explicitly offering guidance on how to incorporate considerations of high-risk AI into audit execution.

Based on these conclusions, the following recommendations are proposed:

1. **Develop AI-specific audit guidance** Standard-setters and professional bodies should provide more explicit guidance on how to audit financial reporting in the environment of high-risk AI systems. This guidance should outline the impact of characteristics related to AI on inherent risk, control risk and detection risk and provide examples of risk assessment, control and substantive procedures that are specific to AI affected processes.

2. **Strengthen professional skepticism in AI contexts.** Big Four firms and other major audit organisations should strengthen the explicit articulation of professional Skepticism in their public AI-related guidance and audit communication. Since professional Skepticism represented the weakest theme in the analysed corpus, firms should more clearly signal the need for auditors to critically evaluate AI system outputs, challenge management assumptions embedded in AI-driven financial reporting, and recognise the limitations of AI-generated audit evidence.

3. **Link governance language to engagement-level audit procedures.** Big Four firms should translate high-level AI governance and assurance language into concrete engagement-level audit procedures. This includes identifying AI-related key controls, designing tests of those controls, involving multidisciplinary specialists in model evaluation where necessary, and documenting how AI governance considerations informed the audit strategy

4. **Enhance multidisciplinary auditor competence.** Audit teams working with clients that deploy high-risk AI systems should be equipped with competence beyond traditional financial accounting expertise. Firms should invest in structured training on AI system architecture, algorithmic risk assessment, data governance, model documentation, and AI-related control evaluation so that auditors can apply informed professional Skepticism rather than relying only on management explanations or third-party assurance reports.

5. **Improve client-side AI documentation and auditability.** Organisations using high-risk AI systems in financial reporting should maintain clear documentation of AI model design, data sources, validation procedures, monitoring activities, access controls and human review responsibilities. Such documentation would support auditability by helping auditors understand how AI-generated outputs are produced, controlled and reviewed. It would also help reduce accountability gaps and improve the quality of audit evidence in AI-intensive reporting environments.

6. **Encourage further empirical research on AI audit practice.** Future research should go beyond public reports and examine how auditors actually respond to high-risk AI systems in practice. Interviews with auditors, regulators, AI specialists and audit methodology teams could help explain whether the governance-oriented public discourse identified in this thesis is consistent with real engagement-level audit procedures. Further studies could also compare Big Four disclosures with mid-tier audit firms or examine how AI-related audit guidance develops after the implementation of the EU AI Act.

This thesis therefore concludes that high-risk AI systems create specific audit risk, governance and professional skepticism challenges in financial reporting. While the Big Four publicly recognise the importance of AI governance and assurance, their public communication provides limited detail on how auditors should operationalise these concerns in concrete audit procedures. The main contribution of this thesis is to show that the audit profession needs to move from broad AI governance discourse towards more explicit, engagement-level guidance for assessing and auditing high-risk AI systems.

List of references

1. Abadi, A., & Berrada, M. (2018). Peeking inside the black-box: A survey on explainable artificial intelligence (XAI). *IEEE Access, 6*, 52138–52160. https://doi.org/10.1109/ACCESS.2018.2870052
2. Abiyyu, A. D., & Mustafida, N. (2024). Auditors' perceptions of artificial intelligence, institutional pressure, and auditor personality on audit quality. *Infestasi: Jurnal Akuntansi dan Keuangan, 20*(2). https://doi.org/10.21107/infestasi.v20i2.27849
3. Abu-Shakra, E. (2025, April 9). *EY announces large-scale integration of leading-edge AI technology into global assurance technology platform.* EY. https://www.ey.com/en_gl/newsroom/2025/04/ey-announces-large-scale-integration-of-leading-edge-ai-technology-into-global-assurance-technology-platform
4. Adeoye, I. O., Akintoye, R. I., Agugom, T. A., & Olagunju, O. A. (2023). Artificial intelligence and audit quality: Implications for practicing accountants. *Asian Economic and Financial Review*, *13*(11). https://doi.org/10.55493/5002.v13i11.4861
5. Afsay, A., Tahriri, A., & Rezaee, Z. (2023). A meta-analysis of factors affecting acceptance of information technology in auditing. *International Journal of Accounting Information Systems, 49*, 100608. https://doi.org/10.1016/j.accinf.2022.100608
6. Al-Ateeq, B., Sawan, N., Al-Hajaya, K., Altarawneh, M., & Al-Makhadmeh, A. (2022). Big data analytics in auditing and the consequences for audit quality: A study using the technology acceptance model (TAM). *Corporate Governance and Organizational Behavior Review, 6*(1), 64–78. https://doi.org/10.22495/cgobrv6i1p5
7. Ali, I. (2024). *AI transparency and explainability* [Conference paper]. Seminar Talk, Frankfurt University of Applied Sciences. ResearchGate. https://www.researchgate.net/publication/386416207_AI_Transparency_and_Explainability
8. Aliferis, C. (2024). Overfitting, underfitting and general model overconfidence and under-performance pitfalls and best practices in machine learning and AI. *In Artificial intelligence and machine learning in health care and medical sciences* (pp. 477-522). Springer. https://www.ncbi.nlm.nih.gov/books/NBK610560/
9. Al-Mawali, H., Allozi, Y., Nawaiseh, A., Zaidan, H., Al Natour, A. R., & Alshurideh, M. (2025). AI-based audit acceptance and auditors' technology readiness. *International Journal of Data and Network Science, 9,* 525–540. https://doi.org/10.5267/j.ijdns.2024.8.013
10. Anwar, A., & Akeel, M. O. (2026). Integrating artificial intelligence in audit workflow: Opportunities, architecture, and challenges: A systematic review. *Preprints*. DOI:10.20944/preprints202601.2060.v1
11. Assarroudi, A., Heshmati Nabavi, F., Armat, M. R., Ebadi, A., & Vaismoradi, M. (2018). Directed qualitative content analysis: The description and elaboration of its underpinning methods and data analysis process. *Journal of Research in Nursing*, *23*(1), 42–55. https://doi.org/10.1177/1744987117741667.
12. Bahangulu, J. K. (2025). Algorithmic bias, data ethics, and governance: Ensuring fairness, transparency and compliance in AI-powered business analytics applications. *World Journal of Advanced Research and Review, 25*(2), 571–583. https://doi.org/10.30574/wjarr.2025.25.2.0571

