School of Social Sciences

Master in Business Administration (MBA)

Postgraduate Dissertation

A Literature Review of the Impact of Artificial Intelligence into Risk Management

Dimitrios E. Souflas

Supervisor: Apostolos Bournetas

Athens, Greece, May 2025

A Literature Review of the Impact of Artificial Intelligence into Risk Management

Dimitrios E. Souflas

Supervising Committee

Supervisor:
Apostolos Bournetas
Hellenic Open University

Co-Supervisor:
Persefoni Polychronidou
Hellenic Open University

Athens, Greece, May 2025

I would like to express my deepest gratitude to my family, Yiouli, Eleana and Marilia, for their patience, understanding, and unwavering support throughout this journey. Their encouragement and belief in me have been invaluable, providing me with the strength and motivation to complete this dissertation.

I also wish to acknowledge the opportunities I have had through my professional experiences. Each role I have undertaken has contributed to my knowledge, shaping my perspective on risk management and artificial intelligence. The challenges I faced and the lessons I learned in my career have been instrumental in developing this research.

This work is dedicated to my father Evaggelos Souflas and my mother Maria Soufla who taught me the importance of personal integrity, ethics and human values and continues to teach the same values to my own children.

.

Abstract

This dissertation evaluates Artificial Intelligence (AI) effects on Risk Management functions and demonstrates how AI technologies improve conventional methods of risk identification, assessment, and mitigation. This research explores how AI applications including machine learning, neural networks, predictive analytics and explainable AI become integrated into risk management for financial sectors, cybersecurity operations, and operational risk management domains.

Is also outlines the major drawbacks of traditional risk management which typically face challenges due to data overload and reactive decision-making while relying heavily on human resources. Artificial Intelligence technologies resolve these issues by enabling real-time monitoring and predictive modeling alongside automated risk assessment to enhance both efficiency and accuracy. The comparative evaluation between AI-based and conventional risk management models demonstrates that AI takes precedence over predictive accuracy while being more adaptable and better at integrating multiple data sources.

Research shows that AI-based risk management strengthens proactive decision-making while building better defenses against new threats. The dissertation ends by advising organizations on how to effectively use Artificial Intelligence in Risk Management through strategic implementation and continuous monitoring while maintaining transparency.

Keywords

Artificial Intelligence (AI)

Risk Management

Machine Learning (ML)

Predictive Analytics

Cybersecurity Risk

Financial Risk Assessment

Περίληψη

Η συγκεκριμένη διατριβή αξιολογεί τις επιπτώσεις της Τεχνητής Νοημοσύνης (AI) στις λειτουργίες Διαχείρισης Κινδύνου και αναδεικνύει τον τρόπο με τον οποίο οι τεχνολογίες Τεχνητής Νοημοσύνης βελτιώνουν τις συμβατικές μεθόδους αναγνώρισης, αξιολόγησης και μετριασμού των κινδύνων. Η έρευνα εξετάζει πώς οι εφαρμογές Τεχνητής Νοημοσύνης, συμπεριλαμβανομένης της μηχανικής μάθησης, των νευρωνικών δικτύων, της προβλεπτικής αναλυτικής και της ερμηνεύσιμης AI, ενσωματώνονται στη διαχείριση κινδύνου σε τομείς όπως τα χρηματοοικονομικά, η κυβερνοασφάλεια και η διαχείριση επιχειρησιακών κινδύνων.

Επιπλέον, περιγράφονται τα κύρια μειονεκτήματα της κλασικής διαδικασίας διαχείρισης κινδύνου, η οποία συνήθως αντιμετωπίζει προκλήσεις λόγω του υπερβολικού όγκου δεδομένων και της αντιδραστικής λήψης αποφάσεων, ενώ εξαρτάται σε μεγάλο βαθμό από ανθρώπινους πόρους. Οι τεχνολογίες Τεχνητής Νοημοσύνης επιλύουν αυτά τα ζητήματα επιτρέποντας τη συνεχή παρακολούθηση σε πραγματικό χρόνο και τη δημιουργία προβλεπτικών μοντέλων, παράλληλα με την αυτοματοποίηση της αξιολόγησης κινδύνων, ενισχύοντας έτσι τόσο την αποδοτικότητα όσο και την ακρίβεια.

Η συγκριτική αξιολόγηση μεταξύ των παραδοσιακών και των βασισμένων στην AI μοντέλων διαχείρισης κινδύνου καταδεικνύει ότι η Τεχνητή Νοημοσύνη υπερέχει σε προβλεπτική ακρίβεια, ενώ είναι πιο προσαρμοστική και ικανή να ενσωματώνει πολλαπλές πηγές δεδομένων.

Η έρευνα δείχνει ότι η διαχείριση κινδύνου με τη χρήση Τεχνητής Νοημοσύνης ενισχύει την προληπτική λήψη αποφάσεων, ενώ συμβάλλει στην καλύτερη άμυνα έναντι νέων απειλών. Η διατριβή καταλήγει με προτάσεις προς τους οργανισμούς για την αποτελεσματική αξιοποίηση της Τεχνητής Νοημοσύνης στη Διαχείριση Κινδύνου, μέσω στρατηγικής εφαρμογής και συνεχούς παρακολούθησης, διασφαλίζοντας παράλληλα τη διαφάνεια.

Λέξεις – Κλειδιά

Τεχνητή Νοημοσύνη

Διαχείριση Κινδύνου

Μηχανική Μάθηση

Προβλεπτική Αναλυτική

Διαχείριση Κυβερνοασφάλειας

Αξιολόγηση Χρηματοοικονομικού Κινδύνου

Contents

1. Introduction

1.1. Background and Context

The examination of risk management began, in a systematic way, after the 2nd world war. Since then, many techniques have been developed and various risk management approaches have been applied in a variety of fields. (Banks, 2013)

Risk management is the systematic process of identifying, assessing, and mitigating threats or uncertainties that can affect an organization. It involves analyzing risks' likelihood and impact, developing strategies to minimize harm, and monitoring measures' effectiveness. (Williams et al, 2013, Harvard Business School).

Furthermore, in the last decade, Artificial Intelligence (AI) has emerged as a transformative technology due to its capacity to analyze and utilize vast amounts of data, generate predictive insights, and support decision-making processes. (Enholm et al).

AI is the ability of a machine to imitate human-like capabilities such as reasoning, learning, planning and creativity. It enables technical systems to perceive their environment, deal with what they perceive, solve problems and act to achieve a specific goal. The computer receives data - already prepared or gathered through its own sensors such as a camera - processes it and responds. AI systems are capable of adapting their behavior to a certain degree by analysing the effects of previous actions and working autonomously. (WebPortal of European Parliament, "What is artificial intelligence and how is it used?", https://www.europarl.europa.eu/topics/en/article/20200827STO85804/what-is-artificial-intelligence-and-how-is-it-used)

Especially in the field of risk management, AI is very promising by enhancing traditional risk assessment techniques and enabling organizations to adopt more effective, efficient, and proactive approaches to risk mitigation (Jordan & Mitchell, 2015).

Furthermore, Artificial Intelligence can significantly enhance the process of risk identification, leveraging capabilities such as the existence of continuous, iterative risk-management processes that span the entire lifecycle of the AI system. (REGULATION (EU) 2024/1689).

Risk management relied, for years, on manual analysis and static models that could not keep pace with the dynamic nature of modern risk landscapes, often resulting in a reactive rather than proactive approach. By integrating Artificial Intelligence in the Risk Management processes, organizations may utilize predictive models, automate risk assessments, and respond to potential threats rapidly and accurately. (Yuqi, Xue. (2021))

As organizations face increasingly complex and interconnected risks—including financial, operational, cybersecurity, and compliance threats—the role of AI in risk management has become more and more crucial. Machine learning algorithms, neural networks, and predictive analytics are now being employed to develop comprehensive risk management systems that not only forecast risks but also provide recommendations for timely intervention. For executives and managers, AI offers a strategic tool that improves decision-making capabilities, allowing leaders to shift from reactive to proactive risk management practices (Baryannis et al., 2019).

1.2. Purpose and Objectives

As a contribution to the discipline, its objective is to critically analyze the impact of AI in Risk Management through theoretical, methodological and practical perspectives on the adoption of AI technologies in Risk Management. This study aims at exploring the advantages, disadvantages and effectiveness of AI for augmentation of Risk Management procedures through a comparative analysis of traditional approaches, with their AI powered counterparts. It will further examine practical case studies focusing on how organizations are leveraging AI to mitigate a range of risks, with insights on the relative benefits and downsides of implementing AI for risk management.

After the analysis of the role of Artificial Intelligence in Risk Management, the detection of the advantages, the future challenges and the gaps will be discussed.

1.3. Rationale for the Study – Key benefits and challenges for organizations and society

AI technologies enable fast and accurate processing of expansive data sets, improving precision in risk assessment and allowing for the quicker identification of potential issues. Risk management is no longer a retrospective process – it offers real-time information and intelligence, enabling organizations to react to risk faster and smarter.

AI improves data-driven decision-making by recognizing patterns and trends that might not be obvious to human analysts. It uses the data of the past to predict the future threats, based on machine learning algorithms to help organizations prepare early for threats.

Use of AI enables data-informed decision making by analyzing patterns and trends that might not be easily discernible to human analysts. AI analyzes historical information to forecast future risks, which helps organizations preempt potential threats. (Barnea, 2020)

The need for good data management practices and trust in AI-empowered risk management system through transparency and explainability are fundamental for practical and effective AI risk management. AI in risk management can be crucial for enterprises, as it

strengthens risk identification, evaluation, and mitigation, which ultimately improves enterprise resilience and decision-making; still, challenges persist for society and industries.

The task of the current literature review is to address the following objectives in order to achieve the aim of this thesis, as outlined above.

- Exploring AI Technologies & Techniques: AI Technologies e.g. machine learning, neural networks and predictive analytics, along with applied mechanisms with respect to Risk Management needs to be studied.
- Insight into Practical Use Cases through Case Studies: They would also reflect the specific implementation of artificial intelligence in real world within Risk Management across different sectors. This will provide pragmatic perspectives on the benefits, limitations and implications of AI-aid approaches in the field of risk management.
- Comparison of risk management based on traditional techniques and based on artificial intelligence: A comparative analysis will be performed between risk management based on traditional techniques and risk management based on artificial intelligence, assessing the strengths, weaknesses and effectiveness of the two methods.
- Recognising and grasping the strategic implications for management: This refers to the impact of AI-based risk management in support of strategic decision-making by senior and middle managers, proactive principles to risk, among other considerations.
- Report of challenges and future perspectives for further research: The main challenges in the use of the artificial intelligence approach to risk management, addressed for example to ethical, regulatory and technical barriers need to be recorded. These challenges in answering questions in this area will be noted, including suggestions for further research.

This dissertation creates contributions in stringent academic, but also professional fields. From an academic view, it adds to the existing literature on AI in Risk Management, identifying how AI applications are redefining the processes of risk identification, risk assessment and risk mitigation. The present study offers a detailed study of the theoretical structures as well as the functional solutions for Artificial Intelligence since the purpose of this research. It meets a gap in literature regarding thorough exploration of this area.

The advantages and disadvantages of implementing Artificial Intelligence in Risk Management, will be of particular interest to those in leadership positions. As organizations increasingly embrace AI technologies, it is essential to understand the impact these

applications have on risk management processes to make informed strategic choices that may enhance organizational resilience and responsiveness.

1.4. Outline of the Dissertation

This thesis is structured to provide a comprehensive analysis of the impact of Artificial Intelligence (AI) on Risk Management (RM), beginning with an introduction to the basic framework of AI and RM, followed by a critical review of existing literature, practical applications through case studies, a comparative analysis of AI-driven and traditional methods, and concluding with recommendations, limitations, and suggestions for future research.

The structure and the main contents of each chapter are the following:

Chapter 2: Methodology and Limitations

It includes the Literature review methodology focusing on systematic and thematic analysis, the databases used with inclusion/exclusion criteria, the keywords used to define the research questions, the categorization of publications/articles/journals and finally the limitations that have to be followed.

Chapter 3: Review of Existing Literature

This chapter provides a thorough analysis of earlier research, summarizing methods, predetermined conclusions, and theoretical frameworks before pointing out any potential similarities or differences between studies. It includes presentation of traditional approaches to risk management, the key AI concepts and technologies relevant to risk management, an introduction of the way AI transforms risk identification, assessment, and mitigation processes, some AI -Driven Applications in specific risk domains and finally, we will define unexplored areas in AI-driven risk management research.

Moreover, it covers topics related to the ways that AI evolves all steps of risk management, such as risk identification, assessment, mitigation and monitoring. Finally, issues related to challenges and ethical considerations will be presented, like AI biases and data inefficiency.

Chapter 5: Business Case Studies / Practical Applications

This chapter analyzes how Artificial Intelligence is used and how it can improve contemporary risk management to three specific cases, in the fields of credit risk, cybersecurity and operational risk. At the end of this chapter a synthesis of lessons learned and cross-industry insights will be presented.

Chapter 6: Conclusion and Recommendations

Firstly, the main differences and similarities identified in the fields of application of AI technology in risk management will be presented. Then, a summary of the strengths and limitations identified from the use of AI technology will be presented, and the trends emerging in immediate rather.

In addition, proposals for additional research will be recorded on topics that either arose during the development of the thesis, or could not be covered due to limitations in scope.

2. Methodology and limitations

2.1. Research Approach

This dissertation employs a literature review methodology, focusing on thematic analysis to examine the influence of Artificial Intelligence (AI) on risk management. Finding, analyzing, and putting together relevant academic papers, industry reports, mainly from the last ten years (2015–2024), and case studies is part of this method. We do this to ensure that the results accurately reflect current trends and practices.

Key research questions such as "how AI enhances risk management," "what challenges exist in AI implementation," and "how AI-driven approaches differ from traditional methods" guided the literature review. I utilized databases such as ELSEVIER SCOPUS/SCIENCE DIRECT, RESEARCHGATE, and SEMANTIC SCHOLAR to locate peer-reviewed articles, using search terms like "AI in risk management," "machine learning in risk assessment," and "predictive analytics for risk." I selected articles based on their relevance, methodological rigor, and contributions to the designated topic areas of this study.

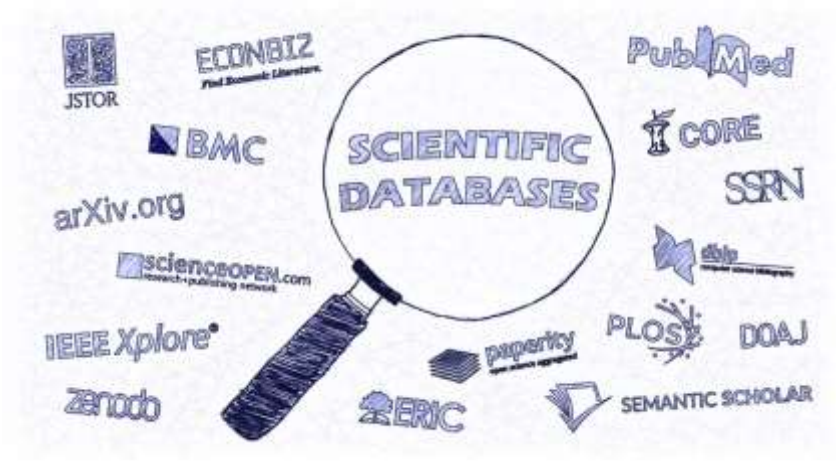

Image Source: https://enriquemoralesorcajo.com/scientific-databases-which-one-should-you-use/ - Scientific databases – which one should you use

I used a thematic analysis to classify and assess the reviewed material, highlighting recurring patterns and key themes. The method involved sorting data from certain studies into themes, such as AI's ability to predict the future, its role in cybersecurity and supply chain risk management, and the moral problems that come up when AI is used. The theme study provided a methodical framework to examine the influence of AI technology on traditional risk management practices across several industries. This methodology enabled a comprehensive knowledge of AI's strengths, limitations, and practical applications by thematically categorizing

related material, thus building a foundation for critical analysis and comparative evaluations in later chapters.

2.2. Data Sourcing / Selection of bibliographic sources

The dissertation will rely on secondary data, including peer-reviewed research articles, scientific papers, government publications (e.g. European Regulations or Directives), information from web sites or published books to gather comprehensive insights into AI applications in risk management.

The main sources of information will be specific web sources such as ELSEVIER SCOPUS/SCIENCE DIRECT, RESEARCHGATE and SEMANTIC SCHOLAR that I can access through the National Library of Greece e-services and Google Scholar.

Literature review of this dissertation aims to summarize the research already accomplished with regard to the topic. This dissertation also provides an extensive review of academic publications, papers, and articles on the applications of Artificial Intelligence in Risk Management.

I reviewed existing literature organized thematically extracted using keywords such as "AI in risk management", "machine learning in finance"}, and "predictive analytics in risk".

This literature review identifies gaps in the literature and lays the groundwork for future research efforts geared at enhancing the adoption of AI technologies in risk management systems. To evaluate the credibility of each source I used the CRAAP test methodology. The CRAAP test was developed by the California State University in 2004 to help students remember best practices for evaluating content.

The 5 components of the CRAAP test are:

- **C**urrency: Is the source up-to-date?
- **R**elevance: Is the source relevant to the research?
- **A**uthority: Where is the source published? Who is the author? Are they considered reputable and trustworthy in their field?
- **A**ccuracy: Is the source supported by evidence? Are the claims cited correctly?
- **P**urpose: Is there a motive behind publication of the source?

2.3. Keywords and Search Strategy

A targeted keyword-based search strategy was used to find relevant AI risk management papers for a full literature evaluation. According to the dissertation's main themes, keywords included "Artificial Intelligence in risk management," "machine learning in financial risks,"

"predictive analytics for operational risks," "AI in cybersecurity," and "neural networks in compliance."
The search was further refined with domain-specific terms like "credit risk assessment," "fraud detection," and "supply chain disruption prediction".

AND, OR, and NOT were used to refine search queries and remove irrelevant results. The search was undertaken across ScienceDirect, Semantic, and Google Scholar for peer-reviewed articles published between 2015 and 2024 to include recent AI and risk management advances.

The search method prioritized high-quality publications with filtering. Filters included publication type (journal articles, conference papers) and risk domain relevance. Following seminal article citations led to further resources, and backward snowballing traced field foundational investigations.

This structured and systematic methodology identified literature that addressed major research topics and balanced theoretical, methodological, and practical viewpoints.

2.4. Categorization of Publications

The publications identified through the keyword search were categorized into three primary domains: financial risk, cybersecurity and operational risk. This categorization was essential for organizing the literature and aligning it with the thematic areas addressed in the dissertation.

Publications under financial risk focused on topics such as credit scoring, fraud detection, and investment risk analysis, highlighting how AI models like machine learning and predictive analytics enhance traditional financial risk management practices.

Studies in cybersecurity risk examined the application of AI in threat detection, anomaly identification, and proactive responses to cyberattacks, showcasing the effectiveness of neural networks and deep learning algorithms in improving organizational security.

For operational risk, the literature emphasized AI's role in supply chain risk management, with case studies demonstrating its ability to predict disruptions and optimize logistics.

This categorization enabled a structured analysis of AI's impact across these diverse risk domains, providing a foundation for critical comparisons and practical insights in subsequent chapters. By organizing the literature into these three categories, the review captured a comprehensive view of AI's multifaceted contributions to risk management.

2.5. Limitations of the study

This dissertation analyzes AI's impact on risk management; however, it has limits.

Firstly, the study uses only secondary data, making it difficult to assess AI's impact on risk management systems. Organizational AI implementation data may provide greater detail.

Secondly, AI technologies are evolving swiftly, and new advancements may change AI risk management. Some findings and conclusions may become obsolete as AI models and methodologies improve.

Finally, this study focuses on finance, cybersecurity, and supply chain management, which may limit its applicability to healthcare and education. However, I cannot do my study in a fair period if I don't limit to these sectors.

The lack of openness of AI models, especially of deep learning algorithms, makes risk management evaluation difficult. These models lacked transparency, making AI risk management decision-making harder to understand (Miller, 2019).

3. Chapter 3: Review of Existing Literature

3.1. Risk Management

From the perspective of ISO 31000:2022, risk management is a set of "coordinated activities to direct and control an organization concerning risk." This description highlights the need for a disciplined process for managing the uncertainties that could impact an organization's goals. Risk, in this definition, is defined as "the effect of uncertainty on objectives," embracing the uncertainty that attends to goals organizations are trying to achieve. (ANSI/ASSP/ISO 31000-2018 Risk Management - Guidelines)

Risk management fundamentally should be designed to preserve and create value within an organization. Through sound risk management, organizations can improve performance, drive innovation and ensure strategic objectives are achieved.

The risk management principles share an ideal of perfect integration into an organization's governance structure and decision-making processes as defined in Chapter 4 of ISO 31000:2022. Risk Management is not a random activity.

Key steps in risk management include:

- **Identifying Risks**: Recognizing potential risks.
- **Rik Analysis - Assessing and Evaluating Risks**: Evaluating the likelihood and potential impact of identified risks and comparing assessed risks against predefined criteria to determine their significance.
- **Mitigating Risks**: Planning and Implementing measures to reduce the likelihood or impact of risks.
- **Monitoring and Reviewing Risks**: Continuously tracking threats and the effectiveness of mitigation measures and regularly updating risk assessments and mitigation strategies to adapt to new threats and changes in the organization's environment.

(ANSI/ASSP/ISO 31000-2018 Risk Management – Guidelines, COSO Enterprise Risk Management – Integrated Framework, Project Management Institute's (PMI) PMBOK Guide, Chapter on Risk Management)

Image Source: https://www.alertmedia.com/blog/risk-management-lifecycle/ - Risk Management Lifecycle: 5 Steps to a Safer, More Resilient Organization

The structured risk management process delineated in ISO 31000:2022 is a useful resource that helps an organization navigate its journey through uncertainty, toward achieving its objectives. In this sense, thanks to identifying, evaluating, treating, monitoring risks, organizations can protect and create value to formulate an environment for innovation and strategic growth.

3.2. Artificial Intelligence Technologies– Theory and Practice

Artificial Intelligence (AI) is the ability of machines to perform tasks that would usually put a strain on human intelligence. Such tasks are reasoning, learning, decisional, problem-solving, language understanding, and pattern recognition. AI now is trying to imitate parts of human thinking and behavior.

Key branches of AI include:

- Narrow AI: AI focused on particular domains (e.g. virtual assistants, spam filters).
- General AI: A theoretical AI capable of human-level intelligence across all tasks.
- Superintelligent AI: A speculative form surpassing human intelligence.

Machine Learning (ML) enables an AI system to evolve and become better with additional data. AI is the umbrella term that describes many techniques for achieving intelligent behavior, and Machine Learning specifically means learning based on data.

AI refers to the broader field of developing intelligent systems, while ML is a specific type of AI aimed at allowing these systems to learn from their experiences and improve their capabilities over time without needing to be directly programmed. ML uses algorithms and statistical models to find patterns and make decisions. (Morandín-Ahuerma, 2022)

NNs (Neural Networks) are a branch of the ML in the sense that they are inspired by the human brain structure. They are composed of layers of nodes (neurons) that are connected and work together to process data and learn complex patterns. Neural networks are a big reason AI can do such sophisticated things.

Deep Learning (DL) is a more sophisticated branch of ML based on Neural Networks. DL trains very large, deep neural networks, which can then be used for image recognition, natural language processing, autonomous driving, etc.

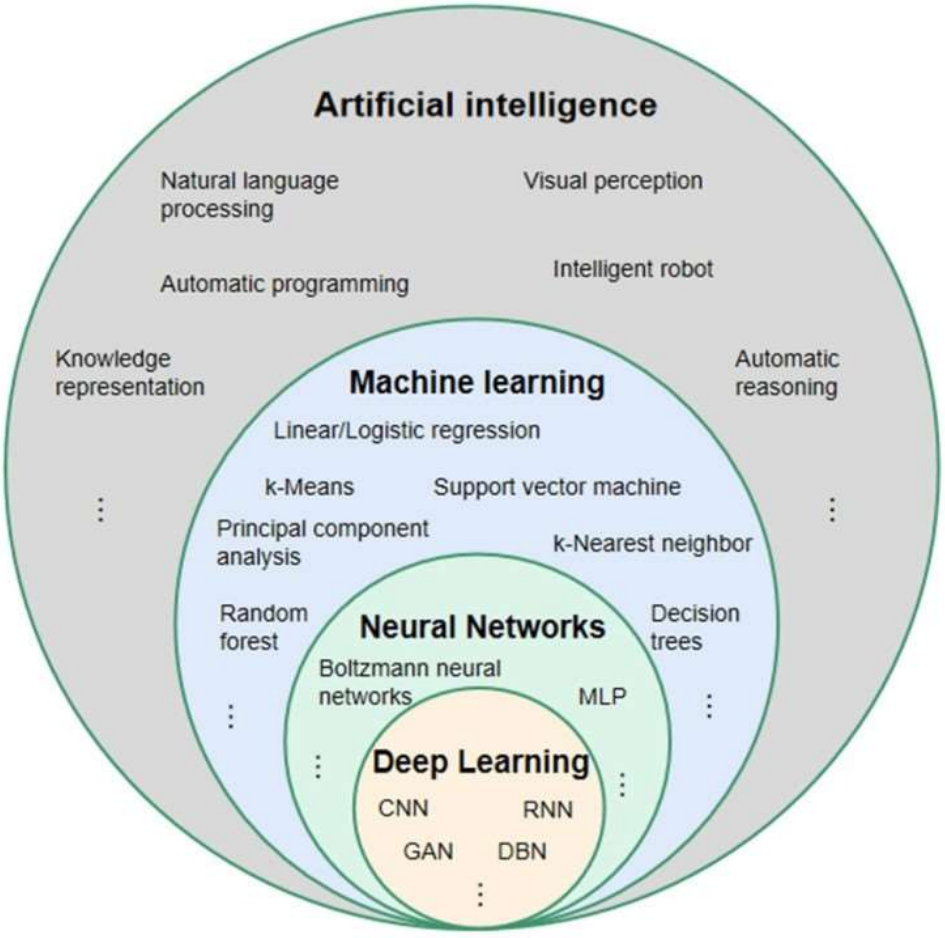

Image Source: https://www.linkedin.com/pulse/deep-learning-dl-vs-machine-ml-neural-networks-nn-examples-s-m-hhqic/ - Deep Learning (DL) vs Machine Learning (ML) & Neural Networks (NN) with examples

Predictive Analytics is another area that uses statistical techniques, ML models, and data mining on historical data to make predictions about future events. It is an application of AI and ML application. Predictive analytics mean predicting trends and generating predictions, which are enabled by AI models, especially ML and neural networks. Predictive analytics is commonly employed in sectors such as healthcare (to forecast disease likelihoods), finance (to predict stock movements), and marketing (to estimate customer actions).

AI is the broad umbrella area with the aim to mimic human intelligence. ML refers to a subset of AI that allows systems to learn from data. Neural networks serve as the underpinnings for ML architectures (specifically Deep Learning) to manage complex tasks, and predictive analytics leverages AI and ML techniques to produce informed predictions. (Zhang, 2023)

3.2.1. Machine Learning (ML)

Machine learning is one of the primary methods used in artificial intelligence (AI). The idea was first articulated in the 1950s by the prominent AI pioneer Arthur Samuel, who described the field as "the field of study that gives computers the ability to learn without being explicitly programmed." This definition highlights an important change in the way machines can now be built to improve their performance over time as a result of experience, instead of requiring direct human involvement in every single task. (Abioye et al., 2021)

As Sara Brown explains in her article "Machine Learning, Explained, (2021)": *"machine learning is a targeting of a small subset of artificial intelligence itself."*

Branded as AI, artificial intelligence is defined broadly as the ability of a machine to perform intelligent behavior that is considered to be associated with the thinking of a human being, covering a spectrum of features including reasoning, problem-solving, perception, and language understanding.

One of the key differentiators of machine learning is its focus on creating algorithms and statistical models that allow computers to recognize and interpret complex data patterns. Enhanced update correction, machine learning, automated analytics systems update their processes incrementally. With the massive training datasets, it has unlocked a whole new world of applications in multiple domains such as healthcare, finance, and autonomous systems, where acting intelligently on available data is paramount.

However, this is actually just part of the story as machine learning is a field in a constant change through data which enable machines to do work previously thought possible only by human intelligence.

AI systems perform complex tasks in a fashion that is similar to human problem-solving. Furthermore, as she points out, the objective of AI is to mimic "intelligent behaviors" in computer models the way humans do. That is, we build machines that can analyze a visual scene, interpret a passage of natural language text, or take an action in the physical world.

(Machine learning, explained | MIT Sloan. (2021, April 21). MIT Sloan. https://mitsloan.mit.edu/ideas-made-to-matter/machine-learning-explained)

3.2.2. Neural Networks

A neural network is a machine learning program, or model, that makes choices in a way that resembles the human brain's, employing processes that mimic how biological neurons work together to detect phenomena, consider options and reach conclusions.

Neural Networks are advanced computational models that can perform and imitate the way the human mind processes information. They learn patterns and make predictions based on large amounts of training data, and they improve the accuracy of their predictions through learning. During training, these networks learn to fine-tune their internal parameters to reduce errors, thus becoming better at the task with each iteration. Neural networks are interesting because once they are properly trained, they are very powerful classifiers and clustering tools in the communities of computer science and artificial intelligence that work fast in nature.

They are powerhouses for just about any pattern recognition task, but they're doing much more than crunching numbers. In applications like speech recognition or image recognition, the analyses performed by a neural network can happen in just a few minutes, while the best human expert would take hours to identify and categorize the same data. This unprecedented speed boost increases productivity and creates new useability for industries that require real-time capabilities including healthcare and autonomous vehicles. ("Overview of Neural Network," 2022)

Google search algorithm is one of the most liked examples of a neural network putting to use; Google uses advanced neural network architectures to find relevant search results in milliseconds. For example, this dynamic learning algorithm a neural network that can adapt over time as it processes more and more user requests and learns about users and the type of interaction they have, allowing it to find new and improved ways of fetching the most appropriate piece of content quickly. (https://www.ibm.com/topics/neural-networks)

3.2.3. Predictive Analytics

Predictive analytics is an advanced analytical approach that uses statistical algorithms and machine learning techniques to identify the likelihood of future outcomes based on historical data. This sophisticated method is widely employed in the field of financial risk management,

where it is instrumental in predicting different types of risks such as market fluctuations, credit risk, and risks associated with investments.

Predictive analytics brings organizations the power to detect and assess potential risks before they materialize into major problems. Such proactive approach enable organizations to take timely actions that can significantly reduce financial losses and operational downtime. In this scenario, predictive models are used to evaluate historical data and economic indicators to predict potential market changes; thus, companies may allocate their resources and exposure according to their predictions. (Henrys, 2021)

In addition, predictive analytics improves credit risk assessment, whereby it utilizes historical repayment behaviors, repayment history and relevant economic conditions to be utilized to accurately assess the credibility of the borrowers which will lead to minimizing defaults. The insights gained from these analytical techniques can, in turn, help with trend analysis which, in investment risk management, can help understand potential downturns or opportunities for the organization to respond to. (Makridakis, 2017).

