International Journal of Science and Research (IJSR)
ISSN: 2319-7064
Impact Factor 2024: 7.101

Risks of Using Artificial Intelligence in Financial Activities: Approaches to their Identification and Minimization

Svetlana Gadzhieva

Audit Manager at KPMG, San Francisco, USA

Abstract: ***The article focuses on the risks associated with the use of artificial intelligence in financial reporting. The purpose of this study is to identify the primary risks associated with the use of artificial intelligence in the financial statement preparation process and to develop strategies to mitigate them. The study hypothesizes that the use of a risk management system specifically designed to consider the features of AI can significantly reduce the likelihood of errors and abuses in the process of forming financial statements. The relevance of the study is that in recent years, the use of artificial intelligence (AI) technologies in various industries has increased significantly, including financial reporting. The introduction of AI into financial processes promises to increase efficiency, improve the accuracy of reports, and reduce data analysis time. However, the use of AI is also associated with many risks that can affect the reliability of financial information and, as a result, management decision - making. In conclusion, it is concluded that despite the significant advantages that artificial intelligence provides in the field of financial reporting, it is necessary to carefully consider the risks that arise. Identifying and minimizing these risks requires an integrated approach that includes data quality management, algorithm transparency, model testing, performance monitoring, and compliance with regulatory standards.***

Keywords: AI, financial reporting, accounting, minimization, identification, standards

1. Introduction

With the development of technology, artificial intelligence (AI) is becoming an increasingly important tool in the field of financial reporting. However, along with its benefits, such as increased efficiency and accuracy, the use of AI also entails certain risks. In this article, we will consider the main risks of using AI in financial reporting and approaches to identifying and minimizing them [1].

2. Materials and Methods of Research

To achieve the stated goal, the following materials and methods were used in the study: literature analysis (study of scientific articles, reports and standards in the field of accounting and financial analysis, as well as publications devoted to the use of AI in business), the use of quantitative methods for processing the collected data to identify patterns and establish relationships between risks and their impact on the quality of financial reporting.

3. Results and Discussions

One of the significant risks of using AI in financial reporting is the possibility of leaking personal data. Storing and processing large amounts of information, including the personal data of clients, creates vulnerabilities that can be used by hackers to carry out cyberattacks. Modern AI - based solutions can facilitate the emergence of more complex types of attacks, such as falsifying data, using fake reports, or attacking the critical infrastructure of financial institutions. When client information is leaked, organizations may face not only financial but also reputational damage [3].

Many AI models, especially those based on deep neural networks, are “black boxes, ” meaning it is difficult to understand how decisions are made and on what basis. This lack of transparency makes it difficult to monitor the AI’s actions, which can lead to errors or misconduct if, for example, the system decides to approve a loan based on inaccurate information. In the financial sector, where every decision can have serious consequences, this flaw can be extremely dangerous. Although AI systems are good at data analytics, they are not foolproof. Misunderstandings of data, lack of context, or even random errors in processing can lead to AI “hallucinations,” where the system generates unreliable information. This could cause serious financial damage if decisions based on such data are wrong [2].

As AI adoption in financial practices increases, concerns arise about over - reliance on automated systems. Financial institutions must take a balanced approach that combines the strengths of AI with human expertise. With the ability to learn and adapt, humans can provide a more critical view of the system’s performance, which can help avoid errors and improve decision - making [4].

Table 1: Risks of using AI

1	Threats to data privacy and security	Artificial intelligence (AI) requires access to significant amounts of financial data, increasing the likelihood of unauthorized use, theft, or distortion. Moreover, financial systems using AI are susceptible to cyberattacks and data breaches, which can lead to financial losses, reputational damage, and regulatory sanctions.
2	Bias in model outputs	Artificial intelligence that is trained on biased or incomplete data may produce incorrect results. This may lead to distorted decision - making and possible financial losses.
3	Dependency on third - party suppliers	The use of specialized hardware, cloud services, and pre - trained models increases the risk of dependence on external suppliers.

