Educational Administration: Theory and Practice
2024, 30(4), 2130-2140
ISSN: 2148-2403
https://kuey.net/

Research Article

"Navigating Risk In The Age Of Artificial Intelligence: Assessing And Identifying Risks With AI Strategies"

Ravindra Sharma[1*], V. Harish[2], Geeta Rana[3]

[1*]Assistant Professor, Himalayan School of Management Studies, Swami Rama Himalayan University, Jolly Grant, Dehradun, India ravindrasharma@srhu.edu.in
[2]PSG Institute of Management PSG College of Technology. Coimbatore, India, harish@psgim.ac.in
[3]Associate Professor, Himalayan School of Management Studies, Swami Rama Himalayan University, Jolly Grant, Dehradun, India geetarana@srhu.edu.in

Citation: Ravindra Sharma At Al. (2024), "Navigating Risk In The Age Of Artificial Intelligence: Assessing And Identifying Risks With Ai Strategies", *Educational Administration: Theory And Practice*, *30*(4), 2130-2140
Doi:10.53555/kuey.v30i4.1824

ARTICLE INFO

ABSTRACT

As organizations increasingly adopt artificial intelligence (AI), the need for effective risk assessment and identification strategies becomes paramount and this paper explores the potential barriers and risks that come along with adoption of AI and emphasizes the criticality of management of risk connected with AI and the evolving landscape of AI is discussed, including its types and the potential risks it poses. The paper further highlights the need for AI risk management, particularly in the setting of Industry 6.0, where cutting-edge automation and interconnected systems prevail and have the potential to cause potential risky situations. The various risks involved in AI are outlined, emphasizing the significance of proactive risk identification and mitigation practices to ensure that these potential risks are mitigated in a better way and additionally, risk identification strategies specific to AI in Industry 6.0 are discussed, recognizing the complexities and vulnerabilities present in this domain. By understanding and effectively managing AI risks, organizations can navigate the age of AI with confidence and reap the rewards of this transformative technology.

Keywords: AI(AI), Risk assessment, Risk identification, AI risk management, Industry 6.0

1. Introduction:

In recent years, Artificial Intelligence (AI) has developed as a progressive force, restructuring the way of life both personal and professional and revolutionizing a variety of industries. The accelerated development of AI technologies has captured the world's attention, ushering innovation and promises (Lu et al. 2018). From “autonomous vehicles and virtual assistants to advanced data analytics and machine learning algorithms”, AI has become profoundly ingrained in our daily lives and businesses (Duan et al. 2019).
Several factors contribute to the exponential growth and advancements of AI. First, the accessibility of vast quantities of data and a robust computational infrastructure have enabled AI structures to learn and analyze information at an unparalleled scale and velocity. In addition, advancements in algorithmic techniques, such as deep learning, have enabled new capabilities, enabling AI models to extract complex patterns, make accurate predictions, and execute complex tasks with remarkable precision (Janiesch et al. 2021).

2. Literature Review:

AI has far-reaching and prevalent effects, transforming industries such as “healthcare, finance, manufacturing, and transportation” (Haluza & Jungwirth, 2023). AI algorithms analyze market data, identify anomalies, and fuel automated trading strategies in the financial sector (Cao, 2022). Automation propelled by AI is revolutionizing manufacturing processes, enhancing productivity, and enabling smart factories (Soukup, 2022). In addition, AI is improving transportation systems with autonomous vehicles, logistics operations, and traffic management.
AI continues to stretch the boundaries of what was once considered science fiction with each passing day. AI can bring about noteworthy societal aids, ranging from the improvement of healthcare outcomes and

