Computer Science & Economics

Universiteit Leiden
The Netherlands

AI Legislation in the EU Financial Sector:
Challenges and Compliance Strategies

Derk Doekes

First supervisors:
Dr. Guus Ramackers

Second supervisor:
Dr. Niki van Stein

BACHELOR THESIS

Abstract

This thesis focuses on the challenges faced by companies operating in the EU financial sector, and is relevant to other industries. It examines the difficulties they face in interpreting, applying and complying with AI legislation, with a particular focus on the EU AI Act. The aim of this thesis is to explore the implication for appropriate regulation, specifically the EU AI Act, to ensure the ethical and responsible use of AI in the financial sector. The study highlights the importance of regulations that prioritise human intervention and accountability within AI systems to mitigate risks.

The research is guided by two main questions: Firstly, what are the challenges faced by EU financial sector firms in interpreting, applying, and complying with the EU AI law? Secondly, how can these firms implement monitoring and enforcement mechanisms to ensure compliance with the responsible use of AI? The findings from the literature review, the survey and the AI audit model are used to propose guidelines and recommendations for financial firms to comply with the EU AI legislation. The study also examines the impact of the EU AI Act on innovation and competitiveness in the financial sector, highlighting the potential long-term benefits and competitive advantages for EU firms.

The contributions of this work include a deeper understanding of the challenges faced by financial firms in complying with AI legislation, the introduction of an AI Law Audit Model to facilitate compliance with the EU AI Act, and the provision of guidelines and recommendations for the responsible use of AI in the financial sector. The limitations of the study are acknowledged, such as its focus on the EU financial sector and its reliance on draft versions of the EU AI Act. Opportunities for future research include validating the AI Law Audit Model in different scenarios, regularly updating the model to reflect changes in legislation, and extending the research beyond the financial sector to other sectors and regions. The implications of this study extend to policymakers, regulators and financial firms, highlighting the importance of robust mechanisms for auditing AI systems and the potential for the EU to influence global AI regulation and foster global collaboration in AI development and deployment.

Contents

1 Introduction

The financial industry is increasingly harnessing the power of artificial intelligence (AI) due to rapid technological advancements. However, this adoption is fraught with complex benefits and risks, necessitating appropriate legislation to ensure ethical and responsible AI use [28]. This thesis focuses on the primary challenges faced by the EU financial sector, and partly FinTech companies, in interpreting, applying, and adhering to AI legislation, predominantly within the European Union (EU).

Research Questions:

1. What are the main challenges EU financial sector companies face in interpreting, applying, and complying with the EU AI Act?

2. How can these companies implement monitoring and enforcement mechanisms to assure responsible AI use compliance?

The growth of AI in the financial sector presents regulatory challenges, including increased information asymmetries, enhanced data dependencies, and elevated interdependencies [27]. These challenges underline the need for regulations that ensure accountability by involving humans in the decision-making process [28].

The upcoming EU AI Act is expected to be stringent and comprehensive, potentially influencing product changes in non-EU countries and the adoption of similar regulations worldwide, known as the "Brussels effect" [21]. Hence, the careful design of this regulation is of global importance [21].

It is crucial to distinguish the application of the law to non-EU companies operating in the EU from its potential impact on other geographical regions that may adopt similar regulations. Additionally, the impact of the AI Act on EU companies operating outside the EU in their non-EU operations requires further consideration during the legislative process [24].

1.1 Problem Statement

The landscape of AI legislation, particularly the EU AI Act, is multifaceted and rapidly evolving. While existing regulations like the General Data Protection Regulation (GDPR) offer a data privacy and protection framework, continuous review and modification are necessary to keep up with AI technology's swift advancement [27]. Financial companies must navigate these intricacies, address potential risks, and transparently communicate their compliance efforts to stakeholders and society.

Key challenges for financial companies involve balancing the benefits and risks of AI use. While AI can enhance financial services, risk assessment, and fraud detection, concerns arise regarding data privacy, security, and biases in decision-making [10]. Mitigating these risks and ensuring compliance with relevant laws and regulations are essential for financial firms [27].

Transparent communication about EU AI Act compliance is another hurdle for financial firms. Openly sharing information about AI use, potential risks or issues, and engaging in dialogue with stakeholders, government regulators, and the public is necessary [10].

1.2   Solution Direction

This research aims to understand the challenges faced by financial sector companies in interpreting and adhering to AI legislation, specifically the EU AI Act. It will employ literature reviews, surveys, and the design of an AI Audit Model to propose effective strategies for monitoring and enforcement mechanisms implementation. By conducting extensive online research and consulting with two experts specializing in data science and business, comprehensive guidelines to ensure responsible AI use and provide public assurance have been developed [10].

An AI audit model, inspired by accounting audit practices, will be developed to help companies validate their compliance with the EU AI Act and adherence to best practices.

The research will explore the correlation between ISO standards (e.g., ISO 9000 and ISO 10000) and AI implementation and regulation. By investigating how ISO compliance aligns with the EU AI Act, the study aims to uncover how companies can leverage ISO standards to fulfill AI Act requirements [21]. Additionally, it will examine how ISO standards and the EU AI Act can jointly foster ethical, transparent, and secure AI practices, identifying best practices for AI implementation and regulation.

To fully explore the complexities surrounding AI legislation and its implications for the financial sector, the research will delve into various related topics, including:

- The development and evolution of AI legislation within the EU and other countries, including the United States.

- The implications of AI legislation for various aspects of the financial sector, such as data privacy, security, decision-making, operations, and risk assessment.

- The role of ethics and corporate responsibility in shaping AI legislation and compliance efforts.

- The potential impact of AI legislation on innovation and the competitiveness of financial companies.

1.3   Research Objective

The primary research objectives are to identify the challenges financial sector companies face when interpreting, applying, and complying with the EU AI Act. The study aims to understand the factors influencing these companies' interpretation and application of AI regulations, as well as develop the most effective monitoring and enforcement mechanisms for AI compliance. The goal is

to establish guidelines that assure society of financial companies' compliance and responsible AI use [10, 24].

Designing an AI Audit model is a significant objective. This model will provide financial companies with a clear roadmap for handling AI compliance, simplifying the process of ensuring adherence to the EU AI Act [10].

Another key objective is to analyze the role of ethics and corporate responsibility in shaping AI legislation and compliance efforts. Insights into how ethical considerations and corporate social responsibility can contribute to more effective AI compliance strategies will be provided.

Finally, the research will assess the potential impact of the EU AI Act on the innovation and competitiveness of financial sector companies, shedding light on the broader implications of AI regulation for the industry [21].

1.4 Deliverables

This thesis will conduct an extensive literature review on AI legislation within the European Union and other countries, including the United States, highlighting its relevance to the financial sector. Through surveys involving financial companies, industry experts, and regulators, the study will delve into the interpretation, application, and compliance with AI legislation.

Key findings will inform the development of practical guidelines for financial companies to demonstrate their compliance with AI legislation, with a specific focus on the role of ethics and corporate responsibility. Additionally, the study will assess the impact of AI legislation on innovation and competitiveness within the financial sector.

A central deliverable of this research will be the design of an AI Audit model, inspired by traditional auditing practices, aimed at helping financial companies evaluate and ensure their adherence to AI legislation.

In summary, the key deliverables include:

- Literature review on AI legislation

- Analysis of stakeholder surveys

- Guidelines for AI compliance in financial companies

- Examination of the role of ethics and corporate responsibility

- Assessment of the influence of AI legislation on innovation and competitiveness

- Design of an AI Audit model

1.5 Thesis Overview

Chapter 1: Introduction - Provides an overview of the research, highlighting the problem statement, objectives, and findings.

Chapter 2: Literature Review - Reviews existing research on AI legislation, focusing on the EU and the US, and explores the influence of ethics and corporate responsibility.

Chapter 3: Methodology and Framework Development - Outlines the research methodology, including literature review, surveys, interviews, and the development of the AI audit model.

Chapter 4: AI Audit Analysis Framework - Examines the AI Audit Model, its components, and its effectiveness in ensuring compliance in financial firms.

Chapter 5: Guidelines, Discussion, and Recommendations for AI Regulatory Compliance - Provides actionable guidelines for regulatory compliance and discusses the impact on innovation and competitiveness.

Chapter 6: Conclusion and Future Work - Summarizes the research, its contributions, limitations, and potential areas for future study, highlighting the proposed AI Audit model.

2 Background and Related Work

2.1 General EU AI act

The European Union's proposed Artificial Intelligence Act (EU AI Act) aims to create a holistic legal framework to regulate the development and use of AI, with a strong emphasis on data quality, transparency, human oversight, and accountability [6]. The ambitious proposal aims to address the ethical dilemmas and operational challenges in various sectors, from healthcare and education to finance and energy. In addition, the Act aims to tackle the hazards and perils posed by AI biometric surveillance systems to core liberties, democracy, and the principles of justice. It also raises doubts regarding the adequacy of the AI Act in addressing these apprehensions. [16].

The AI Act's innovative risk-based classification system categorizes AI systems into four risk levels: minimal, limited, high, and unacceptable. Regulations range from minimal obligations for low-risk AI systems, such as spam filters or video games, to strict regulations for high-risk AI systems, such as autonomous vehicles and medical devices, to outright bans on AI systems that pose an unacceptable risk, such as real-time biometric identification systems in public spaces [8]. However, while the draft EU AI Act acknowledges that some AI practices should be banned, it offers numerous exceptions and loopholes that should be closed [16].