13. Bin-Nashwan, S. A., Li, J. Z., Jiang, H., Jiang, H., Bajary, A. R., & Ma'aji, M. M. (2025). Does AI adoption redefine financial reporting accuracy, auditing efficiency, and information asymmetry? An integrated model of TOE-TAM-RDT and big data governance. *Computers in Human Behavior Reports*, *17*, 100572. https://doi.org/10.1016/j.chbr.2024.100572
14. Center for Audit Quality. (2025, August 11). *Auditors and artificial intelligence in the new era of auditing.* The CAQ. https://www.thecaq.org/aia-auditors-and-ai-in-the-new-era-of-audit
15. Chaker, I. (2024).Man & machine: Artificial intelligence's role in shaping auditors' professional skepticism. *Journal of Modern Accounting and Auditing*, *20*(4), 171–181. https://doi.org/10.17265/1548-6583/2024.04.002
16. Chun, W. (2026, February 4). *The revenue recognition principle: ASC 606, IFRS 15 & AI.* DualEntry. https://www.dualentry.com/blog/the-revenue-recognition-principle
17. Commerford, B. P., Dennis, S. A., Joe, J. R., & Ulla, J. W. (2022). Man versus machine: Complex estimates and auditor reliance on artificial intelligence. *Journal of Accounting Research*, *60*(1), 171–201. https://doi.org/10.1111/1475-679X.12407
18. Davarzani, H. (2025). Artificial intelligence and the transformation of financial reporting. *International Journal of Scientific Research and Management*, *13*(09), 9764–9769. DOI: 10.18535/ijsrm/v13i09.em12
19. Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, *13*(3), 319–340. https://www.jstor.org/stable/249008
20. De Jongh, R. (2017). A proposed best practice model validation framework for banks. *South African Journal of Economic and Management Sciences, 20*(1), Article 1490. https://doi.org/10.4102/sajems.v20i1.1490
21. Deniswara, K., Henky, T., Mulyawan, A. N., Armand, W. K., & Mustapha, M. (2023). The role of external auditor in the adoption of Computer-Assisted Audit Techniques with unified theory of acceptance and use of technology: An empirical study in public audit firms in Jakarta. *The Winners*, *24*(1), 1–11. https://doi.org/10.21512/tw.v24i1.8124
22. DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American Sociological Review*, *48*(2), 147–160. https://doi.org/10.2307/2095101
23. Elo, S., & Kyngäs, H. (2008). The qualitative content analysis process. *Journal of Advanced Nursing, 62*(1), 107–115. https://doi.org/10.1111/j.1365-2648.2007.04569.x.
24. Farley, E. A., & Lansang, C. R. (2025). AI auditing: First steps towards the effective regulation of artificial intelligence systems. *Harvard Journal of Law & Technology Digest*, *38*, 1-41. https://jolt.law.harvard.edu/assets/digestImages/Farley-Lansang-AI-Auditing-publication-2.13.2025.pdf
25. Fedyk, A. (2022). Is artificial intelligence improving the audit process? *Review of Accounting Studies, 27*, 938–985. https://doi.org/10.1007/s11142-022-09697-x
26. Fidyah, F. (2024). The impact of artificial intelligence on auditing processes and accuracy: A future outlook. *Digital Journal of Emerging Fields in Accounting*, 5(4), 4350-4358. https://doi.org/10.38035/dijefa.v5i4.3224

27. Gryz, J. (2021). Black box algorithms and the rights of individuals: No easy solution to the "explainability" problem. *Computer Law & Security Review, 41*, 105539. https://doi.org/10.14763/2021.2.1564
28. Hardies, K.., Dierckx, M.., Commerford, B.., & Jans, M. (2026). *When do auditors rely on (bad) AI advice?* Foundation for Auditing Research. https://foundationforauditingresearch.org/publications/when-do-auditors-rely-on-bad-ai-advice/
29. Hemati, H., Schreyer, M., & Borth, D. (2021). Continual learning for unsupervised anomaly detection in continuous auditing of financial accounting data. *arXiv*. https://doi.org/10.48550/arXiv.2112.13215
30. Hsieh, H.-F., & Shannon, S. E. (2005). Three approaches to qualitative content analysis. *Qualitative Health Research, 15*(9), 1277–1288. https://doi.org/10.1177/1049732305276687.
31. Hurtt, R. K., Brown-Liburd, H., Earley, C. E., & Krishnamoorthy, G. (2013). Research on auditor professional skepticism: Literature synthesis and opportunities for future research. *Auditing: A Journal of Practice & Theory*, 32(Supplement 1), 45–97. https://research.ebsco.com/c/7a7sn3/viewer/pdf/wncp5aahrv?route=details
32. Jackson, R. J.. (2025, July 28). How auditors harness responsible AI to identify trends and sharpen focus on risk. *Center for Audit Quality*. https://www.thecaq.org/aia-auditors-harness-responsible-ai
33. Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal of Financial Economics*, 3(4), 305–360. https://josephmahoney.web.illinois.edu/BA549_Fall%202012/Session%205/5_Jensen_Meckling%20(1976).pdf
34. Johri, A., Sayal, A., Chong, K. M., Khoja, M., N, C., Jha, J., & Tyagi, N. (2026). Enhancing audit quality and reducing costs: The impact of AI in banking and financial services. *Frontiers in Artificial Intelligence, 8*, Article 1718854. https://doi.org/10.3389/frai.2025.1718854
35. Khemka, A. (2025). Automated revenue recognition using AI-driven reconciliation agents: Case study on AI's role in ASC 606 compliance. *International Journal of Research in Management, Economics and Emerging Technology, 13*(4), Article 15. https://doi.org/10.63345/ijrmeet.org.v13.i4.15
36. Koç, D. (2024). A machine learning and deep learning-based account code classification model for sustainable accounting practices. *Sustainability*, *16*(20), 8866. https://doi.org/10.3390/su16208866
37. Kokina, J., & Davenport, T. H. (2017).The emergence of artificial intelligence: How automation is changing auditing.*Journal of Emerging Technologies in Accounting*, *14*(1), 115–122. https://doi.org/10.2308/jeta-51730
38. Kokina, J., Blanchette, S., Davenport, T. H., & Pachamanova, D. (2025). Challenges and opportunities for artificial intelligence in auditing: Evidence from the field. *International Journal of Accounting Information Systems*, 56, 100734. https://doi.org/10.1016/j.accinf.2025.100734
39. KPMG. (2025, September 25). *KPMG expands AI Trust services with new AI Assurance capabilities.* https://kpmg.com/us/en/media/news/kpmg-expands-ai-trust-services-with-new-ai-assurance-capabilities.html