The use of artificial intelligence (AI) in financial reporting creates new risks that need to be carefully assessed and managed. In this context, several approaches are highlighted that allow identifying and minimizing the risks associated with the use of AI:

1) **Benchmarking**
   Benchmarking is the process of comparing your model with the most successful models used by other organizations. This approach allows you to understand which methods and practices have proven most effective in similar conditions, as well as identify potential weaknesses in your system. When benchmarking, it is important not only to compare the model's performance but also to analyze the context in which it operates. Effective practices can serve as a good guide for improving your algorithms and reducing risks [5].
2) **Stress testing**
   Stress testing involves testing the resilience of a model to extreme but plausible shocks. This approach involves modeling various scenarios that could lead to high risks or losses, such as changes in macroeconomic conditions or sudden market fluctuations. Stress testing helps identify model vulnerabilities and enables a strategy to be developed in advance to respond to potential risks.
3) **Backtesting**
   Backtesting is a method of testing a model on historical data. It helps to assess how well it will work in real conditions. The main goal of backtesting is to identify discrepancies between the model's predictions and actual results. This method allows not only the assessment of the effectiveness of the model but also the identification of its possible weaknesses that can lead to errors in the future.
4) **Cross - validation (cross - validation)**
   Cross - validation involves dividing the data into training and testing sets. The model is trained on one set of data and tested on another. This method helps to avoid overfitting the model when it is too adjusted to the training data and cannot generalize to new data. Cross - validation helps to provide a more reliable assessment of the model's performance and increases its resilience to unexpected changes in the external environment [6].
5) **MPP approach**
   MPP (Model Performance Monitoring) is an approach that involves creating an auxiliary model that monitors the performance of the main model. This auxiliary model is trained on the errors of the main model, which allows for a quick response to deterioration in its performance and adjustment of algorithms. The MPP approach ensures continuous monitoring of the model's performance and rapid identification of potential risks associated with its use.

One of the most significant vulnerabilities of AI algorithms is their high sensitivity to changes in customer behavior, especially during economic crises or other stressful situations. For example, a sudden change in purchasing behavior or a mass exit of customers from financial products can lead to a disruption of the usual relationships. This, in turn, can cause failures in the algorithms, as they may not adapt to new conditions and continue to act based on outdated data. AI systems are trained on specific examples, which can cause distortion of information. If the system encounters data that is outside its training set, it may not provide correct results. As a result, financial statements may become not only irrelevant but also misleading. This is especially true for non - standard situations when the system must make decisions based on data that was not considered during training [7].

Risks associated with personal data leakage are also a significant issue. Data containing sensitive information, such as banking or tax data, may be used to train AI models. This creates the risk of unauthorized access to such information, which can have serious consequences for both customers and the company itself. In addition, fraudulent attacks can be launched against AI systems, which further aggravates the situation. Equally important is the issue of the ethics of using AI in the financial sector. Machine logic can sometimes seriously contradict human notions of fairness and ethics. For example, AI systems may consider discriminatory factors, such as the religion or race of customers, when assessing risks or setting prices. This can lead to ambiguity in decision - making and even legal consequences for companies.

Using AI solutions from third - party providers, including cloud computing and external databases, also entails its risks. This may lead to data leaks, difficulties in interpreting AI results, and inconsistencies in data processing methodology. Outsourcing may increase operational risks and reduce the level of control over processes related to data processing and analysis [8].

To ensure the safety and reliability of financial data, it is important to apply proactive measures to minimize threats. Incorrect use of AI can lead to both financial losses and reputational risks for companies. In this regard, approaches to risk minimization are becoming more relevant than ever.

The first and perhaps most significant approach is the implementation of ethical AI principles and explainable algorithms. Ethical AI involves developing technologies that consider not only the benefits of use but also the consequences for users and society. Such technologies reduce the risk of fines from regulators and ensure transparency in decision - making. Explainable algorithms, in turn, allow us to understand how and why AI came to certain conclusions. This is critical in the financial sector, where customers need

to know how the system that makes decisions about loans, investments, and other financial transactions works. Transparency helps increase customer trust, which is a key factor in a successful business [9].

Detailing self - regulatory mechanisms is also an important tool in risk management. Voluntary adoption of certain ethical principles by market participants is a step towards forming a responsible approach to the use of AI. Codes and charters developed with the participation of experts and stakeholders help establish norms of behavior and expectations regarding the use of AI. Self - regulation creates a space for open dialogue, where market participants can exchange experiences and best practices, which ultimately leads to improved technologies and reduced risks.