The EU AI Act's risk-based approach, exemplified by Kop's (2021) pyramid of criticality (figure 1) [12], applies a layered enforcement mechanism. As risk increases, regulation becomes more stringent, ranging from non-binding, self-regulatory, soft-law impact assessments with codes of conduct, to strict, externally audited compliance requirements throughout the application lifecycle [12]. However, the unpredictability of AI requires rigorous policy debates to focus on potential risks and benefits in the context of societal acceptance, with implications for existing regulatory frameworks such as product safety, liability, and consumer protection [14].
Furthermore, the overarching goal of the legislation is to strengthen Europe's position as a global AI hub and ensure that AI technologies developed and deployed in the EU are in line with its values and rules [8]. This legislation promotes ethical considerations, greater transparency, and the strengthening of data protection laws, providing individuals with more rights and remedies [16]. To ensure uniform application of the law across the EU, it proposes the establishment of the European Artificial Intelligence Board, which would provide guidance to national authorities and issue opinions and recommendations on emerging issues [8].

The EU AI Act is presently under discussion in the European Parliament, and trilogue negotiations are set to commence once the Parliament adopts its stance on the legislation. [6]. Despite the potential complexity of the negotiations due to the broad scope of the legislation, the EU AI Act represents a significant step towards addressing the need for comprehensive regulation and ethical guidance in the rapidly evolving AI landscape. It seeks to strike a balance between fostering innovation and ensuring the responsible development and use of AI technologies, which is particularly relevant in areas such as the financial sector where AI is disrupting traditional business models [14].
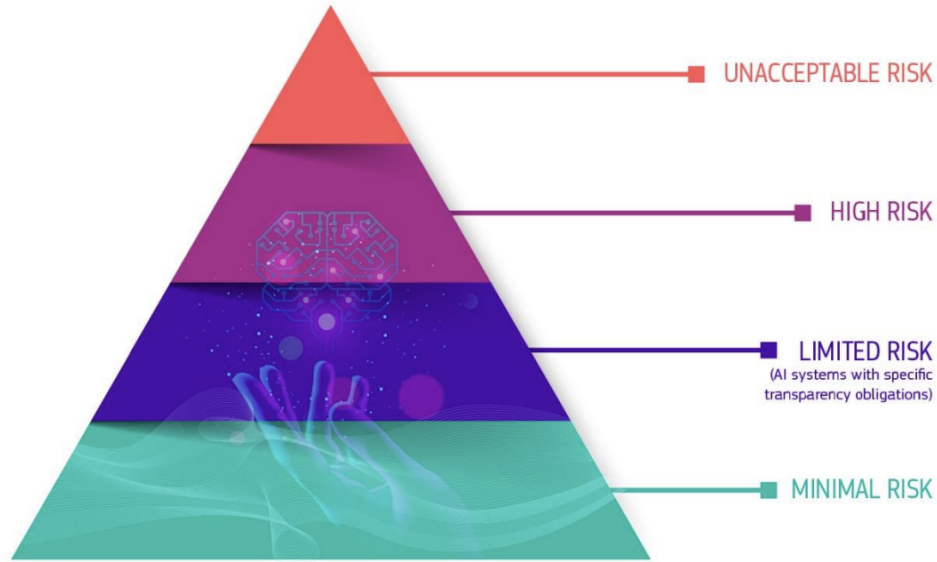
Figure 1: The Pyramid of Criticality for AI Systems [12].

The inclusion of data provenance and governance considerations in the EU AI Act discussions is of paramount importance. It is particularly important in light of the recent ratification of the EU Data Governance Act (2022), a legislative proposal that aims to create a framework that facilitates efficient data sharing [20].

The Data Governance Act represents a significant step forward in the regulation of AI, with the aim of improving data-sharing mechanisms. The Act embodies the potential to catalyse the advancement of AI, while ensuring strict data protection. It is therefore crucial that the principles embedded in the Data Governance Act are reflected in the EU AI Act [7].

The EU AI Act needs to clarify explicit provisions on data governance, with an emphasis on the ethical dimensions of data handling, including informed consent and transparency. In addition, the Act should address the nuances of data provenance and promote ethical data sourcing and collection practices.

The institutionalisation of these principles will strengthen the alignment of AI technologies with the EU's established data protection standards, and drive the development of ethically informed AI. Therefore, the proposed EU AI law should benefit from the progressive steps taken by the Data Governance Act, highlighting the need for robust data sourcing and governance within its legal framework [20].

2.2   EU AI Act in the financial sector

The EU AI Act represents a significant shift towards the regulation of AI in a variety of sectors, including financial firms [16]. Pre-existing regulations that implicitly or explicitly encompass AI, such as the General Data Protection Regulation (GDPR), were conceived before the modern surge in AI capabilities and its widespread acceptance, as described by Mazzini (2019) [14].

According to the framework of the EU AI Act, AI systems that have a significant impact on the fundamental rights, security and general welfare of the public will be classified as high risk. This could include AI applications used in various sectors of the financial industry, including banking and investment management. [16] Nesterova (2020) explains that these high-risk systems will be subject to stricter regulation under the EU AI Act.

In contrast, the EU AI Act encourages providers and users of lower-risk AI systems to voluntarily and proportionately adhere to the same standards as their high-risk counterparts. Article 69 of the EU AI Act ensures a certain level of oversight and regulation even for lower-risk AI applications, such as chatbots in the financial sector [14].

While the EU AI Act doesn't directly address liability concerns arising from AI systems, [2] Buczynski (2022) suggests that the European Commission is preparing to introduce additional initiatives to address this in the future.

The EU AI Act places the financial sector in an ambiguous position, categorising it as a 'high impact' sector rather than a 'high risk' sector like aviation or healthcare [2]. This distinction remains nebulous, as explained by Nesterova (2022)[16], and warrants further clarification in future versions of the law. While the EU AI Act does not list financial services as high-risk systems, various sections refer to credit institutions and banks. The EU AI Act also identifies credit scoring as a high-risk case, but aligns it more closely with the prohibited social credit scoring than with financial services [14].

By default, the financial services sector would likely fall within the scope of Article 69 of the EU AI Act, given its emphasis on proportionality [16].

The EU AI Act specifies the roles of 'provider' and 'user' as the primary stakeholder functions. However, Mazzini (2019) [14] argues that the real-world AI supply chain is more complex, involving third parties that provide AI systems to financial firms, which in turn provide these systems to their customers.

The European Commission's estimates of the costs of compliance with the EU AI Act range from €6,000 to €7,000 for providers and €5,000 to €8,000 per year for users. As [16] Nesterova (2022) argues, given the diversity of AI systems, these estimates may not accurately represent compliance costs across all sectors. Certain AI systems may require stricter oversight for both providers and users, leading to increased costs and potential disputes.

In conclusion, the existing draft of the EU AI law leaves room for interpretation when it comes to the financial sector. [14] Mazzini (2019) suggests that future drafts should provide clearer guidance

on its classification and treatment within the regulatory framework.

In conclusion, the EU AI Act could have a significant impact on the financial services industry. Its risk-based approach and emphasis on transparency and compliance, as suggested by both Nesterova (2022) [16] and Mazzini (2019) [14], could help ensure the ethical and responsible use of AI systems in the financial sector, while promoting innovation and growth.

2.3 Incorporating ISO Standards in AI Implementation and Regulation

The International Organisation for Standardisation (ISO) is a non-governmental organisation recognised for creating and publishing international standards applicable to various industries, including technology and AI. Two particular ISO standards, ISO 9000 and ISO/IEC 27701:2019, warrant consideration in the context of the EU AI Act [13].

ISO 9000 provides a comprehensive guide for organisations to improve product quality and customer satisfaction through effective quality management systems. As Siougle (2019) [22] found, adopting ISO 9000 certification is associated with improved financial performance, highlighting the value of systematic management processes and customer-centric operations. Although it wasn't explicitly designed for AI systems, ISO 9000 provides a robust framework for managing quality within the AI development and deployment process.

The ISO/IEC 27701:2019 standard, as explored by Lachaud(2020) [13], establishes a management system for the protection of personal data, with the ability to certify compliance. While this new ISO standard offers practical benefits to organisations looking to streamline data protection and information security, it also presents potential complications, particularly in relation to the EU AI Act. With the potential for ISO/IEC 27701:2019-based certification to dominate the data protection certification market, the public may become confused, especially when it comes to Article 42/43 certification under the EU AI Act.

However, despite these potential complications, the ISO/IEC 27701:2019 standard could provide opportunities to spread data protection principles beyond EU borders. It also sets a valuable precedent for the relationship between ISO standards and certification under the EU AI Act [13].

In Malaysia, companies registered to ISO 9000 outperformed those not registered, particularly in terms of return on assets (ROA), return on sales (ROS) and working capital (WC), as noted by [15]. This suggests that adherence to such ISO standards can bring significant benefits, which could potentially extend to companies developing and deploying AI under the EU AI Act. However, it is important to consider that this correlation may also imply that only companies that are already performing well can afford the time and financial resources to apply for such standards, as is certainly the case in software development, for example.

In the context of the EU AI Act, the ISO 9000 and ISO/IEC 27701:2019 standards can provide valuable guidance. The objectives of the EU AI Act to ensure the safe and ethical use of AI, with sufficient transparency and accountability, align well with these ISO standards [13]. Companies

that have already achieved compliance with these standards may find it easier to comply with the EU AI Act, given the pre-existing structures for quality management and customer satisfaction [22, 15].