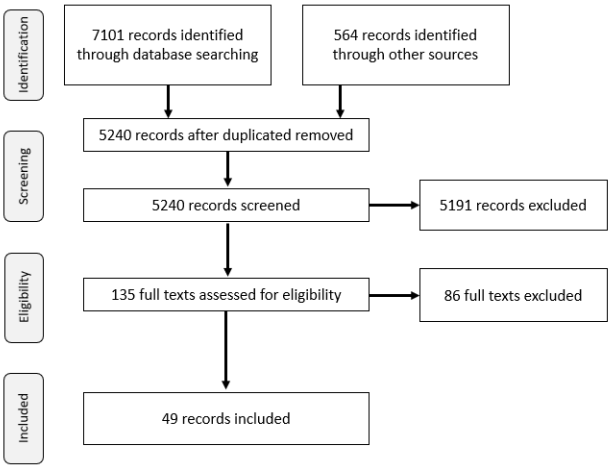
productivity to the resolution of complex global issues (Horgan et al. 2019). Nonetheless, as AI becomes more pervasive, it raises significant issues and hindrances, such as ethical implications, privacy apprehensions, and the possible impact on jobs (Stahl et al. 2023).
Individuals, Organizations, and policymakers must comprehend AI's implications, opportunities, and risks as its growth accelerates (Feijóo et al. 2020). Adopting AI technologies while addressing these concerns is vital for realizing AI's complete possible and maximizing its capabilities for the benefit of society. By nurturing responsible and ethical AI development, promoting transparency and accountability, and ensuring the equitable distribution of AI benefits, can lead to a transformative and inclusive AI-powered future (Bankins & Formosa, 2023).
In this article, we will examine the upsurge of AI and its impact on various facets of society, with a particular emphasis on its function in risk management and also explore how AI is revolutionizing risk assessment, detection, and mitigation processes, as well as the prospects and hindrances that arise with AI's incorporation into managing risk by comprehending the implications and leveraging the power of AI, we can navigate the evolving landscape of risk management and drive innovation in a world that is becoming increasingly complex and interconnected.
The accelerated development of AI(AI) technologies has resulted in revolutionary shifts in numerous industries, including risk management and AI offers new opportunities and capabilities that have had a substantial impact on how businesses identify, evaluate, and mitigate risks and this article deliberates the rise of AI and its profound influence on risk management practices, including its benefits, challenges, and considerations.

3. Objectives:

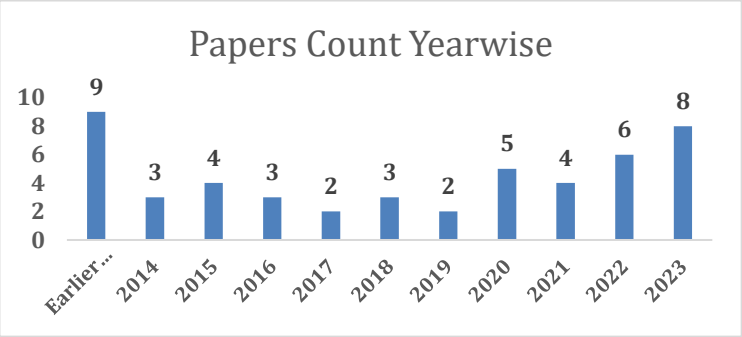
The objectives of the paper grounded on the literature review are as follows
1) Identify the probable risks of AI
2) Identify the need of AI Risk Management in the Industry 6.0 Scenario
3) Classify the various risks due to AI in Industry 6.0 and list the potential risks of AI in Industry 6.0 to various stakeholders
4) Identify various Risk Management strategies with respect to AI in Industry 6.0

4. Methodology:

PRISMA approach was undertaken to comprehend the analysis to perform the literature review and the steps included were as mentioned in the below given figure. Relevant papers were searched in major databases namely Scopus and the search string composed of using "AND" operator. As a first phase the keywords "Risk Management" and "AI" was searched in the title of the articles followed by a refined search in the “title, abstract and keywords”. Considering the scope of the paper was managing risk in the age of AI ,the string searches were done to understand the concept and some of the keywords used to generate the articles were "Artificial Intelligence, Risk management, Risk Mitigation, Risk Assessment, Risk Management Strategies, Ethical Risks, Cybersecurity Risks, Regulatory Compliance and Keywords related to AI were AI Governance, AI Ethics, AI Security, Algorithmic Transparency, AI Risk Factors, AI Decision-Making Risks" The various criteria that were considered for "inclusion and exclusion" are indicated in the above table and the papers. The researcher had adopted a snowballing approach where subsequent paper were identified using the references and citations in the paper identified and this resulted in identifying three additional articles that were not identified in the earlier search in the database.