In conclusion, by effectively utilizing predictive analytics, organizations can gain a comprehensive understanding of potential financial risks and better position themselves to mitigate their impacts (Makridakis, 2017).

3.2.4. Explainable AI

XAI or Explainable Artificial Intelligence is a field designed to make AI systems more interpretable for humans, tackling the 'black-box' problem of many AI models. This is essential in fields where AI judgments have a major influence on human living, including finances, and judicial frameworks, as it develops confidence, openness, and liability in AI usages. (Gunning et al., 2019)

Explainable artificial intelligence (XAI) is a set of processes and methods that allows human users to comprehend and trust the results and output created by machine learning algorithms. (https://www.ibm.com/think/topics/explainable-ai)

In this regard, Physics-Informed Neural Networks (PINNs) are an attractive alternative for developing interpretable AI as they offer a high degree of physical fidelity with less performance decreased by uncertainty-based methods; while XAI methods, such as LIME (Local Interpretable Model-agnostic Explanations) and SHAP (SHapley Additive exPlanations), emerge to create interpretable explanations of AI models with little to no performance loss, leading to trust and ethical conformance. It also highlights the trade-off in between performance and transparency of XAI from the perspective of combining with other AI paradigms like deep learning and reinforcement learning. (De et al., 2020)

In addition to these, XAI must also face several technical challenges and limitations, such as collinearity of features, for example the Additive Effects of Collinearity (AEC) that improve stability and robustness of model explanations. There are techno-scientific, philosophical, and social-institutional dimensions to the multidisciplinary nature of XAI, all of which are based on ensuring that AI systems are intelligible and accountable, and retaining user trust. (Salama et al., 2019)

This knowledge paves the way for success along with the other XAI approaches to integrate AI into multiple domains while designing reliable AI/ML solutions having a balance between accuracy and interpretability while also supporting future governance policies for the carbon of ethical deployment of AI.

3.3. Identified Problems in Conventional Risk Management

3.3.1. Data Overload

Traditional risk management systems frequently encounter significant difficulties when tasked with processing and analyzing large, intricate datasets effectively. A prime illustration of this challenge is the evaluation of real-time data pertaining to financial risks. Conventional risk assessment models typically fall short in their capacity to manage the sheer volume and complexity of information that modern financial environments generate. (Jordan & Mitchell, 2015).

While financial markets continue to evolve, the limitations of traditional risk management systems become increasingly apparent, particularly in their inability to adapt to rapid market changes. This inflexibility not only hampers timely decision-making but also exposes organizations to heightened risks due to outdated assessments and methodologies that rely heavily on historical data.

Without real-time monitoring capabilities, firms can miss key signals of potential threats, making it harder to reduce risk. Therefore, there is a urgent requirement for novel solutions that utilise complex technologies, like artificial intelligence, that are able to process much larger data sets and deliver predictive insights that traditional models cannot provide. (Abikoye al, 2024)

3.3.2. Limited Predictive Capabilities

Detection in example of rare events in behavior leads to difficulties with conventional risk management as they are sensitive to classes with imbalanced dataset. If untouched, this imbalance can lead to corrupt analytical outputs and wrong interpretations. This could lead one into a false sense of security with regards to performance when only using standard

performance metrics like accuracy. This happens because high true negative rates can disguise the actual problem, which are the false negatives, and correspond to missed AEs.

In these instances, a model might excel at the aggregate level, but miss the nuances of the minority class — the one that's not just rare but impactful adverse outcome! Such a lack of consideration is costly in many domains, for example health, finance, and safety-critical systems, where the price to pay for neglecting a negative event is high. For this reason, it is important to adopt more advanced evaluation metrics and techniques that offer a better understanding of performance, especially when dealing with imbalanced data. This upgraded predictive prowess will allow risk managers to make better-informed decisions, resulting in improved outcomes. (Vannucci & Colla, 2016)

3.3.3. Reactive Nature of Traditional Methods

Risk management has traditionally evolved around conventional methodologies that naturally retain a reactive bent. Traditional approaches tend to work on a reactive model, one that puts its focus on identifying and remediating risks after they materialized. Consequently, organizations have been left hanging, struggling with the fallout of unexpected challenges that sometimes result in major monetary losses, reputational damage, and breaks in service. This reactive approach is inherently wrong, and restricts the organization's ability to take proactive steps to potentially decrease future threats before they can build.

These constraints of traditional approaches underscores a fundamental disconnect in the risk management landscape, signalling an urgent need for more nimble and proactive approaches. To be effective and sustain their risk management capability, organizations should not just settle for learning from the past and imposing defensiveness — they should progress to a forward-looking perspective. This highlights the importance not just of identifying and responding to risks that emerge, but developing forward-looking models and frameworks that allow for the preemptive identification of potential risks.

Thus, by encouraging a culture of diligence and forward-thinking risk assessment, enterprises can fortify their ability to withstand challenges, reduce the effects of negative incidents, and achieve a safer working ecosystem in the long run. (Mishra et al., 2024)

3.3.4. High Human Resource Dependency

A bastion of risk assessment, the cognitive insight of humans has always been seen as a critical fraction of the total equation. Although invaluable, with human resources based evaluation this factor introduces a certain percentage of subjectivity and variance into the process, thus causing inconsistencies in risk assessment.

Traditional methodologies, which relied heavily on expert judgment, can be fraught with challenges, given they are resource and time intensive. Hence, different contention and perception over risk carrying leads to differences in domains per individual leading to differences in assessments generated.

In addition, the traditional dependence on human expertise can cause bottlenecks and delays in risk assessment, since organizations are often hemmed in by the availability and workload of their experts. Consequently, organizations' agility to perform effectively in a changing milieu is often impaired when it comes to responding to evolving risks. While risks are changing more rapidly than ever, the conventional frameworks that rely heavily on human jurisdiction can restrict proactive risk management practices.

Therefore, organizations need to reassess their risk assessment methods, acknowledging that it is essential to have a greater equilibrium between human expertise and sophisticated analytical tools in the decision making process. Such practice serves to improve the uniformity, productivity and success of risk assessments, and thus encourages a stronger operating model against the backdrop of ambiguity. (Sarioguz & Miser, 2024)

3.3.5. Difficulty in Integrating Multiple Data Sources

Integrating Diverse Data Sources for effective Risk Management is a multifaceted endeavor that necessitates seamless integration of data from a variety of sources. This includes but is not limited to financial reports that give a glimpse of an orgs economic health, market trends that give a snapshot of the flux of the industry, and regulatory updates that outline changes in compliance requirements.

This is because data have been generated in different formats, structures, and contexts. Whereas, financial reports may be prepared in different accounting standards, market data varies largely in terms of frequency and granularity.

Further, multiple jurisdictions have their own regulatory updates with varying requirements and timelines. This all means that organizations need to invest in data integration tools and processes that are able to deal with these different types of data. This often requires building out standardized processes around how the data will be collected, validated and analyzed, which certainly goes beyond the technology itself. Without such measures, organizations run the risk of making misinformed decisions leading them down a path of an unknown risk that will act against their strategic goals and operational resiliency.

Ultimately, the data integration challenge is deeply technical in nature but foundational to a complete risk management program designed for strict execution and continuous improvement. (Yazdi et al., 2024)

3.4. AI's Impact on Risk Management

Image Source: https://www.leewayhertz.com/ai-in-risk-management/ - AI in risk management: Applications, benefits, solution and implementation

3.4.1. AI in Risk Identification and Assessment

Automated techniques in risk management Historical data and manual processes are often used in traditional strategies, making them both time-consuming and error-prone. Unlike this, AI utilizes machine learning algorithms and data analytics to improve the precision and efficiency of detecting such risks.

Image Source: https://www.leewayhertz.com/ai-in-risk-management/ - AI in risk management: Applications, benefits, solution and implementation

The use of AI in risk identification greatly benefits from risk analysis of large volumes of data comprising various sources such as financial records, market trends, social media, or even news articles. It helps organizations identify emerging risks that might not be immediately visible with traditional analysis. As an example, AI systems can recognize patterns and outliers in data indicative of possible operational, financial or reputational risks, enabling businesses to mitigate situations before they turn into problems. Furthermore, AI strengthens risk assessment by offering predictive analytics capable of estimating the probability and consequences of detected risk. AI also uses complex models to create simulations of possible scenarios and their respective outcomes, and it helps organizations see the risk landscape more clearly. Not only this predictive ability help prioritize risks according to the severity but also facilitate strategic decision-making processes.

Furthermore, AI-based tools help to continuously track risk elements in real time. This keeps organizations alert and adaptable to changes in their risk landscape. This automating of data collection and analysis allows the risk manager to concentrate on strategic initiatives and not get bogged down with routine assessments. Overall, from in-depth sensitivity analysis, risk modelling predictions to predictive factors, and machine learning-based algorithms to improve upcoming risk analysis, all of these are linked to AI technology as organizations greatly rely on AI to help them identify and assess risks more effectively than ever. As organizations adapt to the evolution of their respective fields, AI will be critical for organizations to manage their risk management processes more effectively to ensure resilience and sustainability. (Aziz et al., 2018)

3.4.2. AI in Risk Mitigation

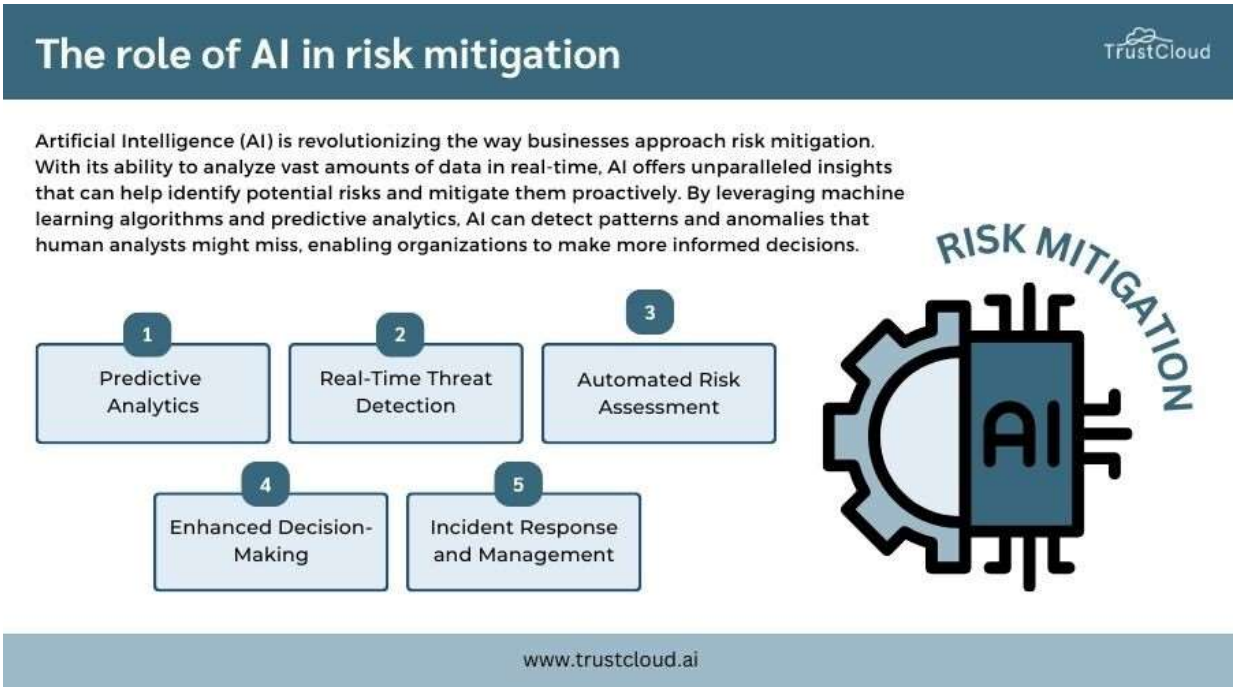

Image Source: https://community.trustcloud.ai/docs/grc-launchpad/grc-101/risk-management/risk-mitigation-strategies-the-role-of-artificial-intelligence-in-enhancements/ - Risk mitigation strategies: the role of artificial intelligence in enhancements

AI is revolutionizing the role of risk management at breakneck speed, introducing new technology and new approaches that can help organizations better detect, assess, and mitigate risks like never before. In this section, I will explore the unique dimensions of AI's role in risk mitigation, its applications, capabilities, and advantages to businesses across different industries.

AI is but a wide umbrella of technologies that drive machine learning, natural language processing, and predictive analytics, which are capable of interpreting tremendous amounts of data in real time at unmatched speeds. This allows organizations to better understand prospective risks and build processes to address them proactively. AI plays a critical role here, with improved data analysis, real-time monitoring, and predictive modeling augmenting risk management processes in the enterprise.

The most crucial benefit of AI in the realm of risk mitigation is its capability to process and analyze massive data sets from a variety of sources. Traditional risk management techniques depend heavily on historical information and unchanging models, which is able to miss rising threats. While traditional systems often rely on pre-defined rules or heuristics, AI-powered solutions can adapt to emerging risk factors by continuously learning from new data inputs,

recognizing patterns, and identifying hidden correlations that may signal a potential threat. Organizations can leverage this dynamic analysis to proactively protect themselves against emerging threats and make informed decisions based on real-time insights.

AI Tools enable organizations to ensure ongoing monitoring of relevant risk factors, which makes it possible to identify anomalies or issues as they emerge. In the finance industry, AI can analyze transaction data and flag potential fraud in real time, or detect unusual spending behaviors. Likewise, in manufacturing, AI can track monitoring equipment performance and anticipate maintenance requirements, thereby reducing operational risks. By taking such initiatives, organizations can effectively identify and mitigate risks, limiting the probability of negative occurrences.

AI's predictive abilities are especially useful when it comes to risk mitigation. With sophisticated algorithms, organizations can predict potential risks and their impacts. For instance, AI can determine the probability of claims in insurance from different aspects, based on which the insurers can optimize their policies and pricing. Moreover, in cybersecurity, AI is being used to predict potential breaches by analyzing historical data on previous attacks and identifying weak spots, allowing organizations to strengthen their defenses before an attack happens.

By offering risk managers actionable insights and with integrating AI into risk management processes, those decision-making capabilities can be amplified. AI-driven analytics can identify an organization's highest risks and recommend mitigation strategies that are proven, guided by historical data and predictive models. These are designed to provide risk practitioners with enough data to enhance their focus and to optimize their resource allocation, leading to more intelligent and beneficial risk-related decisions.

Through the use of advanced data analysis, real-time monitoring, and predictive modeling, AI is transforming how organizations can mitigate risk. AI allows organizations to refine their risk governance, identify potential risks beforehand and take strategic actions to protect the business and safeguard the brand. In an increasingly complex world, the use of AI for risk mitigation will become a necessity for organizations seeking to remain competitive and sustainable in the long run. (Conforti et al., 2012)

3.5. How Artificial Intelligence Aims to Address These Challenges

3.5.1. Data Processing and Scalability

Image recognition is one of the most common area of AI using deep learning algorithms, where such algorithms enable understanding a risk very quickly and accurately. With the automation of data collection and analysis, AI minimizes human error and expedites decision-

making processes, making it possible for organizations to quickly adapt to new challenges as they arise. (Goodfellow et al., 2016).

Besides improving data processing and scalability, AI is also crucial in risk mitigation, providing advanced predictive analytics capabilities. With the help of machine learning models that keep learning with new inputs, organizations can not only predict possible risks but also simulate multiple events to identify scope of influence (Goodfellow et al., 2016). Using foresight, companies can take preemptive measures to address potential problems before they arise, reducing downtime and losses significantly.

Moreover, as operational frameworks increasingly leverage high-risk AI systems, it is imperative to enforce strong cybersecurity practices to defend against exploitable weaknesses that draw the attention of adversaries. With a holistic approach to these challenges, organizations can unlock the complete promise of AI whilst protecting their assets and operations.

For organizations grappling with the challenges of today, the infusion of Artificial Intelligence into risk management strategies is not just an opportunity, but a fundamental shift in how to promote resilience. AI enables speedier analysis of the vast datasets in use by enhancing data processing and scalability, which improves predictive accuracy and allows real-time risk assessments. Also, the implementation of advanced machine learning models enables organizations with the ability to assess the likelihood of risk in a timely manner and run different scenarios against potential risks so that they can put in place specialized solutions, ultimately preventing disruption. Yet as organizations rely more on high-risk AI systems, it is critical to prioritize robust cybersecurity practices to guard against such vulnerabilities. By overcoming these complex challenges, organizations can harness AI to not only enhance their risk management processes but also protect their assets and maintain operational resilience in a constantly evolving landscape. (Zohuri & Rahmani, 2019)

3.5.2. Predictive Modeling and Early Detection

Pattern detection by machine learning models would be useful to capture early signals of when these databases pose heightened risks. It is particularly useful in financial risk management; AI can better analyze market trends, and predict downturns more accurately than conventional models (Ng & Jordan, 2020).

Machine learning is one of the best things that has happened to us, especially in predictive modeling and early detection. These models utilize the potential of sophisticated algorithms to identify potential risk patterns well before they develop into sizeable threats. Your predictive ability is particularly vital in financial risk management, where anticipating market movements can prevent losses and guide decision-making. Traditional models typically use historical data

and static assumptions, whereas machine learning techniques can dynamically analyze trends in the market, allowing for greater accuracy in predicting downturns (Ng & Jordan, 2020). Particularly, they can harness AI to aggregate massive datasets, including financial news articles or social media, allowing banks to identify potential risks to their operations.

Machine learning models can identify red flags that indicate risk. This is especially beneficial in the field of financial risk management, where artificial intelligence observes market trends and predicts downturns more accurately than standard models (Ng & Jordan, 2020). Through large-scale access to real-time data, these algorithms can dynamically respond to fluctuations in the market, allowing for proactive decision making by the institution that manages risk and opens new revenue streams.

And as the finance industry continues to embrace machine learning for predictive modeling, both the ethical implications, and the responsibility for the outcomes, of these technologies will emerge into stark relief. However, algorithms function as "black boxes" and it becomes tricky to interpret their internal workings. Therefore, there needs to be more balance, one that not only focuses on predicting risk accurately but also an insight into the determinants of that risk. Combining these two elements may build trust with users and remain compliant with developing regulations designed to protect data and encourage responsible AI within financial institutions. Therefore, the inclusion of human input in the automated systems could be an important scruple to safeguard from bias and errors existing in algorithm decision-making procedures.

3.5.3. Automation and Efficiency

Artificial intelligence (AI) is that new thing: it opened a new era of automation and efficiency in different areas. So, one big advantage of AI is that it can undertake repetitive tasks, i.e., it would speed up operations, and allow human experts to focus more on strategic decision-making processes. An relevant example is found in the area of credit risk assessment in which AI models are used to quickly assess applicants based on hundreds of facets. Such capacity not only accelerates the evaluation process, it also lightens the working burden of credit analysts, allowing them to focus their skills on more complex analyses and judgments (Russell & Norvig, 2020). With organizations adopting AI technologies in increasing numbers, both practitioners and researchers will need to consider what the consequences of automation will be with regard to workforce dynamics and operational efficiency.

AI can replace the monotonous tasks and let human experts focus on the domain that require numerous decisions. For example, regarding credit risk assessment, AI models can quickly evaluate applicants on multiple metrics, alleviating some burden from credit analysts. This not only increases productivity, but also promotes a more strategic view of risk

management, resulting in better decision-making and improved financial results (Russell & Norvig, 2020).

Artificial intelligence increasingly becomes embedded into operational structures, not only rendering them more efficient but also requiring a reassessment of core workforce skills. With the automation of routine tasks by advanced technologies, organizations will need to invest in training programs that up-skill employees with higher-level analytical and technological capabilities that can navigate a newer and different job market. In this scenario, an organisational culture that supports lifelong learning and adaptability is an essential competitive advantage for individuals and companies alike (Whittick, 2016). Moreover, while companies utilize AI innovations to increasingly sophisticated decision-making processes, there are new ethical questions that they must grapple with: data privacy and algorithmic bias, which could erode trust and accountability within financial systems. Although automation provides massive opportunities to improve productivity, it also places considerable demands on organizations to deliver equitable outcomes for all stakeholders.

3.5.4. Enhanced Integration of Diverse Data

The concern is that you get divergent data sources in modern-day risk analytics, where we live in the Age of Infobesity! AI stands as a transformative tool, capable of synthesising structured and unstructured data, a term that covers a wide range of different types of information, from regulatory news to social media insights. This function does not just increase the depth and breadth of risk assessments, but also allows for a more totalistic view into potential threats and opportunities that may slip through the cracks of conventional analysis (Miller, 2019). Utilising AI to combine these multiple streams of data allows organisations to take analysis to new heights, providing an insight that would be impossible with traditional methods on their own, and enabling organisations to make the most of the 21st century.

The ability of AI technologies to combine information from structured and unstructured data sources—from regulatory news, social media sentiment to other unstructured data—allows for a more holistic approach to risk analysis in a way that is difficult to achieve through conventional approaches (Miller, 2019). By integrating this approach with with data intelligence systematically it helps to not just highlight next layer of risks but also identify changing market trends to help business to prepare proactively to give an advantage in competitive environment. With these powerful analytical tools at their disposal, companies will be able to create more comprehensive strategies that incorporate their long-term objectives, while also neutralizing risks they may face.

Artificial Intelligence is transforming risk analysis in a data-drenched world by integrating disparate data sources like never before. Through the successful synthesis of structured and

unstructured data, organizations can perform extensive assessments that identify complex relationships and insights obscured by traditional methodologies. This capability can help in identifying emerging risks while enabling proactive decision-making, which contributes to competitiveness. As events unfold, organizations will need to address the complexities arising from the situation and equip themselves with the insights provided by integrated data by leveraging the latest AI-powered data integration solutions and their technology.

3.5.5. Real-Time Monitoring and Proactive Decision-Making

The future of organizational management melds real-time data analysis via artificial intelligence (AI) into risk management — a game changer. Organizations have traditionally been reactive, with risks addressed after they materialize into real challenges. The emergence of real-time monitoring capabilities, on the other hand, enables a shift in this paradigm towards proactive decision-making. By leveraging advanced analytics techniques VUCA helps organizations to proactively spot and mitigate potential risks, enabling detection and resolution of issues ahead of time, minimizing potential areas of loss and increasing overall resilience (Makridakis, 2017)

AI can help organizations transition from a reactive to a proactive approach to risk management using real-time data analysis. This transition aids in reducing the impact of potential losses by acting on risks before they become severe (Makridakis, 2017). Such a change not only enables better forecasting and risk management but also creates an environment of continuous improvement where organizations can rapidly respond to rising challenges while taking advantage of new opportunities. AI-enabled risk management models leverage real-time data and analytics to predict risks more accurately, allowing organizations to enhance their operational resilience and improve their risk response capabilities.

3.5.6. Real-Time Risk Monitoring and Proactive Decision-Making

Artificial Intelligence (AI) in Risk Management In an age where the pace of change is relentless and organizations have increasingly to navigate uncertainty, the augury of AI in risk management is not only opportunistic but also strategic to bolster operational resilience and establish enhanced foresight.

Among the critical benefits delivered by AI is real-time risk monitoring, enabling businesses to assess and analyze many lines of threats — financial, operational, reputational, and compliance, among others. Real-time risk monitoring uses advanced algorithms and machine learning models to analyze large volumes of data, detecting patterns and anomalies that could point to potential risks. Thus, this functionality not only improves the speed and accuracy of risk detection but also equips organizations to proactively address potential concerns before they escalate into bigger issues. For instance, banks can implement AI to analyze patterns in

transactions, allowing them to flag unusual activity that may indicate fraud or money laundering, preventing potential financial loss and ensuring adherence to regulations.

In addition, AI enables risk managers to make more proactive decisions by offering them actionable insights from predictive analytics. Through the analysis of past data and present trends, AI systems can predict potential risks and recommend measures to prevent them proactively. By taking a proactive approach to risk management, organizations can make better use of their resources, prioritize their risk responses efficiently, and create contingency plans that address the most likely risks. Essentially, this dynamic partnership between the two promotes accuracy in risk assessment, but also encourages organizations to act with both agility and foresight.

With enterprises confronted by complexities and uncertainties magnified by globalization and technological shifts, the need for real-time monitoring and informed proactive decision-making will be critical for sustaining competitive advantage and long-term success. (Bedi et al., 2020)

3.6. Leveraging the AI into Specific Areas of Risk Management

Risk management is a strategic approach in all industries, disciplines and sectors that include processes to identify, evaluate and minimize risks so that organisational goals and objectives are not compromised. In an era where technology is constantly evolving, especially in the realm of Artificial Intelligence (AI), the future of risk management is changing dramatically. It covers the different uses of AI in improving risk management practices in various areas, like financial, cybersecurity, operational, etc.

In the field of the finance domain risk management, AI-based algorithms are enhancing risk management models by more accurately scoring individuals with credit risk, refining algorithmic trading approaches for risk management in marked asset portfolios, and improving the efficacy of fraud detection frameworks in banks and other major financial institutions. Together these developments not only improve prediction but also create a more nuanced perspective on exposure to risk.

In cybersecurity, too, artificial intelligence is just as important, as AI-based threat intelligence tools help enhance the precision and immediacy for detecting and responding to cyber attacks. However, technologies such as these come with important ethical implications that must be carefully explored in order to minimize the risks of bias and privacy violations Image credit: Microsoft AI's contribution to improving security awareness training programs highlights its potential in strengthening human defenses against cyber threats.

AI innovations are also positioned to positively impact operational risk management as well. Predictive analytics in identifying and mitigating operational risks in complex systems, the role of automation in risk management and its implication for organizations. IA can also improve the accuracy of operational risk assessments and loss forecasting, contributing to more effective decision-making.

This review provides an overview of existing literature on these topics, providing rich insights into the transformative potential of AI in risk management, as well as the challenges and ethical concerns involved in its use. By delving into this domain, we aim to shed new light on how artificial intelligence can be employed to improve risk management across the continuum of organizational structures, ultimately leading to more robust performance management paradigms.

3.6.1. Leveraging AI in Financial Risk Management

AI-driven algorithms significantly enhance the accuracy of credit risk scoring models by leveraging advanced machine learning techniques and alternative data sources. These algorithms can capture complex, non-linear patterns in data that traditional models often miss, leading to more precise risk assessments. By improving the accuracy of identifying potential defaulters, AI models not only reduce credit risk but also minimize unfair credit rejections, thereby promoting economic growth and financial inclusion. The following sections detail how AI-driven algorithms achieve these improvements.

Image Source: https://www.westfordonline.com/blogs/financial-risk-management-strategies/ - Financial Risk Management: Strategies for Optimal Asset Protection

3.6.1.1. Enhanced Predictive Accuracy

Machine learning AI models like random forest and ensemble learning have shown more accurate results than traditional scorecards like logistic regression in scoring credit risk. In another case, the accuracy improved from 0.69 to 0.83 with the use of a random forest model on Azerbaijani SMEs data (Karimova, 2024).

Furthermore, AI's role in financial risk management does not limit itself to credit scoring, but also involves liquidity and market risk. With the help of machine learning algorithms that can analyze large datasets in real time, organizations are better able to predict changes in market conditions, allowing them to optimize their asset allocations. As an example, reinforcement learning methods can continuously adapt trading strategies based on real-time analysis of the market, improving responsiveness to volatility.

In addition, sentiment analysis from news articles and social media through NLP tools further bolsters this approach as traditional models may not account for such dynamics in the market. By integrating both the sets of policies, this comprehensive mechanism not only enables better decision-making but also increases resilience towards unforeseen economic shifts, eventually ensuring more financial stability overall. With the integration of such advanced technologies, businesses will be able to establish frameworks that not only react to the current state of the market but also proactively position themselves as forerunners in navigating the trajectory of the future alongside the latest trends in this highly competitive market.

AI methods are capable of processing large quantities of data and also detect complex patterns, resulting in increased predictive power and robustness in credit scoring models (Hussain et al., 2024). Which provides organizations with the ability to make data-driven decisions in real-time, allowing them to pivot quickly and continuously update their business strategies while reducing their exposure to market risk.

3.6.1.2. Real-Time Risk Assessment

As AI systems allow for real-time data analysis, they enable financial institutions to track and respond to risks on-the-fly. This enables proactive risk management and helps decrease the likelihood of loan defaults (Shen, 2024).

This allows for more comprehensive risk assessment because Machine Learning Algorithms can help to detect patterns and anomalies in data across a wide variety of a bank's operations, which ultimately contributes to a more informed decision-making process and a more stable financial system.

Furthermore, the use of AI in risk management allows for immediate analysis while also providing predictive modeling capabilities that identify potential risks in the future by looking

for trends in my historical data. Data science, aided by deep learning and natural language processing, empowers financial institutions to predict changes in the market environment or consumer behavior with greater accuracy and accuracy than ever before, enabling us to avoid potential threats (before they become a reality). One prominent examples is how companies such as ZestFinance have implemented these technologies to improve the way they make loan decisions, increasing the accuracy of their creditworthiness assessments and lowering their default rates.

As this technology continues to progress, it is crucial for organizations to confront fundamental issues like algorithmic bias and data privacy concerns, as they may compromise the efficacy of AI-powered solutions if not dealt with responsibly.

3.6.1.3. Enhanced Risk Assessment and Management

By analyzing large and complex datasets, AI algorithms help to assess the level of risk with greater accuracy, leading to better forecasting of volatility and more effective portfolio optimization (Leng, 2024) (Sari & Indrabudiman, 2024).

Moreover, the use of AI in risk management goes beyond mere risk assessment, also proving instrumental in strategies for proactive risk mitigation. Financial institutions can already detect potential threats before they arise by employing machine learning algorithms capable of adapting to changing market conditions.

Furthermore, by incorporating natural language processing, firms can assess the sentiment of the market as expressed in news articles and social media, adding another dimension by measuring how public perception could affect news and market risks. By incorporating a more nuanced risk perspective, this approach not only effectiveness in decision making processes but also develops a greater robustness against uncertainties in the marketplace which ultimately leads to better financial security in an increasingly intricate world.

QT systems enable improved functioning of financial institutions using AI providing lower market churn as well as better data-based decision-making becoming an important aspect of overall market stability (Kuzior,2024).

The use of AI algorithms can improve risk assessment, risk management and risk evaluation, the number of advantages could only be outweighed by the disadvantages. Due to the complexity of AI systems, there is a high risk of overfitting, which is when models are accurate neither on historical data (on which they were trained) nor on projections about future market behavior. Such dependence on vast data sets may miss vital qualitative elements to which human analysts pay heed, which could mean misguided investment strategies (Smith & Johnson, 2024).

Furthermore, the pre-emptive risk management techniques afforded by AI may lead to a false sense of security within financial institutions. Retrained machine learning models to adapt to changing market conditions do not ensure that they will accurately predict black swan events, which can fundamentally derail market activity irrespective of algorithmic predictions (Brown 2024).

Furthermore, incorporating natural language processing to combat market sentiment raises ethical and practical problems. Quantifying and interpreting the influence of social media and news on markets is not straightforward and leads to decisions based on noise (Davis, 2024), not substance.