In conclusion, examining the interplay between these ISO standards and the EU AI Act can shed light on best practices for implementing the EU AI Act's provisions. By understanding how these ISO standards can complement the EU AI Act, companies can leverage existing processes to ensure ethical, transparent, and safe AI practices [13]. The research aims to identify ways to integrate these standards into AI implementation strategies, highlighting the value of ISO certifications in improving the financial and operational performance of AI-oriented businesses [22, 15].

2.4 Ethical Considerations in AI Development and Deployment

The advent of AI has raised not only technical challenges, but also ethical dilemmas that extend into the realms of fairness, bias and transparency [4]. As AI systems become deeply embedded in our societies and economies, the practical challenges of developing and deploying ethical AI become more complex and diverse [3].

For example, the growing computational intensity of AI has given rise to the "computational divide" [1]. The resources needed for AI research and development are increasingly concentrated in large technology companies and elite universities, which in turn are becoming major players in AI conferences [1]. The result is a systemic bias that disadvantages mid- and lower-tier universities and undermines efforts to democratise AI [1].

This power dynamic within the AI sector mirrors the biases that can manifest in AI technologies themselves. While powerful and efficient, AI systems can produce disparate outcomes for different demographic groups, posing significant legal and reputational risks for companies and organisations [26]. AI fairness technologies have been developed to mitigate these biases, but their use is not without cost. For example, in an e-commerce scenario, enforcing AI fairness resulted in an increase in financial costs, even though fairness requirements were successfully met [26].

At the same time, businesses are using AI to accelerate their digital transformation, often with the aim of improving productivity and performance [4]. In the financial sector, AI is driving business model innovation and shaping new products and services [19]. While this revolution offers many opportunities, it also brings its own set of challenges, including risks and regulatory implications, changes to the competitive landscape and the impact on employment [19].

Critically, the ethical implications of AI are not merely academic concerns, but are closely linked to practical, operational realities [3]. The holistic consideration of ethics in the development and deployment of AI systems is paramount, not only to mitigate potential risks, but also to ensure that AI technologies are truly beneficial to all stakeholders [3].

However, there are growing concerns that the current approach to AI ethics, which is primarily anchored in ethical principles, is vulnerable to manipulation, particularly by industry actors [18].

Without robust implementation mechanisms, AI ethics may be perceived as toothless, more of a performative gesture than a genuine commitment to ethical practice [18].

In conclusion, ethical considerations in the development and deployment of AI need to be comprehensive and substantive, addressing the technical, social, economic and regulatory challenges that AI presents. A more robust and consistent regulatory environment, coupled with an unwavering commitment to fairness, transparency and accountability, is critical to ensuring that AI technologies serve as tools for equitable growth and societal well-being, rather than instruments of systemic bias and exclusion.

As AI continues to evolve, the ethical considerations will become increasingly complex. But by committing to a thorough and consistent approach to AI ethics, we can ensure that AI serves the broader interests of society.

3 Methodology

This section describes the methodology used to develop the AI audit model and conduct the research. The proposed research uses a mix of methods, including an in-depth literature review, a survey-based study and the development of an AI audit model.

Literature review: A comprehensive literature review has been carried out to establish the foundational knowledge required for this research. Topics covered included the development and evolution of AI legislation in the EU and other countries, the impact of AI on various aspects of the financial sector, and the role of ethics and corporate responsibility in shaping AI legislation and compliance.

Development of the AI audit model: The AI audit model is inspired by accounting audit principles and adapted to the unique challenges and opportunities presented by artificial intelligence. In addition, the model draws on the Business Model Canvas (BMC) concept to provide a holistic view of an organisation's AI-related activities. To ensure legality, the model is built in accordance with the EU AI Act.

The model is developed in three layers, each providing a different perspective but integrating seamlessly to provide a comprehensive audit approach.

Phase Diagram: The phase diagram is the foundational layer that traces the trajectory of an AI audit from its inception to its conclusion. It contains several key phases:

- Scope and objectives: The scope and objectives of the AI audit are defined, outlining the specific areas or processes to be audited.

- Audit process: The actual audit process involves reviewing and evaluating the organization's AI systems, data governance, algorithm transparency, bias mitigation efforts, privacy measures, regulatory compliance, model development, and performance monitoring.

- Reporting and communication: Following the audit, findings are compiled into a comprehensive report, and recommendations and action plans are effectively communicated to stakeholders.

Business Model Canvas (BMC): The BMC layer translates the abstract audit process into tangible business components, aligning the organisation's key partners, activities, resources, value propositions, channels and customer relationships with each step of the audit process.

- Governance and policies: The governance component assesses the organizational structure and policies related to AI, including roles and responsibilities, decision-making processes, and accountability mechanisms.

- Risk assessment: The risk assessment component focuses on potential biases, fairness issues, security vulnerabilities, and stakeholder impacts, helping the organization identify and mitigate risks.

- Data management: The data management component examines data collection, storage, quality, and lifecycle management practices in the context of AI systems.

- Algorithmic transparency and accountability: This component examines the transparency and explainability of AI algorithms and models.

- Model validation and testing: This includes procedures for validating and testing AI models, assessing the suitability of data sets, performance evaluation methods, and proper documentation of AI models.

- Performance monitoring and metrics: Mechanisms for ongoing monitoring of the performance of AI systems will be established, including key metrics and indicators.

- Training and awareness: This component includes training staff on AI testing practices, ethical considerations, and emerging trends.

- Continuous improvement: This establishes a feedback loop for continuous improvement of the AI testing model.

EU AI Act: The third layer aligns the model with the EU AI Act, ensuring that each step of the audit process and its corresponding BMC element complies with the relevant articles and provisions of the legislation.

By harmonising these three layers - Phase Diagram, BMC and EU AI Act - the AI Audit Model provides a practical and compliant approach to auditing AI in financial organisations. The ultimate goal of the model is to promote responsible AI practices, mitigate AI-related risks and ensure that organisations comply with the EU AI Act.

This comprehensive approach enables organisations to identify shortcomings and areas for improvement, thereby enhancing the compliance, transparency, fairness and ethical considerations of their

AI systems. By following this model, organisations in the financial sector can effectively navigate the complexities of AI governance and ensure the responsible and beneficial use of AI technology.

The adaptability and comprehensiveness of the model has been praised by industry experts, establishing it as a valuable tool for AI testing in the financial sector. By ensuring thorough compliance with the EU AI Act and promoting best practices in AI governance, it enables financial organisations to minimise the risks and maximise the benefits of AI technology.

Survey dissemination and data collection: The final part of this research involves the development and dissemination of a survey to financial firms and institutions. The purpose of the survey is to assess the readiness of these firms to comply with the forthcoming EU AI legislation. The data collected from this survey will provide insight into the current state of compliance with EU AI legislation within these organisations, the challenges they face, and the strategies they employ for monitoring and enforcement.

Analysis and interpretation: The data collected through the survey will be statistically analysed and the findings will be interpreted in the context of the existing literature and the AI audit model. This process will help to understand the practical aspects of AI compliance within financial firms, as well as the effectiveness of the developed model.

Recommendations and guidelines: Based on the literature review, the survey results and the model development, recommendations for financial firms will be proposed. These recommendations will relate to the interpretation, application and compliance with the EU AI Act, as well as potential monitoring and enforcement mechanisms to ensure the responsible use of AI.

The outcome of this methodology will be a comprehensive exploration of the implications of the EU AI Act for EU financial firms, a novel AI audit model, and a set of recommendations to facilitate compliance with the EU AI Act.

4   AI Audit Analysis Framework

In this chapter, we navigate the complexities of the AI audit model (Figure 2), its connection to the business model canvas (BMC) (Figure 3 and 4), and its harmonisation with the European Union's AI law. These elements come together to form an integrated and multifaceted model (Figure 5) that facilitates a robust AI audit process.
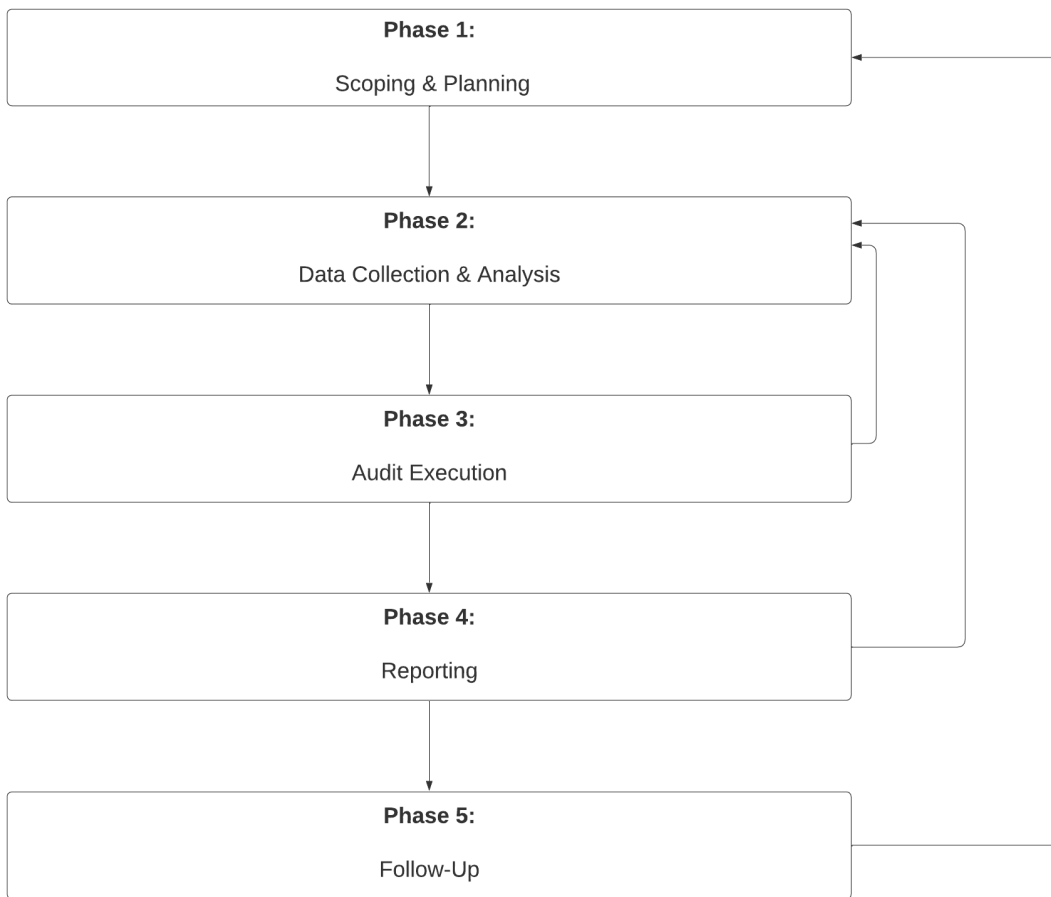
4.1 AI Audit Model