An equally important measure is the development of appropriate legislative regulations and rules that would govern the use of AI in the financial sector. Legislation should be flexible enough to keep up with the rapid changes in the world of technology and, at the same time, strict enough to ensure the protection of clients' interests. Regulation can include requirements for testing algorithms, their explainability, and the use of ethical principles in the development and implementation of new technologies. This not only minimizes risks and protects clients but also creates a more sustainable and responsible ecosystem for all market participants [10].

One of the main approaches to minimizing risks is to implement reliable data protection rules. Financial institutions must ensure that all customer data is stored and processed following high - security standards. Effective security measures include data encryption, multi - user authentication, and intrusion detection systems. Such actions will help prevent unauthorized access to the system, minimize the risk of information leakage, and protect customers' data from theft. Artificial intelligence is becoming an important tool in the financial sector, but it also entails new risks. AI systems must be carefully monitored and evaluated to ensure that they are fair and do not reinforce existing biases. Ensuring transparency of algorithms and regular audits can help in this regard. In addition, it is necessary to consider ethical aspects and develop systems that can withstand bias, maintaining a balance between the interests of customers and institutions.

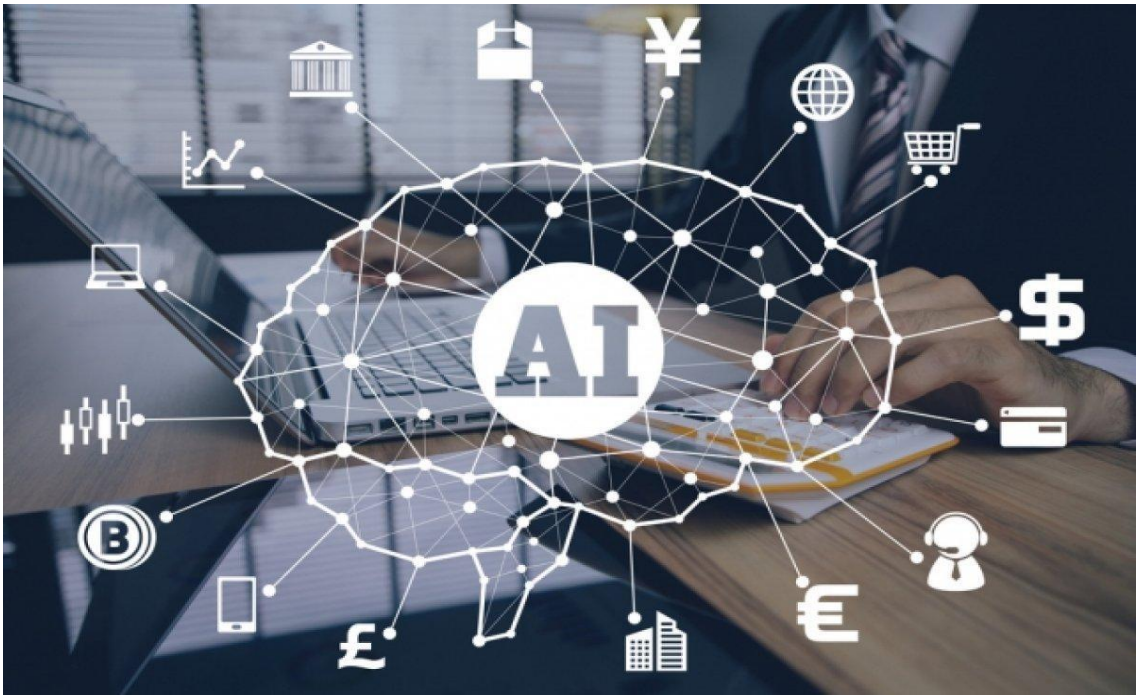

Figure 1: AI in the financial sector

Work on accountable AI technologies is already underway at many financial institutions. These technologies allow for transparent explanations of AI - based decisions, which in turn helps build trust with customers and reduce fraud risks. For example, developing templates to explain AI decisions can help customers better understand how certain financial decisions were made, thereby increasing trust in the institution. To minimize the risks associated with the use of AI in the financial sector, it is necessary to develop strict legislative norms and rules. Regulators should pay attention not only to the implementation of new technologies but also to the protection of customer interests. This includes creating standards for the use of AI in lending, risk assessment, and other processes, which will make the financial system safer and more predictable [1].