Specifically, it will show that AI can be harnessed as a useful aid to assist humans to make better decisions in some cases, if humans are aware of the limitations and risks that come with AI technologies. Over-growing reliance on AI can erode human discernment and create systemic risk vectors that harm the stability of financial markets, rather than bolstering their resilience (Lee & Thompson, 2024).

3.6.1.4. Dynamic Portfolio Optimization

AI-driven systems use real-time data to dynamically adjust investment allocations, optimizing returns while minimizing risk exposure in volatile markets (Ambuli et al., 2024).

Reinforcement learning algorithms are employed to dynamically optimize portfolio weights, adapting to changing market conditions (Leng, 2024).

3.6.1.5. Enhancement of the effectiveness of fraud detection and prevention systems in financial institutions

AI can substantially improve upon the effectiveness of fraud detection and prevention systems in financial institutions by employing more advanced algorithms and data analytics to detect and mitigate fraudulent activities with comparatively higher efficiency than legacy systems. The potential of AI technologies, notably machine learning and deep learning, enables a better accuracy, scalability, and adaptability, making them better equipped to tackle the growing threat of financial fraud. These technologies allow for the analysis of extensive data sets to identify irregularities and patterns that suggest fraudulent activities, minimizing false positives and improving real-time detection abilities. Later, the articles explains how AI could be integrated into fraud detection and prevention systems. (Wang, 2023)

Machine Learning and Deep Learning

Supervised, unsupervised, and deep learning AI models can handle large quantities of transactional data, enhancing the detection of anomalies that might indicate potentially harmful financial activity (Ismaeil, 2024).

Machine learning models, especially adaptive learning ones like decision trees and neural networks, do a great job of detecting patterns that may not be obvious-no matter how subtle it might be in large datasets, these patterns might be missed using traditional methods (Adewumi et al., 2024).

ML can improve the efficiency of fraud detection and prevention systems employed by financial institutions in multiple ways:

- ✓ Data Processing and Analysis: ML algorithms were also able to process large batches of transactional data in minimum time and maximum speed. By studying historical transaction data, these algorithms are able to learn what typical behavior looks like for individual users or accounts.
- ✓ Anomaly Detection: Financial behaviors can be monitored using ML models, especially unsupervised learning techniques, to flag instances that deviate from the norm. These models can detect aberrations in transaction behavior that is often missed by traditional approaches by flagging transactions that deviate substantially from established patterns.
- ✓ Adaptive learning: Adaptive machine learning models like decision trees, and neural networks, learn continuously from new data. These models can adapt and improve their detection capabilities as fraudsters change their tactics, ensuring that the system remains effective against emerging threats.
- ✓ Enhancing Fraud Detection Systems: ML can reduce false positives by analyzing patterns and improving the detection system. It leads to a reduction in false positives, wherein actual transactions are less often flagged as fraudulent transactions, enhancing the customer experience and lowering operating costs. For example, time series data analysis techniques enable real-time detection of complex fraudulent patterns. Being able to respond quickly is essential to mitigating losses and blaming customers.
- ✓ Pattern Recognition: Machine Learning can recognize complex patterns and relationships in large data sets that may signal fraud. This capacity to identify subtle patterns helps financial institutions detect sophisticated fraud schemes that could slip through traditional approaches.

To conclude, ML plays a crucial role in improving fraud detection and prevention systems by providing advanced analytics, continuous adaptation, and increased accuracy, making it vital in addressing the ever-evolving landscape of financial fraud.

Machine learning can be quite useful in enhancing through noise and sample data, producing real-time data, and using the state and expectations of the time to enhance accuracy (Thakkar, 2024).

Real-Time Detection

Systems based on AI provide real-time fraud detection and the ability to adapt to fraud system patterns (Adhikari et al., 2024); hence, they significantly outperform traditional rule-based systems.

The potential for AI to revolutionize fraud detection and prevention systems in financial institutions is being realized by way of a few key methodologies and technologies. In this article, we'll explore how AI can be effectively used in this field and how you can go about it:

To leverage AI properly, financial institutions need to first collect data from various independent sources and use it as an integrated data set. Aggregate transaction data, consumer behavior data, historical fraud datasets, and external data points like social media and commercial data are all part of this. AI algorithms that combine different data sets can be used to get a holistic view of customer behavior, which often includes red flags for potential fraudulent activities.

Detection Based on Advanced Analytics and Machine Learning

AI combines techniques from advanced analytics, such as machine learning (ML), deep learning (DL), etc., to detect patterns that might suggest fraudulent behavior. They can do this by institutions:

Training Models

Creating machine learning models to learn what normal behavior looks like through historical data and detect deviations from the norm This could include choosing the right features and utilizing algorithms such as decision trees, random forests or neural networks.

Adaptive Learning

Building systems that learn and adapt to new data as fraud patterns change over time. This flexibility is important, as fraudsters tend to alter their methods.

Anomaly Detection

Note systems when combined with AI can cover a very useful suite of transactional data anomalies. Using thresholds to determine what is considered normal behavior, AI can identify atypical transactions that fall outside identified patterns. Clustering and statistical analysis are two techniques that can be used to detect these outliers.

Natural Language Processing (NLP)

Natural Language Processing (NLP) is a subfield of AI that deals with analyzing unstructured text data, such as customer interactions, social media and has been developed for analyzing unstructured data. This is a task AI can tackle effectively, as it allows systems to learn patterns and behaviours through natural language processing of emails, calls, and other forms of interaction.

Behavioral Biometrics

Behaviroal biometrics —an area in which AI can improve security— assesses how users move via metrics like typing speed, mouse movements and browsing habits. AI can establish a baseline of user behavior and if any behavior deviates from that baseline, it allows for identification of made-up activity like account takeover attempts.

Solving Complex Problems With Real Time Alerts And Decision Systems

AI systems can help fraud analysts by text messaging them in real time whenever it detects suspicious activity. By merging AI with decision-making frameworks, these systems can triage alerts according to their fraud probability, enabling human analysts to better focus on high-value cases.

Joining Forces and Exchanging Information

By working together, financial organizations can leverage each others' insights on emerging fraud trends and tactics to improve their fraud detection capabilities. AI helps in addressing this by collating and analysing data from multiple institutions to look for broader patterns of fraud.

Compliance and Regulatory Reporting

AI can help make sure you comply with fraud detection and reporting regulations. AI systems can assist in meeting regulatory requirements by automating reporting processes and keeping detailed records of transactions.

Customer Education and Engagement

It is paramount to engage your customers in fraud prevention efforts. AI can help tailor communications and inform customers about possible fraud schemes while actively encouraging them to report suspicious activity.

3.6.2. Leveraging AI in Cybersecurity Risk Management

Cybersecurity Risk Management is the process of identifying, analyzing, evaluating, and addressing cybersecurity threats to an organization's information systems. The objective is to safeguard an organization' digital assets, ensure continuity of operations, and meet compliance, regulatory, and industry standards.

Image Source: https://www.ispartnersllc.com/blog/ai-risk-management/ - AI Risk Management

But the tool that cybercriminals are using is neural networks, especially with deep learning models, which they can use to analyze network behavior and detect various patterns that characterize some attacks and make predictions. Organizations can build preventive capacity against cyber threats with the help of predictive analytics and ML algorithms which help organizations in detecting the vulnerabilities in the system to avoid its exploitation (Bostrom, 2017).

By leveraging the power of advanced data processing and machine learning, AI-driven threat intelligence platforms can help businesses greatly improve the accuracy and efficiency of their detection and response to cyber threats. This allows them to act faster than humans can, though it also reduces the need for human analysts.

In the landscape of evolving cyber threats, the use of AI in cybersecurity frameworks creates proactive and adaptive threat management strategies. Authorities are training AI and machine learning in the following manner:

Enhanced Threat Detection

Using machine learning algorithms trained on user behavior and network activity, AI systems can identify patterns of susceptibility in order to detect anomalous activity and predict threats. This technique enables detection of these deviations from normal behaviour which can be used to spot cyber threats (Uzoka et al., 2024) (Nnamani, 2024).

Through certain key mechanisms, threat intelligence platforms powered by AI can improve the accuracy and timeliness of cyber threat detection and response.

Real-Time Data Analysis

These platforms can process vast amounts of data in real time, allowing for the immediate identification of potential threats as they emerge. This capability helps organizations respond quickly to incidents, minimizing potential damage.

Machine Learning Algorithms

Through the use of advanced machine learning algorithms, AI Systems learn from historical data to identify patterns and spot anomalies. The ability to predict, identify suspicious behaviors, or network activity that predicts a cyber attack.

Automated Responses

There is a concern that AI platforms learn about system attacks that eliminate the need for human intervention[a]. The increased automation helps speed up response time and lets cybersecurity teams focus on more nuanced issues that need the human touch.

Behavioral Analysis

AI systems monitor user behavior and network activity to create a baseline of normal operations. It speeds up the process of spotting a threat which might be tripped up with the traditional way.

Integrating with Existing Security Frameworks

You are updated only till October 2023. This integration enables a more holistic approach to threat management and strengthens overall security posture.

Adaptive Learning

AI-powered systems can keep learning and evolving with new threats and update their algorithms with data and intelligence of new threats. This principle enables organizations to adapt their cybersecurity strategies to new emerging threats, ensuring resilience against cyber attacks.

Enhanced Threat Intelligence

Using data from multiple threat intelligence sources, these platforms can detect new threat trends, as well as various tactics employed by cybercriminals. This data allows organizations to forewarn against emerging threats. (Dutta & Kant, 2020)

Utilizing these mechanisms, AI-driven threat intelligence platforms can supercharge the effectiveness of cybersecurity by identifying cyber threats with higher precision and speed than traditional systems.

3.6.2.1. Real-time Monitoring

Powered by AI platforms with real-time monitoring capabilities, threat detection rates are significantly enhanced. AI applications in the cloud computing environment have achieved quite high accuracy and precision for threats detection, which can provide the expert level in detecting security flaws and finding vulnerabilities (Dorothy et al.,2024).

Real-Time Data Analysis

These platforms analyze gigantic amounts of data in real time from multiple sources. Real-time detection this is the new way, identifying threats as they enter and respond instantaneously to minimize the damage.

Machine Learning Algorithms

AI systems leverage machine learning to train on historical data, identify patterns, and detect anomalies. They are capable of examining user behavior and network activity to spot anomalies from regular operations that could signal a cyber threat.

Automated Responses

AI platforms can automate the response process when a threat is detected. This minimizes the requirement of human involvement, accelerates response times, and frees up cybersecurity specialists to handle more intricate problems that need human insight.

Behavioral Analysis

AI systems monitor user behavior and network activity in real time, establishing a baseline of normal activity. They can therefore also quickly detect threats that would otherwise go unnoticed using traditional measurements by identifying deviations from this baseline.

Co-existence (Integration) with Existing Security Flows

Integrating with existing cybersecurity tools and complementing them makes it even easier to adapt to the threat landscape.

Adaptive Learning

Unlike traditional security measures that need to be manually updated, AI systems constantly evaluate their algorithms against fresh data and threat intelligence, enabling them to adapt to changing cyber threats. So organizations stay resilient to ever-evolving threats.

Enhanced Threat Intelligence

AI platforms aggregate and analyze threat data from numerous sources including blogs, forums and more to deliver insights about the latest threats and cybercriminal tactics so that organizations can stay ahead of potential issues.

By leveraging these mechanisms, AI-powered threat intelligence platforms enhance the accuracy and timeliness of cyber threat detection and response, thus making cybersecurity measures more impactful. (Amarasinghe et al., 2019)

3.6.2.2. Personalized Learning Experiences

AI can customise training modules based on the unique learning style and profile of the individual so that tinformation is relevant and engaging to the user (Al-Dhamari & Clarke, 2024)

The ability of AI to tailor training module is boon for the education and professional development sector. Data analytics and machine learning algorithms can analyze the learning patterns of a student, their interests and performance metrics. The information is driven by relevance making the content that individuals recieve interesting and engaging, which results in better retention and understanding. Some learn best from visual content, some tactile exercises, and some in auditory sessions.

Ittailors training materials according to user interactions and feedback. This AI can also adjust training speed, target additional apps/solutions/etc. or provide alternative explanations to help the person better understand the concept they are struggling with.

In addition, AI can learn from user interaction, so it is able to improve over time. This is an iterative process and learners advance at different rates so that as training becomes more complete, it is able to adjust to the learners based on their threshold which determines reward vs challenge outcome to keep them engaged and willing to learn more. AI might not only enhance educational outcomes—but create a more inclusive setting that caters to different learning needs by letting people learn more individually.

And the bottom line is that finding a new way with AI to customize the modules of the training process is a major shift in the method of education; it brings you a closer experience to

the stage of education that you are accustomed to, which is a key to every user, and only with this will everyone work at their best. (Goodfellow et al., 2016)

3.6.2.3. Real-Time Feedback and Adaptation

Conversely, AI technologies provide real-time monitoring of individual progress and adaptable feedback to ensure that the training is effective and current with contemporary cybersecurity threats (Taherdoost, 2024).

AI technologies are prominent in changing the world of training and development, especially in the domain of security. These technology aided systems enabled the continuous assessment on learner performance and understanding at all times through real time tracking and monitoring. Such a dynamic approach makes certain that training programs remain effective and most importantly, are catered towards the needs of the cybersecurity landscape.

Additionally, they incorporate elements of adaptive feedback that respond immediately to the needs of learners. Such responsiveness is critical in a sector in which threats and challenges are ever-evolving. This helps to ensure that training initiatives are relevant and adapt to the evolving landscape of cybersecurity threats, enabling attendees to be equipped with the knowledge and skills required to identify and prevent potential risks.

Case in point, the AI-driven data analysis enables organizations to proactively address emerging threats and keep their workers readied and cognizant (Taherdoost, 2024).

AI does lead to a lot of benefits in strengthening security awareness training, but that doesn't come without its challenges, including the up-front cost of installing algos, and the complexity of integrating AI systems into training frameworks. Moreover, AI models require ongoing updates and maintenance to keep pace with the organizations' needs and the deployment of new threats. However, the advantages of utilizing AI-based training programs offer a strategic approach to enhancing cyber awareness within organizations, overcoming the hurdles of traditional training methodologies.

3.6.3. Leveraging AI in Operational Risk Management (ORM)

Operational risk management is a vital process through which organizations can identify, evaluate, prioritize, and eliminate risks that stem from business workflows and everyday operations. This process is the systematic process for understanding, managing, and monitoring risk in order to mitigate the impact of potential risk to an organization objectives and outcomes.

Artificial intelligence can transform the operational risk management process by enabling organizations to use advanced data analytics, predictive modeling, and real-time monitoring capabilities to identify and mitigate potential risks before they escalate.

Additionally, the incorporation of AI into ORM streamlines predictive analysis while providing small insights into the correlation of risks across different operational areas. A case in point is how machine learning algorithms may assist in analyzing historical incident data to identify hidden correlates between separate types of risk such as those derived from supply chain disruption and cybersecurity threats. By taking insights from across business functions, this holistic approach enables organizations to create a profile of risks that comprehensively informs strategic decision making, enabling enhanced resilience to unforeseen challenges. (Qureshi et al., 2024)

3.6.3.1. Advanced Data Analytics

The potential of Artificial Intelligence (AI) is that it can access and analyze large datasets from various sources. AI allows for the detection of complex interdependencies and emerging trends that could represent possible risks to the company by using advanced algorithms and machine learning strategies. This analytical wisdom will help businesses take a deeper look at their operational systems and get a holistic view of their processes. Consequently, organizations can pinpoint areas that require improvement or intervention. Applying and utilizing these insights enables organizations to take the offensive posture in attack mitigation, streamline operations and improve decision making.

Additionally, advanced data analytics enhances a culture of continuous optimization, enabling organizations to react quickly to shifts in market conditions and avert problems before they develop into larger challenges. This approach leads to not just operational efficiency gained from the targeted integration of AI but also to reinforcing an organization's resilience in a world increasingly governed by data. (Yazdi et al., 2024)

3.6.3.2. Predictive Modeling

By using the power of machine learning algorithms, AI can create advanced predictive models that accurately estimate potential operational risks based on historical data. This additional dimension allows organizations to extract valuable knowledge not just from the past events, but also from new relationships regarding future threats. In short, businesses can be proactive in anticipating challenges and implement precautionary measures in advance of risks becoming ceiling pains by implementing those predictive analytics.

Not only does this enable operational efficiency, but it also promotes a culture of preparedness that helps organizations navigate uncertainties through confidence and agility. (Eder, 2016)

3.6.3.3. Real-time Monitoring

AI systems have this surprising ability to monitor and analysis activities and workflows in real-time—offering a unique types of management for any organization. These systems can recognize anomalies or deviations from established norms in real-time by deploying complex algorithms and machine learning techniques. Such continuous monitoring helps organizations view their processes in real-time, thus keeping a proactive approach against various flaws. Therefore, companies can quickly respond to emerging threats, reducing interruptions and improving operational performance.

Having the capability to receive immediate feedback not only gives the organization the power to make informed decisions, but also brings an agile and responsive culture. Building on real-time awareness enables organizations to drive better results in a complex and fast-moving environment through tilting workflows and increasing resource allocation. (Almari & Festijo, 2019)

3.6.3.4. Automated Risk Assessment

AI revolutionizes the risk assessment process by embedding itself within the process of identifying, assessing, and mitigating risk in organizations. Utilizing complex algorithms and machine learning processes, AI systems can comprehensively analyze countless risk factors, all of which have the potential to impact the responses that we are going to provide. Besides improving the precision of risk assessments, this automated approach also dramatically shortened the timeframe of the entire evaluation process.

AI algorithms assess risks by ranking them according to their impact and probability of occurrence, helping organizations quickly determine which risks are most threatening to organizational objectives. Furthermore, this efficient process allows for data-driven decision making as stakeholders can defer their time and resources to mitigate the critical risks that would have the greatest impact on the organization. Through effectively prioritizing these risks, businesses will be capable to deploy targeted mitigation tasks, spend money on resource allocation efficiency, and as a result, protect their operations from potential disruptions. Such a proactive approach increases not only the organizational resilience but also the climate of risk awareness and risk responsiveness.

3.6.3.5. Enhanced Decision-making

AI Artificial intelligence has transformed the decision-making process using its brilliant ability to quickly analyse and process huge amounts of data. By utilizing this advanced ability, decision-makers can deepen their understanding of complex situations, allowing them to make informed decisions that drastically improve their risk mitigation** AI analytics enables organizations to analyze data effectively, pinpointing them as potential threats and

vulnerabilities, and even giving them a heads up to avoid any potential risks before they start damaging.

Consequently, this enhanced collaborative effort greatly bolsters the organization's overall operational resilience, enabling it to withstand uncertainties and ensure continuity even in the face of adversity. This fundamentally shifts decision-making from a reactionary process to a proactive strategy and promotes an environment where informed decisions yield long-term growth and sustainability.

AI empowers organizations with the ability to detect, evaluate, and mitigate operational risks, which leads to improved business performance and reduced negative effects on achieving organizational goals. (Prasanth et al., 2023)

3.7. Limitations and challenges of AI Models in Risk Management

The risk management process, important to both the private and public sectors, faces challenges related to the need to rapidly adapt to emerging threats such as financial instability, cyber security risks and operational failures. Traditional risk management techniques are primarily based on static models and manual oversight, which inevitably limits their effectiveness in fast-changing, data-driven environments. (BOOK - Artificial Intelligence for Risk Mitigation in the Financial Industry - 2024 – Mishra pg.9)

The perception of risk depends on the observer's cognitive biases and world view which nuance risk related decisions. How an observer decides also depends on the metric used to quantify risk. While there is extensive literature on how people perceive risk, and on how to price risk in relation to the market, there is little on how to price risk according to how risks interact within the firm. (Annette, Hofmann., Nicos, A., Scordis. (2017). Challenges in Applying Risk Management Concepts in Practice. Social Science Research Network, DOI: 10.2139/SSRN.3083144)

Moreover, the need for continuous operation of the risk management system as well as its continuous adaptation to changing environments is a given. This is not only about identifying known risks, but also anticipating unforeseen threats through iterative processes and involving all stakeholders (REGULATION (EU) 2024/1689 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL).

While AI-based models offer considerable advantages, they also present limitations:

3.7.1. Complexity and Interpretability

Advanced AI models, and particularly deep neural networks, bring major complications with regards to risk management. These models, extremely strong in terms of its predictive

capabilities, are commonly used as a black box which hides all information about the processes behind its conclusions. This lack of transparency creates a significant barrier for managers and others who depend on these systems to make informed decisions about risk. The dismal interpretability of these complex models can entail a deep lack of transparency. This makes it harder for risk managers to link specific inputs to the outputs they help achieve, a critical step in validating the statistical significance of risk predictions.

In areas where risk assessments have significant implications, such as the financial sector, such non-interpretable nature can result in lack of trust in AI-driven insights. States holders might avoid making steps based on suggestions that are primarily based on models they don't comprehend, leading it to mistrust inside the effectiveness of AI in fundamental decision making processes (Miller, 2019).

Additionally, a lack of transparency regarding the justification for AI-generated predictions can impede regulatory compliance and risk governance. Balance this with your own judgment and understanding of the liability of explaining to regulators or clients or others the rationale of an AI-derived decision. This is why the complexity and interpretability of AI models are critical components that organizations need to overcome to make the most of artificial intelligence in reducing risk.

3.7.2. Data Quality and Availability

AI models can only be effective in risk management if they are backed by quality and quantity of data. These models rely heavily on data — lots of it, and high quality, to render accurate predictions and decisions.

But then a major stumbling block comes when the data is inconsistent, incomplete, or of inferior quality. These shortcomings can critically compromise the models' accuracy and reliability, resulting in misguided conclusions and possibly harmful consequences. In many fields—especially those involving risk assessment, like finance, insurance, and healthcare—data can be scarce or intrinsically unreliable. Historical data, for example, may no longer represent what is happening on the ground today, and data collection can be loaded with errors or bias. The situation is further complicated by the fact that organizations might use different data sources and methods for risk measurement, which makes it hard to join and analyze the information on risks.

Additionally, risk factors are dynamic in nature and thus the data on them need frequent updating and validation to keep the model relevant. In dynamic environments—like financial markets or public health crises—AI models may give stale predictions unless they have access to real-time or high-frequency data.

As a result, when those who rely on antiquated or inadequate data gain such insights, it can create enormous risks that compromise organizations' ability to respond to new and emerging threats effectively. In conclusion, the hurdles that data quality and availability present are a key challenge in AI risk management, requiring continuous investment in better methods for collecting, validating, and integrating data so that it is useful for risk decision-making.

3.7.3. Ethical Concerns and Bias

The science examines the ethical implications surrounding the application of AI models in risk management, particularly the problems relating to the potentially compound reinforcement of historical bias present in the data that is implemented in the AI models. This means they can be biased in many different ways, leading to unfair or discriminatory outcomes that affect certain groups of people more than others. To take an example from the world of credit scoring, AI models trained on data from the past may encode the biases prevalent in society, thus resulting in systemic discrimination in loan approvals. These result in biased outcomes that could perpetuate cycles of disadvantage for certain population groups, especially those who are marginalized, further solidifying inequity in financial resource access (Fletcher & Neuberger, 2021).

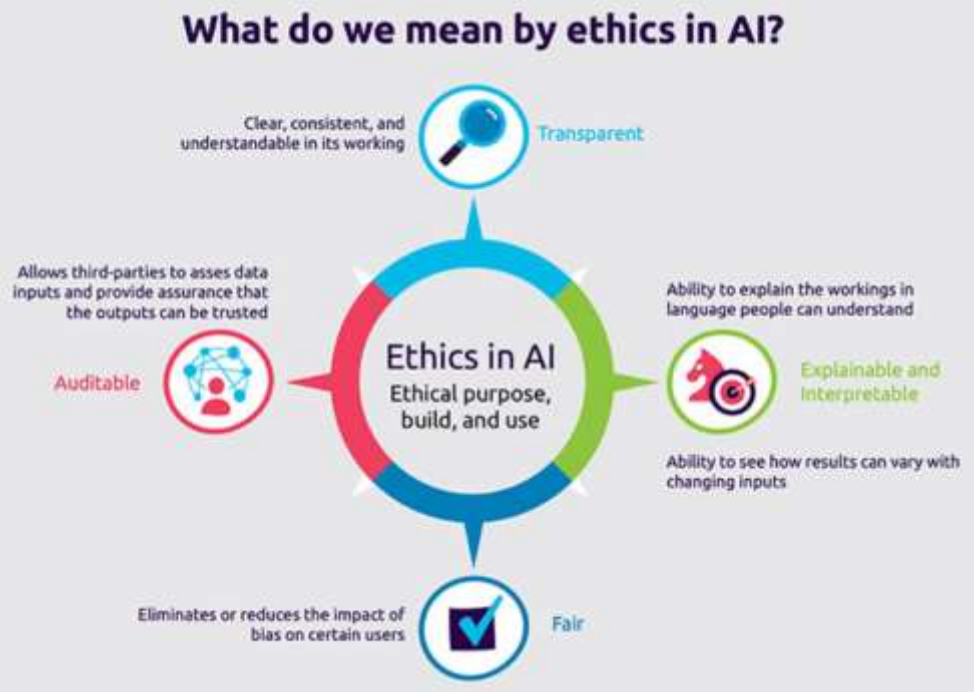

Image Source: https://www.markovml.com/blog/ethical-ai - Navigating Ethical AI: Challenges and Strategies Involved!

These biases are difficult to identify and mitigate, given the lack of transparency in AI algorithms. This makes it difficult for stakeholders to know how decisions are made, and leads

to potential concerns over accountability and transparency. Such vagueness could smooth the path for tech companies to prove that their AI systems run fairly and ethically, weakening trust in these technologies.

With organizations turning to assistive AI to inform more critical risk management decisions, it is crucial to mitigate other ethical concerns through proper governance frameworks, continued bias assessments, and stakeholder inclusivity in the production of AI models.

3.8. Key Themes in the Literature

3.8.1. Predictive Power of AI in Financial Risk

AI has been shown to greatly outperform its predictive power across finances risk managment in the literature. Evidence from research reveals ML (machine learning) algorithms, especially supervised learning models, enhance credit scoring, fraud detection, and investment due-diligence processes. Thus, for example, Jordan and Mitchell (2015) state that ML techniques can identify complex patterns in large financial datasets to enable institutions to accurately predict fraud or predict loan defaults. Further validating this perspective, a meta-analysis conducted by Makridakis (2017) highlighted that AI-powered models consistently outperformed traditional models by 10–15% in financial risk prediction, demonstrating substantial advancement in forecasting risks.

Despite these advances, problems remain with the interpretability of complex models. As a result, many of these AI models, like deep neural networks, are considered black-box models, which makes it hard for financial professionals to comprehend how decisions are made (Miller, 2019). In highly regulated financial environments, such opacity can be problematic since decisions must be explainable for compliance reasons. Literature argues that the opacity associated with the use of AI models leading to questions about the ethical implications of their use, particularly in high-stakes domains like credit risk, as developers of opaque models may inadvertently reinforce biases against certain demographics (Fletcher & Neuberger, 2021).

3.8.2. AI's Role in Cybersecurity Risk Management

In the cybersecurity domain AI models has shown great findings in detecting and mitigating cyber threats. Using deep learning algorithms and neural networks to analyze network traffic in real-time, organizations can spot anomalous behavior that could indicate an impending attack. According to Fletcher and Neuberger (2021) researches, AI-powered cybersecurity solutions can perform an analysis of relevant information and be able to filter out false alarms in a timeframe that reduce time response by up to 70% compared to the traditional

way of working. AI's capacity for continuous learning also enables these models to adapt to emergent threats faster than signature-based security systems (Bostrom, 2017).

The use of AI in cybersecurity, however, is not without concerns related to data privacy. According to Ng and Jordan (2020), data-driven models require a large amount of data and can invade privacy if not used with caution. Moreover, according to Fletcher and Neuberger (2021), when it comes to surveillance and monitoring, AI may pose ethical concerns, especially when it is implemented to monitor the behavior of either employees or consumers without their consent.

3.8.3. Operational Risk Management in Supply Chains

AI usage in operational risk management—especially for supply chains—is a popular topic of research and literature. Baryannis et al. (2019) show how machine learning can predict supply chain disruptions including delayed or change in demand through analysis of risk factors. Predictive analytics helps organizations in developing proactive strategies to avert disruptions across the supply chain. This view is supported by Brynjolfsson and McAfee (2017), highlighting that AI-enabled models within the context of supply chain management will strengthen resilience up to 30 percent through dynamic adjustment of operations.

These advantages are met with challenges, however, as highlighted in studies related to data standardization. This data inconsistency across regions limits the applicability of AI models in the global supply chain. Goodfellow, Bengio and Courville (2016) pointed out the need for high standardised quality of data for reliable risk prediction, a challenge that continues to be unsolved for most micro/multinational operations.

3.9. Gaps in the Literature

The literature review however shall provide an overview of all previous work that is at least somewhat relevant to the topic of this dissertation. A systematic review of scientific journals, papers and articles related to AI applications in Risk Management is covered in the dissertation.

The review synthesizes theoretical frameworks, methodologies, and findings from previous studies using keywords such as "Artificial Intelligence in risk management," "machine learning in finance" and "predictive analytics in risk." Indeed, this literature review serves to make clear the gaps that exist in the literature and provide a framework for finding new directions for research that could help integrate AI alcohol technologies further into risk practices.

At the same time, there are many different areas within the adoption of Artificial Intelligence (AI) in risk management that have as of yet not been adequately explored. Therefore, this part finds gaps in current literature and points out the potential of further

investigation to be a part of the current world of AI to easen the prevention, managing and control of the risk.

3.9.1.1. Limited Research on AI's Role in Regulatory Compliance

Although the capability of artificial intelligence (AI) to monitor and make sense of complex regulatory frameworks is fairly well accepted, a significant gap in the research literature is the effectiveness of AI systems in appropriately interpreting and responding to the nuanced and frequently nebulous language found in these regulations. Examples include natural language processing (NLP) models used to analyze legal texts, but inherently understanding legal nuances is difficult.

This complexity is exacerbated by the need to make certain you are compliant in different jurisdictions with unique regulations and interpretations. This suggests the need for more expansive studies that look not only at how AI can parse facets of legal language, but also get a sense of how it contextualizes such parsing with the wider regulatory framework. Such investigations are vital in developing AI systems that are robust and reliable enough to assist with compliance with legal obligations, including regulatory analysis and monitoring, thus facilitating legal practice in an increasingly complex global environment

3.9.1.2. Ethical Concerns and Bias Mitigation

The ethical dilemmas posed by artificial intelligence (AI), particularly the biases that often underlie AI algorithms have received considerable attention in recent years. There have been, however, a relative lack of thorough research on specific measures for tackling these biases, even though this awareness is slowly increasing. Fletcher and Neuberger (2021) also note the urgent dangers of discriminatory outcomes in key areas like credit scoring and hiring practices. Their efforts highlight the risk that AI systems could reinforce existing inequalities and amplify social injustices if not carefully regulated.