Figure 2: Phase Diagram
.

The AI audit model, shown in Figure 2, is carried out in five distinct but interrelated phases: Scoping and Planning, Data Collection and Analysis, Audit Execution, Reporting and Follow-up. This model emphasises an iterative methodology that allows for continuous refinement and improvement [17].

4.1.1 Scoping and Planning

The initiation phase, Scoping and Planning, guides the audit process by establishing its intent, scope, objectives and timeline. This phase identifies the AI systems to be audited and the specific regulations, standards, or laws that the audit is intended to enforce. Potential risks associated with the AI system, such as privacy issues, algorithmic bias, or other ethical considerations, are also identified at this stage, allowing auditors to focus their efforts on areas that pose the greatest potential harm.

4.1.2 Data collection and analysis

Next, the data collection and analysis phase involves gathering and reviewing the necessary data and information related to the AI system. This phase may involve interviewing people who interact with the system, reviewing system documentation, or directly inspecting the AI system itself. Data analysis fosters a deeper understanding of how the AI system works, its applications, and potential areas of non-compliance, laying the groundwork for the next phase.

4.1.3 Audit Execution

The Audit Execution phase involves a detailed examination of the AI system. This examination includes evaluating the design and operation of the system, testing the behaviour of the system, and comparing the operation of the system with the previously identified compliance requirements. Any discrepancies found at this stage may lead the auditor to return to the second stage to obtain more information or to reassess the data.

4.1.4 Reporting

Reporting in the AI audit process involves compiling the findings into a comprehensive report. In accordance with the EU AI Act, organisations must follow prescribed reporting guidelines, including documentation required for the EU-wide database. The report should provide clear insights into compliance issues, risks and proposed actions. Accuracy and completeness are critical, with any discrepancies warranting a review of the previous stages.

To ensure compliance, auditors can refer to the capAI procedure [9]. It provides a framework for conformity assessment in line with the EU AI Act. In addition, insights from Veale (2021). [24] inform reporting practices and legal implications.

In summary, reporting and documentation involves creating a comprehensive report that addresses compliance issues, risks and proposed actions. Adhere to reporting guidelines, refer to capAI [9] and consider Veale (2021). [24]

4.1.5 Follow-up

Finally, the follow-up phase involves addressing the report's findings, which may involve re-auditing the system after adjustments have been made, monitoring the system to ensure continued compliance, or providing additional guidance and support to the organisation. This stage often links back to the initial scoping and planning stage, as the findings of one audit may influence the scope and objectives of subsequent audits.

The cyclical structure of the AI audit model promotes a systematic approach to auditing and facilitates continuous improvement in AI system compliance. By facilitating the refinement of audit strategies and the correction of errors, it increases the accuracy and efficiency of the AI audit process

[17]. This methodology is essential for organisations seeking to maintain compliance with EU AI regulations and standards, maximising the benefits and minimising the potential risks associated with AI technology.

4.2 Connection with the Business Model Canvas (BMC)
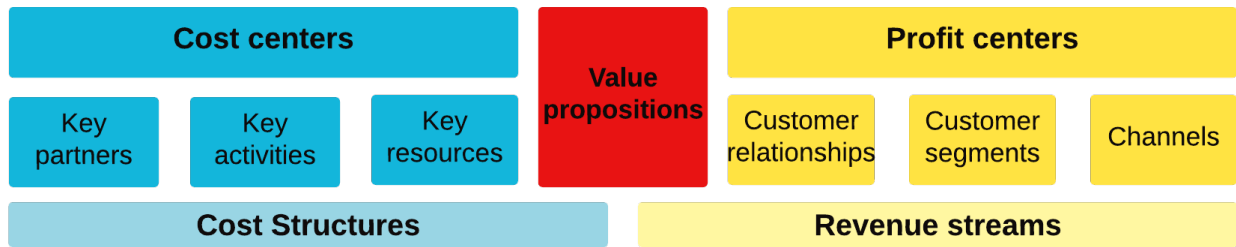
Figure 3: Business Model Canvas Design

.

The architecture of the Business Model Canvas (BMC) employed in this study adheres to the canonical design as demonstrated in Figure 3. In the ensuing section, this standard BMC is populated in full to reflect the specifics of the investigated scenario. The Business Model Canvas (BMC) is a strategic tool for developing and visualising business models. It provides a holistic view of a firm's key activities, encompassing nine components: key partners, activities, resources, value propositions, customer relationships, channels, customer segments, cost structure, and revenue streams. This layout facilitates understanding of interdependencies, identifies areas for innovation, and effectively communicates the business model to stakeholders.

Cost centers

1. Key Activities
What do you need to do to produce, market, and deliver your solution?

1. Assessing AI systems and applications

2. Evaluating data governance practices

3. Ensuring privacy and security compliance

2. Key resources
What do you need to have in order to produce, market, and deliver your solution?

1. AI audit framework and methodology

2. AI regulatory guidelines and standards

3. Internal and external expertise in AI auditing

3. Key Partners
Who should be involved as you produce and deliver your solution?

1. Legal experts speciaizing in AI regulations

2. AI technology vendors

4. Cost structures

1. Human resources for conducting AI audits

2. Legal and regulatory expertise for compliance assessment

5. Value proposition

1. Ensure compliance with AI laws, regulations and standards

2. Identify and mitigate risks associated with AI systems

3. Enhance transparency, fairness, and accountability in AI decision-making

Profit centers

6. Customer relationships
How do you talk to your market about your solution? How do you acquire customers?

1. Collaborative partnerships for knowledge sharing and expertise exchange

2. Regular reporting and updates on AI audit findings and recommendations

7. Customer segments
Who needs your solution? How many people need your solution right now or will eventually need it?

1. Organizations using AI systems and applications

2. Regulatory bodies overseeing AI implementation

8. Channels
How do you deliver your solution to customers and where can they find it?

1. Online platforms for survey distribution and data collection

2. Reports and presentations for sharing audit results and insights

9. Revenue streams

1. Service fees charged for AI audit assessments

2. Consulting fees for providing tailored recommendations and action plans

Figure 4: Business Model Canvas AI audit

The synergistic relationship between the AI audit model and the BMC (Figure 4) enhances the comprehensibility and efficiency of the audit process. The BMC provides a visual representation of the organisation's key activities, resources and partners in each audit phase [11].

For example, at the 'Scoping and Planning' phase (Phase 1 in Figure 2), key partners might include AI technology vendors and legal experts who provide expertise to define the scope and risk assessment process. Similarly, key activities may include identifying the AI systems to be audited and establishing key performance indicators (KPIs).