Criteria	Description
Exclusion:	• Records not in English • While keywords are mentioned the paper not related to Risk management and AI
Inclusion:	• Article published in the database searched • Main content is related to risk management in AI • Management of risks in the era of AI is discussed



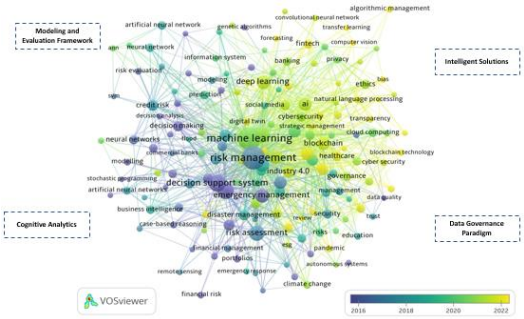


Fig No 1: Keyword Analysis of Risk management in AI era

The keyword analysis can be segregated into four major categories namely Cognitive analytics containing "Decision support system, Business intelligence, Artificial neural networks, Modelling, decision analysis", Data governance paradigm containing "Management, industry 4.0, security, risks, education ,data quality, cyber security, trust, review, esg" (Bécue et al. 2021), Intelligent Solutions containing "Machine learning, blockchain, block chain ,cyber security, AI, natural language processing, digital twin, deep learning, computer vision, transfer learning" and Modelling and evaluation framework containing "Prediction, credit risk, modeling, risk evaluation, information system generic algorithms" (Bag et al. 2021).
It also can be inferred that over the year's researchers have focused from cognitive analytics towards intelligent solutions and the emergence reasons could be due to the reasons of the recent technological advancements.

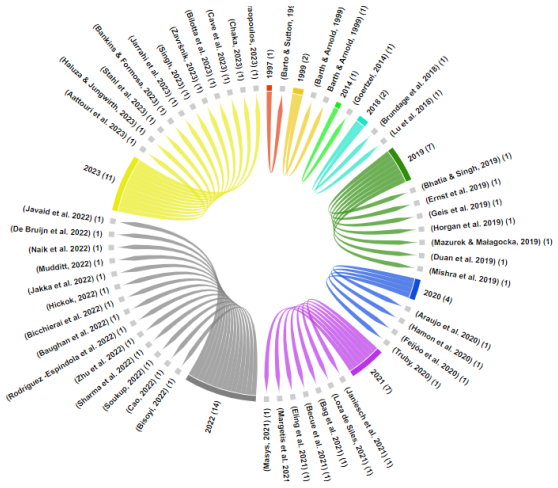


Fig No. 2 Literature analysis

Figure No 2 gives the list of papers that have been considered for the purpose of the study with the years and the author citations.

5. Objective 1: Identify the Potential Risks of AI

The possible risks of AI can be grouped into five main categories, each with several subcategories. These groups comprise a variety of issues and obstacles related to the growth and disposition of AI. Here are the five main categories of potential AI risks, along with their subcategories:

i. Ethical and Societal Risks:

"Bias and Discrimination": AI systems can disseminate biases prevalent in training data, resulting in discriminatory results. Biased algorithms can result in unfair treatment based on factors such as race, gender, or other features. Discrimination can occur in employment, lending, and the criminal justice system (Loza de Siles, 2021). "Privacy and Data Security:" The reliance of AI on massive quantities of data raises privacy and data protection concerns. Sensitive data can be compromised by unauthorized access, misuse, or improper management. The gathering, storage, and usage of personal information without consent increases apprehensions (Mazurek & Małagocka, 2019). "Social Disruption and Job Displacement": The prevalent acceptance of AI may result in substantial changes to the labor market and job displacement. Certain duties and roles may be automated, which could result in unemployment or skill gaps and if AI is not dispersed equitably, social and economic inequalities may grow (Bhatia & Singh, 2019). "Accountability and Responsibility:" It is difficult to determine liability and accountability when AI systems cause damage or make mistakes. Complex AI models that lack transparency and interpretability can make it difficult to designate responsibility. It is vital to safeguard suitable governance and regulations to address accountability issues related to AI (Geis et al. 2019).

ii. Safety and Security Risks:

"Malicious Use of AI": AI systems can be subjugated by malicious people to cyberattacks or generate convincingly false content (Bicchierai et al. 2022). Malware and AI-powered autonomous weapons pose significant security risks. Attacks powered by AI can be further automated, and problematic to notice and defend against (Brundage et al. 2018). "Lack of Robustness and Reliability:" AI systems may exhibit unanticipated behaviors or vulnerabilities, which may result in system malfunctions or accidents (Hamon et al. 2020). Inputs to AI systems can be manipulated by adversarial attacks to produce incorrect or detrimental outputs. The absence of transparency in AI models presents a challenge to detect and correct flaws. "Autonomous Decision-Making:" AI classifications with the skill to take choices can make mistakes or operate outside of intended parameters (Javaid et al. 2022). A lack of human oversight and control may result in unintended outcomes or ethical quandaries (Sharma et al. 2022). Achieving accountability in autonomous policymaking is crucial for the safe and accountable deployment of artificial intelligence.