40. Krippendorff, K. (2018). *Content analysis: An introduction to its methodology* (4th ed.). SAGE Publications https://books.google.lt/books?id=nE1aDwAAQBAJ&lpg=PP1&ots=y_emYuiPdz&dq=41.%20Krippendorff%2C%20K.%20(2018).%20Content%20analysis%3A%20An%20introduction%20to%20its%20methodology%20(4th%20ed.).%20SAGE%20Publications&lr&hl=fr&pg=PR8#v=onepage&q&f=false
41. Louis, J. F. (2025, August 11). Artificial intelligence in auditing: Leveraging benefits and avoiding risk. *Becker Professional Education*. https://www.becker.com/blog/cpe/ai-in-auditing
42. Manogo, C. (2025). AI ethics in business applications: Bias, transparency, and accountability practices. *Zenodo*. https://doi.org/10.5281/zenodo.17372564
43. Mökander, J., Axente, M., Casolari, F., & Floridi, L. (2021). Ethics-based auditing of automated decision-making systems *Science and Engineering Ethics, 27*(4), 44. https://doi.org/10.1007/s11948-021-00319-4
44. Mökander Genovesi, S. (2025). Introducing an AI governance framework in financial organizations: Best practices in implementing the EU AI Act (Practitioner Track). In R. Görge, E. Haedecke, M. Poretschkin, & A. Schmitz (Eds.), *Symposium on Scaling AI Assessments (SAIA 2024)* (Open Access Series in Informatics [OASIcs], Vol. 126, Article 9, pp. 9:1–9:7). Schloss Dagstuhl – Leibniz-Zentrum für Informatik. https://doi.org/10.4230/OASIcs.SAIA.2024.9
45. Murikah, W., Nthenge, J. K., & Musyoka, F. M. (2024). Bias and ethics of AI systems applied in auditing: A systematic review. *Scientific African*, *25*, e02281. https://doi.org/10.1016/j.sciaf.2024.e02281
46. Nelson, M. W. (2009). A model and literature review of professional skepticism in auditing. *Auditing: A Journal of Practice & Theory*, 28(2), 1–34. https://doi.org/10.2308/aud.2009.28.2.1
47. Noordin, N. A., Hussainey, K., & Hayek, A. F. (2022)**.** The use of artificial intelligence and audit quality: Evidence from external auditors. *Journal of Risk and Financial Management*, 15(8), 339. https://doi.org/10.3390/jrfm15080339
48. Novelli, C., Taddeo, M., & Floridi, L. (2024). Accountability in artificial intelligence: What it is and how it works. *AI & Society, 39*, 1871–1882. https://doi.org/10.1007/s00146-023-01635-y
49. Onyenahazi, O. B. (2025). Integrating artificial intelligence in financial auditing to enhance accuracy, efficiency, and regulatory compliance outcomes. *International Journal of Advance Research Publication and Reviews*, 2(7), 23–44. https://doi.org/10.55248/gengpi.6.0725.2402
50. Pollard, J. (2025, October 22). Forrester's AEGIS framework: The new standard for AI governance. *Forrester*. https://www.forrester.com/blogs/forrester-aegis-the-new-standard-for-ai-governance/
51. Raza, M., Qurashi, H., & Haidar, A. (2025). Artificial intelligence in auditing: Transforming fraud detection, risk assessment and assurance quality in financial reporting. *Journal of Asian Development Studies, 14*(3), 453–466. https://doi.org/10.62345/jads.2025.14.3.38
52. Samagaio, A., & Felício, T. (2022).The influence of the auditor's personality on audit quality. *Journal of Business Research*, *141*, 794–807. https://doi.org/10.1016/j.jbusres.2021.11.082
53. Sarker, I. H. (2021). Machine learning: Algorithms, real-world applications and research directions. *SN Computer Science*, 2(3), 160. https://doi.org/10.1007/s42979-021-00592-x