The literature is alarming for ushering into a rare species of publications which promise to deliver actionable approaches to change the landscape of fairness and accountability in risk frameworks only powered by intelligence end-products. That said, this lack of strong guidance brings exclusive challenges if organizations want to implement processes to reduce bias in AI, which means that should put more effort to create and reproductive effective bias mitigation measures.

3.9.1.3. Interpretability and Transparency of AI Models

One of the greatest and most persistent challenges pointed out by the literature is the inherent difficulty, due to the complexity of the systems we could use, to have them explain their mutual understanding, especially deep neural networks. These complex, highly

parameterized black-box architectures effectively hide the decision-making processes underlying their outputs, which can critically undermine trust and usability, especially in high-stakes domains such as financial risk management. These models have become increasingly opaque, a factor that worries stakeholders that demand a clear, comprehensible rationale for decisions that might have significant financial consequences. (Rubin, 2020)

Miller (2019) underscores the critical importance of developing explainable AI (XAI) systems, highlighting the need for approaches that can unveil the functioning of these high-level models. He claims that the practical implementation of XAI in risk management context still needs a lot of explanation. Such a gap highlights one of the main areas of focus for future research and development, as incorporating explainability into AI systems may help increase their reliability and trustworthiness in the eyes of practitioners. Establishing a better understanding around how AI models come to certain conclusions will enable stakeholders to make better decisions, reducing risk and improving overall confidence in AI-backed financial strategies.

3.9.1.4. Inconsistent Data Quality and Availability

The effectiveness of artificial intelligence (AI) is heavily dependent on the quality and consistency of the data it utilizes. This dependency poses a substantial challenge, particularly in sectors characterized by incomplete or inaccessible risk data. The intricate nature of these industries often leads to a scarcity of reliable information, which is crucial for training robust AI models. Ng and Jordan (2020) emphasize the difficulties organizations encounter in their efforts to develop sophisticated AI systems, especially in emerging markets or niche industries where data may be sparse or fragmented. In these contexts, the lack of comprehensive datasets can hinder the ability of AI algorithms to learn effectively, resulting in models that may not perform optimally or make accurate predictions.

Moreover, the variability in data quality can introduce biases, leading to unreliable outcomes that could negatively impact decision-making processes. As organizations strive to harness the power of AI, addressing these data-related challenges becomes paramount. This involves not only improving data collection methods but also ensuring that the data used is representative and of high quality, thereby enabling more effective and trustworthy AI applications.

3.9.1.5. Underrepresentation of AI Applications in Specific Risk Domains

AI Applications Not Fully Explored in Some Risk Domains While AI applications have been explored extensively in the context of financial and cybersecurity risks, the available literature on AI applications in other domains such as health, environmental risk management, and geopolitical risks is scarce. Through robust data and solution extraction from these four domains

— none of which have been sufficiently adopted by AI to address complex decision making and risk mitigation challenges — parallels will be drawn for more advanced AI implementations. In the medical field, AI could transform patient care in ways unimaginable, enabling the disease outbreak forecasting, the creation of personalized treatment strategies, and the milk to herd use of resources in the most efficient way possible. (Guikema, 2020)

Nonetheless, the existing literature contains no studies that examine how AI can be used to mitigate risks in the process of health care delivery, especially in risk-prone situations such as global health crises. Likewise, artificial intelligence could revolutionize environmental risk management, including tackling climate change, natural disasters, and ecological degradation. Utilizing machine learning algorithms in conjunction with big data analytics, we might be able to construct more precise predictive models to better alert policymakers and communities of looming environmental cataclysms. However, the volume of research done on caching to date is relatively scarce, leaving opportunities untapped. In addition, the geopolitical landscape is one where there are many uncertainties that would be ripe for AI-driven insights. AI—by examining conflict patterns, predicting dynamics of international relations and so on—may also help in improving the understanding of global risks. (Wahl et al., 2018)

Yet, AI applications in this space remain scarce, suggesting a critical blind spot we must address in order to take more informed and anticipatory approaches to international affairs. Researching these underexplored areas would help broaden our understanding of what AI is capable of, and how these technologies can be harnessed to mitigate a wider range of risks. Fulfilling this promise will help us realize the potential of AI, which must be an enabler of transformation across sectors and domains.

3.9.1.6. Lack of Longitudinal Studies

While there are various studies of contextualization of AI in risk management, not much is available regarding longitudinal studies. The majority of previous research focuses on short-term effects, largely presenting a current overview of AI's impact on society without returning to analyze future ramifications. Understanding AI as a static tool in this way misses the fluid nature of AI systems and their changing roles within organisations. Longitudinal studies are key to understanding how AI technologies evolve and, in the fast-evolving risk landscape presenting itself to organizations, how they are adapted to address it. These studies can help organisations, which use artificial intelligence systems, valiantly fight against their markets by exchange experiences of how AI systems improve their adaptability.

Also, from a strategic decision-making standpoint, investigating the effects of AI on decision-making processes in the long run would show how these systems shape strategic decisions, risk approaches, and overall governance strategies in organizations. This longitudinal

approach reveals that AI is not simply a tool for mitigating risk, but also a force transforming organizations and their risk management culture.

This new perspective is critical for both organizations that want to use AI effectively and sustainably as part of their risk management strategies. (Aziz et al., 2018)

3.9.1.7. Integration Challenges with Existing Risk Management Frameworks

Much of the research ignores the practical difficulties in embedding AI technologies into conventional risk management systems. For example, work by Brynjolfsson and McAfee (2017) underscored the competitive implications of AI, but did not consider organizational, technical and cultural impediments to its adoption.

Fulfilling these laundry lists in the literature is key to a step forward in AI-based risk management. Further studies should concentrate on designing AI system that is transparent, ethical, and flexible in addition to investigting AI in new risk domains where application is rare. Moreover, initiatives to enhance data quality, regulatory adherence, and integration with conventional structures will guarantee the successful use of AI in the management of intricate and evolving threats.

3.10. Critical Analysis of the Literature

3.10.1. Achievements with AI Based Risk Management

The literature review articulates the transformative capabilities of AI which, particularly in the health sector, in predictive accuracy, in operational speed and adaptability. Notably, AI models when compared to the traditional analytical frameworks have better performance, particularly in the Finance and cyber security domains. In the words of Ng and Jordan (2020), AI's exceptional ability to efficiently process enormous data sets gives organizations the ability to be more evidence-based and proactive in their approach to risk management. Such a shift improves the accuracy of risk-predictions and allows for timely interventions.

Furthermore, the capacity for AI systems to perform monitoring in real time and offer predictive insights has drastically altered the landscape of risk mitigation for many organizations. As noted by Goodfellow et al. (2016) this abilities identifies problems before the mentioned process becomes serious this indicates is the ability that organizations can find out and ensure their assets by taking precautionary measures before issues become bigger.

Incorporating AI into risk management leads to more agile and proactive methodology that allows businesses to tackle the complexities of contemporary challenges with more confidence and efficiency.

3.10.2. Challenges and Limitations

Although there are significant advancements in regards to artificial intelligence, there are still many limitations, particularly in high-stakes industries where the results of decisions made by AI can have monumental consequences. A major problem lies in the fact that highly complex AI systems, especially ones utilizing deep-learning approaches, are "black boxes" in essentially all practical situations. Such black-box nature limits interpretability because stakeholders find it impossible to comprehend the decision-making process (Miller, 2019). In some domains, like those of healthcare, finance, law enforcement or any other area where transparency is critical, failure to explain the reasons behind an outcome on which an AI system that has been applied can generate distrust and unwillingness to use these technologies.

Additionally, the performance of AI systems depends heavily on the existence of large, high-quality datasets. In settings where data may be inconsistent, nonrepresentative, missing or otherwise unreliable (Ng & Jordan, 2020), this reliance poses a significant challenge. In these situations, the chances of using an AI-solutions that provide invalid or misleading results are high, potentially making things worse, rather than helping to solve existing problems. Questions related to the ethics of AI applications are also a hot topic. Fletcher and Neuberger (2021) found that processes like compliance monitoring and credit risk assessment could also produce discriminatory results, and bias in data is one of the most significant issue. The consequences of these biases are significant since they can contribute to systemic inequities and compromise the integrity of decision-making processes in multiple sectors. Moreover, the literature review mentioned some gaps that can be found in the current literature, that bettering them, represent a promising future research line.

Most studies refined on AI used for improvement of financial and cybersecurity risks, but few studies on AI in compliance. We are yet to see how AI can be utilized for compliance, and this is a great gap needs to be filled as AI can well be integrated as part of compliance framework and reduce a major part of regulatory and risks compliance.

Further, the exploration of ethical implications and ways to mitigate bias are still in their infancy in the context of AI derivatives risk management systems. More broadly, some scholars such as Bostrom (2017) and Miller (2019) have not only called for necessary steps to deepen the risk argument but to also wrench the frame of AI beyond a risk paradigm so that we can understand what it means for AI to operate fairly, transparently, and ethically. As AI continues to evolve, these issues must be considered not only for the sake of the continued development of AI technologies, but also for the sake of public trust and equity in society.

3.11. Summary

The AI in risk management literature shows AI is effective in predictive modeling and decision-making especially in finance, cyber security, and operations. Nevertheless, transparency, data quality, and ethical concerns persist as major hurdles to overcome. This review outlines the main themes, successes and limitations, which will set the ground for a more practical analysis of AI in the next chapters.

Artificial intelligence, applied to risk management, overcomes some key constraints behind traditional approaches. Through automated data analysis, improved predictive capabilities, and real-time monitoring, AI helps companies take a more proactive stance on risk management. In addition, this transition not only enhances the quality and swiftness of risk identification, but also developments in better decision-making, enabling leaders to respond wisely and proficiently to probable threats.

Artificial Intelligence (AI) has been adopted in multiple risk domains and is changing the way we manage risk. AI can also increase the accuracy of forecasting market volatility, detecting fraud3, and assessing credit risk4 in the financial sector through powerful machine-learning algorithms that utilize real-time data. Cybersecurity is another area where AI in data science is proving beneficial, as the technology's growth pattern recognition enables organizations to take preventive action against future threats — so security systems become stronger over time.

Moreover, logistics performance analytics language also enables companies to anticipate and mitigate supply chain disruptions, helping them take assure operational resilience as part of operational risk management.

It helps organizations to not only overcome the limitations of traditional risk-related decision-making but also creates a more informed and proactive decision-making environment that helps improve organizational agility and sustainability in the ambiguous risk landscape.

4. Comparative between Traditional and AI -Based Risk Management

4.1. How do AI-Based Risk Management systems compare to traditional method in terms of efficiency and accuracy?

AI-based risk management systems have shown significant improvements in efficiency and accuracy compared to traditional methods. These systems leverage advanced machine learning algorithms and neural networks to enhance predictive capabilities and manage financial risks more effectively. The integration of AI technologies not only improves the precision of risk assessments but also offers resilience against multiple risk factors. However, the adoption of AI in risk management also introduces challenges related to regulatory compliance and model interpretability. Below are the key aspects of how AI-based systems compare to traditional methods:

4.1.1. Efficiency and Accuracy

AI-based systems, such as those using gated recurrent units (GRU) and temporal convolutional networks (TCN), have demonstrated superior performance in risk prediction accuracy and efficiency. For instance, they have reduced floating point operations (FLOPs) by over 46.8% and improved inference time by more than 48.5% on datasets like Lending Club (Quan et al., 2024).

Artificial Neural Networks (ANNs) and Deep Neural Networks (DNNs) have outperformed traditional methods like logistic regression and support vector machines in predicting financial risks, as evidenced by higher accuracy, precision, recall, and F1-scores in model testing (Farazi, 2024).

4.1.2. Integration and Resilience

Combining AI with traditional risk management approaches has resulted in improved performance outcomes and increased resilience to various risk factors. This hybrid approach leverages the strengths of both methodologies to enhance overall risk assessment accuracy (Farazi, 2024).

4.1.3. Regulatory Compliance and Challenges

While AI enhances predictive efficiency, it also poses significant legal and compliance challenges, particularly concerning regulations like Basel III and GDPR. Ensuring compliance while utilizing AI technologies is crucial for maintaining financial stability and customer confidence (Sarioguz & Miser, 2024).

Despite the advantages of AI-based systems, there are concerns regarding the interpretability of AI models and the need for substantial data for effective training. Future research should focus on improving model transparency and exploring reinforcement learning for decision-making in financial risk management (Farazi, 2024).

4.1.4. Literature review - How do AI-Based Risk Management systems compare to traditional method in terms of efficiency and accuracy?

Authors / Year / Title / Journal / DOI	Literature Survey	Contributions	Research Gap
Jomthanachai, S., Wong, W. P., & Lim, C. P. (2021). **An Application of Data Envelopment Analysis and Machine Learning Approach to Risk Management**. *IEEE Access*, *9*, 85978–85994. DOI: 10.1109/ACCESS.2021.3087623	- This literature review covers risk management methodologies, specifically focusing on the applications of Failure Mode and Effects Analysis (FMEA) and Data Envelopment Analysis (DEA) methods, as well as the integration of DEA cross-efficiency and machine learning approaches in risk management. It highlights the limitations of the standard FMEA model, particularly the issues related to the crisp Risk Priority Number (RPN) scores and the inadequacy of the RPN technique in complex systems with multiple subsystems. - The review emphasizes the advantages of using the DEA method to address the mathematical formula issues associated with RPN computation, allowing for the consideration of both direct and indirect relationships between failure modes. It also discusses the effectiveness of machine learning as a predictive tool in the risk management process, particularly in the mitigation and monitoring stages, demonstrating its robustness when combined with DEA for reliable results.	- The paper proposes an **integrated method that combines the DEA cross-efficiency model with the FMEA technique for risk assessment**, enhancing the existing methodologies by providing a higher discrimination capability of decision units and addressing some limitations of both FMEA and traditional DEA. - It introduces the **application of machine learning (ML) algorithms, specifically neural network models, for predicting the new level of risk based on efficiency scores**, demonstrating that the predictive power of ML is superior to that of the DEA re-conducted scheme, thereby improving the accuracy of risk treatment and monitoring processes.	- The paper highlights the limitations of traditional FMEA and DEA methods, indicating a **gap in their effectiveness for risk assessment and management**. While the proposed FMEA-DEA cross-efficiency method addresses some of these drawbacks, there remains a need for further exploration of integrated models that can enhance qualitative risk management, especially in contexts where comprehensive quantitative data is not available. - Although the study demonstrates the predictive power of machine learning (ML) in risk treatment and monitoring, it suggests that the DEA cross-efficiency method may not be as reliable for prediction purposes. This indicates a **gap in understanding the comparative effectiveness of various predictive models in risk management**, warranting further research into optimizing the integration of

			DEA and ML approaches for improved accuracy and robustness in risk assessments.
Katib, I., Albassam, E., Sharaf, S., & Ragab, M. (2024). **Harnessing probabilistic neural network with triple tree seed algorithm-based smart enterprise quantitative risk management framework.** *Dental Science Reports*. DOI: 10.1038/s41598-024-73876-w	- The paper discusses the importance of Enterprise Risk Management (ERM) frameworks in fostering a consistent risk management culture across organizations, emphasizing the role of statistical pattern recognition, artificial intelligence, and data science in enhancing enterprise management systems (EMS) for long-term success. - It highlights recent advancements in artificial intelligence, machine learning, and deep learning that have led to the development of effective risk assessment models, specifically introducing the Improved Metaheuristics with a Deep Learning Enabled Risk Assessment Model (IMDLRA-SES) which utilizes feature selection and deep learning to estimate business risks and classify financial hazards.	- The study **introduces the Improved Metaheuristics with a Deep Learning Enabled Risk Assessment Model (IMDLRA-SES) for Smart Enterprise Systems**, which utilizes feature selection and deep learning models to effectively estimate business risks by transforming original financial data into a usable format through preprocessing. - The paper **employs a triple tree seed algorithm (TTSA) in conjunction with a probabilistic neural network (PNN) model** to classify the presence or absence of financial hazards in firms, enhancing the efficiency of the PNN-based categorization and achieving superior accuracy values of 95.70% and 96.09% on German and Australian credit datasets, respectively.	- The paper emphasizes the **need for further exploration of interdisciplinary applications of applied probability and statistics within enterprise risk management frameworks, indicating a gap in existing research that integrates these fields effectively for enhanced risk assessment models**. - There is a lack of comprehensive studies that evaluate the long-term effectiveness and adaptability of the Improved Metaheuristics with a Deep Learning Enabled Risk Assessment Model (IMDLRA-SES) in various industry contexts, suggesting a **gap in understanding how these models perform across different enterprise environments and conditions**.

Tian, X., Tian, Z., Khatib, S. F. A., & Wang, Y. (2024). **Machine learning in internet financial risk management: A systematic literature review.** *PLOS ONE* DOI: 10.1371/journal.pone.0300195	- The literature review in the paper focuses on the **current status of the application of various machine learning models and algorithms in internet finance risk management across different institutions**. - Scholars have conducted studies comparing different algorithms within specific platforms and contexts, highlighting the advancements made by machine learning in predicting accuracy, time efficiency, and robustness in internet finance risk management compared to traditional credit scoring methods.	- The paper conducts a systematic literature review on **the application of machine learning in internet finance risk management**, analyzing trends in publications, geographical distribution, and the focus of existing literature, which provides a comprehensive overview of the current state of research in this domain. - **It highlights the advancements of machine learning over traditional credit scoring methods in terms of prediction accuracy, time efficiency, and robustness**, while also noting the disparities among different algorithms and the influence of model structure, sample data, and parameter settings on prediction accuracy, emphasizing the need for tailored machine learning solutions for different internet finance platforms.	- The paper highlights a **lack of comprehensive discourse and summary on the utilization of machine learning in internet finance risk management**, as existing studies predominantly focus on comparing different algorithms within specific platforms and contexts rather than providing a holistic view of the application across various institutions. - There is no optimal machine learning algorithm identified that is suited for the majority of internet finance platforms and application scenarios, indicating a **research gap in determining a standardized approach that can be effectively applied across different platforms, taking into account their unique characteristics and data.**
Babaei, G., Giudici, P., & Raffinetti, E. (2024). **A Rank Graduation Box for SAFE AI**. *Expert Systems with Applications*. DOI: 10.1016/j.eswa.2024.125239	- The paper contributes to the development of Artificial Intelligence risk management models by proposing a Rank Graduation Box (RGB), which integrates statistical metrics to measure key aspects of AI applications, including "Sustainability," "Accuracy," "Fairness," and "Explainability." These metrics are derived from a common statistical methodology, the Lorenz curve, ensuring consistency among them.	- The paper contributes to the development of Artificial Intelligence risk management models by **proposing a Rank Graduation Box (RGB), which is a set of integrated statistical metrics designed to measure the "Sustainability", "Accuracy", "Fairness", and "Explainability" of any AI application**. These metrics are derived from a common statistical methodology,	- **The paper does not explicitly identify or discuss any limitations or gaps in the proposed Rank Graduation Box (RGB) metrics**, which could be important for understanding the boundaries of their applicability and effectiveness in various contexts of Artificial Intelligence applications.

	- The validity of the RGB metrics is demonstrated through their application to both simulated and real data, showing that they provide more interpretable and consistent results compared to standard metrics like AUC, RMSE, and Shapley values. The findings indicate that different machine learning models exhibit varying strengths, with linear regression models being the most accurate, regression tree models being the most fair, and Random Forest models being the most robust.	the Lorenz curve, ensuring consistency among them. - The validity of the RGB metrics is demonstrated through their application to both simulated and real data, showing that they provide more interpretable and consistent results compared to standard metrics like AUC, RMSE, and Shapley values. The findings indicate that different machine learning models exhibit varying strengths, with linear regression models being the most accurate, regression tree models being the most fair, and Random Forest models being the most robust.	**- There is no mention of how the RGB metrics perform in comparison to other emerging risk management models or frameworks in the field of Artificial Intelligence**, which could provide insights into their relative strengths and weaknesses.
Liu, Y. (2023). **Discussion on the Enterprise Financial Risk Management Framework Based on AI Fintech**. *Decision Making*. DOI: 10.31181/dmame712024942	- The paper discusses the challenge of interpretability in deep learning algorithms for financial risk management, highlighting the importance of understanding the decision-making process to enhance trust and acceptance of risk decisions by enterprises. - The study introduces an improved random forest algorithm based on the decision tree algorithm, which shows a significant improvement in the AP value compared to the traditional RF algorithm, indicating a better balance between precision rate and recall rate.	- The paper **introduces an improved random forest algorithm based on the decision tree algorithm to enhance interpretability in the decision-making process of financial risks**. This improvement addresses the issue of understanding the judgment basis and decision-making process of algorithms, potentially increasing trust and acceptance of risk decisions by enterprises. - Through experimental analysis, the paper shows that the enhanced random forest algorithm **achieves a significant**	- The paper highlights the **lack of interpretability in deep learning algorithms, which affects the understanding of the decision-making process in financial risk management**. This research gap emphasizes the need for more transparent and interpretable AI models in the field of enterprise financial risk assessment. - The study introduces an improved random forest algorithm but **does not extensively compare it with other state-of-the-art algorithms in the field of financial risk prediction**. This research gap

		improvement in the AP value compared to the previous RF algorithm, demonstrating a good balance between precision rate and recall rate. Additionally, the algorithm outperforms other algorithms like SVM and CRAT in financial risk prediction, showcasing higher test values and accuracy rates.	suggests the potential for further research to conduct more comprehensive comparative analyses with a wider range of algorithms to validate the superiority of the proposed model.
Thekdi, S. A., & Aven, T. (2024). **Evaluation of information quality derived from AI-related information systems used for risk applications.** *Journal of Risk Research*. DOI: 10.1080/13669877.2024.2340013	- The paper focuses on the increasing prevalence and accessibility of artificial intelligence technologies, such as text and image generators, which have been both criticized and promoted for their potential to automate tasks and increase efficiencies. - It highlights the need to vet these new technologies for use in risk applications, regardless of their original design purpose, and proposes 14 criteria based on current risk science quality indicators to gauge the quality of information derived from AI-related information systems for risk applications.	- The paper **develops 14 criteria based on current risk science quality indicators to evaluate the quality of information derived from AI-related information systems used for risk applications**. - These criteria are then **applied to a widely used AI-based information system to demonstrate their effectiveness in assessing the quality of information generated by such systems for risk purposes**.	- The paper highlights the need to vet AI-related technologies for use in risk applications, but **it does not delve into specific methodologies or frameworks for conducting this vetting process**. - While the paper provides 14 criteria for evaluating the quality of information derived from AI-related information systems, **it does not discuss potential limitations or challenges in applying these criteria in real-world scenarios**.

	- The paper highlights the limited amount of research that has evaluated AI tools' performance in risk management, emphasizing the gap in the literature regarding the accuracy of AI tools like ChatGPT in this domain. - It discusses the findings of the study, indicating that ChatGPT has a moderate level of performance in managing risks, with more accurate knowledge provided in risk response and risk monitoring compared to risk identification and risk analysis sub-processes.	- The paper **investigates the accuracy of ChatGPT in risk management across different project types**, providing insights into its performance and establishing a foundation for future research in the application of AI tools for risk-based decision-making in the construction industry. - The findings **reveal that ChatGPT demonstrates a moderate level of performance, particularly excelling in risk response and risk monitoring, while showing less accuracy in risk identification and risk analysis**, thereby informing decision-makers on the potential of technology-driven risk management to enhance resilience in business operations.	- Limited research has been conducted to evaluate the performance of AI tools, specifically ChatGPT, in the domain of risk management, highlighting **a gap in understanding the effectiveness of AI in this context**. - The paper **identifies a need for further investigation into the accuracy of ChatGPT across different project types**, emphasizing the importance of expanding research to encompass a broader range of construction projects for a more comprehensive assessment.
Fraisse, H., & Laporte, M. (2022). Return on Investment on Artificial Intelligence: the Case of Bank Capital Requirement. *Journal of Banking and Finance* DOI: 10.1016/j.jbankfin.2022.106401	- The paper contributes to the literature by utilizing AI techniques to compute banks' capital requirements for predicting corporate defaults, highlighting the impact of these techniques on banks' incentives to invest in AI. - It singles out neural networks as a promising AI technique that not only meets regulatory expectations but also leads to significant reductions in Risk-Weighted Assets (RWA), outperforming the traditional approach in terms of performance.	- The paper **provides an empirical exercise that computes banks' capital requirements using AI techniques to predict corporate defaults**, thereby contributing to the literature on the intersection of AI and banking regulations. - **It identifies neural networks as the most effective AI technique for meeting regulatory expectations and achieving significant reductions in risk-weighted**	- The paper highlights a **research gap in the literature regarding the impact of AI techniques, specifically neural networks, on banks' capital requirements for predicting corporate defaults**. It emphasizes the need for further exploration into the incentives for banks to invest in AI models based on the potential reduction in capital requirements.

		assets (RWA), highlighting the limitations of traditional models that rely on logistic regression and expert judgment.	- Another research gap identified is the **variation in capital requirements depending on the statistical methodology used by banks in developing their internal credit risk models**. The paper suggests the importance of investigating how different AI techniques, such as random forest, gradient boosting, ridge regression, and neural networks, can influence the level of capital required by banks.
Dhieb, N., Ghazzai, H., Besbes, H., & Massoud, Y. (2020). **A Secure AI-Driven Architecture for Automated Insurance Systems: Fraud Detection and Risk Measurement.** *IEEE Access*. DOI: 10.1109/ACCESS.2020.2983300	- The literature review highlights the growing interest in blockchain technology beyond finance and banking, emphasizing its potential applications in various sectors, including information security, healthcare, logistics, and insurance. It discusses how blockchain can enhance transparency and automation in the insurance domain, particularly for health insurance companies, by ensuring the integrity and validation of health data records. - It also notes that while many machine learning algorithms are traditionally batch-based, the paper proposes the use of the XGBoost algorithm for predicting risky clients and detecting fraudulent claims. The review indicates that XGBoost outperforms other algorithms, such as decision trees, naive bayes, and nearest neighbor algorithms, in terms of accuracy for fraud	- The paper **proposes a novel Smart Insurance System based on Blockchain and Artificial Intelligence (SISBAR) that aims to automate claims processing, estimate client risk levels, and detect fraudulent claims**, thereby enhancing the efficiency of insurance operations and reducing reliance on traditional, time-consuming methods that depend on human scrutiny. - It introduces the use of the extreme gradient boosting (XGBoost) machine learning algorithm for fraud detection and risk measurement, demonstrating significant performance improvements, such as achieving 7% higher accuracy in detecting fraudulent claims compared to decision tree models, and providing an	- The paper primarily focuses on the implementation of the XGBoost algorithm for fraud detection and risk measurement but **does not explore the potential limitations or challenges associated with the deployment of machine learning models in real-world insurance scenarios, such as data quality issues, model interpretability, and the impact of changing regulations on model performance**. - While the proposed framework integrates AI and blockchain technologies, the paper **lacks a comprehensive discussion on the scalability of the blockchain component, particularly in handling large volumes of transactions and data sharing among multiple insurance agents**, which could

	detection and risk prediction in the insurance sector.	online learning solution to adapt to real-time updates in the insurance network.	affect the overall efficiency and effectiveness of the automated insurance system.
Sun, J. (2023). **Theoretical and practical research on mathematical modeling of economy and finance based on artificial intelligence.** *Applied Mathematics and Nonlinear Sciences* DOI: 10.2478/amns.2023.2.00199	- The paper focuses on developing an artificial intelligence economy in China to benefit economic transformation, industrial upgrading, and enhancing international competitiveness. - The research constructs a financial mathematical model of the AI economy based on the theoretical foundation of financial mathematics, consisting of a portfolio model, capital asset pricing model, and financial derivatives pricing model, to address the unstable development of China's AI economy.	- The paper **constructs a financial mathematical model of the AI economy**, which includes a portfolio model, capital asset pricing model, and financial derivatives pricing model, providing a theoretical foundation for financial mathematics in the context of artificial intelligence and economic development. - It **develops a theoretical framework for investment risk management that enables investors to intelligently implement risk management plans and countermeasures**, and verifies the performance of the proposed risk investment optimization model through empirical testing with varying investment scales, demonstrating superior convergence performance compared to traditional models.	- The paper **does not address the potential limitations or challenges in implementing the proposed financial mathematical models in real-world scenarios**, particularly in the context of varying market conditions and investor behavior, which could affect the effectiveness of the investment risk management strategies. - There is a **lack of exploration into the integration of other emerging technologies**, such as blockchain or machine learning techniques beyond the scope of the mentioned models, which could enhance the robustness and adaptability of the financial optimization solutions presented in the study.