iii. Economic Risks:

"Job Displacement and Inequality:" Widespread adoption of automation and AI may result in employment displacement and economic disparities. Certain industries or professions may be disproportionately impacted by task automation (Erns et al. 2019). Concentration of Power: Few potent entities can exert control over AI technologies, resulting in a concentration of economic power. Inequitable access to AI capabilities may lead to monopolistic or limited competitive behavior (Truby, 2020). It is essential for a thriving economy to ensure equal access and competition in the deployment of AI. "Economic Dependency and Disruption:" Dependence on AI systems can create economic vulnerabilities in the event that they malfunction or become unavailable. Disruption of vital AI-powered infrastructure or services can have significant economic repercussions (Barth & Arnold, 1999). Risks associated with economic reliance on AI systems must be mitigated with robust fallback plans and contingency measures.

iv. Legal and Regulatory Risks:

"Intellectual Property and Patent Issues:" AI systems can produce novel outputs, which raises concerns regarding ownership and patent rights. Attributing intellectual property rights to AI-generated creations and determining their legal status can be difficult. It may be necessary to update intellectual property laws to accommodate content and inventions generated by AI (Bisoyi, 2022). "Liability and Accountability:" Determining legal liability when AI cause damage or make mistakes is a challenging legal question. Existing laws may not adequately address AI-related issues, necessitating revisions and clarifications and it is crucial to create rules for responsibility and accountability in AI development (Završnik,2023). "Privacy and Data Protection:" The reliance of AI systems on extensive data collection and processing raises privacy concerns. Adherence to regulations, such as the "General Data Protection Regulation" (GDPR), becomes crucial for AI systems that handle personal data. It is essential to balance use data for AI advancements and protecting privacy rights (Mazurek & Małagocka, 2019). "Ethical and Regulatory Frameworks:" It is necessary to develop comprehensive ethical and regulatory frameworks for AI to address societal concerns. For AI systems to be

transparent, equitable, and accountable, robust regulatory measures are required. Governments and Organizations must collaborate to create rules and standards for the accountable use of AI (Zhu et al. 2022).

v. Human-Machine Collaboration Risks:
"Human Autonomy and Control:" An excessive reliance on AI systems can impair human decision-making and control. To guarantee productive collaboration, and balance created in roles of humans and AI. When AI systems exert influence or control over human decision-making, ethical considerations arise (Rodríguez - Espíndola et al. 2022). "Social and Psychological Impacts:" Individuals and society may experience psychological effects as a result of increased interaction with AI systems. Reduced human-to-human interaction and reliance on AI systems are issues that require careful consideration (Jarrahi et al. 2023). It is vital to evaluate and resolve the possible social and psychological effects of AI adoption. Human Bias and Decision-making: Human biases in training data or algorithm design can be reflected and amplified by AI systems. Social injustices and discrimination can be perpetuated by prejudice in decision-making. It is necessary to make efforts to mitigate biases in AI systems and assure transparency and fairness in decision-making processes (Loza de Siles, 2021).

To gain the benefits of AI while justifying potential risks and ethical use, proactive measures, including robust regulations, transparent AI development practices, and continuous evaluation, are required.

Objective 2: The Need of AI Risk Management in the Industry 6.0 Scenario
Industry 6.0, the era of advanced automation and interconnected systems, has introduced a fresh set of difficulties and complexities. As industries adopt cutting-edge technologies and employ AI solutions, robust risk management practices become essential (Bankins & Formosa, 2023). It is crucial for organizations to implement effective AI risk management strategies because AI itself presents both opportunities and threats (Hickok, 2022). The article discusses the importance of AI risk management in Industry 6.0 and how it can assist organizations in avoiding potential pitfalls and ensuring the safe and effective implementation of AI technologies (Singh, 2023).

(a). Enhanced Complicatedness and Vulnerabilities: Industry 6.0 is a paradigm transition categorized by the merging of cyber-physical systems, Internet of Things (IoT) devices, and AI-powered technologies. While these innovations bring about unprecedented productivity and efficiency (Jakka et al. 2022), they also introduce intricate interdependencies and risks (Mudditt, 2022). The interdependence of systems generates a ripple effect in which a single failure can propagate throughout the entire network. To identify and mitigate potential risks arising from system malfunctions, cyber threats, and data breaches, AI risk management becomes essential (Eling et al. 2021). By proactively resolving these vulnerabilities, organizations can protect vital infrastructure and forestall widespread disruption.