4.3   Alignment with the EU AI Act

The provisions of the EU AI Act fit seamlessly into the phases of the AI Audit Model. Figure 5 illustrates how the model aligns with Articles 1, 2 and 3 of the EU AI Act during the 'Scoping and Planning' phase. These articles define the purpose, scope, and definitions of AI systems that need to be considered when determining the scope of the audit [23].
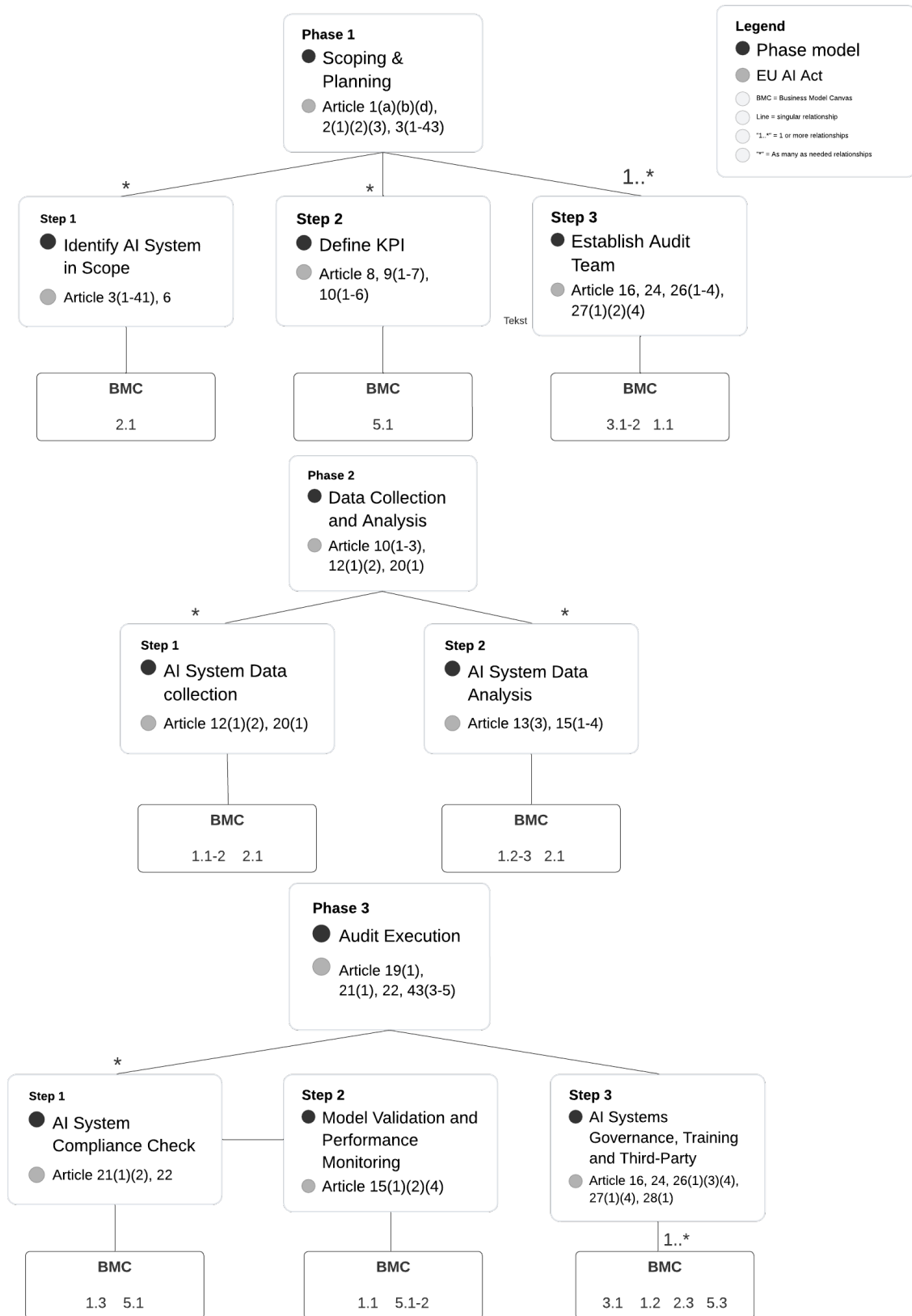
In the subsequent phases of the AI audit model, other articles of the EU AI Act come into play, embedding compliance requirements in each step of the audit process. This not only ensures compliance with the Act, but also serves as a tool for interpreting and implementing the regulations within the organisation's operations [5].

However, real-world applications of the model may face challenges due to the complexity of AI legislation and technological intricacies. Figure 5 depicts the AI audit model, which provides practical solutions to overcome these challenges and ensure smooth compliance with regulatory requirements.

4.4   A Comprehensive AI Audit Model

Overview of the Comprehensive Model
Introducing the comprehensive model depicted in Figure 5, we explore the connections between the AI audit model, the components of the BMC, and the relevant articles of the EU AI Act. Figure 4 presents a comprehensive model that links the AI audit model, the components of the Business Model Canvas and the relevant articles of the EU AI Act. This model not only brings together each step and phase of the AI audit process, but also delineates their interrelationships with corresponding elements of the Business Model Canvas and the EU AI Act.
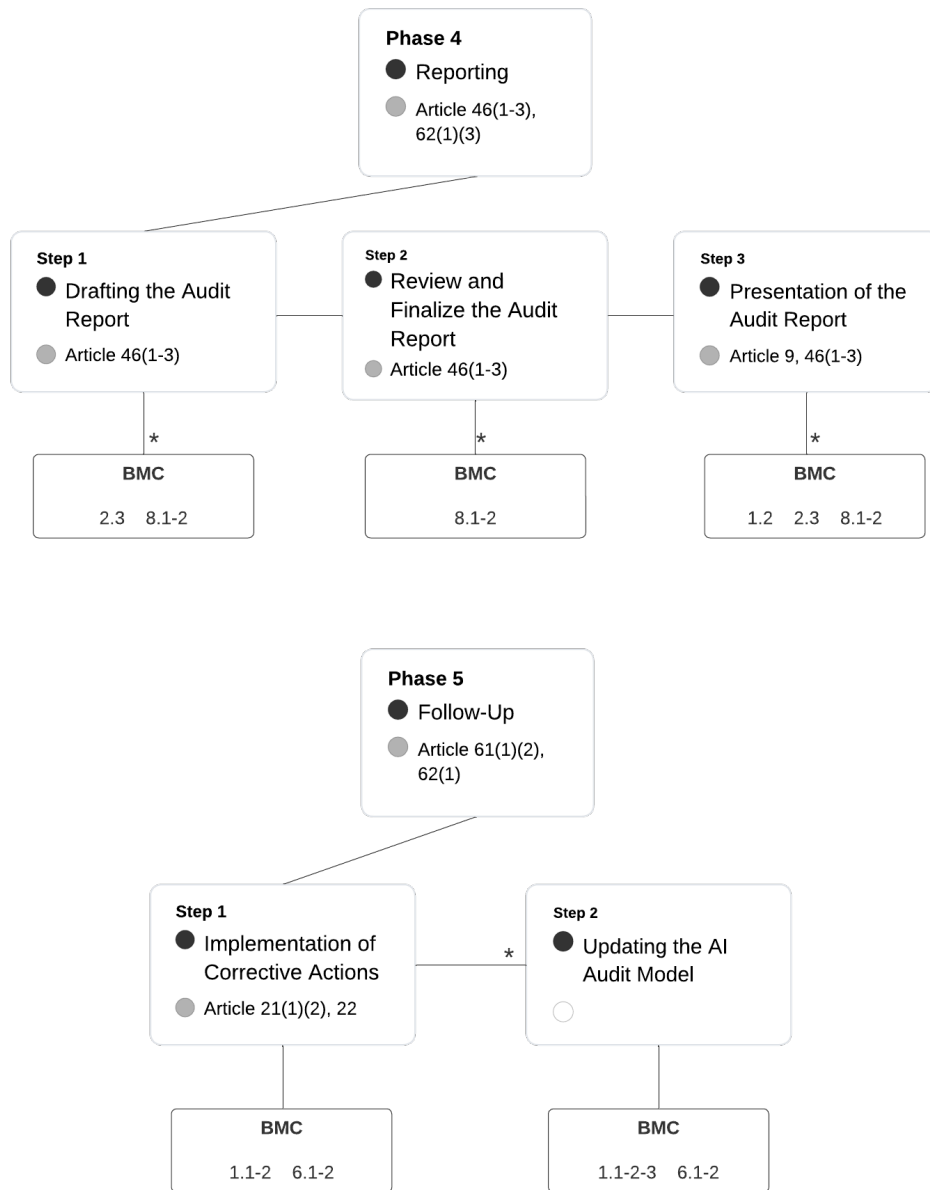
Phase 1
- Scoping & Planning
- Article 1(a)(b)(d), 2(1)(2)(3), 3(1-43)

Legend
- Phase model
- EU AI Act
- BMC = Business Model Canvas
- Line = singular relationship
- "1..*" = 1 or more relationships
- "*" = As many as needed relationships

*

*

1..*

Step 1
- Identify AI System in Scope
- Article 3(1-41), 6

Step 2
- Define KPI
- Article 8, 9(1-7), 10(1-6)

Tekst

Step 3
- Establish Audit Team
- Article 16, 24, 26(1-4), 27(1)(2)(4)

BMC

2.1

BMC

5.1

BMC

3.1-2   1.1

Phase 2
- Data Collection and Analysis
- Article 10(1-3), 12(1)(2), 20(1)

*

*

Step 1
- AI System Data collection
- Article 12(1)(2), 20(1)

Step 2
- AI System Data Analysis
- Article 13(3), 15(1-4)

BMC

1.1-2   2.1

BMC

1.2-3   2.1

Phase 3
- Audit Execution
- Article 19(1), 21(1), 22, 43(3-5)

*

Step 1
- AI System Compliance Check
- Article 21(1)(2), 22

Step 2
- Model Validation and Performance Monitoring
- Article 15(1)(2)(4)

Step 3
- AI Systems Governance, Training and Third-Party
- Article 16, 24, 26(1)(3)(4), 27(1)(4), 28(1)

1..*

BMC

1.3   5.1

BMC

1.1   5.1-2

BMC

3.1   1.2   2.3   5.3

Phase 4
● Reporting
○ Article 46(1-3), 62(1)(3)

Step 1
● Drafting the Audit Report
○ Article 46(1-3)

Step 2
● Review and Finalize the Audit Report
○ Article 46(1-3)

Step 3
● Presentation of the Audit Report
○ Article 9, 46(1-3)

BMC
2.3   8.1-2

BMC
8.1-2

BMC
1.2   2.3   8.1-2

Phase 5
● Follow-Up
○ Article 61(1)(2), 62(1)