Jongsma, K. R., Sand, M., & Milota, M. (2024). **Why we should not mistake accuracy of medical AI for efficiency.** *Npj Digital Medicine* DOI: 10.1038/s41746-024-01047-2	- The paper discusses how promising results regarding the accuracy of medical AI are often presented as claims for increased efficiency, but this can be misleading as accuracy does not necessarily equate to efficiency. - It highlights that the promise of AI reducing human workload may be too narrow, as human operators still require new skills, deal with new responsibilities, and need to manage the infrastructure and support systems of AI, which can actually increase human work in the long term.	- The paper **highlights that the assumption that AI will reduce human workload is based on a narrow understanding of what constitutes workload**, as implementing AI systems requires human operators to acquire new skills and take on new responsibilities, which can lead to an overall increase in human work rather than a decrease. - It **emphasizes the importance of the human-side of technology implementation, noting that human knowledge, competencies, and trust are critical factors that can either enhance or hinder the efficiency of AI systems in medical settings**, thus calling for a more cautious and critical approach when discussing the expected benefits of AI.	- The paper highlights a **gap in understanding the broader definition of human workload in the context of medical AI**, suggesting that the current assessments are too narrow and do not account for the new skills and responsibilities that human operators must adopt when implementing these systems. - There is a **lack of exploration into the human-side factors that influence the efficiency of AI technology implementation**, such as the role of human knowledge, competencies, and trust, which can either enhance or hinder the expected efficiency gains from AI systems.
Raffinetti, E. (2023). **A Rank Graduation Accuracy measure to mitigate Artificial Intelligence risks.** *Quality & Quantity* DOI: 10.1007/s11135-023-01613-y	- The paper introduces a new predictive accuracy measure called Rank Graduation Accuracy (RGA) which evaluates the concordance between the ranks of predicted values and actual values, providing a universal alternative predictive model selection criterion. - The RGA measure is based on ranks rather than values, making it robust to the presence of outlying observations, unlike standard measures such as Root Mean Squared Error.	- The paper focuses on predictive accuracy and explainability in the context of machine learning models in Artificial Intelligence (AI). - The paper introduces a new predictive accuracy measure called Rank Graduation Accuracy (RGA), which evaluates the concordance between the ranks of predicted values and actual values, providing a universal alternative predictive	- The paper suggests that future research should consider the case of a multivariate response variable, indicating a gap in the current application of the Rank Graduation Accuracy (RGA) measure to multidimensional settings. This would require generalizing the concordance curve to accommodate multiple response variables, which is not addressed in the current study.

		model selection criterion that is robust to outlying observations.	- There is a mention of the need for the RGA measure to be employed in other comparison settings, particularly those involving applications of machine learning models. This highlights a gap in the exploration of the RGA's applicability and effectiveness across various domains and types of machine learning applications beyond the specific use-case of financial risks from crypto assets presented in the paper.
Lin, S.-J., & Hsu, M.-F. (2017). **Incorporated risk metrics and hybrid AI techniques for risk management.** *Neural Computing and Applications*, *28*(11) DOI: 10.1007/S00521-016-2253-4	- The study introduces a novel technique that extends balanced scorecards by incorporating risk management considerations, specifically focusing on risk metrics and insolvency risk, to enhance the assessment of corporate operating performance. This approach aims to provide a more comprehensive evaluation framework that integrates traditional performance metrics with risk factors. - The research establishes a fusion mechanism that combines hybrid filter-wrapper subset selection (HFW), random vector functional-link network (RVFLN), and ant colony optimization (ACO) for forecasting operating performance. This mechanism is designed to optimize feature selection, improve forecasting accuracy, and	- The study enhances the traditional balanced scorecard (BSC) framework by incorporating risk management measures, specifically risk-adjusted returns and insolvency risk, to provide a more comprehensive assessment of corporate operating performance. This integration allows for a better understanding of a firm's risk exposure, which is crucial in a volatile economic environment. - The proposed hybrid mechanism for corporate operating performance forecasting includes feature selection, forecasting model construction, and knowledge visualization. This approach not only improves forecasting quality but also	- The Balanced Scorecard (BSC) approach, while widely accepted, has critical weaknesses such as being a top-down method that limits communication between high-level managers and employees, and it lacks a systematic strategy, often emphasizing short-term financial measures over long-term performance and risk considerations. - Previous research on corporate operating performance predominantly focuses on monetary indicators, which fail to provide a comprehensive view of a corporate's operating situation, potentially leading to misleading conclusions and negatively

	extract decision logic in a human-readable format, addressing the challenges of interpretability in machine learning models.	ensures that the extracted knowledge is presented in a human-readable format, thereby aiding decision makers in interpreting and verifying the information, which is essential for making reliable judgments.	impacting decision-making in a competitive environment.
Arno A, Thomas J, Wallace B, Marshall IJ, McKenzie JE, Elliott JH. **Accuracy and Efficiency of Machine Learning–Assisted Risk-of-Bias Assessments in "Real-World" Systematic Reviews. (2022).** *Annals of Internal Medicine*. DOI: 10.7326/m22-0092	- The paper addresses the increasing difficulty of maintaining up-to-date, high-quality health evidence and proposes automation, specifically through the use of RobotReviewer, as a solution for conducting risk-of-bias (RoB) assessments in systematic reviews. It highlights the lack of evidence assessing the effectiveness of semi-automated data synthesis in this context. - The study aims to determine whether RobotReviewer-assisted RoB assessments are noninferior in accuracy and efficiency compared to assessments conducted solely by human reviewers, with findings indicating that the integration of RobotReviewer resulted in noninferior overall RoB assessment accuracy.	- The study demonstrates that RobotReviewer-assisted risk-of-bias assessments in health-related systematic reviews are noninferior in accuracy compared to assessments conducted solely by human reviewers, with accuracy rates of 88.8% for the intervention group and 90.2% for the control group. - The research provides insights into the efficiency of using RobotReviewer, indicating that while the time saved per assessment was inconclusive, the integration of automation in the review process could potentially streamline the risk-of-bias assessment workflow in systematic reviews.	- The study indicates a lack of evidence assessing the effectiveness of semiautomated data synthesis, particularly in the context of risk-of-bias assessments, highlighting a gap in understanding how automation can enhance systematic reviews in health evidence. - The inconclusive data regarding the person-time outcome suggests variability in user behavior and a limited number of assessable reviews, indicating a need for further research to accurately estimate the efficiency gains from using RobotReviewer in different review contexts.

Chandrinos, S. K., Sakkas, G. K., & Lagaros, N. D. (2018). **AIRMS: A risk management tool using machine learning.** *Expert Systems With Applications* DOI: 10.1016/J.ESWA.2018.03.044	- The paper presents one of the first efforts in the literature to utilize supervised machine learning as a risk management tool in the financial industry, specifically focusing on using machine learning technology as a consultant for trading decisions rather than merely a source of investment ideas. - Two AIRMS systems are developed based on well-known machine learning algorithms, artificial neural networks and decision trees, and are applied to five major currency pairs in the FOREX market, demonstrating significant improvements in portfolio performance by classifying trading signals into profitable and non-profitable categories.	- The paper presents the artificial intelligent risk management system (AIRMS), which utilizes supervised machine learning as a risk management tool, marking one of the first efforts in the literature to apply ML technology in this capacity within the financial industry. - The development of two AIRMS systems based on artificial neural networks and decision trees demonstrates significant improvements in trading performance, with the classification of signals into profitable and non-profitable categories leading to a profit increase of more than 50% compared to original portfolios.	- The paper highlights the need for further research on the application of supervised machine learning in risk management within the financial industry, indicating a gap in the existing literature regarding utilizing ML algorithms specifically for this purpose. - The authors propose technical improvements in the application of ML algorithms to financial data, suggesting a need for more research on enhancing evaluation metrics and smoothing inputs when developing risk management tools using machine learning.
R. R. Althar, D. Samanta, M. Kaur, D. Singh and H. -N. Lee**, Automated Risk Management Based Software Security Vulnerabilities Management. (2022).** *IEEE Access* DOI: 10.1109/access.2022.3185069	- The literature review highlights the exploration of neural networks, deep learning techniques, and ensemble methods in cybersecurity, specifically targeting areas such as intrusion detection, prediction of cyber-attacks, and malware identification. It emphasizes the need for further exploration to enhance algorithm efficiency based on specific data, while noting that these approaches have not been adequately applied within software development processes. - The review identifies research gaps, including the lack of focus on understanding customer	- The paper proposes a quantitative threat modeling approach that reduces dependency on expert input, aiming to create a more extensive system of smart security in software development. This approach integrates conventional risk assessment methods with threat modeling to leverage the strengths of both methodologies, ultimately enhancing the predictability and efficiency of identifying software vulnerabilities. - It emphasizes the importance of	- There is a lack of focus on learning the structure of customer requirements in agile development methodology from a security perspective, which is currently missing. This gap highlights the need to better understand how customer needs can be integrated into security considerations during the software development process. - The integration of customer, industry, and software processes data sources to derive implicit security needs has not been adequately addressed. This gap

	requirements from a security perspective in Agile development, and the need to integrate customer, industry, and software process data sources to derive implicit security needs. This integration is essential for bridging conventional threat modeling and risk assessment approaches with machine learning capabilities, ultimately providing a comprehensive view of security vulnerabilities in software systems.	combining industry knowledge with company-specific data to build a robust information system for threat modeling. This integrated model aims to standardize threat detection across software development teams, serving as a knowledge management tool that reconciles data available across different sources, thereby improving the overall security posture of software systems.	necessitates deeper exploration to create a comprehensive view of security vulnerabilities and to effectively bridge conventional threat modeling and risk assessment approaches with machine learning capabilities.
Petrone, D., Rodosthenous, N., & Latora, V. (2022). **An AI approach for managing financial systemic risk via bank bailouts by taxpayers.** *Nature Communications* DOI: 10.1038/s41467-022-34102-1	- The paper focuses on managing financial systemic risk through bank bailouts by governments using an AI approach, specifically as a Markov Decision Process (MDP) where equity investments are the actions taken. - The authors highlight that by providing additional capital to banks, governments can control the systemic risk of the network, lowering the probability of default (PD) for banks at the expense of increased exposure in case of failure, ultimately aiming to limit the effects of financial crises.	- Daniele Petrone devised and performed the research, conceived the model, and wrote the paper, contributing to the overall framework and theoretical approach for managing financial systemic risk through bank bailouts by taxpayers. - Neofytos Rodosthenous mathematically defined and structured the model, enhancing the clarity and rigor of the research, while also co-authoring the paper to ensure comprehensive coverage of the topic.	- The paper does not explicitly mention any specific research gaps within the scope of their study on managing financial systemic risk via bank bailouts using AI and MDP. - The authors focus on presenting their AI technique and optimal investment policy for controlling systemic risk, providing direct indications to governments and regulators, without discussing any limitations or areas for further research within their study.

Darwiesh, A. M. N., El-Baz, A. H., Abualkishik, A. Z., & Elhoseny, M. (2022). **Artificial Intelligence Model for Risk Management in Healthcare Institutions: Towards Sustainable Development.** *Sustainability* DOI: 10.3390/su15010420	- Hammoda and Durst developed a knowledge risks taxonomy in healthcare, identifying 25 types of knowledge risks classified into human, technology, and operational categories, demonstrating the efficiency of their approach in improving causal relationships and ranking risk factors. - Salih et al. examined IoT risk management features in healthcare, proposing a detailed IoT model for risk management based on a case study from a hospital in Sudan, showing good usability of the model in evaluating and implementing IoT for risk management purposes.	- The paper proposes an artificial intelligence model that utilizes social media data and natural language processing techniques to manage risks in healthcare institutions. This model aims to identify and assess potential risks by analyzing users' interactions, particularly tweets, to provide insights into the types and magnitudes of risks. - The authors develop a mathematical model for the proposed AI model and derive closed-form relations for risk analysis, identification, and assessment. Additionally, a case study on the CVS institute of healthcare in the USA is presented, showing that a significant portion of patients' tweets refer to operational, financial, and technological risks, with varying magnitudes of high risk, medium risk, and low risk.	- The paper does not explicitly mention any limitations or challenges faced during the development and implementation of the proposed artificial intelligence model for risk management in healthcare institutions. Addressing these limitations could provide insights into potential research gaps. - While the paper presents a case study on the CVS institute of healthcare in the USA, it does not discuss the generalizability of the proposed model to other healthcare institutions or different healthcare systems. Exploring the scalability and adaptability of the model across various settings could be an area for further research.

Avelar, E. A., & Jordão, R. V. D. (2024). **The role of artificial intelligence in the decision-making process: a study on the financial analysis and movement forecasting of the world's largest stock exchanges.** *Management Decision*. DOI: 10.1108/md-09-2023-1625	- The paper focuses on analyzing the role and performance of different artificial intelligence (AI) algorithms in forecasting future movements in the main indices of the world's largest stock exchanges. - The study expands knowledge on the topic and provides robust evidence on the role of AI in financial analysis and decision-making, as well as in predicting the movements of the largest stock exchanges in the world.	- The study provides robust evidence on the role of artificial intelligence in financial analysis and decision-making, demonstrating that AI algorithms can outperform market return expectations, which supports financial, strategic, and organizational decisions in the context of stock market movements. - It expands the discussion on the efficient market hypothesis (EMH) by applying AI methodologies to analyze the main indices of the world's largest stock exchanges, thereby contributing to theoretical, strategic, and managerial insights in a complex economic reality where automation and AI are increasingly utilized.	- The paper highlights the need for further investigation into the efficiency of the market hypothesis (EMH) in the context of the expanding use of automation and artificial intelligence in financial analysis and decision-making. - The study suggests the exploration of new avenues for future research, particularly in the extensive utilization of technical analysis as a support for decisions and machine learning in the realm of financial forecasting and stock market movements.

4.2. What are the key differences in risk assessment and mitigation strategies between traditional and AI-based risk management approaches?

AI-based risk management approaches offer significant advancements over traditional methods, primarily through enhanced data processing capabilities, real-time monitoring, and predictive analytics. Traditional risk management often relies on manual processes and predefined risk matrices, which can be slow and less adaptive to emerging threats. In contrast, AI-driven systems leverage machine learning, big data analytics, and other AI technologies to provide more dynamic and accurate risk assessments. The following sections outline the key differences between these approaches.

4.2.1. Data Processing and Analysis

Traditional methods struggle with processing large volumes of data and often rely on manual analysis, which can be time-consuming and prone to human error (Sindiramutty et al., 2024) (Yadav et al., 2024).

AI-based systems utilize machine learning algorithms and big data analytics to process vast amounts of structured and unstructured data, enabling more comprehensive and accurate risk assessments (Nabeel, 2024) (Daiya, 2024).

4.2.2. Real-Time Monitoring and Predictive Capabilities

Traditional risk management typically involves periodic assessments and lacks real-time monitoring capabilities, leading to delayed responses to emerging risks (Aderamo et al., 2024).

AI systems provide real-time monitoring and predictive analytics, allowing for proactive risk management by identifying potential risks before they materialize (Sindiramutty et al., 2024) (Aderamo et al., 2024).

4.2.3. Adaptability and Responsiveness

Traditional approaches are often rigid, relying on static models that do not adapt well to changing conditions (Nabeel, 2024). AI-driven systems are highly adaptable, continuously learning from new data to adjust risk assessments and mitigation strategies dynamically (Nabeel, 2024) (Yadav et al., 2024).

4.2.4. Automation and Efficiency

Manual processes in traditional risk management can be inefficient and resource-intensive (Aderamo et al., 2024). AI enhances efficiency by automating routine tasks, such as data analysis and reporting, freeing up human resources for more strategic activities.

While AI-based risk management offers numerous advantages, it also presents challenges such as data quality, model interpretability, and integration with existing systems. These challenges must be addressed to fully realize the potential of AI in risk management (Nabeel, 2024) (Daiya, 2024).

4.2.5. Literature Review - What are the key differences in risk assessment and mitigation strategies between traditional and AI-based risk management approaches?

Authors / Year / Title / Journal / DOI	Literature Survey	Contributions	Research Gap
Sindiramutty, S. R., Jhanjhi, N. Z., Akbar, R., Soomro, T. R., & Ghazanfar, M. A. (2024). **Risk assessment and mitigation with generative AI models. In Proceedings of the International Conference on AI & Risk Management**. DOI: 10.4018/979-8-3693-8944-7.ch002	- The paper discusses the limitations of traditional risk assessment and mitigation strategies in cybersecurity, highlighting their inability to adapt to the rapidly evolving landscape of cyber threats that often require manual analysis for effective judgment. - It emphasizes the transformative potential of AI techniques, such as generative adversarial networks (GANs) and variational autoencoders (VAEs), in enhancing risk assessment methods by simulating scenarios to identify anomalies and predicting future risks in real-time through unsupervised learning.	- The paper discusses how the adoption of AI techniques, such as generative adversarial networks (GANs) and variational autoencoders (VAEs), can enhance risk assessment methods by simulating scenarios to identify anomalies more efficiently than traditional manual analysis approaches. - It highlights the integration of threat intelligence into AI models, which improves the understanding of contextual factors and aids in identifying abnormal high-risk behaviors, thereby enabling real-time predictions of potential future risks through unsupervised learning methods.	- The paper highlights that traditional risk assessment approaches struggle to keep pace with the evolving landscape of cyber threats, indicating a gap in the effectiveness of current methodologies in adapting to new and complex risks that require more dynamic and automated analysis. - While the integration of AI techniques like GANs and VAEs is discussed, there is a lack of exploration into the specific challenges and limitations of implementing these advanced models in real-world cybersecurity scenarios, suggesting a need for further research on practical applications and their effectiveness in diverse environments.

Daiya, H. (2024). **AI-driven risk management strategies in financial technology. Journal of Artificial Intelligence in Global Strategy**. DOI: 10.60087/jaigs.v5i1.194	- The literature review of the paper focuses on the integration of Artificial Intelligence (AI) into financial technology (FinTech) and its impact on risk management strategies. - It explores how AI-driven risk management offers innovative solutions to longstanding challenges in the financial sector, particularly in areas such as predictive accuracy, fraud detection, and regulatory compliance.	- The paper discusses how AI integration in FinTech has revolutionized risk management strategies by offering innovative solutions to longstanding challenges. - It highlights AI's ability to enhance risk assessment, improve fraud prevention, and optimize compliance processes in the financial sector.	- The paper identifies regulatory adaptation as a research gap in AI-driven risk management strategies in FinTech, suggesting a need for further exploration into how regulations can keep pace with technological advancements to ensure compliance and security. - Another research gap highlighted in the paper is the ethical considerations surrounding the use of AI in risk management, indicating a need for more in-depth analysis on how to address ethical dilemmas and ensure responsible AI implementation in the financial sector.
Yadav, P., Gupta, P., Sijariya, R., & Sharma, Y. K. (2024). **Artificial intelligence in risk management. In Handbook of AI in Risk Management.** DOI: 10.1002/9781394175574.ch1	- The literature review of the paper focuses on the limitations of traditional risk management methods in the financial industry, such as the inability to manage large amounts of data, react quickly to market changes, and provide real-time monitoring of trends. - The paper highlights how artificial intelligence (AI) can enhance risk management practices by utilizing deep	- Artificial intelligence (AI) can enhance risk management in the financial sector by utilizing deep learning, machine learning algorithms, and natural language processing to analyze huge amounts of data, react quickly to market changes, and provide real-time monitoring of market trends. - The application of AI in risk management has the potential to improve decision-	- The paper does not explicitly mention any specific research gaps in the field of artificial intelligence in risk management within the financial industry. - It does not provide insights into areas where further research is needed to enhance the application of AI in risk management practices.

	learning, machine learning algorithms, and natural language processing to analyze data, detect potential threats, uncover fraudulent activities, and provide predictive analytics for decision-making.	making, reduce risks, and enhance overall financial stability by identifying potential threats, detecting fraudulent activities, and offering predictive analytics for informed decision-making.	
Yazdi, M. S., Zarei, E., Adumene, S., & Beheshti, A. (2024). **Navigating the power of artificial intelligence in risk management: A comparative analysis.** Safety. DOI: 10.3390/safety10020042	- The literature review of the paper highlights the significance of artificial intelligence (AI), particularly intense learning methodologies like convolutional neural networks (CNNs), in extracting meaningful insights from image data for risk management. - It contrasts traditional risk management approaches with AI-augmented methods, emphasizing the potential of AI in identifying and managing risks across various industries.	- The study highlights the pivotal role of artificial intelligence, particularly through intense learning methodologies like convolutional neural networks (CNNs), in extracting meaningful insights from image data, which is crucial for identifying and managing risks across various industries. This demonstrates the potential of AI to enhance traditional risk management approaches. - The research introduces three case studies that serve as benchmarks for evaluating the application of AI in risk management, showcasing its ability to identify hazards, evaluate risks, and suggest control measures. The comparative evaluation emphasizes the	- The paper highlights the need for a synergy between technological capabilities of AI and domain-specific expertise in risk management, indicating a research gap in exploring how to effectively combine these two aspects to maximize the benefits of AI in risk assessment. - Another research gap identified is the need for continued research to further integrate AI into risk assessment frameworks, suggesting a gap in understanding the optimal methods for incorporating AI technologies into existing risk management practices.

		accuracy, relevance, and practicality of AI-generated findings, while also acknowledging the need for a synergy between technological capabilities and domain-specific expertise.	
Shen, Q. (2024). **AI-driven financial risk management systems: Enhancing predictive capabilities and operational efficiency. Journal of Risk & Security Engineering**. DOI: 10.54254/2755-2721/69/20241494	- The paper discusses the integration of artificial intelligence (AI) in financial risk management systems, highlighting how it has revolutionized traditional approaches by providing enhanced predictive capabilities and operational efficiency. - It explores various applications of AI in credit risk assessment, market risk analysis, operational risk management, and regulatory compliance, emphasizing the use of advanced machine learning algorithms to analyze vast datasets, including real-time market data and non-traditional sources, to improve risk predictions and enable proactive risk management.	- The paper discusses how AI-driven financial risk management systems enhance predictive capabilities by leveraging advanced machine learning algorithms to analyze vast datasets, including real-time market data and non-traditional sources, improving risk predictions and enabling proactive risk management. - It also highlights the benefits of AI in automating routine tasks, enhancing data analytics, and ensuring regulatory compliance, ultimately reducing the incidence of loan defaults, enhancing portfolio quality, and improving the overall resilience of financial institutions.	- The paper does not explicitly mention any specific research gaps in the current literature regarding the integration of AI in financial risk management systems. - It does not address potential limitations or challenges faced in the implementation of AI-driven systems in the context of financial risk management.

Qureshi, N. I., Garg, A., Singh, R., & Retzlaff, N. (2024). **AI and corporate risk management: Identifying and mitigating technological and ethical risks. In International Conference on AI and Emerging Technologies** DOI: 10.1109/ickecs61492.2024.10617141	- The literature review in this paper explores existing methodologies related to AI risk management, identifying gaps in current approaches that need to be addressed to effectively manage the technological and ethical risks associated with AI deployment in corporate settings. - It emphasizes the importance of understanding the multifaceted risks posed by AI technologies, which necessitates a comprehensive examination of prior research and practices to inform the development of a novel framework that integrates risk identification algorithms with ethical oversight mechanisms.	- The paper proposes a novel framework that integrates advanced risk identification algorithms with ethical oversight mechanisms, aiming to safeguard against technological failures and ethical oversights in AI deployment within corporate risk management. - It contributes to the development of more resilient and responsible AI applications by bridging the gap between technological advancements and ethical considerations, thereby enabling companies to harness the benefits of AI while minimizing its inherent risks.	- The paper identifies existing methodologies in AI risk management but highlights significant gaps in the current approaches, indicating a need for more comprehensive frameworks that effectively integrate both technological and ethical considerations in corporate risk management. - The proposed novel framework aims to address these gaps by combining advanced risk identification algorithms with ethical oversight mechanisms, suggesting that current practices may lack sufficient integration of ethical dimensions in the assessment and mitigation of AI-related risks.
Li, H., Yazdi, M., Nedjati, A., Moradi, R., Adumene, S., Dao, U., Moradi, A., Haghighi, A., Obeng, F., Huang, C.-G., Kang, H.-S., Pirbalouti, R. G., Zarei, E., Dehghan, M., Darvishmotevali, M., Ghasemi, P., Shayan Fard, P., Garg,	- The literature review of the paper emphasizes the significance of project risk management in contemporary organizations, highlighting its crucial role in ensuring the success of endeavors amidst a complex and competitive business environment.	- The integration of artificial intelligence (AI) in project risk management reshapes strategies and enhances decision-making processes, allowing for proactive risk anticipation and the development of simulation-based mitigation strategies through the use of predictive analytics and machine learning. This enables	- The paper does not explicitly mention specific research gaps within the realm of AI-driven project risk management, leaving room for further exploration into areas where AI may not be as effective or where additional research is needed to enhance its application.

H. (2024). Harn. DOI: 10.1007/978-3-031-51719-8_16	- It discusses how the integration of artificial intelligence (AI) represents a paradigm shift in project risk management by reshaping strategies, enhancing decision-making processes, and leveraging predictive analytics and machine learning to anticipate risks, simulate mitigation strategies, and foster agility in response strategies through real-time communication and collaboration among project teams.	organizations to uncover hidden patterns in historical project data, ultimately elevating project outcomes. - AI's cognitive capabilities facilitate expedited risk assessment by aggregating diverse data sources, which fosters agility in response strategies through real-time communication and collaboration among project teams. Additionally, AI-driven algorithms continuously adapt to evolving risk landscapes, refining risk management strategies and optimizing resource allocation.	- While the chapter discusses the multifaceted impact of AI on project risk management, it does not delve into potential limitations or challenges that organizations may face when implementing AI for risk management, indicating a potential gap in understanding the practical implications of AI integration in this context.
Sharma, R., Harish, V., & Rana, G. (2024). **Navigating risk in the age of artificial intelligence: Assessing and identifying risks with AI strategies.** *KUEY Journal*,. DOI: 10.53555/kuey.v30i4.1824	- The paper explores the potential barriers and risks associated with the adoption of artificial intelligence (AI), emphasizing the critical need for effective risk assessment and identification strategies as organizations increasingly integrate AI into their operations. It discusses the evolving landscape of AI, including its various types and the specific risks they pose. - It highlights the importance of proactive risk identification and mitigation practices, particularly in the context of Industry 6.0,	- The paper explores the potential barriers and risks associated with the adoption of artificial intelligence (AI), emphasizing the critical need for effective risk assessment and identification strategies to manage these risks in organizations, particularly in the context of Industry 6.0 where advanced automation and interconnected systems are prevalent. - It highlights the importance of proactive risk identification and mitigation practices	- The paper emphasizes the need for effective risk management strategies in the context of AI adoption, particularly in Industry 6.0, but does not provide specific methodologies or frameworks for implementing these strategies, indicating a gap in practical guidance for organizations. - While the paper outlines various risks associated with AI and the importance of proactive risk identification, it lacks a comprehensive analysis of the specific

	where advanced automation and interconnected systems can lead to complex and potentially risky situations. The paper outlines risk identification strategies tailored to AI in this domain, acknowledging the complexities and vulnerabilities that organizations must navigate.	specific to AI, recognizing the complexities and vulnerabilities present in this domain, which enables organizations to navigate the age of AI confidently and leverage the benefits of this transformative technology.	complexities and vulnerabilities unique to different sectors within Industry 6.0, suggesting a need for further research in sector-specific risk assessment approaches.
Kanupriya. (2024). *Financial Economics and Financial Systems*. DOI: 10.59400/fefs1758	- The study utilizes existing literature on AI's opportunities and challenges, primarily focusing on corporate study reports and journal articles, to discuss the implications of AI in financial risk management and future policy considerations. - It emphasizes the transformative role of AI technologies, such as natural language processing, machine learning, and predictive analytics, in revolutionizing risk management strategies and fostering a culture of innovation and adaptability within financial organizations.	- The study emphasizes the transformative role of AI in financial risk management, highlighting how AI-driven systems enhance operational efficiency, compliance with regulatory standards, and the ability to navigate complex financial environments. This integration of AI technologies is positioned as essential for the sustainability and resilience of financial institutions in a rapidly changing market. - It underscores the importance of cultivating a workplace culture that equips employees with the skills necessary to effectively leverage AI technologies. This focus on labor welfare is crucial for ensuring that financial organizations can fully harness the potential of AI, fostering	- The study primarily focuses on the opportunities and challenges of AI in financial risk management but does not delve into specific case studies or empirical data that illustrate the practical implementation of AI technologies in various financial institutions. This lack of real-world examples may limit the understanding of how AI can be effectively integrated into existing risk management frameworks. - While the paper emphasizes the importance of cultivating a workplace culture that equips employees with AI skills, it does not address the potential resistance to AI adoption among employees or the strategies needed to overcome such challenges. Exploring employee perspectives and the impact

		innovation and adaptability within the sector.	of AI on job roles could provide a more comprehensive view of the labour-centric implications of AI in financial risk management.
Quan, C., Yuan, Y.-H., Wang, G., & Wu, H.-T. (2024). **Optimization of enterprise financial risk management and crisis early warning system supported by AI.** *Journal of Global Information Management*, DOI: 10.4018/jgim.356490	- The study highlights the limitations of traditional financial risk management methods, particularly their challenges in processing large-scale data, which leads to decreased accuracy in risk assessment. - It introduces a novel approach that combines gated recurrent units (GRU), temporal convolutional networks (TCN), and attention mechanisms to enhance the accuracy of financial risk assessments and improve the effectiveness of crisis warnings, demonstrating superior performance compared to baseline models.	- The study introduces a novel approach that combines gated recurrent units (GRU), temporal convolutional networks (TCN), and attention mechanisms to enhance the accuracy of financial risk assessments and the effectiveness of crisis warnings, addressing the limitations of traditional financial risk management methods. - Experimental results demonstrate that the proposed algorithm significantly outperforms baseline models, achieving over 46.8% reduction in FLOPs and more than 48.5% improvement in inference time on the LendingClub loan dataset, thereby contributing to the stability and operational efficiency of enterprises.	- The study highlights the limitations of traditional financial risk management methods, particularly their challenges in processing large-scale data, which can lead to decreased accuracy in risk assessment. However, it does not address potential limitations or challenges associated with the implementation of the proposed AI-based methods in real-world scenarios. - While the research demonstrates improvements in risk prediction accuracy, efficiency, and stability using the new algorithm, it lacks a comprehensive analysis of how these improvements translate into practical applications for different types of enterprises or industries, leaving a gap in understanding the broader applicability of the findings.

Swanson, T., Zelner, J., & Guikema, S. D. (2022). **COVID-19 has illuminated the need for clearer AI-based risk management strategies**. *Journal of Risk & Safety*, DOI: 10.1080/13669877.2022.2077411	- The paper discusses the potential of machine learning methods to enhance pandemic response and risk management by complementing traditional modeling approaches, utilizing diverse data sources at various levels from local to global scales. - It highlights the challenges faced due to inconsistent reporting and availability of detailed COVID-19 data in the US, limiting the application of artificial intelligence methods for projecting disease spread and impacts in communities, emphasizing the need for standardized data collection and sharing protocols in collaboration with AI researchers and industry experts for future preparedness.	- Machine learning methods can enhance pandemic response and risk management by integrating diverse data sources, which can improve decision-making processes at local to global levels. This integration can supplement traditional mechanistic modeling approaches used in pandemic planning and response. - The paper highlights the importance of establishing consistent data collection and sharing standards in collaboration with AI researchers and industry experts. This collaboration is essential to ensure the effective application of AI methods in projecting the spread and impacts of diseases, thereby facilitating better preparedness for future pandemics and disasters.	- The paper highlights a lack of consistency in the reporting and availability of disaggregated, detailed data on COVID-19 in the US, which limits the application of artificial intelligence methods for projecting the spread and impacts of the disease in communities. - It emphasizes the need for governing bodies to develop data collection and sharing standards in collaboration with AI researchers and industry experts to enhance preparedness for pandemics and other disasters in the future.
Sari, Y., & Indrabudiman, A. (2024). **The role of artificial intelligence (AI) in financial risk management.** *Financial Journal of Strategic Research*,. DOI: 10.55927/fjsr.v3i9.11436	- The literature review explores the role of artificial intelligence (AI) in financial risk management, highlighting how AI is utilized to analyze financial data and market trends for identifying and managing risks effectively. - The findings from the literature review indicate that AI enhances the speed of risk detection and improves the effectiveness and efficiency of risk management processes, marking a significant shift in	- AI enhances the efficiency and effectiveness of financial risk management by automating tasks traditionally performed by humans, which leads to reduced costs and improved accuracy in risk detection and assessment. This transformation allows financial institutions to respond more swiftly to market fluctuations and uncertainties. - The integration of AI into financial risk	- Future research could focus on enhancing AI's predictive capabilities, particularly in terms of long-term financial risks. While AI has shown effectiveness in identifying immediate risks, improving its ability to foresee long-term challenges could provide financial institutions with greater strategic advantages. - There is a need for further

	technology-based risk management practices.	management practices not only improves risk identification and mitigation but also ensures long-term business sustainability. By utilizing advanced technologies such as machine learning and neural networks, organizations can better protect their financial assets and comply with legal and regulatory requirements, ultimately contributing to overall company performance and resilience.	investigation into the ethical implications of AI in financial risk management, particularly concerning bias and transparency in decision-making processes. Ensuring that AI systems are explainable and fair should be a key focus of future research efforts, especially in high-stakes areas like credit scoring and risk assessment.
Zhu, J. (2024). **Application of artificial intelligence data mining algorithm in enterprise management risk assessment.** *International Journal of Information Systems & Supply Chain Management*, DOI: 10.4018/ijisscm.342119	- The literature review highlights the increasing importance of risk management in enterprises due to factors such as financial market volatility, commercial fraud, and poor management, which have led to the collapse of capital chains in many businesses. It emphasizes that small businesses are particularly vulnerable to bankruptcy due to a lack of risk awareness and a focus on virtual financial markets rather than the real economy. - It discusses the evolution of risk assessment methodologies, noting that traditional risk control models are limited in their ability to evaluate risks accurately. The review points out that the integration of big data tools and machine learning techniques has become essential for conducting	- The study utilizes LSTM networks to track and predict Total Water Storage Change (TWSC) and Groundwater Storage Change (GWSC) for five basins in Saudi Arabia from 2003 to 2025, providing valuable insights into water resource management in the region. - A novel automated weed-identifying method is developed using convolutional neural network (CNN) classification on a real-world dataset of UAV images, significantly enhancing the accuracy of weed detection in agricultural practices.	- The paper does not explicitly mention any comparison with other existing AI-based data mining algorithms for enterprise risk assessment, leaving a research gap in terms of benchmarking against alternative methods. - There is no discussion on the scalability of the proposed MSVM+EFCNN algorithm for larger enterprises or different industry sectors, indicating a research gap in exploring the algorithm's applicability beyond the scope of the current study.

	thorough analyses of financial data, thereby improving the accuracy and effectiveness of enterprise risk management strategies.		
Tirmizi, S. F. A., & Arif, F. (2022). **Conceptual approach for the use of artificial intelligence for contractual risk assessment in infrastructure projects**. *Engineering Proceedings*, DOI: 10.3390/engproc2022022012	- The literature review conducted for the paper focused on identifying various risk factors in infrastructure projects within the oil and gas sector, with a particular emphasis on risks related to contract preparation and project performance. - Previous research highlighted a total of ninety-seven risks for infrastructure projects, which were further categorized into precontract, contractual, and allied risks. Contractual risks, which could be addressed at the tender preparation and contract stage, comprised sixty-one out of the ninety-seven identified risks.	- The paper highlights that despite extensive experience in project execution, oil and gas companies struggle to meet cost and schedule targets due to inadequate risk management during the pre-project execution stage. This indicates a critical gap in the planning and risk assessment processes that needs to be addressed to improve project outcomes. - It points out organizational issues that complicate the tender process, including a prevalent fear among stakeholders to document risks encountered in projects. This fear often stems from a lack of confidence and the potential for negative repercussions from leadership, which hinders effective risk management and knowledge sharing within organizations.	- Lack of emphasis on the specific challenges faced by different types of infrastructure projects in relation to contractual risk assessment using artificial intelligence. - Limited discussion on the potential barriers or resistance from stakeholders within organizations towards implementing an AI-based framework for contractual risk assessment in infrastructure projects.