(b). Ethical and Regulatory Considerations AI can promote ethical apprehensions, including bias in decision-making, violations of privacy, and lack of transparency. In Industry 6.0, in which AI systems are profoundly integrated into a variety of processes, the significance of ethical AI risk management grows (Naik et al. 2022). Organizations must establish ethical guidelines and frameworks to assure the accountable application of AI. In addition, regulatory bodies are intensifying their scrutiny of AI applications, requiring compliance with data protection regulations, algorithmic accountability, and Explainability. By implementing AI risk management practices, organizations can proactively address ethical and regulatory considerations, thereby protecting their reputation and averting legal repercussions (Barto & Sutton, 1997).

(c). Operational Continuity and Resilience: Industry 6.0's reliance on AI systems necessitates an emphasis on operational resilience. Organizations are required to evaluate potential risks that could impede operations and to implement risk mitigation strategies (Bilotta et al. 2023). AI risk management enables the proactive identification of singular points of failure, AI algorithm vulnerabilities, and third-party system dependencies. By developing contingency plans, organizations can safeguard productivity and customer satisfaction by ensuring business continuity and minimizing the impact of disruptions.

(d). Trust and Transparency: The fruitful implementation of AI in Industry 6.0 is contingent on establishing trust among stakeholders. AI risk management fosters confidence and openness. Organizations must safeguard that AI systems operate in a fair manner and that their decisions are adequately explained (Cave et al. 2023). By adopting explainable AI algorithms and undertaking comprehensive risk assessments, organizations can increase transparency, instill confidence in AI-driven processes, and earn the trust of stakeholders (Mishra et al. 2019).
Industry 6.0 emphasizes the partnership amid humans and AI systems and effective risk monitoring requires the incorporation of human knowledge and AI capabilities. Organizations must assess the hazards associated with human-AI interaction, including challenges associated with accountability, responsibility, and authority to make decisions (Chaka, 2023). Frameworks for AI risk management can assist organizations in defining

distinct roles, establishing guidelines for human oversight, and addressing potential problems that may arise from human-AI collaboration (Margetis et al. 2021).
AI risk management emerges as a crucial discipline in Industry 6.0 to safeguard the safe and successful implementation of AI (De Bruijn et al. 2022) can confidently navigate the Industry 6.0 landscape if they proactively address complexities, vulnerabilities, ethical concerns, and operational disruptions and effective AI risk management practices foster confidence, facilitate operational resilience, and align with regulatory requirements and as industries continue to embrace the potential of Industry 6.0, a robust AI risk management strategy becomes an essential element of their strategic planning (Masys, 2021).

Objective 3: Risks due to AI and potential risks of AI in Industry 6.0 to various stakeholders

As industries continue to progress towards Industry 6.0, which is characterized by the widespread adoption of AI(AI) and other advanced technologies, a number of risk-related considerations must be made. In this article, we will examine the significant hazards related to AI in Industry 6.0 (Barto & Sutton, 1997).

i. Data Security and Privacy Risks

The possiblity for data intrusions, privacy violations, and other security-related issues is one of the most significant dangers associated with AI in Industry 6.0 and AI systems generate and process enormous quantities of data, which increases the likelihood of cyberattacks, hacking, and data theft (Mazurek & Małagocka, 2019) and this risk is exacerbated by AI algorithms, making it challenging to identify and mitigate security vulnerabilities.

ii. Bias and Discrimination Risks

The probability for bias is additional significant risk associated with AI in Industry 6.0 and AI is effective based on the training data, and if biased data is used, result can be compromised (Loza de Siles, 2021) and this can result in discrimination against minority groups, women, and people with disabilities and to alleviate this risk, correct data is to be used (Aattouri et al. 2023).

ii. Job Displacement Risks

The extensive acceptance of AI in Industry 6.0 is also likely to result in employment displacement, as many previously human-performed tasks are now automatable (Araujo et al. 2020) and this can result in increased productivity and efficiency, but also job losses and economic disruption and to mitigate this risk, it is vital to capitalize in education that facilitate the transition of employees into new roles and industries (Erns et al. 2019).