Step 1
● Implementation of Corrective Actions
○ Article 21(1)(2), 22

Step 2
● Updating the AI Audit Model
○

BMC
1.1-2   6.1-2

BMC
1.1-2-3   6.1-2

Figure 5: AI Audit Model

4.4.1 Phase 1: Scoping and Planning

The comprehensive model begins with Phase 1: Scoping and Planning, and details each step involved in this phase. This phase includes identifying the AI systems in scope, defining key performance indicators (KPIs) and setting up the review team. The Business Model Canvas and the EU AI Act are woven into these steps - for example, Step 1 links to 'Key Resources' in the Business Model Canvas, indicating the essential resources required to conduct the audit, and also corresponds to Articles 3 and 6 of the EU AI Act, highlighting the regulations that determine the scope of the AI systems.
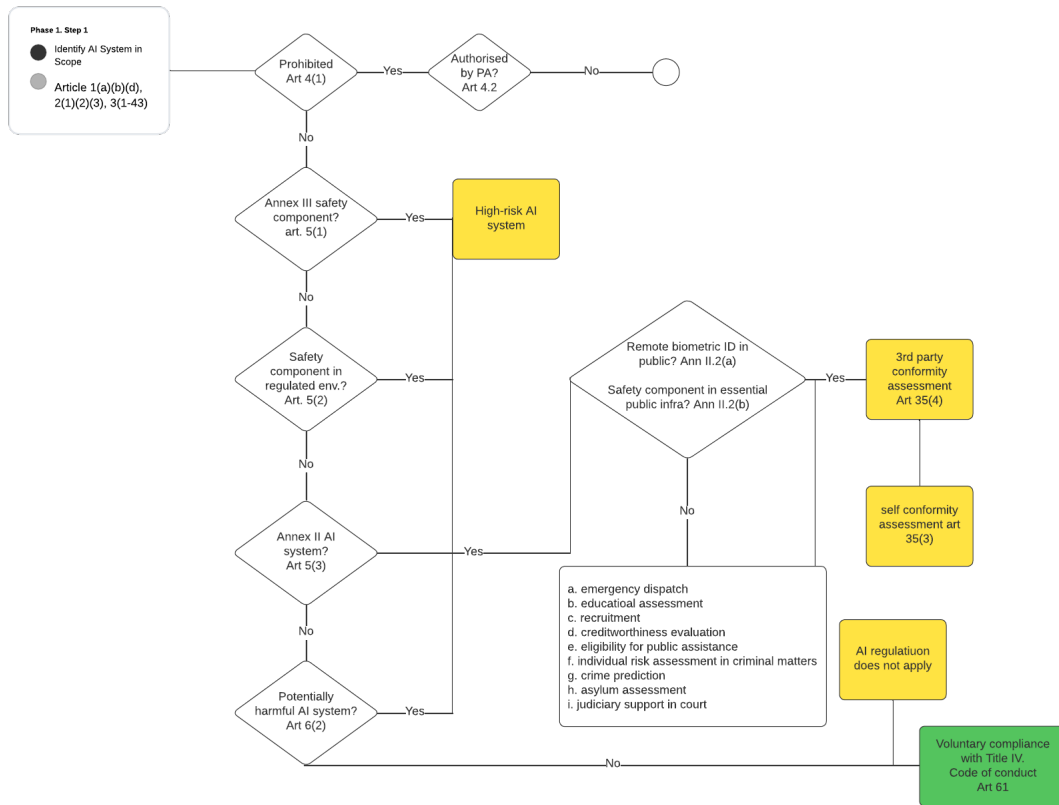

Figure 6: Phase 1: Step 1

.

Embarking on the initial step of Phase 1, as illustrated in Figure 6, the importance of this stage is paramount, laying the groundwork for the entire audit process. This stage meticulously delineates the identification process for the AI system in scope, necessitating an exhaustive examination of all elements as depicted. Figure 6 also provides a comprehensive framework for assessing whether an AI system engages in prohibited activities. This systematic evaluation assists in establishing whether

20

the AI system is operating within acceptable parameters, referencing the EU AI Act articles 4(1)(2), 5(1)(2)(3), 6(2), and 35(3)(4).

4.4.2 Subsequent Phases: From Data Collection to Follow-up

The model then proceeds to Phase 2: Data Collection and Analysis, Phase 3: Audit Execution, Phase 4: Reporting, and concludes with Phase 5: Follow-up. Each phase unfolds detailed steps that together form a systematic path to the AI audit process. These steps are deeply intertwined with the elements of the Business Model Canvas, illustrating the role of different business components at each stage. They are also linked to relevant articles of the EU AI Act, ensuring a seamless integration of legal components into the audit process.

As an illustration, Step 4: Data Collection in Phase 2 refers to 'Key Activities' and 'Key Resources' from the Business Model Canvas, indicating that data collection is a central activity that requires essential resources. At the same time, this step corresponds to Articles 12 and 20 of the EU AI Act, emphasising the importance of compliance in data collection.

The interdependencies intensify and become more complex in Phase 3. Here, for example, Step 3: Governance, Training and Third Party Relationships intersects with several components of the business model canvas ('Key Partners', 'Key Activities', 'Key Resources' and 'Value Proposition') and numerous articles of the EU AI Act (Articles 16, 24, 26, 27 and 28). This illustrates the extensive confluence of these areas in the context of governance, training and relationships with third parties.

Finally, the model culminates in the follow-up phase, which focuses on the implementation of corrective actions and the refinement of the audit model. These steps are linked to the 'Key Activities' and 'Customer Relationships' from the business model canvas and to Articles 21, 22, 10 and 84 of the EU AI Act.

Model summary
In essence, Figure 5 represents a comprehensive, integrative model that links the AI Audit Model, the Business Model Canvas and the EU AI Act. This model serves as an indispensable guide for organisations in the financial sector seeking to maintain compliance while maximising the benefits of AI technology. The comprehensive understanding of this model provides the foundation for effective AI audit implementation and further advances the field of AI audit and compliance.

4.5 Survey Analysis and Findings

This section provides an overview of the stakeholder survey conducted as part of our research methodology, with responses received from three major organizations within the financial sector. The detailed survey questions can be found in Appendix A.

The survey showed a moderate level of familiarity with the EU AI Act, indicating the need for

enhanced awareness and education within the sector. Most organizations have assigned resources for understanding and preparing for the EU AI Act, however, the assignment of specific responsibilities for this task was inconsistent, indicating a potential area for organizational improvement.

Participants reported a range of strategies for AI Act compliance, from gap analyses to specific policy implementation. Despite limited resources and complex regulations being cited as major challenges, there was a positive inclination towards undergoing an AI law audit for ensuring compliance.

The results connect well with our AI Audit Model discussed in this chapter. Despite the limited number of respondents, the feedback underscored the relevance of our proposed Audit Analysis Framework and the need for comprehensive guidelines to facilitate understanding and application of the EU AI Act within the financial sector.

5 Guidelines, Discussion, and Recommendations for AI Legislation Compliance

Given the significant impact of the EU's AI legislation on the financial sector, it is vital to ensure compliance. This chapter provides a guide that financial organisations can follow to comply with AI legislation. It highlights the implementation of the AI audit model and considers the role of ethics, corporate responsibility and compliance in AI applications. Finally, it suggests ways to ensure transparency and accountability in AI, while considering the impact of the law on innovation and competitiveness.

5.1 Guidelines for AI regulatory compliance

To effectively adapt to the rapidly evolving AI landscape, financial institutions must emphasize transparency, accountability, and the ethical use of AI systems. These pillars are at the heart of the EU's AI legislation and are echoed in discussions about applications in the financial sector [16]. To successfully address these challenges, the following extended guidelines are proposed:

1. **Risk-based approach:** The financial sector needs to recognize and adhere to the risk-based approach introduced in the EU AI Law and align its operations accordingly. This approach helps distinguish between different levels of risk associated with different AI applications. The AI audit model, as discussed in Chapter 4, provides an in-depth understanding of the risk levels of AI systems, providing a sound basis for implementing AI solutions and complying with the law.

2. **Understanding and monitoring AI systems:** Using the AI audit model (Chapter 4), financial institutions can maintain a comprehensive understanding of all operational AI systems. Regular audits and assessments should be conducted to ensure that systems are performing as expected and meeting defined KPIs. Such continuous monitoring facilitates the

timely identification and resolution of potential issues, improving the overall reliability and effectiveness of the system [25].

3. **Establish accountability mechanisms:** Accountability, as outlined in the AI Act, needs to be a fundamental aspect of all AI operations. Clearly defining the responsibilities of AI system providers, users, and third parties is critical, as suggested by Mazzini (2019)[14]. Innovative accountability frameworks, such as considering AI systems as creative employees or independent contractors, offer interesting approaches to AI accountability [25].

4. **Improve transparency:** Financial firms should take concerted steps to enhance the transparency of their AI practices. This includes providing clarity on the functionality of AI systems, openly communicating their use, and ensuring the transparency of the decision-making process. Such measures are in line with the requirements of the AI Act and increase public trust in AI practices [16].

5. **Promoting ethical AI practices:** The EU AI Act encourages the strengthening of ethical AI applications, promotes greater transparency, and strengthens data protection laws. Financial firms should respond by implementing ethical frameworks for AI systems, with a focus on data protection and user rights [6].