Darandale, S., & Mehta, R. (2022). In *Proceedings of the International Conference on AI & Innovation* DOI: 10.1109/ICAAIC53929.2022.9792870	- The paper discusses the significance of risk management in the software development lifecycle, emphasizing that risks can adversely affect project growth and the integrity of software components if not properly identified and managed. It highlights the importance of activities such as recognizing, analyzing, planning, and controlling risks to ensure successful project development. - It explores the application of various machine learning classifiers, including Naive Bayesian, Decision Tree, Artificial Neural Network, and K Nearest Neighbor, in the context of software risk assessment. The paper provides a comparative analysis of these classifiers and suggests future directions to enhance the use of machine learning models in risk assessment practices.	- The paper provides a comparative analysis of various machine learning classifiers, including Naive Bayesian, Decision Tree, Artificial Neural Network, and K Nearest Neighbor, highlighting their applicability in developing a software risk assessment estimator. - It outlines future directions for researchers and stakeholders to enhance the usage of machine learning models in the field of risk assessment, aiming to improve the effectiveness of risk management in software development lifecycles.	- The paper indicates that the application of machine learning in risk assessment is still in its preliminary phase, suggesting a need for further research to explore and expand the applicability of these models in software risk management. - While the paper discusses various machine learning classifiers such as Naive Bayesian, Decision Tree, Artificial Neural Network, and K Nearest Neighbor, it highlights the necessity for comparative analysis and future directions to enhance the effectiveness and integration of these models in developing software risk assessment estimators.
Rajka, L., & Pollák, Z. (2024). **Artificial intelligence for credit risk model, or how do machine learning algorithms compare to traditional models?** *Economic Forum*, 3(1). DOI: 10.33908/ef.2024.3.1	- The paper discusses the evolution of credit risk management models, highlighting the transition from expert systems in the past to traditional statistical models like logistic regression in the present, and the anticipated future shift towards machine learning methods, particularly focusing on the XGBoost algorithm as a promising	- The study empirically analyzes the classification algorithm XGBoost, demonstrating its efficiency in credit risk management compared to traditional statistical models like logistic regression, indicating a significant advancement in predictive capabilities through machine learning methods.	- The study highlights the challenge of interpreting machine learning models, such as XGBoost and Artificial Neural Networks, due to their "black box nature," which limits their application in banks. This indicates a gap in developing methods or frameworks that enhance the interpretability of these models for

	example of this new generation of models. - It emphasizes that while machine learning methods, such as Artificial Neural Networks (ANN) and XGBoost, have demonstrated superior efficiency in classification compared to traditional models, they present challenges in terms of interpretability due to their "black box nature," which currently limits their application in banking and necessitates a review of existing rules and guidelines for credit risk management.	- The authors highlight the challenges associated with the interpretability of machine learning models, particularly their "black box nature," and propose a review of current rules and guidelines for traditional models to facilitate the adoption of machine learning techniques in banking, ultimately aiming to enhance credit risk management efficiency.	practical use in credit risk management. - There is a need for a review of the current rules and guidelines associated with traditional credit risk models to facilitate the adoption of machine learning methods. This suggests a gap in understanding how regulatory frameworks can evolve to accommodate the innovative capabilities of machine learning algorithms in the financial sector.
Dwivedi, D. N., Mahanty, G., & Pathak, Y. (2024). **AI applications for financial risk management.** In *Financial Technologies and AI Systems*. DOI: 10.4018/979-8-3693-0082-4.ch002	- The paper discusses the vulnerabilities of financial systems exposed during the 2008 global financial crisis and emphasizes the importance of financial risk management to prevent similar catastrophic events in the future. - It highlights the adoption of AI applications, big data, and computational frameworks in the finance sector for risk management purposes, aiming to enhance accuracy, efficiency, and productivity while reducing costs for companies to maintain competitiveness.	- The paper highlights the critical role of financial risk management in avoiding catastrophic events like the global financial crisis of 2008 by utilizing AI applications. - It discusses how AI technologies in financial risk management aim to improve accuracy, efficiency, and productivity while reducing costs for companies to enhance competitiveness in the market.	- The paper does not explicitly mention any specific research gaps in the field of AI applications for financial risk management. - It does not highlight areas where further research is needed to enhance the effectiveness or implementation of AI technologies in financial risk management.

Kuzior, A. (2024). **Optimizing financial market stability through AI-based risk management**. In *Proceedings of the International Conference on Financial Markets* DOI: 10.21741/9781644903315-26	- The study utilizes econometric analysis and real-world case studies to examine the impact of AI-based risk management on financial market stability, focusing on institutions like JPMorgan Chase, Goldman Sachs, and BlackRock that have successfully implemented AI algorithms for market analysis and trading pattern evaluation. - The research identifies a positive and statistically significant relationship between AI-based risk management and financial market stability, highlighting that institutions using AI technologies experience lower volatility, improved risk assessment, and enhanced decision-making, which collectively contribute to greater stability in financial markets.	- The study demonstrates a positive and statistically significant relationship between AI-based risk management and financial market stability, indicating that institutions utilizing AI technologies experience lower levels of volatility, better risk assessment, and improved decision-making, which collectively contribute to greater overall stability in financial markets. - The research identifies key challenges faced by financial institutions in implementing AI-based risk management systems, such as the necessity for high-quality data, algorithm complexity, and regulatory compliance, and proposes recommendations to address these challenges, including investing in data quality, enhancing regulatory frameworks, and fostering collaboration and knowledge sharing.	- The study identifies challenges faced by institutions implementing AI-based risk management systems, such as the need for high-quality data, algorithm complexity, and regulatory compliance, but does not delve deeply into specific strategies or frameworks to overcome these challenges, indicating a gap in practical guidance for institutions. - While the research highlights the positive impact of AI on financial market stability, it does not explore the long-term effects of AI adoption on market dynamics or the potential unintended consequences, suggesting a need for further investigation into the broader implications of AI in financial markets.

Aderamo, A. T., Olisakwe, H. C., Adebayo, Y. A., & Esiri, A. E. (2024). **Leveraging AI for financial risk management in oil and gas safety investments.** *CSIT Journal*. DOI: 10.51594/csitrj.v5i10.1619	- The paper discusses the integration of artificial intelligence (AI) into financial risk management within the oil and gas industry, emphasizing its potential to analyze safety data and inform financial decisions. This integration aims to transform traditional approaches by enabling proactive risk management and optimizing resource allocation towards safety investments. - It highlights the use of machine learning algorithms to analyze extensive datasets, including historical safety incidents and operational performance metrics, to identify patterns and forecast potential risks. This predictive capability allows organizations to evaluate the financial implications of various safety investment strategies through scenario analysis, ultimately enhancing the financial viability of safety investments.	- The paper proposes a framework that leverages artificial intelligence (AI) tools to analyze safety data, enabling organizations in the oil and gas industry to proactively address safety concerns while optimizing financial investment strategies. By utilizing machine learning algorithms to analyze vast datasets, AI can identify patterns and forecast potential risks, allowing for strategic resource allocation towards areas that significantly impact safety outcomes and operational resilience. - It highlights the capability of AI to facilitate scenario analysis, which allows organizations to evaluate the financial implications of different safety investment strategies. By simulating various risk scenarios and their potential impacts on financial performance, companies can make informed decisions that balance safety with cost efficiency, ultimately enhancing the financial viability of safety investments and fostering a culture of proactive risk management.	- The paper discusses challenges and limitations of implementing AI in financial risk management, including data quality issues, but does not provide specific examples or case studies that illustrate these challenges in real-world applications within the oil and gas sector. This gap highlights the need for further research to understand how organizations can effectively address data quality and integration issues when adopting AI methodologies. - While the paper emphasizes the importance of transparency and accountability in AI decision-making processes, it lacks a comprehensive exploration of the ethical considerations and frameworks necessary for ensuring responsible AI use in safety investments. Further research is needed to develop guidelines and best practices that organizations can follow to navigate the ethical implications of AI in financial risk management.

Schnitzer, R., Hapfelmeier, A., Gaube, S., & Zillner, S. (2023). **AI hazard management: A framework for the systematic management of root causes for AI risks.** *Arxiv Preprints*. DOI: 10.48550/arxiv.2310.16727	- The paper builds upon a comprehensive state-of-the-art analysis to create an AI hazard list, which serves as a foundation for identifying and managing AI risks effectively. This analysis highlights the specific challenges and risks associated with AI that differ from traditional software systems. - A taxonomy is provided within the framework to support the optimal treatment of identified AI hazards, ensuring that the management process is systematic and tailored to the unique characteristics of AI technologies.	- The paper introduces the AI Hazard Management (AIHM) framework, which provides a structured process for the systematic identification, assessment, and treatment of AI hazards, ensuring that risks are addressed early in the AI system's life cycle. - The framework includes a comprehensive AI hazard list derived from a state-of-the-art analysis and offers a taxonomy to support the optimal treatment of identified AI hazards, ultimately enhancing the overall quality of AI applications, such as in a power grid use case.	- The paper highlights the need for existing risk management processes in related fields, such as software systems, to adequately consider the specific challenges and nuances associated with AI, indicating a gap in current methodologies that do not fully address AI risks. - There is a lack of systematic and transparent identification and treatment of AI hazards, which the proposed AI Hazard Management (AIHM) framework aims to address, suggesting that previous approaches may not have effectively captured or mitigated the root causes of AI risks throughout the AI system's life cycle.
Bedi, P., Goyal, S. B., & Kumar, J. (2020). **Basic structure on artificial intelligence: A revolution in risk management and compliance.** In *Proceedings of ICISS*. DOI: 10.1109/ICISS49785.2020.9315986	- The paper provides a non-technical description of key AI strategies that are beneficial to risk management, highlighting how these strategies can transform risk assessment processes across various domains. - It includes a study on the application of AI methods in specific risk management fields such as credit risk, market risk, organizational risk, and enforcement,	- The paper provides a non-technical description of key AI strategies that are beneficial to risk management, highlighting how these strategies can transform risk assessment processes across various fields such as credit risk, market risk, organizational risk, and enforcement. - It presents a study that utilizes existing experience and empirical data to	- The paper acknowledges existing constraints in effective data management practices, which may hinder the full potential of AI in risk management and compliance, indicating a gap in addressing how to overcome these data management challenges. - There is a noted lack of requisite skill sets within organizations, suggesting a gap in the research regarding the

	supported by existing experience and empirical data.	demonstrate the application of AI methods in risk management, while also reflecting on the constraints faced by organizations, including challenges in effective data management practices, accountability, and the lack of requisite skill sets.	development and implementation of training programs or strategies to equip personnel with the necessary skills to effectively utilize AI in risk management.

4.3. How do AI-based risk management systems improve predictive accuracy compared to traditional methods?

AI-based risk management systems significantly enhance predictive accuracy compared to traditional methods by leveraging advanced machine learning algorithms and neural networks. These systems can process vast amounts of data, identify complex patterns, and adapt to new information, thereby improving the precision and reliability of risk predictions. The integration of AI in risk management not only enhances predictive capabilities but also offers resilience against multiple risk factors, making it a superior choice over conventional approaches. Below are the key aspects of how AI-based systems improve predictive accuracy:

4.3.1. Enhanced Data Processing and Pattern Recognition

AI systems, particularly those using machine learning (ML) and artificial neural networks (ANNs), can handle large datasets and identify intricate patterns that traditional methods might miss. This capability allows for more accurate predictions of financial risks (Farazi, 2024).

Deep neural networks (DNNs) have been shown to outperform conventional methods like logistic regression and support vector machines in predicting financial risks, demonstrating their superior pattern recognition abilities (Farazi, 2024).

4.3.2. Improved Model Performance Metrics

AI models are evaluated using metrics such as accuracy, precision, recall, and F1-score, which are crucial for assessing their predictive performance. Studies have shown that AI models consistently achieve higher scores in these metrics compared to traditional methods (Sarioguz & Miser, 2024) (Farazi, 2024).

The integration of AI with traditional approaches further enhances performance outcomes, providing a more comprehensive risk assessment framework (Farazi, 2024).

4.3.3. Real-Time Monitoring and Adaptability Nabeel

AI systems can continuously monitor and analyze real-time data, allowing for dynamic adjustments to risk predictions as new information becomes available. This adaptability is a significant advantage over static traditional models (Nabeel, 2024).

By leveraging big data analytics, AI systems can predict outcomes with higher accuracy, enabling proactive risk management and timely decision-making (Nabeel, 2024).

While AI-based systems offer substantial improvements in predictive accuracy, they also present challenges such as data quality, model interpretability, and integration with existing

systems. Addressing these issues is crucial for maximizing the benefits of AI in risk management. Additionally, regulatory compliance remains a significant concern, as AI systems must adhere to frameworks like Basel III and GDPR to ensure financial stability and customer confidence(Sarioguz & Miser, 2024).

4.3.4. Literature review - How do AI-based risk management systems improve predictive accuracy compared to traditional methods?

Authors / Year / Title / Journal / DOI	Literature Survey	Contributions	Research Gap
Sarioguz, O., & Miser, E. (2024). **Integrating AI in financial risk management: Evaluating the effects of machine learning algorithms on predictive accuracy and regulatory compliance.** International Journal of Scientific Research and Applications DOI: 10.30574/ijsra.2024.13.2.2206	- The literature review compares traditional risk management methods with newer AI-based methodologies, focusing on the evaluation of standard measurements such as accuracy, precision, and recall to assess the effectiveness of machine learning models in risk management. - It highlights the compliance risks associated with the adoption of AI technologies, particularly in relation to significant regulations like Basel III and GDPR, which are crucial for maintaining financial stability and customer confidence.	- The research presents a comprehensive literature review comparing traditional risk management methods with AI-based methodologies, meticulously evaluating standard measurements such as accuracy, precision, and recall, thereby enhancing the understanding of the effectiveness of machine learning models in risk management. - The study identifies compliance risks associated with the use of AI in financial institutions, particularly in relation to significant regulations like Basel III and GDPR, and provides guidelines for employing AI to improve operational risk management while ensuring strict adherence to current and future regulations.	- The research does not explicitly identify specific gaps in the existing literature regarding the integration of AI in financial risk management, particularly in terms of the limitations of current machine learning models and their applicability across different financial sectors. A more detailed exploration of these gaps could enhance understanding of where further research is needed. - While the study evaluates the predictive efficiency of AI approaches and compliance risks associated with regulations like Basel III and GDPR, it lacks a thorough examination of the long-term implications of AI adoption on risk management practices and how these practices may evolve with ongoing technological advancements.

Nabeel, M. Z. (2024). **AI-Enhanced Project Management Systems for Optimizing Resource Allocation and Risk Mitigation.** Asian Journal of Management Research and Review DOI: 10.55662/ajmrr.2024.5502	- The literature review highlights the inadequacies of traditional project management methodologies, which often rely on manual processes and linear models, in addressing the complexities of modern projects characterized by dynamic, data-driven environments and multifaceted interdependencies. It emphasizes the need for a more sophisticated approach to managing resources and mitigating risks, which AI-enhanced systems can provide. - It discusses the role of AI technologies, such as machine learning algorithms, neural networks, and natural language processing, in improving project management efficiency, accuracy, and responsiveness. The review focuses on how these technologies can optimize resource allocation by analyzing historical data and real-time inputs, as well as enhance risk mitigation through continuous monitoring and proactive management of potential risks.	- The paper highlights the optimization of resource allocation through AI-enhanced systems, which analyze historical project data and real-time inputs to predict future resource needs with greater precision. This dynamic adjustment of resource allocations helps minimize delays, cost overruns, and resource bottlenecks, ensuring timely and cost-effective project completion. - It discusses the role of AI in risk mitigation by continuously monitoring project performance metrics and analyzing trends to detect early warning signs of potential risks. AI systems can process vast amounts of unstructured data to identify correlations and patterns indicative of risk factors, allowing for proactive risk management and real-time alerts to mitigate risks before they escalate into critical issues.	- The paper highlights the challenges of data quality, indicating that poor data quality can lead to flawed analyses and suboptimal decisions. This suggests a research gap in developing methodologies or frameworks to ensure high-quality data for training AI models in project management systems. - Another research gap identified is the complexity of AI models, particularly deep learning algorithms, which can hinder project managers' understanding of how decisions are made. This points to a need for further investigation into model interpretability and transparency in AI-driven project management systems to enhance accountability and trust among users.

Farazi, M. Z. R. (2024). **Exploring the role of artificial intelligence in managing emerging risks: an in-depth study of AI applications in financial institutions' risk frameworks.** The Asian Journal of Management and Education Integration, DOI: 10.37547/tajmei/volume06issue10-04	- The research investigates the effectiveness of machine learning (ML) and artificial neural networks (ANNs) in financial risk management (FRM) compared to traditional methods such as logistic regression, random forest, and support vector machine, highlighting the advancements in predictive capabilities offered by AI technologies. - The study emphasizes the importance of integrating traditional and AI-based approaches, which not only improves performance outcomes in risk assessment but also enhances resilience against multiple risk factors, suggesting a significant shift towards AI-enhanced risk management frameworks in financial institutions.	- The research demonstrates that artificial neural networks (ANNs), particularly deep neural networks (DNNs), outperform traditional methods such as logistic regression, random forest, and support vector machines in predicting financial risks, indicating a significant advancement in financial risk management (FRM) methodologies. - The study highlights the benefits of integrating traditional risk assessment approaches with AI-based methods, resulting in improved performance outcomes and greater resilience to multiple risk factors, thereby enhancing the accuracy of financial risk assessments.	- The research highlights a need for improvements regarding the interpretability of the AI models used in financial risk management, suggesting that understanding how these models make decisions is crucial for their effective application in real-world scenarios. - Future work should focus on testing the AI models on a more substantial number of data records to validate their effectiveness and reliability, as well as experimenting with reinforcement learning to enhance decision-making processes in financial risk cases.

Quan, C., Yuan, Y.-H., Wang, G., & Wu, H.-T. (2024). **Optimization of Enterprise Financial Risk Management and Crisis** Early Warning System Supported by AI. Journal of Global Information Management, DOI: 10.4018/jgim.356490	- The study highlights the limitations of traditional financial risk management methods, particularly their challenges in processing large-scale data, which leads to decreased accuracy in risk assessment. - It introduces a novel approach that combines gated recurrent units (GRU), temporal convolutional networks (TCN), and attention mechanisms to enhance the accuracy of financial risk assessments and improve the effectiveness of crisis warnings, demonstrating superior performance compared to baseline models.	- The study introduces a novel approach that combines gated recurrent units (GRU), temporal convolutional networks (TCN), and attention mechanisms to enhance the accuracy of financial risk assessments and the effectiveness of crisis warnings, addressing the limitations of traditional financial risk management methods. - Experimental results demonstrate that the proposed algorithm significantly outperforms baseline models, achieving over 46.8% reduction in FLOPs and more than 48.5% improvement in inference time on the LendingClub loan dataset, thereby contributing to the stability and operational efficiency of enterprises.	- The study highlights the limitations of traditional financial risk management methods, particularly their challenges in processing large-scale data, which can lead to decreased accuracy in risk assessment. However, it does not address potential limitations or challenges associated with the implementation of the proposed AI-based methods in real-world scenarios. - While the research demonstrates improvements in risk prediction accuracy, efficiency, and stability using the new algorithm, it lacks a comprehensive analysis of how these improvements translate into practical applications for different types of enterprises or industries, leaving a gap in understanding the broader applicability of the findings.

Aderamo, A. T., Olisakwe, H. C., Adebayo, Y. A., & Esiri, A. E. (2024). **AI-Driven HSE management systems for risk mitigation in the oil and gas industry.** Critical Review of Research in Engineering and Technology, DOI: 10.57219/crret.2024.2.1.0059	- The paper discusses the limitations of traditional HSE management systems in the oil and gas industry, which often rely on manual processes and reactive approaches, leading to inefficiencies and delayed responses to potential hazards. It emphasizes the need for a more proactive and data-driven approach to enhance safety and risk management. - It highlights the integration of AI technologies such as machine learning, computer vision, and predictive analytics into HSE management systems, which can process vast amounts of data in real-time, enabling continuous monitoring of hazardous conditions and allowing for predictive risk management to foresee potential risks before they materialize.	- The paper proposes the integration of Artificial Intelligence (AI) into HSE management systems, which enhances real-time safety monitoring and predictive risk management. By utilizing AI-driven technologies such as machine learning, computer vision, and predictive analytics, companies can proactively identify and mitigate risks, leading to a significant reduction in accidents, equipment failures, and environmental incidents. - It highlights the role of AI in automating routine safety checks and providing real-time alerts to enhance worker safety, thereby minimizing human error. The paper also discusses case studies demonstrating successful implementation of AI-driven HSE systems, resulting in substantial improvements in safety performance and operational efficiency within the oil and gas industry.	- The paper discusses the challenges and limitations of integrating AI into existing HSE frameworks, such as data security, workforce training, and technology costs, but does not provide specific strategies or solutions to address these challenges, indicating a gap in actionable recommendations for implementation. - While the paper highlights case studies of successful AI-driven HSE systems, it lacks a comprehensive analysis of the long-term impacts and sustainability of these systems in varying operational contexts within the oil and gas industry, suggesting a need for further research on the adaptability and scalability of AI technologies in diverse environments.

Aderamo, A. T., Olisakwe, H. C., Adebayo, Y. A., & Esiri, A. E. (2024). **AI-enabled predictive safeguards for offshore oil facilities: Enhancing safety and operational efficiency**. Critical Review of Research in Engineering and Technology, DOI: 10.57219/crret.2024.2.1.0060	- The paper explores the integration of Artificial Intelligence (AI) into predictive safety safeguards for offshore oil platforms, emphasizing the shift from traditional reactive safety systems to proactive risk mitigation strategies. It highlights the importance of real-time monitoring, data analytics, and machine learning algorithms in predicting potential hazards and enhancing safety and operational efficiency. - It discusses the development of machine learning models trained on historical data from previous offshore operations, which enable predictive maintenance and early warning systems for critical equipment. The framework proposed in the paper includes key components such as data acquisition, sensor integration, and a risk-based decision-making process to prioritize safety actions based on real-time threats.	- The paper presents a comprehensive framework for operationalizing AI-driven safety systems in offshore oil facilities, which includes key components such as data acquisition, sensor integration, and algorithm development. This framework aims to enhance safety by enabling predictive maintenance and early warning systems for critical equipment, thereby minimizing the risk of catastrophic incidents. - It contributes to the understanding of AI applications in industrial safety by providing a roadmap for the adoption of predictive safeguards in high-risk environments. The research highlights the importance of continuous data updating and human oversight to ensure that AI systems remain effective in adapting to evolving operational conditions, while also addressing challenges such as improving AI model accuracy and integrating with existing regulatory frameworks.	- The paper outlines key challenges such as improving the accuracy of AI models, which indicates a gap in the current capabilities of AI systems to reliably predict hazards in offshore oil facilities. This suggests a need for further research to enhance the precision and reliability of machine learning algorithms used in predictive safety systems. - Another identified gap is addressing cybersecurity risks associated with the integration of AI in offshore operations. As AI systems become more prevalent, ensuring their security against potential cyber threats is crucial, highlighting the need for research focused on developing robust cybersecurity measures tailored for AI-enabled safety systems in high-risk environments.

Shen, Q. (2024). **AI-driven financial risk management systems: Enhancing predictive capabilities and operational efficiency.** Journal of Financial Innovations, DOI: 10.54254/2755-2721/69/20241494	- The paper discusses the integration of artificial intelligence (AI) in financial risk management systems, highlighting how it has revolutionized traditional approaches by providing enhanced predictive capabilities and operational efficiency. - It explores various applications of AI in credit risk assessment, market risk analysis, operational risk management, and regulatory compliance, emphasizing the use of advanced machine learning algorithms to analyze vast datasets, including real-time market data and non-traditional sources, to improve risk predictions and enable proactive risk management.	- The paper discusses how AI-driven financial risk management systems enhance predictive capabilities by leveraging advanced machine learning algorithms to analyze vast datasets, including real-time market data and non-traditional sources, improving risk predictions and enabling proactive risk management. - It also highlights the benefits of AI in automating routine tasks, enhancing data analytics, and ensuring regulatory compliance, ultimately reducing the incidence of loan defaults, enhancing portfolio quality, and improving the overall resilience of financial institutions.	- The paper does not explicitly mention any specific research gaps in the current literature regarding the integration of AI in financial risk management systems. - It does not address potential limitations or challenges faced in the implementation of AI-driven systems in the context of financial risk management.

Yadav, P., Gupta, P., Sijariya, R., & Sharma, Y. K. (2024). **Artificial Intelligence in Risk Management**. In Advances in Risk Management Wiley. DOI: 10.1002/9781394175574.ch1	- The literature review of the paper focuses on the limitations of traditional risk management methods in the financial industry, such as the inability to manage large amounts of data, react quickly to market changes, and provide real-time monitoring of trends. - The paper highlights how artificial intelligence (AI) can enhance risk management practices by utilizing deep learning, machine learning algorithms, and natural language processing to analyze data, detect potential threats, uncover fraudulent activities, and provide predictive analytics for decision-making.	- Artificial intelligence (AI) can enhance risk management in the financial sector by utilizing deep learning, machine learning algorithms, and natural language processing to analyze huge amounts of data, react quickly to market changes, and provide real-time monitoring of market trends. - The application of AI in risk management has the potential to improve decision-making, reduce risks, and enhance overall financial stability by identifying potential threats, detecting fraudulent activities, and offering predictive analytics for informed decision-making.	- The paper does not explicitly mention any specific research gaps in the field of artificial intelligence in risk management within the financial industry. - It does not provide insights into areas where further research is needed to enhance the application of AI in risk management practices.

Steimers, A., & Schneider, M. (2022). **Sources of Risk of AI Systems. International** Journal of Environmental Research and Public Health, DOI: 10.3390/ijerph19063641	- The literature review of the paper focused on the importance of artificial intelligence in occupational safety and health, highlighting the increasing use of AI systems for protective devices and assistance systems. - The authors analyzed the differences between AI systems, particularly those based on modern machine learning methods, and traditional software to identify new sources of risk specific to AI technologies.	- The paper highlights the increasing number of accidents in systems utilizing artificial intelligence, including fatal accidents in automated vehicles, emphasizing the importance of defining criteria based on the sources of risk for AI systems. - It addresses the need to assess the risk of an AI application not only to determine its level but also to effectively reduce it by identifying sources of risk, incorporating them into the overall risk assessment, evaluating their criticality, and managing them early to prevent system failures.	- The paper identifies the need for adapting risk management measures for AI systems due to the new sources of risk they introduce, but it does not delve into specific strategies or frameworks for addressing these gaps. - While the paper provides a taxonomy of AI-specific sources of risk, it does not extensively discuss potential solutions or mitigation strategies for each identified risk category.

Hu, W., & Chen, Y. (2022). **Application of Artificial Intelligence in Financial Risk Management. In Advances in AI Applications** Springer. DOI: 10.1007/978-3-031-06794-5_15	- The paper discusses the current application status of artificial intelligence (AI) in financial risk management, highlighting its growing importance and the need for innovation in financial risk management systems to effectively utilize AI technologies. - It also addresses the potential risks associated with the use of AI in financial risk management and proposes countermeasures and suggestions to enhance the effectiveness of AI applications in this field, aiming to improve China's financial risk management system.	- The paper discusses the current application status of artificial intelligence (AI) in financial risk management, highlighting its role in enhancing the control and management of financial risks, which is essential for building a new intelligent financial prevention and control system. - It offers countermeasures and suggestions to address potential risks associated with AI in financial risk management, aiming to improve China's financial risk management system and providing meaningful references for future developments in this field.	- The paper discusses the application status and potential risks of AI in financial risk management but does not explicitly identify specific research gaps that need to be addressed in the field. - While it offers countermeasures and suggestions for improving financial risk management systems, it lacks a detailed exploration of the limitations and challenges faced in the current implementation of AI technologies in this domain.

Thekdi, S. A., & Aven, T. (2024). **Evaluation of information quality derived from AI-related information systems used for risk applications**. Journal of Risk Research, DOI: 10.1080/13669877.2024.2340013	- The paper focuses on the increasing prevalence and accessibility of artificial intelligence technologies, such as text and image generators, which have been both criticized and promoted for their potential to automate tasks and increase efficiencies. - It highlights the need to vet these new technologies for use in risk applications, regardless of their original design purpose, and proposes 14 criteria based on current risk science quality indicators to gauge the quality of information derived from AI-related information systems for risk applications.	- The paper develops 14 criteria based on current risk science quality indicators to evaluate the quality of information derived from AI-related information systems used for risk applications. - These criteria are then applied to a widely used AI-based information system to demonstrate their effectiveness in assessing the quality of information generated by such systems for risk purposes.	- The paper highlights the need to vet AI-related technologies for use in risk applications, but it does not delve into specific methodologies or frameworks for conducting this vetting process. - While the paper provides 14 criteria for evaluating the quality of information derived from AI-related information systems, it does not discuss potential limitations or challenges in applying these criteria in real-world scenarios.