iii. Legal and Ethical Risks

Additionally, the usage of AI in Industry 6.0 poses a number of legal and ethical hazards and concerns (Lampraopoulos, 2023) exist, which has the likelyness to violate the privacy rights and concerns exist regarding the use of AI for taking decisions, such as in the criminal justice system, where there is a risk of bias and discrimination (Završnik, 2023) and to combat these risks, it is crucial to have in place defined legal frameworks and ethical guidelines.

iv. Reliability and Accountability Risks

Lastly, there is the possibility that AI systems in Industry 6.0 may not always be trustworthy or accountable because AI algorithms can be opaque and complex (Haluza & Jungwirth, 2023), it can be difficult to comprehend how decisions are made or to determine when something has gone awry and this can result in a lack of accountability, making it challenging to hold individuals or Organizations accountable for errors or misconduct and in order to mitigate this risk, it is indispensable to implement AI that are clear and explicable, and to establish clear lines of accountability (Hamon et al. 2020).
The pervasive adoption of AI in Industry 6.0 raises a number of risk-related concerns that must be considered and this includes data security and privacy, prejudice and discrimination, job displacement, legal and ethical concerns, and dependability and accountability and mitigate risks, it is essential to have transparent and explicable AI systems and explicit legal frameworks and investing in education to assist employees in their transition to new roles and industries is also crucial.

Table 1: Identified Risks of AI in Industry 6.0

Risk	How to Identify	Sub-Points
Data Security and Privacy Risks	Conduct regular security assessments and audits	1. Identifying critical data assets 2.Classifying potential hazards to the assets identified. 3.Forming a security plan to mitigate vulnerabilities 4.Implementing security controls 5. Monitoring and updating the security plan and controls.
Bias and Discrimination Risks	Conduct regular bias assessments and audits	1. Investigating the training data sources 2. Recognizing potential biases in the data sources 3. Evaluating the AI system's bias 4.Fine-tuning the AI system to mitigate any biases

		5. Monitoring the AI system for fairness and accuracy.
Job Displacement Risks	Conduct workforce analysis and forecasting	1. Defining duties that are the most likely to be automated. 2. Analyzing the workforce's abilities. 3. Identifying prospective new roles 4. Developing education and training Programmes 5. Monitoring the efficacy of the training
Legal and Ethical Risks	Conduct regular legal and ethical reviews	1. Examining the legal and ethical implications. 2. Identifying violations of privacy or discrimination. 3. Preparing guidelines and policies to mitigate these risks and training employees 4. Reviewing the policies and guidelines on a regular basis.
Reliability and Accountability Risks	Conduct regular performance and accountability reviews	1. Monitoring the system's performance to identify any errors or issues. 2.Developing procedures for addressing and resolving these blunders and problems. 3. Establishing distinct lines of responsibility for the AI system, including who is accountable for monitoring its performance and resolving problems. 4. Developing procedures for monitoring and documenting. 5. Reviewing and updating as necessary the performance and accountability processes on a regular basis.

Table 2: Risks of AI in Industry 6.0 to various stakeholders:

S.No.	Stakeholder	Category of Risk	Description
1	Employees	Job Displacement Risks	The automation of tasks by AI will displace of human labourers.
2	Customers	Bias and Discrimination Risks	The training of AI systems with Biased or discriminatory data may result in unequal treatment of customers.
3	Shareholders	Legal and Ethical Risks	Legal and ethical violations caused by AI systems may result in monetary losses and reputational harm for corporations and their shareholders.
4	Society	Bias and Discrimination Risks	AI systems that are Biased may perpetuate inequalities and discrimination in society.
5	Society	Data Security and Privacy Risks	AI may effect in the collection and use of personally identifiable information or without consent of individuals, posing potential security and privacy risks
6	Society	Reliability and Accountability Risks	Concerns regarding accountability and responsibility may arise if AI systems make decisions that are challenging to comprehend or challenge.

Objective 4: Risk Management strategies with respect to AI in Industry 6.0:

A detailed literature review of the analysis provided the following risk management strategies and insights as given below