54. Semenova, G. N., Mustafin, T. A., Telegina, Z. A., & Bodiako, A. V. (2023).Audit of quality management at a smart company: Independent expertise vs. artificial intelligence.*International Journal for Quality Research*, *17*(1), 1–12. https://doi.org/10.24874/IJQR17.01-01
55. Shahrour, M. H., Girerd-Potin, I., & Taramasco, O. (2022). Corporate social responsibility and firm defauCOSO (2024)lt risk mitigation: The moderating role of the legal context. *Finance, Contrôle, Stratégie*, *25*(1), 1–30. https://doi.org/10.4000/fcs.8784
56. Tornatzky, L. G., & Fleischer, M. (1990). *The processes of technological innovation*. Lexington Books. https://www.researchgate.net/publication/226145805_The_Technology-Organization-Environment_Framework
57. Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, 27(3), 425–478. https://www.jstor.org/stable/30036540
58. Wang, P., Yuan, L., & Wu, J. (2017). The joint effects of social identity and institutional pressures on audit quality: The case of the Chinese audit industry. *International Business Review, 26*(4), 666–682. https://doi.org/10.1016/j.ibusrev.2016.12.007

List of information sources

1. Committee of Sponsoring Organizations of the Treadway Commission. (2021). *Realize the full potential of artificial intelligence: Applying the COSO framework and principles to help implement and scale artificial intelligence*. https://www.coso.org/_files/ugd/3059fc_e17fdcd298924d4ca4df1a4b453b4135.pdf
2. Committee of Sponsoring Organizations of the Treadway Commission. (2026). *Achieving effective internal control over generative AI (GenAI)*. 719ba0_08f358f2c8f946fa9d26bd51d37b7117.pdf
3. Deloitte. (2024a). *2024 audit quality report*. https://www2.deloitte.com/content/dam/Deloitte/us/Documents/audit/2024-audit-quality-report.pdf
4. Deloitte. (2024b). *Audit transparency report: Annual review 2024*. https://www.deloitte.com/uk/en/about/governance/annual-review-2024/audit-transparency-report.html
5. Deloitte. (2025). *Audit transparency report: Annual review 2025*. www.deloitte.com/content/dam/assets-zone2/uk/en/docs/about/2025/deloitte-uk-annual-review-2025-audit-transparency-report-accessible.pdf
6. European Commission. (2021). *Proposal for a regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206
7. EY. (2024a). *Responsible AI principles*. https://www.ey.com/content/dam/ey-unified-site/ey-com/en-gl/insights/ai/documents/ey-gl-responsible-ai-principles-09-2024.pdf
8. EY. (2024b). *UK 2024 audit quality report*. https://www.ey.com/content/dam/ey-unified-site/ey-com/en-uk/about-us/documents/ey-uk-2024-audit-quality-report.pdf
9. EY. (2025). *EY Gibraltar transparency report 2025*. https://www.ey.com/content/dam/ey-unified-site/ey-com/en-gi/documents/ey-gi-transparency-report-gibraltar-2025.pdf
10. Institute of Internal Auditors. (2024). *The IIA's artificial intelligence auditing framework*. https://www.theiia.org/globalassets/site/content/tools/professional/aiframework-sept-2024-update.pdf
11. International Auditing and Assurance Standards Board. (2019). *ISA 315 (Revised 2019): Identifying and assessing the risks of material misstatement*. https://www.iaasb.org/publications/isa-315-revised-2019-identifying-and-assessing-risks-material-misstatement
12. International Auditing and Assurance Standards Board. (2020a). *Non-authoritative support material: Audit documentation when using automated tools and techniques*. https://www.iaasb.org/publications/non-authoritative-support-material-audit-documentation-when-using-automated-tools-and-techniques
13. International Auditing and Assurance Standards Board. (2020b). *Non-authoritative support material: Using automated tools and techniques when identifying risks of material misstatement*. https://www.iaasb.org/publications/non-authoritative-support-material-using-automated-tools-and-techniques-when-identifying-risks
14. International Auditing and Assurance Standards Board. (2021). *2021 handbook of international quality control, auditing, review, other assurance, and related services*

pronouncements. International Federation of Accountants. https://www.iaasb.org/publications/2021-handbook-international-quality-control-auditing-review-other-assurance-and-related-services

15. International Organization for Standardization. (2023a). *Information technology — Artificial intelligence — Guidance on risk management* (ISO/IEC Standard No. 23894:2023). https://www.iso.org/standard/77304.html
16. International Organization for Standardization. (2023b). *Information technology — Artificial intelligence — Management system requirements* (ISO/IEC Standard No. 42001:2023). https://www.iso.org/standard/42001
17. KPMG. (2023). *2023 KPMG Hong Kong audit quality report*. https://assets.kpmg.com/content/dam/kpmgsites/cn/pdf/en/2024/05/2023-kpmg-hk-audit-quality-report.pdf.coredownload.inline.pdf
18. KPMG. (2024). *AI in financial reporting and audit: Navigating the new era*. https://assets.kpmg.com/content/dam/kpmgsites/xx/pdf/2024/04/ai-in-financial-reporting-and-audit-web.pdf.coredownload.inline.pdf
19. KPMG. (2025). *Transparency report 2024*. https://kpmg.com/kpmg-us/content/dam/kpmg/pdf/2025/2024-transparency-report-jan-2025.pdf
20. National Institute of Standards and Technology. (2023). *Artificial intelligence risk management framework (AI RMF 1.0)* (NIST AI 100-1). U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf
21. PricewaterhouseCoopers. (2021). *Responsible AI: Maturing from theory to practice*. https://www.pwc.com/gx/en/issues/data-and-analytics/artificial-intelligence/what-is-responsible-ai/pwc-responsible-ai-maturing-from-theory-to-practice.pdf
22. PricewaterhouseCoopers. (2024). *Audit quality report 2024*. https://www.pwc.com/jp/en/about/member/assurance/assets/pdf/audit-quality-report1.pdf
23. PricewaterhouseCoopers. (2025). *Transparency report 2024/2025*. https://www.pwc.nl/nl/onze-organisatie/jaarbericht2025/pdf/pwc-transparency-report-2024-2025.pdf
24. Public Company Accounting Oversight Board. (2024). *Staff update on outreach activities related to the integration of generative artificial intelligence in audits and financial reporting*. https://pcaobus.org/documents/generative-ai-spotlight.pdf
25. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). (2024). *Official Journal of the European Union*, L 2024/1689. https://eur-lex.europa.eu/eli/reg/2024/1689/oj

Appendices

Appendix 1. Directed content analysis codebook.