Bedi, P., Goyal, S. B., & Kumar, J. (2020). **Basic Structure on Artificial Intelligence: A Revolution in Risk Management and Compliance**. Proceedings of the International Conference on Intelligent Systems and Security, DOI: 10.1109/ICISS49785.2020.9315986	- The paper provides a non-technical description of key AI strategies that are beneficial to risk management, highlighting how these strategies can transform risk assessment processes across various domains. - It includes a study on the application of AI methods in specific risk management fields such as credit risk, market risk, organizational risk, and enforcement, supported by existing experience and empirical data.	- The paper provides a non-technical description of key AI strategies that are beneficial to risk management, highlighting how these strategies can transform risk assessment processes across various fields such as credit risk, market risk, organizational risk, and enforcement. - It presents a study that utilizes existing experience and empirical data to demonstrate the application of AI methods in risk management, while also reflecting on the constraints faced by organizations, including challenges in effective data management practices, accountability, and the lack of requisite skill sets.	- The paper acknowledges existing constraints in effective data management practices, which may hinder the full potential of AI in risk management and compliance, indicating a gap in addressing how to overcome these data management challenges. - There is a noted lack of requisite skill sets within organizations, suggesting a gap in the research regarding the development and implementation of training programs or strategies to equip personnel with the necessary skills to effectively utilize AI in risk management.

Banja, J. (2020). **How Might Artificial Intelligence Applications Impact Risk Management.** AMA Journal of Ethics, DOI: 10.1001/AMAJETHICS.2020.945	- The literature review of the paper focuses on the ethical considerations and risks associated with the integration of artificial intelligence (AI) applications in various fields, particularly in healthcare operations. - It discusses the potential risks related to system malfunctions, privacy protections, and consent to data repurposing, highlighting the need for collaboration between traditional risk managers and experts in computer science, bioinformatics, information technology, and data privacy and security.	- The paper discusses the ethical implications and risks associated with the integration of artificial intelligence (AI) applications in health care, specifically focusing on system malfunctions, privacy protections, and consent to data repurposing. It emphasizes the need for traditional risk managers to collaborate with experts in computer science, bioinformatics, information technology, and data privacy to effectively manage these emerging risks. - It highlights the potential for AI technologies to dramatically alter health care practices and delivery, suggesting that while AI models may enhance diagnostic and prognostic accuracy, they also introduce new forms of risk that require proactive management strategies. The paper speculates on the evolving role of risk management in addressing these challenges, indicating that risk managers may need to specialize in AI applications to navigate the complexities of this new landscape.	- The paper does not explicitly address the potential impact of AI applications on medical liability and malpractice considerations, which could be a significant research gap in understanding the overall risk management implications. - Another research gap could be the lack of discussion on the ethical considerations surrounding the use of AI in healthcare, particularly in terms of patient autonomy and decision-making processes.

İnal, İ. H. (2023). Journal of Sustainable Development. DOI: 10.31567/ssd.865	- The literature review conducted in this study focuses on the use of artificial intelligence algorithms in fintech tools specifically for risk management, examining various studies to understand the current state of AI applications in this field. - The review aims to provide insights and inferences for future research by analyzing how AI can enhance risk management processes in financial institutions, including areas such as fraud detection, credit risk assessment, operational risk management, and market risk management.	- The study aims to determine the current situation of artificial intelligence in fintech risk management and make inferences for the future by examining existing research, thereby providing a comprehensive overview of the field. - It is expected that the findings will contribute to the literature by guiding future research on the use of artificial intelligence algorithms in fintech tools, particularly in the context of risk management.	- The paper aims to determine the current situation regarding the use of artificial intelligence in fintech risk management but does not explicitly identify specific research gaps that exist in the current literature, which could limit the understanding of areas needing further exploration. - While the study conducts a literature review on AI algorithms used in fintech tools for risk management, it does not address the potential challenges or limitations faced by financial institutions in implementing these AI technologies, which could be critical for guiding future research directions.

Sah, J., Padma, S., Ramakrishna, Y., & Irfan, M. (2024). **Risk Management of Future of DeFi Using Artificial Intelligence as a Tool. In Advances in Blockchain and DeFi Technologies** IGI Global. DOI: 10.4018/979-8-3693-6321-8.ch011	- The chapter evaluates the effectiveness of AI, particularly machine learning, in addressing emerging risks within the DeFi landscape, focusing on its strategic implementation to enhance risk assessment, management, and decision-making processes. - It emphasizes the importance of identifying and managing risks that could hinder the future of DeFi, highlighting key AI techniques such as data preparation, modeling, stress testing, validation, data quality assurance, text mining, and fraud detection.	- The chapter evaluates the effectiveness of AI, particularly machine learning, in managing emerging risks within DeFi, focusing on its applications in data preparation, modeling, stress testing, and validation to enhance risk assessment and decision-making processes. - It highlights the role of AI in ensuring data quality, conducting text mining, and detecting fraud, which are crucial for identifying and managing risks that could impede the future development of DeFi, thereby fostering transparency and decentralization in the financial industry.	- The chapter does not explicitly identify specific research gaps within the context of AI's application in DeFi, leaving an opportunity for further exploration of unaddressed areas in risk management and decision-making processes that could enhance user experience. - While the study evaluates AI's effectiveness in managing market and credit risks, it lacks a comprehensive analysis of the limitations and challenges faced by AI technologies in the DeFi space, which could provide a more balanced understanding of their potential and constraints.

Pasupuleti, M. K. (2024). **AI-Driven FinTech: Revolutionizing Fraud Detection and Risk Management in Finance.** New Era Science Journal, DOI: 10.62311/nesx/46656	- The chapter discusses the transformative impact of AI-driven technologies in FinTech, particularly in enhancing fraud detection through advanced machine learning algorithms that enable real-time monitoring and detection of various fraudulent activities, including credit card fraud, money laundering, and account takeovers. - It also highlights the role of AI in improving predictive analytics for risk management, allowing financial institutions to forecast credit, market, and operational risks with greater precision, while integrating AI with regulatory compliance systems and anti-money laundering programs to enhance overall financial security and efficiency.	- The chapter highlights the use of advanced machine learning algorithms in AI-driven technologies to enable real-time monitoring and detection of fraudulent activities, such as credit card fraud, money laundering, and account takeovers, resulting in faster and more accurate responses to these threats. - It discusses the enhancement of predictive analytics in risk management through AI, which allows financial institutions to forecast credit, market, and operational risks with greater precision, thereby improving overall financial security and efficiency.	- The chapter discusses the transformative impact of AI in fraud detection and risk management but does not explicitly identify specific research gaps or areas that require further investigation within these domains. This leaves an opportunity for future research to explore unaddressed challenges or limitations in the current AI applications in FinTech. - While ethical considerations and data privacy are mentioned, the chapter does not delve into the complexities of these issues or propose frameworks for addressing them in the context of AI-driven technologies in finance. This indicates a potential research gap in understanding how to balance innovation with ethical standards and privacy concerns in the financial sector.

Abikoye, B. E., Adelusi, W., Umeorah, S. C., & Adelaja, A. O. (2024). **Integrating Risk Management in Fintech and Traditional Financial Institutions Through AI and Machine Learning.** Preprints, DOI: 10.20944/preprints202407.1609.v1	- The paper highlights the significant transformation in the financial services landscape due to the rapid evolution of fintech, which has introduced new opportunities for innovation while also presenting substantial risks such as cyber threats, data privacy concerns, and regulatory compliance challenges. It emphasizes the need for a unified approach to risk management that addresses these emerging risks in the context of both fintech and traditional financial institutions. - It identifies the divergence in operational models and risk management practices between traditional financial institutions, which prioritize stability and compliance, and fintech companies, which focus on efficiency and customer satisfaction. This fragmentation in risk management creates challenges for the overall stability and security of the financial system, underscoring the necessity for an integrated framework that leverages AI and machine learning for comprehensive risk assessment.	- The paper proposes a comprehensive framework for integrating risk management practices between traditional financial institutions and fintech companies, addressing the fragmented risk landscape created by their divergent operational models and risk management approaches. This framework leverages advanced technologies such as artificial intelligence (AI) and machine learning (ML) to enhance the accuracy and comprehensiveness of risk assessments. - The integrated risk management approach includes unified policies covering critical areas such as cybersecurity, operational risk, regulatory compliance, and financial crime, along with real-time monitoring and reporting tools. This ensures robust risk management protocols and a prompt response to potential risks, ultimately enhancing the stability, security, and public confidence in the financial ecosystem.	- The paper identifies a critical need for a unified framework that integrates the risk management practices of traditional financial institutions and fintech companies, but it does not specify the exact methodologies or processes that would be employed to achieve this integration effectively. This gap highlights the necessity for further research into practical implementation strategies and the challenges that may arise during the integration process. - While the paper discusses the use of AI and machine learning for enhancing risk assessments, it does not address the potential limitations or biases associated with these technologies. Further research is needed to explore how these advanced technologies can be effectively utilized while ensuring fairness, transparency, and accountability in risk management practices across different financial entities.

Al Balooshi, A. (2018). **A Study on Artificial Intelligence And Risk Management.** *Journal of Risk Management Studies*	- The literature review highlights that artificial intelligence (AI) has been recognized as an effective tool for enhancing organizational success through the integration of search algorithms, statistical analysis, and machine learning. It emphasizes that AI has significantly improved problem-solving capabilities, making processes easier and faster, while also enhancing information security across various business sectors. - It discusses the necessity of AI in companies and government, noting that its implementation has led to the development of security measures against business threats and vulnerabilities. The review also addresses the challenges faced by organizations in maintaining security during communication and networking processes, which have become targets for attacks, thereby necessitating effective risk management strategies in conjunction with AI adoption.	- The study provides an analysis of the challenges faced by government and organizations in implementing artificial intelligence, highlighting the difficulties encountered during the integration of AI technologies into existing processes and systems. - It investigates the opportunities presented by artificial intelligence in enhancing organizational performance, demonstrating how AI can effectively fulfill the needs of organizational processes and improve risk management strategies.	- The research faced limitations in data collection due to a lack of sufficient time and financial resources, which may have hindered the comprehensiveness and authenticity of the data gathered. This gap suggests that further studies could benefit from a more extensive data collection process that addresses these constraints. - The study prioritized data collection in English, which may have restricted the diversity and breadth of perspectives included in the research. Future research could explore multilingual data collection to capture a wider range of insights and experiences related to artificial intelligence and risk management.

John, B., & Ghate, A. D. (2024). International Journal of Information Systems Security, DOI: 10.51983/ijiss-2024.14.4.03	- The literature review highlights the significant rise in the use of AI services within the banking industry over the past decade, emphasizing the improvements in client satisfaction and operational efficiency that have resulted from the adoption of machine learning (ML) technologies. It notes that these advancements have led to a paradigm shift in banking services, necessitating a thorough understanding of the associated digital risks and threats. - It discusses the importance of a structured risk management strategy that encompasses three key stages: planning ahead, executing risk management tasks, and maintaining and enhancing risk management practices. The review underscores that risk management is not a one-time effort but a continuous process that requires ongoing attention to effectively mitigate risks and improve overall service quality.	- The paper highlights the significant impact of AI services, particularly machine learning, on improving client satisfaction and efficiency within the banking industry, indicating a paradigm shift in banking services due to technological advancements. - It emphasizes the importance of a structured risk management strategy that involves three stages: planning ahead, executing risk management tasks, and maintaining and enhancing risk management, underscoring that risk management is a continuous process requiring ongoing attention to mitigate new threats effectively.	- The paper does not explicitly identify specific research gaps within the context of digital risk management in the banking industry, particularly regarding the integration of AI services and their associated risks. Further exploration is needed to understand the unique challenges posed by emerging technologies and how they can be effectively managed. - There is a lack of detailed discussion on the practical implementation of the proposed three-stage risk management strategy, including how firms can continuously monitor and enhance their risk management processes in the face of evolving digital threats. This presents an opportunity for further research into best practices and frameworks that can be adopted by organizations.

Abikoye, B. E., Adelusi, W., Umeorah, S. C., Adelaja, A. O., & Agorbia-Atta, C. (2024). **Integrating Risk Management in Fintech and Traditional Financial Institutions through AI and Machine Learning**. Journal of Economics and Management Studies. DOI: 10.9734/jemt/2024/v30i81236	- The literature review highlights the rapid evolution of financial technology (fintech) and its transformative impact on the financial services industry, emphasizing the need for a comprehensive understanding of the unique characteristics and risk profiles of both traditional financial institutions and fintech companies. It discusses the challenges posed by the divergence in operational models and regulatory requirements, which complicate the integration of risk management practices between the two sectors. - The review also examines the role of artificial intelligence (AI) and machine learning (ML) in enhancing risk management, noting their scalability, adaptability, and cost-effectiveness. It underscores the importance of integrating these technologies into various aspects of risk management, such as fraud detection, credit risk assessment, and regulatory compliance, while addressing challenges related to data quality, model interpretability, and ethical concerns.	- The paper identifies the critical need for a unified framework that integrates the risk management practices of traditional financial institutions and fintech companies, addressing the fragmented risk landscape created by their divergent operational models and risk management approaches. This integration aims to enhance the stability and security of the financial system by ensuring consistent and effective risk assessment across the sector. - It highlights the role of advanced technologies such as artificial intelligence (AI) and machine learning (ML) in improving risk management capabilities. By leveraging these technologies, the proposed framework enhances the accuracy and comprehensiveness of risk assessments, facilitates real-time monitoring and reporting, and promotes proactive rather than reactive approaches to managing risks, ultimately fostering public confidence in the financial services industry.	- The paper highlights the challenge of data quality and availability as a significant limitation in integrating AI and ML into risk management. It suggests that poor data quality can lead to erroneous risk assessments, indicating a gap in research focused on improving data collection, management, and validation processes to enhance the effectiveness of AI and ML models in financial risk management. - Another research gap identified is the issue of model interpretability, where many AI and ML models are considered "black boxes," making it difficult to understand their decision-making processes. This lack of transparency can hinder trust and regulatory acceptance, suggesting a need for further exploration into developing interpretable AI models that can provide clear explanations for their outputs, thereby fostering greater confidence among stakeholders in the financial sector.

Aziz, S., & Dowling, M. (2019). **Machine Learning and AI for Risk Management. In Advances in Machine Learning** Springer. DOI: 10.1007/978-3-030-02330-0_3	- The paper reviews the application of machine learning and AI techniques across various risk management fields, including credit risk, market risk, operational risk, and compliance (RegTech). It highlights empirical evidence and current practices that demonstrate how these technologies enhance risk assessment and management processes, such as improving prediction accuracy in credit risk modeling and automating compliance tasks. - It discusses the historical context of machine learning in risk management, noting that the use of AI techniques for credit risk modeling is not new but is increasingly prevalent. The paper references past studies that compare traditional statistical methods with machine learning algorithms, indicating a trend towards integrating these advanced techniques to achieve better accuracy and efficiency in risk management practices.	- The paper provides a non-technical overview of the main machine learning and AI techniques that are beneficial to risk management, categorizing risk management into credit risk, market risk, operational risk, and compliance. It highlights how these techniques are transforming the approach to financial risk management, including automating repetitive tasks and improving decision-making processes. - It discusses empirical evidence and current practices in applying machine learning and AI to various risk management fields, such as consumer lending and credit risk estimation, demonstrating significant cost savings and improved predictive accuracy compared to traditional methods. The paper also addresses the challenges of implementing these technologies, including data management policies and the need for skilled personnel.	- There is a significant gap in the availability of suitable data for implementing AI and machine learning techniques in risk management. Data is often siloed across departments, held on different systems, or not recorded formally, which restricts the effective use of these technologies. This lack of organized data hampers firms' abilities to leverage machine learning solutions fully. - Another research gap identified is the shortage of skilled staff capable of understanding and implementing AI and machine learning solutions. The readiness and ability of employees to work with these new technologies is a major concern for firms, indicating a need for more training and development programs to build a skilled workforce in this area.

Zekos, G. I. (2021). **AI Risk Management. In Innovations in Risk Management** Springer. DOI: 10.1007/978-3-030-64254-9_6	- The paper discusses how artificial intelligence is driving economic growth and industrial reforms by modernizing economic activities such as production, distribution, exchange, and consumption. - It highlights the role of blockchain technology in creating a token economy, where community revenue is allocated to content producers and service users, leading to a new economic paradigm.	- The paper highlights that artificial intelligence serves as a new engine for economic growth, driving industrial reforms and modernizing economic activities such as production, distribution, exchange, and consumption by leveraging the energy from previous technological revolutions. - It discusses the role of blockchain technology in establishing a token economy, which allocates community revenue to content producers and service users, thereby creating a new economic paradigm that transforms interactions and value generation in society.	- The paper does not specifically address the potential risks and challenges associated with the integration of AI agents into society, leaving a gap in understanding the societal implications of this technological advancement. - There is a lack of discussion on the ethical considerations and regulatory frameworks needed to manage the impact of AI on economic activities, indicating a gap in exploring the governance aspects of AI risk management.

5. Chapter 4: Business Case Studies / Practical Applications

5.1. Introduction to Case Studies

This chapter will explore how AI can be used for risk management through case studies from various sectors like finance, cybersecurity, and supply chains. This reveals how AI techniques are already being applied to reduce risk and paves the way for effective risk mitigation, ranging from AI-driven algorithms for predicting risk and automating operational efficiencies towards building a future-ready organization that can respond to emerging risks.

These industries and companies were selected for their importance, relevance, and pioneering adoption of Artificial Intelligence (AI) in risk management. The chosen industries — finance, cybersecurity, and supply chain management — represent very different domains of potential risk and ensure thorough representation of AI applications in risk management.

These companies are leaders in applying AI to risk management, presiding over innovative practices with proven metrics. Companies like PayPal and IBM are credited with early experiments with AI-based systems, while Amazon has taken predictive analytics to heights by changing the landscape of operational risk management in the process.

The selected companies work globally and have many complex environments where AI-based risk management practices can be implemented. All of these companies and industries have readily available case studies that are publicly accessible, guaranteeing both the transparency and the credibility of the examples used throughout this thesis.

5.2. Case Study 1: Financial Risk Management in PayPal

The financial sector is itself a risk-hungry one faced with issues like fraud, credit risk and the uncertainty of market fluctuations. PayPal, an international frontrunner as a provider of digital payment services, was chosen for its extensive use of AI-based fraud prevention tools and its success in curbing the risk and doing so without affecting the online financial service provider with unnecessary hindrances. For case in point, the picture PayPal processes millions of transactions every day around the world, which serves as very pertinent at an example for AI systems managing large scale and real time data in financial industry risk monitoring.

https://smartdev.com/ai-driven-fraud-detection/

PayPal. (2023). Also Read: AI-Powered Fraud Detection Systems https://www.paypal.com/ (accessed 03 October 2023).

Fraud detection which is an important area in financial risk management and where PayPal's introduction of volatile times has been one of the many practical instances and tangible

results powered by more advanced AI models. PayPal is one of the largest digital payment companies in the world, and its innovations draw a larger image of trends happening financially, making it an ideal business case.

5.2.1. Financial Risk Management: AI-Powered Fraud Detection

As we discussed earlier in previous chapters, one of the most life changing applications of AI in financial risk management is fraud detection. Machine learning models are used by AI applications to study trends in transactional data and detect anomalies, which are signs of potential fraud.

Advanced AI algorithms, such as deep learning models, are used by the payment platform PayPal to process millions of transactions every day. The system recognizes anomalous behavior, like exceeding purchase limits or transferring funds to a new location (i.e. across state lines). This method has allowed to significantly decrease fraud rates, all while maintaining a great customer experience (PayPal, 2023).

AI is useful to make PayPal sustainable especially in risk management related to fraud detection. Fraudulent activities can result in significant financial loss to PayPal. As a result, effective fraud detection protects the company's income and prevents possible losses from chargebacks and illegal transactions. A trusted platform is essential to keeping consumers coming back. The confidence that users have on the safety of their transactions leads for them to user even more PayPal therefore increasing usage and customer retention.

PayPal and other such financial institutions are required to follow strict fraud prevention laws. Advanced fraud detection systems assist with compliance to these regulations, avoiding legal repercussions and reputational harm. PayPal's strong reputation for security can set it apart from the competition in the competitive digital payment space. Outcome PayPal is known for effective fraud detection which increases PayPal's brand image and attracts more users.

5.2.2. Impact of AI in Risk Management in Fraud Detection

AI algorithms are capable of analyzing millions of transactions in real-time, recognizing patterns and anomalies that indicate potential fraudulent behavior. This process of rapid analysis enables quick actions to be taken, like flagging suspicious transactions for further investigation.

The payment platform is one of the biggest and most widely used online payment platforms in the world and facilitates millions of transactions every day. Given the sheer scale of financial activity on its network, combating fraud and securing user data is a key focus for the company. PayPal required a solution that not only scaled with its expanding user base but also efficiently detected and prevented fraud as it occurred.

Before embracing AI for fraud detection, PayPal's approach involved traditional fraud prevention methods, which were primarily manual reviews combined with rule-based systems. Although such techniques were partially effective, they weren't able to keep pace with the sheer number of transactions and the more sophisticated methods used by fraudsters. PayPal were looking for a solution that could provide automatic and greater accuracy in fraud detection, operational efficiency improvement, and enhanced security for its users. (https://smartdev.com/ai-fraud-detection/)

AI systems leverage machine learning to learn from past behavioral data and adjust to new tactics of fraud in a continuous journey. By ensuring that it remains one step ahead of fraudsters, PayPal's basic upgrades make its fraud detection even more effective.

The false positive rates are very high in traditional fraud detection approaches which ignore the rules for legitimate transactions. AI enhances accuracy by adjusting these detection parameters, preventing customer frustration and delivering an easy experience for actual transactions.

AI automates the fraud detection process, reducing reliance on human involvement. This enables PayPal to deploy resources more efficiently, Investigating high-risk instances while automating its processes.

Unlike other anti-fraud solutions that rely heavily on transaction data to analyze possible fraud cases, AI can integrate a broad range of risk factors from user behavior and external threats. By taking a comprehensive view of cyber risk, PayPal is also able to better spot potential weaknesses and proactively address risk.

As PayPal expands and handles a growing number of transactions, AI systems can scale with the volume while ensuring performance and keeping security intact. It is this scalability that allows for growth to be maintained in a fast-changing digital economy.

Overall, AI strengthens PayPal's fraud detection, which is fundamentally important for financial protection, customer trust, regulatory compliance, and competitive advantage. AI enables PayPal to perform real-time analysis, implement machine learning, decrease false positives, improve resource allocation, perform thorough risk assessments, and scale seamlessly. Together, these factors ensure that PayPal continues to innovate as a leading digital payment service provider while maintaining a secure environment for its users.

5.3. Case Study 2: Cybersecurity Risk Management using IBM Watson

The cybersecurity industry is constantly under siege by more complex cyberattacks. IBM Watson for Cybersecurity was chosen because of its innovative application of AI when it came to threat identification and mitigation. IBM's solution is widely deployed across industries and has proved scalability and efficacy against evolving cyber risks.

IBM Watson has the application of Natural Language Processing (NLP) and Real-time Analysis. As it can demonstrate AI's ability to respond to complex, emerging threats in the cybersecurity domain. With the example of leading AI systems developed by IBM in the field of cyber security that are appreciated worldwide, the new metrics are a challenge to those responsible for risk research in accordance with safety the state of the art.

AI plays an important role in defending against cybersecurity threats, especially when it comes to real-time threat detection and mitigation. Artificial intelligence is employed by enterprises to detect suspicious acts that conventional systems can't catch. Using data from malware reports and threat databases, IBM Watson uses NLP (Natural Language Processing) to analyse structured and unstructured data. With up to October 2023 data, the AI system recognized forthcoming risks that facilitate proactive responses for cyberattacks.

In 2022, IBM Watson helped a leading retail company prevent a large-scale ransomware attack by identifying unusual server activity hours before the threat materialized. IBM Watson reduced incident response time by 60%, minimizing potential damage and loss.

IBM Watson. (2022). Watson for Cybersecurity: Use Cases. Retrieved October, 2023, from https://www.ibm.com/watson/cybersecurity.

5.3.1. Traditional Cybersecurity Risk Management

Organizations using traditional risk management practices to address cybersecurity challenges face a number of Material Challenges:

Inefficiency in Threat Detection: Most traditional solutions depend on point-in-time rules and signatures, resulting in slow detection of both new and evolving threats. This somewhat orthodox method can lead to cyberattacks occurring before they are detected.

Overlooked Anomalies: Traditional systems often struggle to sift through large volumes of unstructured data (like social media or dark web activity) that may hold crucial signs of new threats. This negligence can expose organizations to attacks leveraging these gaps.

Slow Incident Response: It generally takes longer, having the manual processes involved in traditional risk management. This delay can increase the damage inflicted by cyberattacks on businesses, as organizations may fail to respond quickly enough to mitigate risks.

Limited Scalability: Traditional approaches may lack the scalability needed to manage evolving cyber threats effectively. Application of risk management methodologies to cyber threats can be challenging for organizations to adapt into their risk due to the overall higher velocity of new policies and practices in cyberspace, compared to physical policy and practices.

Inability to Predict Emerging Threats: Traditional risk management typically operates on historical data, making it difficult to anticipate emerging threats. Without powerful solutions to study trends and patterns, organizations might not be ready for future attacks.

Resource Intensive: Conventional methods can be resource-intensive, with the need for substantial manpower and time to monitor, evaluate, and respond to threats. This can pull resources away from other important business functions.

Fragmented Data Analysis: Traditional systems in this domain may not seamlessly integrate with a variety of data sources, resulting in fragmented insights. This can make it difficult for an organization to gain insight into its overall risk posture. AI-based solutions, such as Watson for Cybersecurity, leverage analytics and real-time data processing to provide a smarter way of addressing these problems, thereby allowing organizations to more efficiently and proactively monitor and mitigate cyber risks.

5.3.2. How IBM Watson helped to solving problems of traditional risk management?

Cybersecurity solutions - especially ones powered by AI technologies similar to IBM Watson for Cybersecurity - have mitigated many troubles from the classical risk management approaches. Here's how they've addressed these problems:

5.3.2.1. Efficiency in Threat Detection

Traditional methods often rely on predefined rules and signatures, which can delay the identification of new threats. AI-driven solutions utilize real-time analysis and machine learning to detect anomalies and emerging threats much faster, reducing the time it takes to respond to potential cyberattacks.

5.3.2.2. Comprehensive Data Analysis

Traditional systems often overlook vast amounts of unstructured data, such as social media activity or dark web information, which can provide critical insights into emerging threats. AI technologies, like Natural Language Processing (NLP), analyze both structured and unstructured data, ensuring that organizations do not miss critical indicators of potential risks.

5.3.2.3. Rapid Incident Response

Manual processes in traditional risk management can lead to slow incident response times. AI-driven solutions automate many aspects of threat detection and response, significantly reducing the time it takes to address incidents. For instance, IBM Watson reduced incident response time by 60%, allowing organizations to mitigate damage more effectively.

5.3.2.4. Scalability

As cyber threats evolve, traditional approaches may struggle to keep pace. AI solutions are designed to scale effectively, adapting to the increasing volume and complexity of cyber threats without requiring proportional increases in resources.

5.3.2.5. Predictive Capabilities

Traditional risk management often lacks the ability to predict future threats. AI-driven solutions analyze trends and patterns in data, allowing organizations to anticipate and prepare for potential cyberattacks before they occur.

5.3.2.6. Resource Optimization

Traditional methods can be resource-intensive, requiring significant manpower and time. AI solutions streamline processes and reduce the need for extensive human intervention, allowing organizations to allocate resources more efficiently to other critical business functions.

5.3.2.7. Holistic Risk Assessment

Traditional systems may suffer from fragmented data analysis, leading to a lack of a comprehensive view of an organization's cybersecurity posture. AI-driven solutions integrate data from various sources, providing a unified perspective that enhances an organization's understanding of its overall risk landscape. By addressing these challenges, cybersecurity solutions like IBM Watson enable organizations to proactively manage and mitigate cyber risks more effectively than traditional risk management methods.

5.4. Case Study 3: Operational Risk in Supply Chains of Amazon

The operational risks presented by supply chain disruptions have gained more attention than before, especially as far as global crises are concerned, with the COVID-19 pandemic being a rather stark example. The selection of Amazon, the leader in e-commerce and supply chain innovation, is based on its use of AI-enabled predictive analytics for improving demand forecasting and inventory management.

Amazon. (2021). The Use of AI in Supply Chain Optimization Retrieved from https://www.aboutamazon.com/

Strong supply chains are a critical risk, and Amazon's AI-driven solutions help address those, as well. Its position as a leading global e-commerce entity allows its practices to be influential in the broader landscape, serving as an example for organizations wishing to adopt AI in supply chain risk management.

AI could play a crucial role in supply chain risk management and perhaps most significantly in forecasting and minimizing the risk of operational disruption. So a sort of demand forecasting using their machine learning-based predictive analytics system. It uses vast amounts of historical sales data, weather conditions, and market trends to predict potential supply-chain disruptions.

For example, during the COVID-19 pandemic, Amazon's artificial intelligence systems accurately predicted increases in demand for essential goods, helping the company deploy resources appropriately and avoid stockouts. This forward-thinking strategy resulted in a 25% increase in delivery efficiency and propelled customer satisfaction amid a global pandemic.

Amazon's Supply Chain Innovations

5.4.1. Problems that traditional risk management faced using traditional risk management methods

Supply chain risk management through traditional methods has not been without its challenges. Traditional approaches also depend on historical data and static models, which may not accurately anticipate the next disruption or fluctuations in demand. Its methods may not be quick enough to handle the fast pace of change in the marketplace or other unexpected events, including natural disasters or orientations. In addition, they also tend to work in silos, resulting in lack of communication and collaboration across departments/stakeholders, which impede meaningful risk identification and feedback.

Traditional risk management approaches are often reactive, dealing with what already happened instead of preemptive. Supply chains have become more interlinked and globalized than ever before, which is significantly challenging traditional approaches to risk management as these frameworks fail to factor in all possible risks and their correlations. Moreover, they might not take full advantage of cutting-edge technology, such as AI and machine learning, that can augment risk identification and mitigation processes.

Last but not least, resource shortages — be it time or budget or a talent pool — can prevent organizations from adopting all-encompassing risk management. Organizations can leverage advanced technologies and innovative practices to get around these challenges and improve their supply chain risk management capabilities.