6. **Collaboration:** Achieving effective compliance with the Act will require collaboration between AI providers, financial firms, and regulators. Creating a common understanding of the law's requirements and developing industry-wide standards and practices could prove instrumental in fostering this collaboration. Such unified efforts can expedite the compliance process and ensure that all parties efficiently navigate the complex AI legislative landscape [23].

5.2   Discussion

The implementation of the EU AI Act in the financial sector presents a unique set of challenges and opportunities, given the complexity of the sector and the transformative impact of the Act.

Analysis of the impact of the EU AI Act
Despite the complexities, the application of the EU AI Act in the financial sector offers several advantages. The Act's risk-based approach provides a nuanced mechanism for dealing with different AI applications, fostering an environment that balances regulation and innovation [7]. However, there is a need to discuss the implications of the user-provider relationship in the financial context and its potential impact on the applicability of the AI Act. In addition, it is important to consider the role of the 'customer' stakeholder and how their interests are addressed in the Act.

Provisions such as Article 69 of the Act also provide a level of regulation for lower risk AI applications [7]. However, there are calls for greater clarity, particularly in relation to financial services within the Act's risk-based classification [14]. The real-world AI supply chain, involving numerous stakeholders, may be more complex than the Act's simplistic categorisation of 'provider' and 'user' [14].

Importantly, the Act sets a precedent for holding AI systems accountable in a legal sense [7]. It is worth mentioning that the AI WMFH (Work-Made-For-Hire) model, proposed by Yanisky-Ravid (2017) [25] and praised by Mazzini (2019) [14], treats AI systems as employees or independent contractors and could serve as a global template for AI governance.

In addition, it is important to compare this research with other frameworks in the context of AI legislation. One such framework is capAI, a conformity assessment process for AI systems [9]. capAI provides practical guidance on how high-level ethical principles can be translated into verifiable criteria to ensure the development and operation of trustworthy AI systems in compliance with the AI Act [9]. By positioning this research in relation to capAI and other academic efforts, it highlights its unique contributions and potential synergies.

Complying with the EU AI Act can be relatively expensive, resulting in higher barriers to entry for starting AI businesses or incorporating AI into existing businesses. This financial burden can make it more difficult for organisations to enter the market and adopt AI technologies, potentially affecting innovation and market competitiveness.

In summary, the implementation of the EU AI Act in the financial sector presents both challenges and opportunities. The discussion should address the implications of the user-provider relationship in the financial context, consider the role of the 'customer' stakeholder, and compare this research to other frameworks such as capAI [9]. In addition, highlighting the financial burden of compliance highlights the potential impact on market entry and innovation.

Implications
The findings of this study have important implications for policymakers, regulators and financial firms, particularly with regard to the interpretation and application of AI legislation. The AI law audit model proposed in this thesis could serve as a valuable tool to ensure compliance with EU AI law. This in turn could lead to a more ethical, responsible and transparent use of AI in the financial sector. By setting a precedent for strong AI legislation, the EU could influence other jurisdictions to adopt similar measures and create a global standard for AI regulation. This could catalyse the development of a universally accepted framework for the use of AI, aligning different sectors and regions under a common, understandable and enforceable set of rules. This global coherence in AI regulation would significantly reduce the legal ambiguity faced by multinational organisations and encourage global collaboration in AI development and deployment. In conclusion, this study highlights the need for organisations to have a robust and efficient mechanism to audit their AI systems for compliance with EU AI law. By developing and implementing such an audit model, they can significantly mitigate the risks associated with the use of AI, safeguard the interests of all stakeholders, and uphold the ethical and responsible use of AI.

5.3 Recommendations

Based on the above discussion and following the guidelines provided by Mazzini (2019)[14], this section provides a set of recommendations for the financial sector to effectively comply with the EU AI Act.

- Establish a dedicated AI compliance team: The complex legal nature of the AI Act requires a dedicated compliance team within financial firms that can ensure compliance with all aspects of the Act [14, 16].

- Invest in AI transparency technologies: Companies will need to invest in technologies that make their AI systems more understandable in order to comply with the Act's transparency requirements [7]. This could include the development of Explainable AI (XAI) models [6].

- Engagement with regulators and industry bodies: Regular engagement with regulators and industry bodies can help organisations stay abreast of changes in legislation and interpret the nuances of the law [14].

- Ongoing education and training: Given the rapidly evolving nature of AI and AI legislation, continuous education and training of employees is critical [14].

- Develop a robust data governance framework: A robust data governance framework is crucial, as many of the provisions of the law relate to the handling of data [7].

5.4 Impact on innovation and competitiveness

The impact of the EU AI Act on innovation and competitiveness in the financial sector, particularly within the European Union, requires careful consideration.

The compliance costs of the EU AI Act have raised concerns about the potential impact on innovation and competitiveness, particularly for smaller firms [16]. However, it is important to note that the Act includes explicit measures to support innovation, reduce regulatory burdens and specifically address the needs of small and medium-sized enterprises (SMEs) and start-ups. According to the AI Act itself, "additional measures are also proposed to support innovation, in particular through AI regulatory sandboxes and other measures to reduce the regulatory burden and to support SMEs and start-ups" [7, p. 3].

The establishment of AI regulatory sandboxes and other supportive measures aims to create an environment conducive to innovation by providing SMEs and start-ups with resources and opportunities to develop and test AI technologies in a controlled and supportive environment. These measures will help lower the barriers to entry for smaller companies and enable them to navigate the regulatory landscape more effectively.

While the law may initially impact the global competitiveness of the European financial sector, EU firms can use the strict regulations as a unique selling point. By emphasising ethical and trustworthy AI practices, EU firms can build a reputation for responsible AI implementation, which can be valued by global customers and investors [14]. Furthermore, EU leadership in AI regulation can influence other jurisdictions to adopt similar regulations, promoting a more standardised and ethical approach to AI on a global scale [14]. This is in line with the objectives of the EU AI Act, which is to promote a level playing field and encourage the development of more trustworthy AI systems.

It is worth noting that the EU AI Act distinguishes between SMEs and larger companies in terms of the application of compliance rules. The Act proposes a governance system at Member State level, building on existing structures, and a cooperation mechanism at Union level with the establishment of a European Artificial Intelligence Board [7]. These mechanisms will help to ensure that compliance requirements and regulatory burdens are appropriate for SMEs and take into account their specific circumstances, enabling them to participate in the AI ecosystem and contribute to innovation.

In summary, the implementation of the EU AI Act in the financial sector presents both challenges and opportunities. While the compliance burden and costs may be significant, the Act includes explicit measures to support innovation, reduce regulatory burdens and specifically address the needs of SMEs and start-ups. By effectively navigating the Act's requirements and leveraging its provisions, financial firms can contribute to innovation in the long term, position themselves competitively, and capitalise on a reputation for responsible AI implementation. The Act's distinction between SMEs and larger companies recognises the specific needs and considerations of different entities in complying with the rules [7].

6   Conclusion and Future Work

6.1   Conclusion and contributions

This thesis concludes with an in-depth analysis of the challenges faced by the EU financial sector in interpreting, applying and complying with the EU AI Act. The study highlights the growing importance of AI in the financial sector and the critical need for comprehensive and effective regulation to manage the associated risks. It highlights the importance of human intervention and accountability within AI systems, addressing concerns around the "black box" issue.

To facilitate compliance with the forthcoming EU AI Act and to promote a more regulated and ethical AI landscape, this thesis presents the AI Law Audit model as a tangible and comprehensive tool. By integrating this model with the Business Model Canvas and aligning it with the EU AI Act, financial organisations can conduct thorough and transparent audit processes to ensure regulatory compliance.

The AI Law Audit Model consists of five distinct phases: Scoping and Planning, Data Collection and Analysis, Audit Execution, Reporting and Follow-up. Each phase has been carefully designed to facilitate an efficient and detailed audit process that complies with the Act and ensures regulatory compliance.

In addition, the reccomendations section provides additional guidance and recommendations for compliance with the EU AI Act. It advocates a risk-based approach and emphasises the importance of transparency, accountability and ethical AI practices. While acknowledging the potential challenges and ambiguities of the AI Act, this thesis highlights the long-term benefits in terms of standardisation, the promotion of trustworthy AI systems, and the potential global influence of EU leadership in AI regulation.

In summary, this thesis has made a significant contribution to the understanding and implementation of AI regulation in the EU financial sector. It provides a comprehensive overview of the challenges facing financial firms in light of new AI legislation, and highlights the importance of understanding and effectively applying the EU AI Act. The development of the AI Law Audit model, integrated with the Business Model Canvas, provides a practical and layered approach to ensuring compliance with the Act. The compliance guidelines and recommendations emphasise the pillars of transparency, accountability and ethical use of AI.

Enforcement Mechanisms

It is important to note that enforcement of the EU AI Act is expected to involve a combination of national authorities within EU Member States and the European Union itself. While the Act establishes a framework for AI regulation across the EU, the specific enforcement mechanisms will likely involve coordination between the national authorities responsible for enforcing the provisions of the Act within their respective countries. In addition, the Act may provide for oversight and coordination at the EU level to ensure consistency and harmonisation of enforcement practices across Member States. The exact enforcement structure and procedures will be further defined as the EU AI Act progresses through the legislative process and subsequent implementation. In the case of the Netherlands, it is expected that enforcement will be carried out by the Autoriteit Persoonsgegevens (AP). This can be compared to the Information Commissioner's Office (ICO).