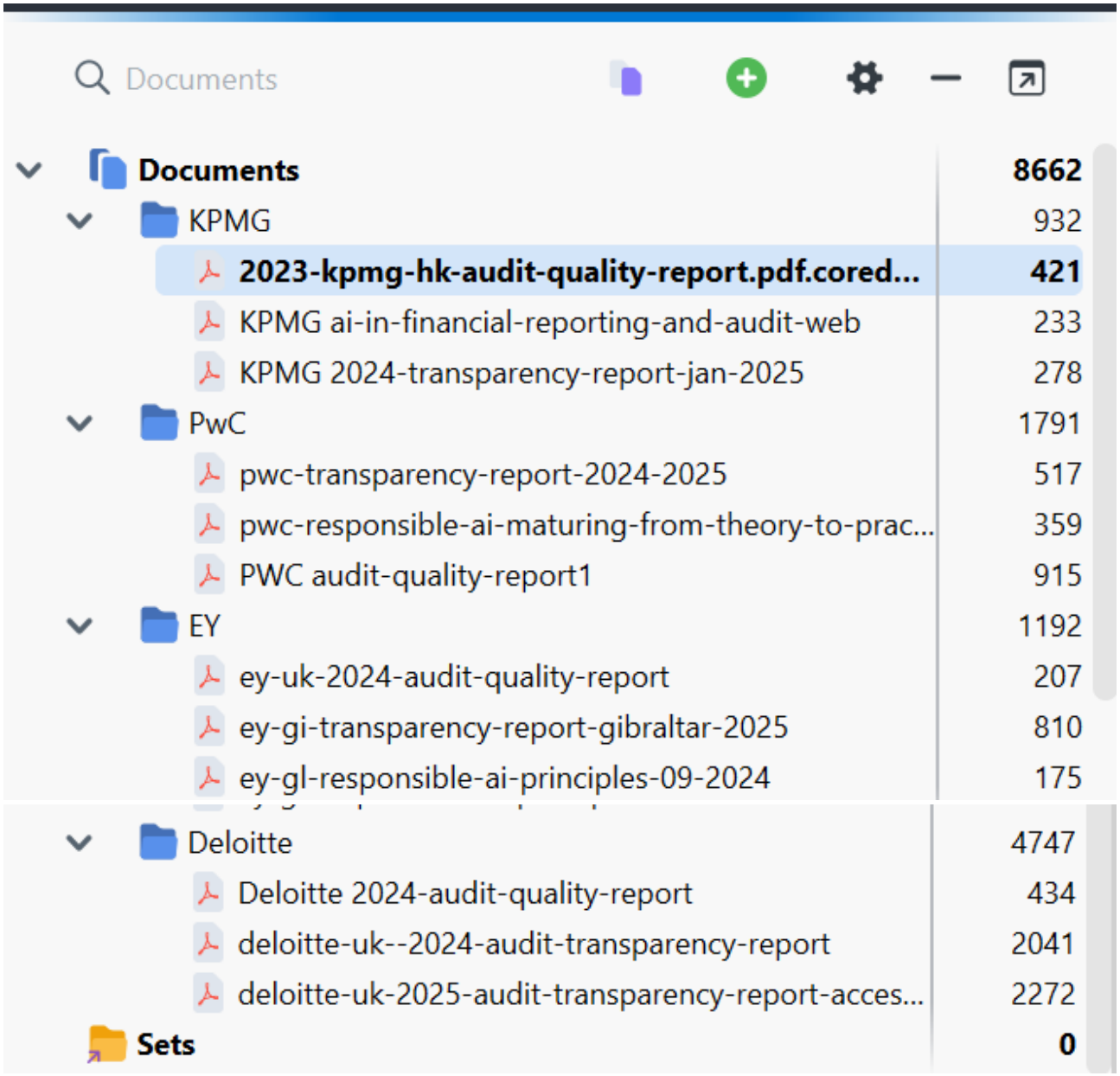
Parent category	Subcode	Operational meaning	Example indicators / keywords
Audit Risk	IR_OPACITY	Inherent risk caused by low explainability or black-box AI logic	black box, opacity, explainability, non-transparent model
Audit Risk	IR_BIAS	Inherent risk from biased, unfair, or skewed AI outputs	bias, unfairness, skewed data, discriminatory outcomes
Audit Risk	IR_MODEL_RISK	Inherent risk from flawed design, assumptions, or unstable performance	model risk, flawed assumptions, unreliable model, model failure
Audit Risk	IR_DATA_QUALITY	Inherent risk caused by poor-quality input data	data quality, completeness, integrity, input errors
Audit Risk	IR_ADAPTIVITY	Inherent risk from models that evolve, drift, or are retrained	adaptive model, drift, retraining, evolving system
Audit Risk	IR_ESTIMATION	Inherent risk where AI affects accounting estimates or judgment-heavy areas	estimates, valuation, forecasting, estimation uncertainty
Audit Risk	IR_REVENUE	Inherent risk where AI affects revenue recognition or transaction classification	revenue recognition, classification logic, transaction timing
Audit Risk	CR_GOVERNANCE	Control risk from unclear governance, ownership, or accountability	governance, accountability, ownership, oversight
Audit Risk	CR_VALIDATION	Control risk from weak validation or insufficient testing	validation, testing, challenge, model approval
Audit Risk	CR_MONITORING	Control risk from weak ongoing monitoring or review	monitoring, incident detection, performance review
Audit Risk	CR_DOCUMENTATION	Control risk from poor documentation, traceability, or logging	documentation, audit trail, traceability, logs
Audit Risk	CR_ACCESS_SECURITY	Control risk linked to weak access rights or cybersecurity	access control, permissions, security, change management
Audit Risk	CR_HUMAN_OVERSIGHT	Control risk caused by insufficient human review of AI outputs	human oversight, review, approval, escalation