Financial institutions should also actively use model risk mitigation techniques to ensure the accuracy and robustness of their predictions. These techniques include benchmarking, stress testing, backtesting, cross - validation, and the MPP approach. These tools allow for the analysis and evaluation of the performance of the models used to assess risks and provide insight into how various factors may affect the results.

Training employees working with AI will help to increase their awareness of potential risks and methods to minimize them. Competent specialists play a key role in the successful integration of AI into financial reporting [12].

4. Conclusion

Thus, despite the significant benefits that artificial intelligence provides in the field of financial reporting, it is necessary to be attentive to the risks that arise. Identifying and minimizing these risks requires a comprehensive approach, including data quality management, algorithm transparency, model testing, performance, and compliance with regulatory standards. Implementing best practices will allow you to make the most of the capabilities of AI, ensuring the reliability and accuracy of financial reporting.

References

[1] Kirilyuk I. L. Model risks in the financial sector in the context of using artificial intelligence and machine learning // Russian Journal of Economics and Law.2022. T.16, No.1. P.40 - 50. DOI: http: //dx. doi. org/10.21202/2782 - 2923.2022.1.40 - 50

[2] Timoshenko F. S. Controlling model risk: best practices of financial modeling in the budgeting process // State audit. Law. Economy.2016. No.1. P.37 - 42.

[3] Zverkova T. N. Risks of generative artificial intelligence in financial intermediation and approaches to their assessment. *Siberian financial school.2*024; (3): 34 - 43. https: //doi. org/10.34020/1993 - 4386 - 2024 - 3 - 34 - 43

[4] Butenko E. D. Artificial intelligence in banks today: experience and prospects // Digest - finances.2020. Vol.25, No.2 (254). P.230 - 242. https: //doi. org/10.24891/df.25.2.230

[5] Letov O. V. Ethical aspects in the field of artificial intelligence development (Review) // Social and humanitarian sciences. Domestic and foreign literature. Ser.3: Philosophy.2024. No.1. P.34 - 44. https: //doi. org/10.31249/rphil/2024.01.03

[6] Vashenyak N. E. Risks for business in connection with the use of artificial intelligence. How to avoid litigation? // Current research.2023. No.49 (179). Part II. P.48 - 50. URL: https: //apni. ru/article/7740 - riski - dlya - biznesa - v - svyazi - s - ispolzovaniem

[7] Fedorova I. A., Orunov A. B. ARTIFICIAL INTELLIGENCE IN THE FINANCIAL SPHERE: MODERN REGULATION PRACTICE // International Student Scientific Bulletin.2023. No.1.; URL: https: //eduherald. ru/ru/article/view?id=21176 (date of access: 15.03.2025). DOI: https: //doi. org/10.17513/msnv.21176

[8] Kashevarova N. A., Panova D. A. Analysis of modern practice of applying artificial intelligence technology in the financial sector and its impact on the transformation of the financial ecosystem / Creative Economy. - URL: https: //creativeconomy. ru/lib/110708?ysclid=ld0cr9y08u596522666 .

[9] Gorbacheva T. A. DIRECTIONS OF USE OF MACHINE LEARNING IN THE FINANCIAL INDUSTRY // Bulletin of the Altai Academy of Economics and Law.2025. No.2 - 2. P.157 - 163 URL: https: //vaael. ru/ru/article/view?id=3997 (date of access: 03/15/2025).

[10] Lotosh, M. R. Barriers to the implementation of artificial intelligence in Russian banks: dimensions, reasons, timing and ways to overcome / M. R. Lotosh, V. V. Platonov, P. P. Tkalich // Issues of innovative economics. - 2021. - Vol.11, No.1. - P.315 - 332. - DOI 10.18334/vinec.11.1.111529

[11] Golodryga L. V. PROSPECTS FOR IMPLEMENTING ARTIFICIAL INTELLIGENCE TECHNOLOGIES IN THE FINANCIAL SPHERE // Proceedings of the International Scientific Conference "Student Scientific Forum 2025".2023. No.14. P.119 - 122; URL: https: //publish2020. scienceforum. ru/ru/article/view?id=757 (accessed: 03/15/2025).

[12] Hess T., Matt C., Benlian A., Wiesböck F. Options for Formulating a Digital Transformation Strategy // MIS Quarterly Executive. – 2016. – Vol.15. – No.2. – pp.123–139. DOI: 10.7892/BORIS.105447