Table 3: Risk Mitigation strategies identified risks of AI in Industry 6.0

Risk	Risk Management Strategy	Risk Mitigation Strategies
Data Security and Privacy Risks	Avoidance	· Use alternative data storage and transmission methods
		Develop new security protocols and policies
		Limit access to sensitive data
	Transfer	Outsource data security to a third-party vendor
Bias and Discrimination Risks	Avoidance	Utilize alternative data sources or diverse data sets
		Analyze the data to detect and remove bias
		Develop new machine learning algorithms or models
	Mitigate	Implement fairness, transparency, and accountability techniques
		Monitor the AI system for bias and discrimination
Job Displacement Risks	Avoidance	Develop and implement training and re-skilling programs for employees
		Utilize alternative technologies or approaches
		Develop new job roles for employees
	Mitigate	Implement job sharing or flexible work arrangements
		Provide severance packages or retirement options for affected employees
Legal and Ethical Risks	Avoidance	Develop and implement policies and guidelines for ethical AI development and use
		Conduct regular legal and ethical reviews
		Develop new contracts or agreements with vendors
	Mitigate	· Implement regular compliance and auditing processes
		· Provide training and education for employees on legal and ethical issues
Reliability and Accountability Risks	Avoidance	· Develop and implement quality control processes for the AI system
		Develop backup plans and redundancies
		Develop processes for tracking and documenting decisions made by the AI system
	Mitigate	Implement error reporting and resolution processes
		Develop processes for system updates and maintenance
General Risks	Accept	Accept that the risk may occur and prepare a contingency plan to minimize the impact

	Exploit	Take advantage of potential positive outcomes of the risk
		Optimize the AI system to gain competitive advantage
	Enhance	Develop strategies to increase the likelihood of positive outcomes
		Invest in R & D to improve the AI
	Share	Share the risk with stakeholders, partners, or customers to minimize the impact

5. Conclusion:

As the use of AI(AI) continues to expand across a variety of industries, it is vital tool for effective risk assessment and identification strategies. With vast quantities of data and autonomous decisions, AI brings numerous benefits, but also introduces new risks and challenges. Throughout this article, we have examined the potential risks and the difficulties in assessing and identifying those risks and as organizations strive to capitalize on the goodness of AI while minimizing negative effects, AI risk management has become increasingly important. An effective AI risk management strategy should include key components such as understanding the nature of AI and its associated risks, establishing a risk identification framework customized for AI applications in specific industries such as Industry 6.0, and involving relevant stakeholders to ensure a holistic perspective and the identified risks should include potential hazards such as cyber-attacks, breaches of privacy, biased decision making, and ethical considerations among the most essential ethical implications are fairness, transparency, and accountability and incorporating these factors into the risk identification and efficacy of the risk identification process and it is essential to continuously monitor and update the risk identification framework to accommodate the changing nature of AI applications and the threat landscape.
Ultimately, it is essential to effectively communicate the identified risks and risk identification strategies to the appropriate stakeholders. In Industry 6.0, fostering a culture of risk awareness and mitigation fosters collaboration, trust, and accountable AI practices. In conclusion, Organizations can gain the gains of AI while proactively managing and minimizing its associated risks by implementing robust risk assessment and identification strategies unique to AI. This not only protects against potential injury, but also ensures the ethical and responsible deployment of AI in Industry 6.0 and beyond.

References:

1. Aattouri, I., Mouncif, H., & Rida, M. (2023). Modeling of an AI based enterprise callbot with natural language processing and machine learning algorithms. *IAES International Journal of Artificial Intelligence*, *12*(2), 943.
2. Araujo, T., Helberger, N., Kruikemeier, S., & De Vreese, C. H. (2020). In AI we trust? Perceptions about automated decision-making by artificial intelligence. *AI & society*, *35*, 611-623.
3. Argyroudis, S. A., Mitoulis, S. A., Chatzi, E., Baker, J. W., Brilakis, I., Gkoumas, K., ... & Linkov, I. (2022). Digital technologies can enhance climate resilience of critical infrastructure. *Climate Risk Management*, *35*, 100387.
4. Atakishiyev, S., Salameh, M., Yao, H., & Goebel, R. (2021). Explainable AIfor autonomous driving: a comprehensive overview and field guide for future research directions. arXiv preprint arXiv:2112.11561.
5. Ayling, J., & Chapman, A. (2022). Putting AI ethics to work: are the tools fit for purpose?. *AI and Ethics*, *2*(3), 405-429.
6. Bag, S., Gupta, S., Kumar, A., & Sivarajah, U. (2021). An integrated AI framework for knowledge creation and B2B marketing rational decision making for improving firm performance. *Industrial Marketing Management*, *92*, 178-189.
7. Bankins, S., & Formosa, P. (2023). The ethical implications of AI(AI) for meaningful work. *Journal of Business Ethics*, 1-16.
8. Barth, T. J., & Arnold, E. (1999). AIand administrative discretion: Implications for public administration. *The American Review of Public Administration*, *29*(4), 332-351.
9. Barto, A. G., & Sutton, R. S. (1997). Reinforcement learning in artificial intelligence. In *Advances in Psychology* (Vol. 121, pp. 358-386). North-Holland.
10. Batin, M., Turchin, A., Sergey, M., Zhila, A., & Denkenberger, D. (2017). AIin life extension: from deep learning to superintelligence. *Informatica*, *41*(4).
11. Bécue, A., Praça, I., & Gama, J. (2021). Artificial intelligence, cyber-threats and Industry 4.0: Challenges and opportunities. *AIReview*, *54*(5), 3849-3886.
12. Bhatia, S., & Singh, A. K. (2019). Developments in AIa global perspective. *Delhi Business Review*, *20*(1), 1-15.
13. Bicchierai, I., Schiavone, E., & Brancati, F. (2022, July). Modelling and Assessing the Risk of Cascading Effects with ResilBlockly. In *2022 IEEE International Conference on Cyber Security and Resilience (CSR)* (pp. 261-266). IEEE.
14. Bilotta, G., Cappello, A., & Ganci, G. (2023). Formal Matters on the Topic of Risk Mitigation: A Mathematical Perspective. *Applied Sciences*, *13*(1), 265.