Parent category	Subcode	Operational meaning	Example indicators / keywords
Audit Risk	DR_SPECIALISTS	Detection risk affected by the presence or absence of specialists	specialists, expert support, IT audit, data science support
Audit Risk	DR_PROCEDURES	Detection risk linked to adapting audit procedures to AI contexts	audit procedures, testing, reperformance, substantive testing
Audit Risk	DR_EVIDENCE_LIMITS	Detection risk arising from limited auditability or weak evidence	sufficient appropriate evidence, verification difficulty
Audit Risk	DR_ANALYTICS_USE	Detection risk linked to auditors' use of ATTs or analytics	analytics, ATTs, automated tools, technology-assisted analysis
Professional Skepticism	SKEP_QUESTIONING	Auditor's questioning mind toward AI outputs or management claims	questioning mind, challenge, inquire, probe
Professional Skepticism	SKEP_SUSPEND_JUDGMENT	Avoiding premature conclusions before verification	suspend judgment, verify first, avoid premature conclusion
Professional Skepticism	SKEP_SEARCH_KNOWLEDGE	Actively trying to understand AI logic and limitations	search for knowledge, understand system, learn limitations
Professional Skepticism	SKEP_CORROBORATE	Seeking independent support or contradictory evidence	corroborate, verify, independent evidence, triangulate
Professional Skepticism	SKEP_CHALLENGE_MANAGEMENT	Challenging management assumptions or AI reliance	challenge management, assumptions, review management judgment
Professional Skepticism	SKEP_AUTOMATION_BIAS	Over-trust in automated outputs	automation bias, overreliance, blind trust
Professional Skepticism	SKEP_ALGO_AVERSION	Rejecting useful AI outputs merely because they are algorithmic	algorithm aversion, unnecessary distrust, undue rejection
Professional Skepticism	SKEP_PROF_JUDGMENT	Use of human professional judgment alongside AI tools	professional judgment, human decision-making
Professional Skepticism	SKEP_ANOMALY_INVEST	Investigating unusual outputs, outliers, or inconsistencies	anomalies, outliers, investigate unusual results
AI Governance and Assurance	GOV_ACCOUNTABILITY	Clear allocation of responsibility for AI design and outcomes	accountability, owner, responsibility, governance role
AI Governance and Assurance	GOV_OVERSIGHT	Oversight by board, committees, or management	oversight, board, committee, supervision
AI Governance and Assurance	GOV_POLICY_FRAMEWORK	Formal AI principles, policy, or governance framework	responsible AI, policy, framework, principles