5.4.2. How AI in Amazon's Risk Management helped to solving problems of traditional risk management?

AI in Amazon's risk management has significantly addressed the shortcomings of traditional risk management methods in several key ways:

5.4.2.1. Proactive Forecasting

Conventional risk management primarily depend on past reference data and fixed models, leading to reactive and unable to foresee future disruptions. So, while Amazon relies on AI-powered predictive analytics using machine learning algorithms to analyze huge volumes of data such as historical sales, market trends, and weather patterns. This allows Amazon to predict demand more accurately and flag potential disruptions before they happen.

5.4.2.2. Dynamic Adaptability

Traditional methods well can have difficulty to adapt to fast changes in the market conditions and unpredictable events, for example natural disasters or pandemics. Amazon has built its AI systems to be dynamic, using new data to recognize patterns and updating forecasts. Such adaptability improves the ability of the company to respond to demand in ways that have been seen during the COVID-19 pandemic, when AI was able to forecast large increases in demand for everyday goods.

5.4.2.3. Enhanced Collaboration

Risk management practices remain within individual departments—these make up silos, which can lead to communication problems and a lack of collaboration between departments. Better data integration across all stakeholders through AI at Amazon leads to better visibility and collaboration. This interconnectedness enables more thorough risk assessments and coordinated responses.

5.4.2.4. Resource Optimization

Both skills and resources for implementing traditional risk management strategies may not be available. By leveraging AI, Amazon can optimize their resources, ensuring that the inventory is managed better to avoid stockouts and improve delivery optimally. Over the pandemic, this pre-emptive distribution of resources led to a 25% increase in delivery efficiency.

5.4.2.5. Comprehensive Risk Analysis

It is increasingly difficult to capture all possible risks and their inter-dependencies in traditional risk methods, with global supply chains becoming more and more complex. AI augments risk identification and mitigation processes by examining a larger number of

variables and scenarios, offering a more comprehensive perspective of the supply chain landscape.

With its use of AI, Amazon has revolutionized its risk management approach to offer more than traditional means can while paving the way as a supply chain innovator.

5.5. Ethical and Practical Aspects When It Comes to Using AI

The use of AI in risk management also presents ethical and practical challenges. Data privacy, model interpretability, and issues of bias remain concerns even as AI Member greatly increases efficiency and accuracy. For example, Fletcher and Neuberger (2021) contend that AI models in cybersecurity could pose a risk of violation of user privacy if such models are deployed without appropriate safeguards. In financial risk management, opaque models can provide black box solutions that may affect client trust and regulatory compliance.

5.5.1. Data Privacy

Cybersecurity and financial applications of AI models are contingent on having access to massive amounts of personal and transaction data, and therefore raise privacy concerns. Data privacy legislation like the GDPR enacts strict controls on how much data can be used, ensuring transparency and consent for the uses of AI in applications (Ng & Jordan, 2020).

5.5.2. Being Clear and Understandable

The black-box phenomenon of advanced AI models, including deep learning systems, complicates transparency. For instance, most sectors, especially finance, need suitable explainable AI models to meet regulatory requirements (Miller, 2019). Model interpretability is essential for organizations to build trust and comply with legal frameworks.

5.5.3. Bias and Fairness

You are biased towards the training data you get trained on. This is particularly troubling in sensitive domains such as the credit industry, where biased AI models can affect whole demographics unfairly. Reducing bias is paramount in preventing unfair and biased AI applications in risk management, as noted by Brynjolfsson and McAfee (2017).

5.6. Summary

This chapter contains case studies that highlights the practical application of AI in financial,risk management, cybersecurity risk, and supply chain risk management. AI's predictive capabilities and real-time nature enable organizations to enhance their risk assessment and improve their business continuity. Despite these benefits, ethical challenges

surrounding data privacy, transparency and bias have continued to be significant hurdles to overcome as organizations adopt AI systems into risk management frameworks.

6. Conclusion and Recommendations

This final chapter synthesizes the key insights from the preceding chapters, drawing conclusions on the impact of Artificial Intelligence (AI) on risk management and highlighting actionable recommendations for organizations looking to leverage AI in their risk strategies. This chapter also addresses the limitations identified in AI-driven risk management and proposes areas for future research to advance the field.

6.1. Summary of Key Findings

6.1.1. AI's Transformative Potential

Artificial intelligence (AI) is rapidly transforming the landscape of risk management, enabling an unprecedented level of predictive accuracy and operational speed, as well as adaptability, across industries from finance to cybersecurity to supply chain management. Chapter 5 shows how AI-driven models have the potential not only to transform existing risk assessment methodologies, but also to help organizations with real-time risk detection, enabling them to detect and address potential risk as it occurs. By taking this proactive step, not only can decision-makers respond effectively, but also the chances for human error — an inevitable element of traditional risk decision-making methods — is greatly reduced.

Artificial intelligence technologies, such as machine learning, have melded in a way that has been noted in the work of Brynjolfsson & McAfee (2017) and Goodfellow et al. (2016) Emphasis is on the deep capacities of all such smart systems to not just deliver efficiencies but strengthen an enterprise in a more effective manner to follow risks of an ever more complex nature.

6.1.2. Challenges and Ethical Concerns

Despite the extensive advantages of artificial intelligence, there are numerous challenges and moral dilemmas that hang over the use of artificial intelligence. The Quality Of Data Used To Train AI Model may lead to Inaccurate predictions and decisions resulting from poor data quality can have severe implications, especially in sensitive domains like healthcare and finance. In addition, the complexity of many AI systems often makes decisions inexplicable for users and stakeholders. This lack of transparency is especially concerning in regulated sectors, where regulatory entities require that decisions must be not just correct, but explainable.

Such applications, as noted by Miller (2019), must not only be capable of interpretation, but also be able to provide sufficient explanations to the end user; the lack of which can destroy trust and accountability, two required qualities for industries working in highly-regulated spaces. Moreover, there are ethical implications of AI, beyond transparency. They can be based on

numerous things, some of them might be related to the training data even or potentially biased algorithms too. These biases can reinforce systemic inequalities found in our society, resulting in the unjust treatment of individuals based on their race, gender, or economic situation. Indeed, as Fletcher and Neuberger (2021) emphasize: "these ethical implications highlight the importance of a balanced and responsible approach to the adoption of AI."

Essentially you should not only focus on technological progress but however make efforts to participate in more fair, accountable and inclusive ethics in ai. We simply cannot afford to ignore the importance of both of these perspectives in this critical juncture in the development of AI.

6.1.3. Comparative Analysis

The conventional approaches to risk assessment and management have been tried, focusing on the core principles of control and regulatory compliance. Such methodologies usually involve established protocols as well as historical data which can breed a sense of security and trust among various stakeholders. But they often fail to deliver the agility and foresight. Static methods make it challenging for organizations to respond quickly to fast changing environments or new threats. On the other hand, AI-powered approaches use sophisticated algorithms and machine learning techniques to process large volumes of data in real time. This allows organizations to not only react to present risks but also predict future risks more accurately.

AI predictive capabilities unveil patterns and insights that may remain hidden with traditional approaches, translating into a more adaptive and proactive approach to risk management. However, both classical and AI-based solutions also have their unique strengths and weaknesses.

While traditional methods are reliable, they may not be as fast and adaptable as needed in the fast-paced landscape of the current era. AI-based approaches, in contrast, although potentially very powerful, can raise issues associated with next-generation data privacy, ethics, and may require significant technology investment. Taking these points into account, an **hybrid model that draws upon the advantages of both approaches presents itself as a strong solution across the different risk domains that an organization may fall under**.

This creates a robust framework for risk management by bringing together the basis of trustworthiness from the traditional methods with the adjustable and forward-looking potential from the AI. This integration not only improves decision-making processes, but further equips organizations to handle complexities of the market with enhanced confidence and resilience (Jordan & Mitchell, 2015).

6.1.4. Recommendations

6.1.4.1. Implement Explainable AI (XAI) in High-Stakes Sectors

With the ever-growing importance of data in the modern world, the incorporation of Explainable AI (XAI) has never been more vital, especially in high-stakes industries like finance and compliance. These are industries that are heavily regulated and require high levels of transparency in the decision-making process. Addressing these problems requires organizations to adopt XAI solutions that shed light on the inner workings of AI models. XAI goes beyond traditional AI systems by delivering thorough explainability of the ways in which a model reaches a conclusion. Such disclosure is critical in building confidence among key constituents, including regulators, customers, and employees. Not only does this increase the trustworthiness of organizations and their products, it also contributes to their conformity to guidelines that require clarity and accountability in the operation of organizations.

Additionally, the introduction of XAI can considerably reduce risks associated with algorithmic biases and errors that can have major impacts in sectors where financial decisions influence consumers and businesses too. With insights into the reasoning behind AI-based decisions, organizations can detect potential biases in their models and correct them to achieve fair and equitable results.

To conclude, the tactical incorporation of Explainable AI in critical domains represents not just a technological evolution, but a fundamental paradigm shift towards a more transparent, accountable, and trustworthy operational environment. This not only is aligned with regulatory demands but also gives organizations the ability to make skilled decisions, resulting in better invoice assurance and increased organizational transparency (Russell & Norvig, 2020).

6.1.4.2. Prioritize Data Quality and Standardization

The adage-so much rub in the realm of artificial intelligence (AI) where the quality of data is paramount, enshrined as the bedrock foundation of AI models. Others need to understand that the effectiveness of AI systems is directly proportional to the consistency and validity of the data they possess. This step becomes increasingly important in fields like supply chain management, where data may be outdated and inconsistent across various geographical regions and operational silos.

Leaders need to invest in mental and physical well-being here in July, and throughout the coming months. This means putting clear protocols and frameworks in place to guide data collection, processing, and storage, enabling comparability between datasets and assuring their accuracy. Standardized data formats and definitions help organizations avoid discrepancies that might occur within localized practices or differences in understanding of data elements. Focus on data quality and standardization pays a lot and ensures compliance, however, it goes a long

way in improving the prediction power of AI. With standardized, high-quality data, AI algorithms can be trained better to provide better predictions and insights. As stressed by Baryannis et al. (2019), organizations that embrace these practices over the long haul can unlock the true power of AI, leading to better decision-making and efficient operations.

Quality and standardization are the most important components and building blocks of data.

6.1.4.3. Mitigate Bias Through Diverse Training Data

The need to consider bias stemming from training data in the creation of fair and equitable artificial intelligence (AI) systems is paramount. It is crucial that we counteract the entrenchment of existing biases in our outcome sets through designing and deploying systems that are trained on a diverse range of training data that captures a broad range of demographic, experience, and conditional settings. Not only does this diversity help to make AI systems more robust, but it also ensures that they reflect the diverse nature of human society.

Having a diverse range of perspectives represented in training data can further mitigate the risks of propagating stereotypes and exclusionary practices that might otherwise occur through a non-representative dataset. In teaching AI models how to make more context-sensitive decisions that account for the complex nature of real-world situations, diversity serves a mainstreaming role, so to speak, by including representation from across the span of age groups, ethnic backgrounds, genders, socio-economic statuses and geographic localities. Additionally, regular audits and evaluations of AI models should be conducted to ensure their performance and fairness across various demographic categories. These audits must be systemic and comprehensive, scrutinizing not only the results generated by models but also the enabling algorithms and data sources.

The solution is to audit AI systems for fairness, which involves examining them for near transparency and finding disparities in treatment or outcomes; stakeholders can understand and correct these discrepancies. It's essential, therefore, to ensure diverse training data, continuous evaluation, and cross-discipline collaboration. Such openness encourages trust and confidence in AI technologies while ensuring that the development process is in line with ethical standards and societal values, which are essential for the progress of human-friendly and responsible AI.

6.1.4.4. Adopt Hybrid Models in Risk Management

Hybrid models represent a powerful strategy for risk management, that combine the best of both worlds between AI and traditional models. By combining these two approaches,

insurers can improve their predictive powers and meet their regulatory obligations, balancing innovative development with compliance. Utilizing traditional risk assessment models allows organizations to retain a degree of decision transparency, which is often vital in regulated environments. Please note that you access conventional models based on known statistical techniques formulated on historical data, which offer a transparent rationale behind decision-making — a crucial aspect in satisfying regulatory scrutiny while gaining stakeholders trust.

At the same time, the use of artificial intelligence technologies can transform data analysis and facilitate the processing of huge information volumes with unprecedented speed and accuracy. Through machine learning, AI algorithms can detect patterns and relationships that might be overlooked in conventional analyses, allowing organizations to predict risks with increased precision. By harnessing this potential, you complement AI with traditional methods, creating a basis for smarter decisions driven by extensive insights. In addition, in many of these organizations, AI would be carefully integrated into a framework, empowering enterprise risk management efforts and risk controls to react in a fine-tuned manner in near-real time.

This flexibility has been critical in the fast-moving business world of today, where new risks can arise in moments and must be addressed promptly. Overall, adopting a hybrid risk management model that blends the tried-and-true reliability of traditional methodologies and frameworks with the innovative possibilities offered by AI can greatly strengthen an organization's capability to manage the complexities of risk. This best of both worlds concept adds predictive power while maintaining compliance, as highlighted by Brynjolfsson and McAfee (2017).

6.1.4.5. Address Ethical and Privacy Concerns in AI

Ethical and Privacy Considerations for AI: Striking the Right Balance In the fast-paced world of artificial intelligence (AI), organizations are faced with the dual challenge of applying strong ethical principles and compliance with rigorous data privacy regulations like the General Data Protection Regulation (GDPR). The reason is that building trust with users is not only important for user engagement, but also on security side, there have been many instances of data breach and misuse of their personal information over the time. What is also profoundly important is when considering usability in potential applications of AI (cybersecurity, financial services, etc.), ethical considerations which cannot be overridden. These sectors often deal with enormous amounts of personal data in a manner that makes them prime candidates for exploitation, and which increases the stakes for ethical failures.

Companies need to strike a balance between proactive measures to ensure that their AI systems are designed and trained to respect user privacy, facilitate transparency and foster accountability. To that end, organizations should adopt broad frameworks that make ethical AI

a priority. This includes careful assessments of potential impacts to evaluate how any particular AI technologies could affect the privacy of individuals and the practices of society. Moreover, establishing a culture of ethical mindfulness via training and education can empower employees to identify and confront potential ethical quandaries where and when they occur. In addition, adherence to data privacy regulations such as GDPR is not just a legal necessity, but it is an essential component of accountable AI implementation.

This means organizations should be using data they need to know, listening in instances where they can with explaining why they support these practices. This allows them to minimize the risk of utilizing data inappropriately and to gain further trust from consumers as well as regulatory bodies.

With AI's ongoing encroachment into life and business, it will be critical to ensure these ethical and privacy concerns are addressed. Such organizations will not only safeguard users but also emerge as a front-runner of responsible AI innovation, thus, inducing a more reliable digital ecosystem.

6.1.5. Suggestions for Future Research

While AI's role in financial and cybersecurity risk management is well-studied, AI **applications in regulatory compliance remain underexplored**. Future research could focus on the specific challenges and benefits of using AI to monitor and ensure compliance.

Additionally, given the ethical implications of AI in decision-making, further studies on ethical AI frameworks and bias mitigation strategies in risk management would be valuable. **Research into fairness, accountability, and transparency could help organizations develop more responsible AI applications**.

Moreover, **empirical studies that assess the effectiveness of hybrid models combining AI-driven and traditional risk management approaches could offer valuable insights**. By examining real-world applications, researchers could determine the optimal balance between AI and traditional models.

Finally, **future research should prioritize exploring explainable AI (XAI) applications in high-risk sectors** like finance, where interpretability and regulatory compliance are essential.

6.1.6. Conclusion

This dissertation exemplifies the transformative diversity of potential for AI in risk management, spotlighting its superior predictive performance, agility, and adaptability across various sectors such as finance, cybersecurity, and operational risk. Although AI-powered approaches have considerable benefits, they also introduce significant issues on the area of

transparency, quality of the data, and ethics. This will lead organizations to developing effective and compliant risk management frameworks encompassing both AI and traditional approaches.

Finally, with developments in both spheres, AI's role in risk management will only continue to grow. Upon addressing the standard ethical and practical challenges laid out in this study, organizations can use AI to build forward-leaning, adaptive risk management systems that are fit for both operational and regulatory purposes.

7. Apendix A: References

1. Banks, E. (2013). Overview of Risk Management. DOI: 10.1002/9781118673270.CH1
2. Williams, R., Sample, J., Rosen, C., Sundar, S., Jones, R., & Borrero, E. (2013). Objectively managing risk. https://online.hbs.edu/blog/post/risk-management
3. Enholm, I. M., Papagiannidis, E., Mikalef, P., & Krogstie, J. (2021). Artificial Intelligence and Business Value a Literature Review. DOI: 10.1007/S10796-021-10186-W
4. WebPortal of European Parliament, "What is artificial intelligence and how is it used?", https://www.europarl.europa.eu/topics/en/article/20200827STO85804/what-is-artificial-intelligence-and-how-is-it-used
5. Jordan, M. I., & Mitchell, T. M. (2015) - "Machine learning: Trends, perspectives, and prospects." *Science*, 349(6245), 255-260.
6. Yuqi, Xue. (2021). Analysis of the Shortcomings of Financial Engineering in Traditional Risk Management Methods. 509-511. DOI: 10.2991/AEBMR.K.210210.082
7. Baryannis, G., Dani, S., & Antoniou, G. (2019) - "Predicting supply chain risks using machine learning: The trade-off between performance and interpretability." *Future Generation Computer Systems*, 101, 993-1004. DOI: 10.1016/j.future.2019.07.059
8. Barnea, A. (2020). How will AI change intelligence and decision-making? DOI: 10.37380/JISIB.V1I1.564
9. Georges Dionne, Risk management: History, definition and critique, 2013
10. Ramachandran, K., K, K., Vinjamuri, L., R, R., Al-Taee, M., & Alazzam, M. (2023). Using AI for Risk Management and Improved Business Resilience. *2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*, 978-982. DOI: 10.1109/ICACITE57410.2023.10182662.
11. Aziz, S., & Dowling, M. (2018). Machine Learning and AI for Risk Management. *Disrupting Finance*. DOI: 10.1007/978-3-030-02330-0_3.
12. Aziz, S., & Dowling, M. (2018). AI and Machine Learning for Risk Management. *CGN: Risk Management Practice (Topic)*. DOI: 10.2139/ssrn.3201337.
13. (2022). Roadmap for Risk Management Integration Using AI. *Journal of Risk & Control*. DOI: 10.47260/jrc/912.
14. Brynjolfsson, E., & McAfee, A. (2017) - "The business of artificial intelligence: What it can–and cannot–do for your organization." *Harvard Business Review*, 95(6), 3-10.
15. Goodfellow, I., Bengio, Y., & Courville, A. (2016) - *Deep learning*. MIT Press. DOI: 10.1126/science.aaa8415
16. Makridakis, S. (2017) - "The forthcoming artificial intelligence (AI) revolution: Its impact on society and firms." *Futures*, 90, 46-60. DOI: 10.1016/j.futures.2017.03.006

17. A. Y., & Jordan, M. I. (2020) - "Artificial intelligence and machine learning in risk management: An overview." *Annual Review of Financial Economics*, 12, 1-22. DOI: 10.1146/annurev-financial-012720-011700
18. Russell, S., & Norvig, P. (2020) - *Artificial intelligence: A modern approach*. Pearson.
19. ANSI/ASSP/ISO 31000-2018 Risk Management – Guidelines
20. COSO Enterprise Risk Management – Integrated Framework
21. (REGULATION (EU) 2024/1689 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL).
22. Project Management Institute's (PMI) PMBOK Guide, Chapter on Risk Management)
23. Morandín-Ahuerma, F. (2022). What is Artificial Intelligence? *International Journal of Research Publication and Reviews*. DOI: 10.55248/gengpi.2022.31261
24. Zhang, C. (2023). *Foundations of artificial intelligence and machine learning*. DOI: 10.4337/9781803926179.00009
25. Abioye, S., Oyedele, L., Akanbi, L., Ajayi, A., Davila Delgado, J. M., Bilal, M., Akinade, O., & Ahmed, A. (2021). *Artificial intelligence in the construction industry A review of present status opportunities and future challenges*. DOI: 10.1016/j.jobe.2021.103299
26. *Machine learning, explained | MIT Sloan*. (2021, April 21). MIT Sloan. https://mitsloan.mit.edu/ideas-made-to-matter/machine-learning-explained
27. Overview of Neural Network. (2022). *International Journal of Advanced Research in Science, Communication and Technology*. DOI: 10.48175/ijarsct-4851
28. Henrys, K. (2021). Role of Predictive Analytics in Business. *Social Science Research Network*. DOI: 10.2139/SSRN.3829621
29. Makridakis, S. (2017). The forthcoming artificial intelligence (AI) revolution: Its impact on society and firms. *Futures*, 90, 46-60. DOI: [10.1016/j.futures.2017.03.006]
30. Gunning, D., Stefik, M. J., Choi, J., Miller, T., Stumpf, S., & Yang, G.-Z. (2019). *XAI—Explainable artificial intelligence*. https://doi.org/10.1126/SCIROBOTICS.AAY7120
31. De, T., Giri, P., Mevawala, A., Nemani, R., & Deo, A. (2020). Explainable AI: A Hybrid Approach to Generate Human-Interpretable Explanation for Deep Learning Prediction.*Procedia Computer Science*. https://doi.org/10.1016/J.PROCS.2020.02.255
32. Salama, A., Linke, A., Rocha, I. P., & Binnig, C. (2019, September 20). XAI: A Middleware for Scalable AI. *International Conference Data Science*. https://doi.org/10.5220/0008120301090120
33. Jordan, M. I., & Mitchell, T. M. (2015). Machine learning: Trends, perspectives, and prospects. *Science*, 349(6245), 255-260.
34. Abikoye, B. E., Adelusi, W., Umeorah, S. C., & Adelaja, A. O. (2024). *Integrating Risk Management In Fintech And Traditional Financial Institutions Through Ai And Machine Learning*. DOI: 10.20944/202407.1609.v1
35. Vannucci, M., & Colla, V. (2016). *Classification of Unbalanced Datasets and Detection of Rare Events in Industry: Issues and Solutions*. DOI: 10.1007/978-3-319-44188-7_26

36. Mishra, A., Anand, S., Debnath, N., Pokhariyal, P., Patel, A., Yadav, P., Gupta, P., Sijariya, R., & Sharma, Y. (2024). *Artificial Intelligence in Risk Management*.
37. Bostrom, N. (2017). *Superintelligence: Paths, dangers, strategies*. Oxford University Press.
38. Sarioguz, O., & Miser, E. (2024). *Integrating AI in financial risk management Evaluating the effects of machine learning algorithms on predictive accuracy and regulatory compliance*. DOI: 10.30574/ijsra.2024.13.2.2206
39. Yazdi, M., Zarei, E., Adumene, S., Article, A., & Beheshti, A. (2024). *Navigating the Power of Artificial Intelligence in Risk Management A Comparative Analysis*. 10.3390/safety10020042
40. Aziz, S., Dowling, M., & Dowling, M. (2018). AI and Machine Learning for Risk Management. *Social Science Research Network*. DOI: 10.2139/SSRN.3201337
41. Conforti, R., ter Hofstede, A. H. M., ter Hofstede, A. H. M., ter Hofstede, A. H. M., La Rosa, M., La Rosa, M., & Adams, M. (2012). *Automated Risk Mitigation in Business Processes*. DOI: 10.1007/978-3-642-33606-5_14
42. Bedi, P., Goyal, S. B., & Kumar, J. (2020, December 3). Basic Structure on Artificial Intelligence: A Revolution in Risk Management and Compliance. *International Conference Intelligent Sustainable Systems*. DOI: 10.1109/ICISS49785.2020.9315986
43. Zohuri, B., & Rahmani, F. (2019). Artificial Intelligence Driven Resiliency with Machine Learning and Deep Learning Components. *Journal of Communication and Computer*. DOI: 10.17265/1548-7709/2019.01.001
44. Wang, Y. (2023). Research on the Model of Preventing Corporate Financial Fraud under the Combination of Deep Learning and SHAP. *International Journal of Advanced Computer Science and Applications*. DOI: 10.14569/ijacsa.2023.0140390
45. Lacruz, F., & Saniie, J. (2021, May 14). Applications of Machine Learning in Fintech Credit Card Fraud Detection. *Electro/Information Technology*. DOI: 10.1109/EIT51626.2021.9491903
46. Bao, Y., Hilary, G., & Ke, B. (2020). Artificial Intelligence and Fraud Detection. *Social Science Research Network*. DOI: 10.2139/SSRN.3738618
47. Dutta, A., & Kant, S. (2020). *An Overview of Cyber Threat Intelligence Platform and Role of Artificial Intelligence and Machine Learning*. DOI: 10.1007/978-3-030-65610-2_5
48. Amarasinghe, A.M.S. N., Wijesinghe, W. A. C. H., Nirmana, D. L. A., Jayakody, A., & Priyankara, A. M. S. (2019, December 1). *AI Based Cyber Threats and Vulnerability Detection, Prevention and Prediction System*. DOI: 10.1109/ICAC49085.2019.9103372
49. Miller, T. (2019). Explanation in artificial intelligence: Insights from the social sciences. *Artificial Intelligence*, 267, 1-38. DOI: [10.1016/j.artint.2018.07.007] (DOI: 10.1016/j.artint.2018.07.007)

50. Hofstetter, M., Riedl, R., Gees, T., Koumpis, A., & Schaberreiter, T. (2020, September 1). *Applications of AI in cybersecurity*. DOI: 10.1109/TRANSAI49837.2020.00031
51. Qureshi, N. I., Singh, P., Garg, A., & Retzlaff, N. (2024). *International Conference on Knowledge Engineering and Communication Systems ICKECS AI and Corporate Risk Management Identifying and Mitigating Technological and Ethical Risks*.
52. Eder, J. S. (2016). *Predictive Model Development System Applied To Enterprise Risk Management*.
53. Almari, M. M., & Festijo, E. D. (2019). Real-Time Monitoring of Computer Resources with Predictive Intelligence and Analytics. *International Journal of Simulation: Systems, Science and Technology*. DOI: 10.5013/IJSSST.A.20.S2.18
54. Barta, G., & Görcsi, G. (2019, May 8). *Assessing and managing business risks for artificial intelligence based business process automation*. DOI: 10.3846/CIBMEE.2019.084
55. Prasanth, A., Vadakkan, D. J., Surendran, P., & Thomas, B. (2023). Role of Artificial Intelligence and Business Decision Making. *International Journal of Advanced Computer Science and Applications*. DOI: 10.14569/ijacsa.2023.01406103
56. Yapo, A., & Weiss, J. W. (2018, January 3). Ethical Implications of Bias in Machine Learning. *Hawaii International Conference on System Sciences*. DOI: 10.24251/HICSS.2018.668
57. Rubin, V. (2020). *AI Opaqueness: What Makes AI Systems More Transparent?* DOI: 10.29173/CAIS1139
58. Earley, S. (2017). The Problem With AI. *IT Professional*. DOI: 10.1109/MITP.2017.3051331
59. Guikema, S. D. (2020). Artificial Intelligence for Natural Hazards Risk Analysis: Potential, Challenges, and Research Needs. *Risk Analysis*. DOI: 10.1111/RISA.13476
60. Wahl, B., Cossy-Gantner, A., Germann, S., & Schwalbe, N. (2018). Artificial intelligence (AI) and global health: how can AI contribute to health in resource-poor settings? *BMJ Global Health*. DOI: 10.1136/BMJGH-2018-000798
61. Brynjolfsson, E., & McAfee, A. (2017). The business of artificial intelligence: What it can–and cannot–do for your organization. *Harvard Business Review*, 95(6), 3-10.
62. Fletcher, D., & Neuberger, L. (2021). Navigating ethical AI in risk management. *AI & Society*, 36(4), 1279-1295. DOI: [10.1007/s00146-020-01062-w] (DOI: 10.1007/s00146-020-01062-w)
63. Baryannis, G., Dani, S., & Antoniou, G. (2019). Predicting supply chain risks using machine learning: The trade-off between performance and interpretability. *Future Generation Computer Systems*, 101, 993-1004. DOI: [10.1016/j.future.2019.07.059] (DOI: 10.1016/j.future.2019.07.059)

64. Jordan, M. I., & Mitchell, T. M. (2015). Machine learning: Trends, perspectives, and prospects. *Science*, 349(6245), 255-260. DOI: [10.1126/science.aaa8415] (DOI: 10.1126/science.aaa8415)
65. Brynjolfsson, E., & McAfee, A. (2017). The business of artificial intelligence: What it can–and cannot–do for your organization. *Harvard Business Review*, 95(6), 3-10.
66. Makridakis, S. (2017). The forthcoming artificial intelligence (AI) revolution: Its impact on society and firms. *Futures*, 90, 46-60. DOI: [10.1016/j.futures.2017.03.006](DOI: 10.1016/j.futures.2017.03.006)
67. Baryannis, G., Dani, S., & Antoniou, G. (2019). Predicting supply chain risks using machine learning: The trade-off between performance and interpretability. *Future Generation Computer Systems*, 101, 993-1004. DOI: [10.1016/j.future.2019.07.059]
68. Brynjolfsson, E., & McAfee, A. (2017). The business of artificial intelligence: What it can–and cannot–do for your organization. *Harvard Business Review*, 95(6), 3-10.
69. Jordan, M. I., & Mitchell, T. M. (2015). Machine learning: Trends, perspectives, and prospects. *Science*, 349(6245), 255-260. DOI: [10.1126/science.aaa8415]
70. Miller, T. (2019). Explanation in artificial intelligence: Insights from the social sciences. *Artificial Intelligence*, 267, 1-38. DOI: [10.1016/j.artint.2018.07.007]
71. AuditBoard: https://www.auditboard.com/blog/operational-risk-management/
72. Thomson Reuters: https://legal.thomsonreuters.com/blog/what-is-operational-risk-management/
73. ZenGRC: https://www.zengrc.com/blog/what-is-operational-risk-management/

8. Apendix B: Image Sources

- https://enriquemoralesorcajo.com/scientific-databases-which-one-should-you-use/ - Scientific databases – which one should you use
- https://www.alertmedia.com/blog/risk-management-lifecycle/ - Risk Management Lifecycle: 5 Steps to a Safer, More Resilient Organization
- https://www.linkedin.com/pulse/deep-learning-dl-vs-machine-ml-neural-networks-nn-examples-s-m-hhqic/ - Deep Learning (DL) vs Machine Learning (ML) & Neural Networks (NN) with examples
- https://www.leewayhertz.com/ai-in-risk-management/ - AI in risk management: Applications, benefits, solution and implementation
- https://www.leewayhertz.com/ai-in-risk-management/ - AI in risk management: Applications, benefits, solution and implementation
- https://community.trustcloud.ai/docs/grc-launchpad/grc-101/risk-management/risk-mitigation-strategies-the-role-of-artificial-intelligence-in-enhancements/ - Risk mitigation strategies: the role of artificial intelligence in enhancements
- https://www.westfordonline.com/blogs/financial-risk-management-strategies/ - Financial Risk Management: Strategies for Optimal Asset Protection
- https://www.ispartnersllc.com/blog/ai-risk-management/ - AI Risk Management
- https://www.markovml.com/blog/ethical-ai - Navigating Ethical AI: Challenges and Strategies Involved!