6.2 Limitations and future work

While this study makes important contributions, it also has limitations that should guide future research. The focus on a small sample of the EU financial sector limits generalisability, suggesting the need to expand the scope and sample size. Applying the AI legal audit model in real-life situations, refining it based on empirical evidence, and exploring more use cases are important for future research.

As the AI landscape and legislation evolve, regular updates to the AI Law Audit model and guidelines are recommended to ensure their relevance. Regular reviews and modifications can align with changes in the law and new insights into AI legislation.

Extending the research to other sectors and regions would provide a comprehensive understanding of AI legislation and its application. This could lead to a universally applicable audit model for AI legislation, promoting standardised interpretation and compliance across sectors and regions.

In summary, this thesis addresses the challenges and opportunities of AI regulation in the EU financial sector. The AI law audit model and associated guidelines provide practical tools for compliance with the EU AI Act. The study's contributions, along with identified limitations, serve as a foundation for future research and improvements in AI regulation and compliance.

References

[1] N. Ahmed. The de-democratization of ai: Deep learning and the compute divide in artificial intelligence research. *ArXiv*, 2020.

[2] W. C. Buczynski. The eu artificial intelligence act and financial services. *Economics, Future States, Standards, Ethics & Regulations (SER)*, 2022.

[3] J. Chen. Beyond fairness metrics: Roadblocks and challenges for ethical ai in practice. *ArXiv*, 2021.

[4] A. C. Ciobanu. Ai ethics in business – a bibliometric approach. *Review of Economic and Business Studies*, 2021. doi: 10.47743/rebs-2021-2-0009.

[5] A. Deaconu. Accounting in relation to the evolution of information and communication technologies. *Bulletin of the Transilvania University of Brasov, Economic Sciences Series*, 5 (54):27–34, 2012.

[6] L. Edwards. The eu ai act: A summary of its significance and scope. *Expert Explainer*, April 2022. URL `https://example.com/article-url`.

[7] European Commission. Regulation on a European approach for Artificial Intelligence (AI), 2023. URL `https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206`. Official Journal of the European Union, L 183/3.

[8] S. Feingold. The proposed artificial intelligence act would classify ai systems by risk and mandate various development and use requirements. *World Economic Forum*, 2023.

[9] Luciano Floridi, Matthias Holweg, Mariarosaria Taddeo, Javier Amaya Silva, Jakob Mökander, and Yuni Wen. capai - a procedure for conducting conformity assessment of ai systems in line with the eu artificial intelligence act. *SSRN*, 2022. Available at SSRN: `https://ssrn.com/abstract=4064091` or `http://dx.doi.org/10.2139/ssrn.4064091`.

[10] J. Y. Huang. Survey of eu ethical guidelines for commercial ai: case studies in financial services. *AI Ethics*, 2021. doi: 10.1007/S43681-021-00048-1.

[11] A. Joyce. The triple layered business model canvas: A tool to design more sustainable business models. *Journal of Cleaner Production*, 2016. doi: 10.1016/J.JCLEPRO.2016.06.067.

[12] M. Kop. Eu artificial intelligence act: The european approach to ai. *Stanford - Vienna Transatlantic Technology Law Forum, Transatlantic Antitrust and IPR Developments, Stanford University*, 2021. URL `https://law.stanford.edu/publications/euartificial-intelligence-act-the-european-approach-to-ai/`.

[13] E. Lachaud. Iso/iec 27701: Threats and opportunities for gdpr certification. *European Data Protection Law Review*, 2020. doi: 10.2139/ssrn.3521250.

[14] G. Mazzini. A system of governance for artificial intelligence through the lens of emerging intersections between ai and eu law. *Social Science Research Network*, 2019.

[15] M. Z. Mokhtar and M. S. Muda. Comparative study on performance measures and attributes between iso and non-iso certification companies. *International Journal of Business and Management*, 7(3):185, February 2012. URL `http://dx.doi.org/10.5539/ijbm.v7n3p185`.

[16] I. Nesterova. Questioning the eu proposal for an artificial intelligence act: The need for prohibitions and a stricter approach to biometric surveillance. *Information Polity*, 2022. doi: 10.3233/ip-211524.

[17] I. D. Raji, A. Smart, R. N. White, M. Mitchell, T. Gebru, B. Hutchinson, J. Smith-Loud, D. Theron, and P. Barnes. Closing the ai accountability gap: Defining an end-to-end framework for internal algorithmic auditing. In *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency*, FAT* '20, pages 33–44, 2020.

[18] A. Rességuier. Ai ethics should not remain toothless! a call to bring back the teeth of ethics. *Big Data & Society*, 2020. doi: 10.1177/2053951720942541.

[19] L. Ryll. Transforming paradigms: A global ai in financial services survey. *Electronic*, 2020. doi: 10.2139/ssrn.3532038.

[20] M. Shabani. The data governance act and the eu's move towards facilitating data sharing. *Molecular Systems Biology*, 2021. doi: 10.15252/msb.202110229.

[21] C. Siegmann and M. Anderljung. The brussels effect and artificial intelligence. *APSA Preprints*, 2022. doi: 10.33774/apsa-2022-vxtsl.

[22] E. Siougle. Does iso 9000 certification matter for firm performance? a group analysis of greek listed companies. *International Journal of Production Economics*, 2019. doi: 10.1016/J.IJPE. 2018.04.028.

[23] J. Truby, R. Brown, and A. Dahdal. Banking on ai: mandating a proactive approach to ai regulation in the financial sector. *Law and Financial Markets Review*, 14(2):110–120, 2020. doi: 10.1080/17521440.2020.1760454.

[24] M. Veale. Demystifying the draft eu artificial intelligence act—analysing the good, the bad, and the unclear elements of the proposed approach. *Computer Law Review International*, 2021. doi: 10.9785/cri-2021-220402.

[25] S. Yanisky-Ravid. Generating rembrandt: Artificial intelligence, copyright, and accountability in the 3a era — the human-like authors are already here — a new model. *IO: Productivity*, 2017. doi: 10.2139/ssrn.2957722.

[26] M. v. Zahn. The cost of fairness in ai: Evidence from e-commerce. *Bus. Inf. Syst. Eng.*, 2021. doi: 10.1007/s12599-021-00716-w.

[27] D. Zetzsche. Regulating artificial intelligence in finance: Putting the human in the loop. *Environment for Innovation eJournal*, 2020.

[28] D. A. Zetzsche, D. W. Arner, R. P. Buckley, and B. W. Tang. Regulating artificial intelligence in finance: Putting the human in the loop. *Environment for Innovation eJournal*, 2020.

A AI Act Compliance Survey

1. What company do you work for?

2. In which sector does your company operate? (Please select one)

   - Fintech
   - Consultancy in Finance sector
   - Finance
   - Other (Please specify: _____)

3. How many employees does your company have?

   - Less than 50
   - 50-100
   - 101-500
   - 501-1,000
   - More than 1,000

4. What is your role within the company?

5. How familiar are you with the AI Act and its requirements?

   - Very familiar
   - Somewhat familiar
   - Not familiar at all

6. Has your company allocated resources (time, personnel, or budget) to understanding and preparing for the AI Act?

   - Yes, extensively
   - Yes, to some extent
   - No, not yet

7. Is the responsibility for the AI Act preparation assigned to a specific department or function, or spread across the organization?

   - Assigned to a specific department or function (Please specify: _____)
   - Spread across the organization

8. Please briefly describe the steps your company has taken or plans to take to comply with the EU AI Act.

9. Which additional steps do you anticipate taking in the future to comply with the EU AI Act?

10. How confident are you in your company's ability to comply with the AI Act?

    - Very confident
    - Somewhat confident
    - Not confident

11. Do you believe your company will require external assistance (e.g., consultants or legal experts) to achieve compliance with the AI Act?

    - Yes
    - No

12. How would you rate the alignment of the AI Act with other relevant regulations, such as GDPR?

    - Strongly aligned
    - Somewhat aligned
    - Not aligned
    - Not sure

13. What do you perceive as the main challenges in implementing the AI Act within your company? (Select all that apply)

    - Lack of understanding about AI Act requirements
    - Resource constraints (time, personnel, budget)
    - Technical complexities
    - Organizational resistance to change
    - Other (Please specify: _____)

14. What is/are the main factor(s) through which the AI Act will impact competitiveness? (Select all that apply)

    - Increased transparency and accountability
    - Improved customer trust
    - Enhanced data protection
    - Other (Please specify: _____)

15. What is/are the main factor(s) through which the AI Act will impact innovation? (Select all that apply)

    - Encouraging responsible AI development
    - Promoting ethical AI use
    - Driving research and development

- Other (Please specify: ————————————)

16. Would your company be interested in undergoing an AI law audit to ensure compliance with the AI Act?

    - Yes
    - No

17. What do you think are the most important aspects to consider in an AI law audit? (Select all that apply)

    - Data privacy and protection
    - Transparency of AI systems
    - Fairness and non-discrimination
    - Human oversight and control
    - Other (Please specify: ————————————)

18. What do you think are the most critical legal aspects to consider in an AI law audit? (Select all that apply)

    - Compliance with AI-specific regulations
    - Intellectual property rights
    - Liability and accountability
    - Compliance with existing data protection laws
    - Other (Please specify: ————————————)

19. Has your company collaborated with other organizations within your industry to address the challenges of AI Act implementation?

    - Yes
    - No

Thank you for participating in this survey! Your responses are valuable in understanding the current state of AI Act compliance and its impact on businesses.