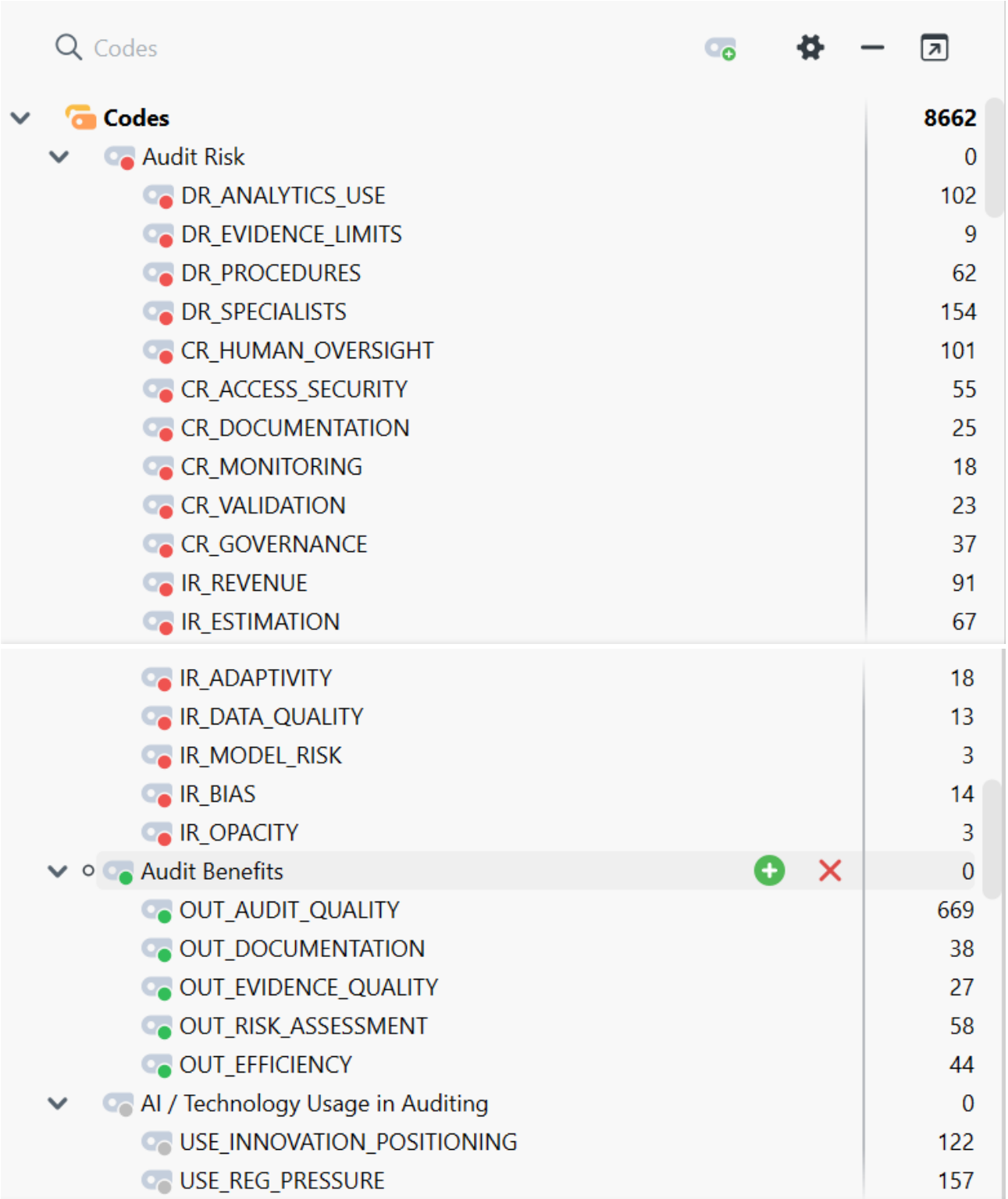
Parent category	Subcode	Operational meaning	Example indicators / keywords
AI Governance and Assurance	GOV_RISK_MANAGEMENT	Structured identification and management of AI risks	AI risk, lifecycle, risk management, controls
AI Governance and Assurance	GOV_VALIDATION	Formal testing and validation of AI models	validation, testing, benchmarking, performance evaluation
AI Governance and Assurance	GOV_MONITORING	Ongoing review of AI performance after deployment	post-deployment, monitoring, incident response, drift
AI Governance and Assurance	GOV_TRANSPARENCY	Transparency of purpose, outputs, or decision process	transparency, disclosure, visible logic
AI Governance and Assurance	GOV_EXPLAINABILITY	Ability to explain how outputs were generated	explainability, interpretability, understandable model
AI Governance and Assurance	GOV_TRACEABILITY	Ability to trace decisions, data, and model changes	traceability, logs, version history, audit trail
AI Governance and Assurance	GOV_HUMAN_OVERSIGHT	Human review, override, or intervention rights	human-in-the-loop, override, escalation
AI Governance and Assurance	GOV_FAIRNESS_ETHICS	Ethical AI, fairness, and responsible-use principles	fairness, ethics, responsible AI, non-discrimination
AI Governance and Assurance	GOV_COMPLIANCE	Compliance with standards or regulations	compliance, NIST, ISO, COSO, EU AI Act
AI Governance and Assurance	ASSURANCE_SERVICE	AI assurance, attestation, or independent verification offerings	assurance, attestation, verification, independent validation
AI Governance and Assurance	ASSURANCE_SCOPE	Description of what AI assurance actually covers	scope, governance review, control assurance, model assurance
AI / Technology Usage in Auditing	USE_USEFULNESS	AI is described as useful for improving audit work	usefulness, efficiency, improved coverage, better detection
AI / Technology Usage in Auditing	USE_EASE	AI use is framed as practical or easy to implement	ease of use, usability, practical, simple
AI / Technology Usage in Auditing	USE_TRUST	Confidence in AI tools or outputs	trust, reliability, confidence, dependable output
AI / Technology Usage in Auditing	USE_PERCEIVED_RISK	Concerns that discourage AI use in auditing	perceived risk, concern, uncertainty, misuse
AI / Technology Usage in Auditing	USE_TRAINING	Training, upskilling, or capability building	training, capability building, digital skills, upskilling

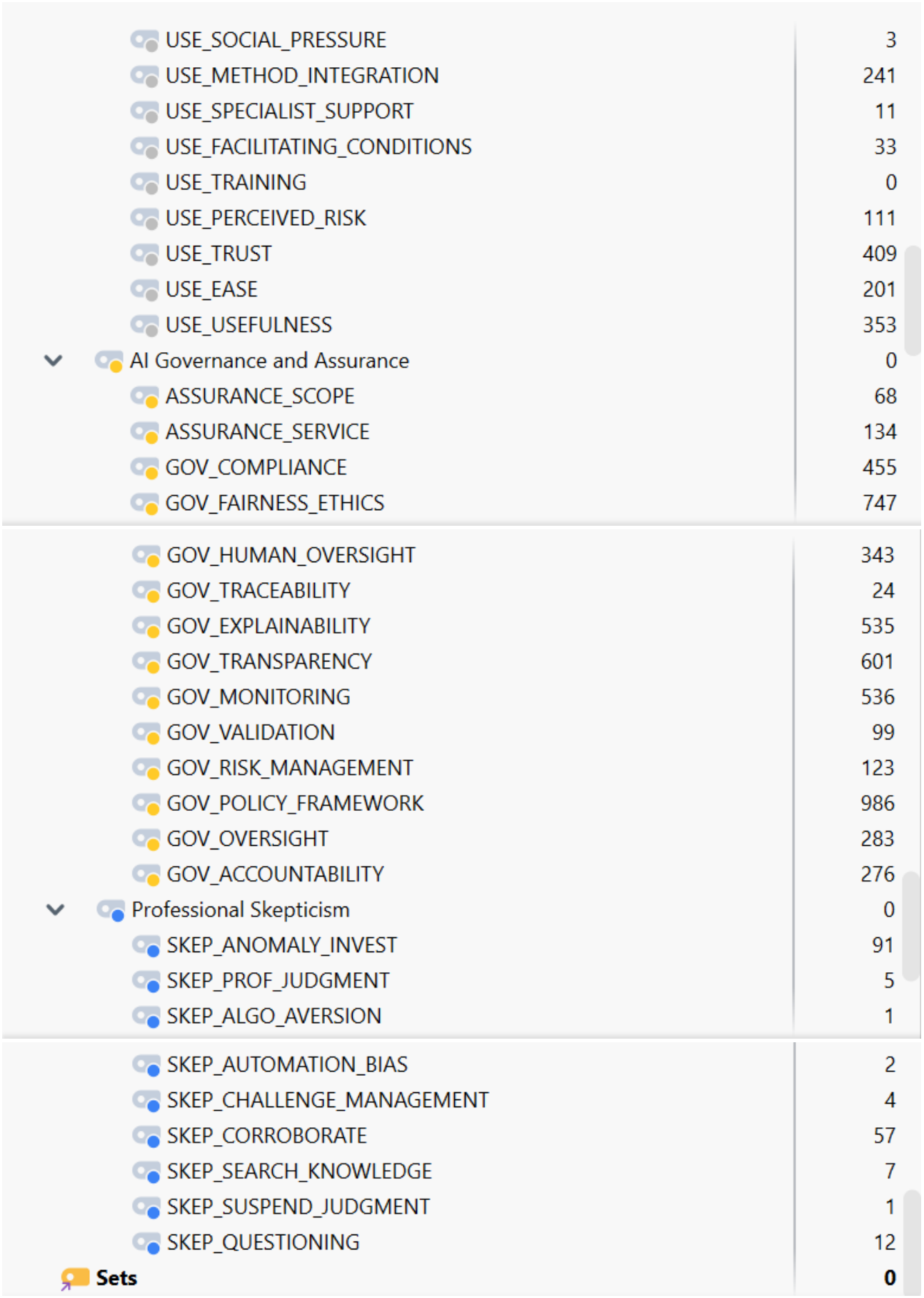
Parent category	Subcode	Operational meaning	Example indicators / keywords
AI / Technology Usage in Auditing	USE_FACILITATING_CONDITIONS	Organizational resources enabling AI use	infrastructure, resources, support, methodology integration
AI / Technology Usage in Auditing	USE_SPECIALIST_SUPPORT	Specialists supporting adoption or use of AI in audits	specialist support, multidisciplinary team, data science team
AI / Technology Usage in Auditing	USE_METHOD_INTEGRATION	AI embedded into audit methodology or workflow	methodology, workflow, embedded, integrated
AI / Technology Usage in Auditing	USE_SOCIAL_PRESSURE	Peer, firm, or professional pressure to adopt AI	expectations, peer pressure, market pressure
AI / Technology Usage in Auditing	USE_REG_PRESSURE	Regulatory or standard-setting pressure affecting AI use	regulatory pressure, inspection, standard setter
AI / Technology Usage in Auditing	USE_INNOVATION_POSITIONING	AI framed as transformation or the future of audit	innovation, transformation, modernization, future of audit
Audit Benifits	OUT_EFFICIENCY	AI linked to efficiency gains in audit work	efficiency, time saving, productivity, coverage
Audit Benifits	OUT_RISK_ASSESSMENT	AI linked to better identification of risks of material misstatement	risk assessment, RMM, better identification
Audit Benifits	OUT_EVIDENCE_QUALITY	AI linked to stronger or weaker audit evidence	evidence quality, supportability, sufficient appropriate evidence
Audit Benifits	OUT_DOCUMENTATION	AI linked to better or worse documentation	documentation, working papers, traceability
Audit Benifits	OUT_AUDIT_QUALITY	AI linked to overall audit quality	audit quality, quality enhancement, quality risk
Audit Benifits	MOD_DATA_QUALITY	Data quality affects whether AI is useful in audit	poor-quality data, reliable data, data dependency
Audit Benifits	MOD_AUDITOR_EXPERTISE	Auditor knowledge affects technology effectiveness	expertise, experience, readiness, competence
Audit Benifits	MOD_ENGAGEMENT_COMPLEXITY	Engagement complexity changes AI usefulness	complexity, high-risk engagement, difficult environment
Audit Benifits	MOD_CLIENT_MATURITY	Client system maturity affects auditability and AI response	system maturity, digital maturity, infrastructure quality

Appendix 2. MAXQDA document corpus and coded segment overview.



Appendix 3. MAXQDA document corpus and coding structure overview.




USE_SOCIAL_PRESSURE 3
USE_METHOD_INTEGRATION 241
USE_SPECIALIST_SUPPORT 11
USE_FACILITATING_CONDITIONS 33
USE_TRAINING 0
USE_PERCEIVED_RISK 111
USE_TRUST 409
USE_EASE 201
USE_USEFULNESS 353
AI Governance and Assurance 0
ASSURANCE_SCOPE 68
ASSURANCE_SERVICE 134
GOV_COMPLIANCE 455
GOV_FAIRNESS_ETHICS 747
GOV_HUMAN_OVERSIGHT 343
GOV_TRACEABILITY 24
GOV_EXPLAINABILITY 535
GOV_TRANSPARENCY 601
GOV_MONITORING 536
GOV_VALIDATION 99
GOV_RISK_MANAGEMENT 123
GOV_POLICY_FRAMEWORK 986
GOV_OVERSIGHT 283
GOV_ACCOUNTABILITY 276
Professional Skepticism 0
SKEP_ANOMALY_INVEST 91
SKEP_PROF_JUDGMENT 5
SKEP_ALGO_AVERSION 1
SKEP_AUTOMATION_BIAS 2
SKEP_CHALLENGE_MANAGEMENT 4
SKEP_CORROBORATE 57
SKEP_SEARCH_KNOWLEDGE 7
SKEP_SUSPEND_JUDGMENT 1
SKEP_QUESTIONING 12
Sets 0