15. Bisoyi, A. (2022). Ownership, liability, patentability, and creativity issues in artificial intelligence. *Information Security Journal: A Global Perspective*, *31*(4), 377-386.
16. Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., ... & Amodei, D. (2018). The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. *arXiv preprint arXiv:1802.07228*.
17. Cao, L. (2022). Ai in finance: challenges, techniques, and opportunities. *ACM Computing Surveys (CSUR)*, *55*(3), 1-38.
18. Castañé, G., Dolgui, A., Kousi, N., Meyers, B., Thevenin, S., Vyhmeister, E., & Östberg, P. O. (2023). The ASSISTANT project: AI for high level decisions in manufacturing. *International Journal of Production Research*, *61*(7), 2288-2306.
19. Cave, S., Dihal, K., Hollanek, T., Katsuno, H., Liu, Y., Taillandier, A., & White, D. (2023). The Meanings of AI A Cross-Cultural Comparison. *Imagining AI: How the World Sees Intelligent Machines*, 16.
20. Chaka, C. (2023). Fourth industrial revolution—a review of applications, prospects, and challenges for artificial intelligence, robotics and blockchain in higher education. *Research and Practice in Technology Enhanced Learning*, *18*.
21. De Bruijn, H., Warnier, M., & Janssen, M. (2022). The perils and pitfalls of explainable AI: Strategies for explaining algorithmic decision-making. *Government Information Quarterly*, *39*(2), 101666.
22. Duan, Y., Edwards, J. S., & Dwivedi, Y. K. (2019). AI for decision making in the era of Big Data–evolution, challenges and research agenda. *International journal of information management*, *48*, 63-71.
23. Eling, M., Nuessle, D., & Staubli, J. (2021). The impact of AI along the insurance value chain and on the insurability of risks. *The Geneva Papers on Risk and Insurance-Issues and Practice*, 1-37.
24. Ernst, E., Merola, R., & Samaan, D. (2019). Economics of artificial intelligence: Implications for the future of work. *IZA Journal of Labor Policy*, *9*(1).
25. Feijóo, C., Kwon, Y., Bauer, J. M., Bohlin, E., Howell, B., Jain, R., ... & Xia, J. (2020). Harnessing AI(AI) to increase wellbeing for all: The case for a new technology diplomacy. *Telecommunications Policy*, *44*(6), 101988.
26. Geis, J. R., Brady, A. P., Wu, C. C., Spencer, J., Ranschaert, E., Jaremko, J. L., ... & Kohli, M. (2019). Ethics of AIin radiology: summary of the joint European and North American multisociety statement. *Canadian Association of Radiologists Journal*, *70*(4), 329-334.
27. Glikson, E., & Woolley, A. W. (2020). Human trust in artificial intelligence: Review of empirical research. *Academy of Management Annals*, *14*(2), 627-660.
28. Goertzel, B. (2014). Artificial general intelligence: concept, state of the art, and future prospects. *Journal of Artificial General Intelligence*, *5*(1), 1.
29. Haluza, D., & Jungwirth, D. (2023). AIand Ten Societal Megatrends: An Exploratory Study Using GPT-3. *Systems*, *11*(3), 120.
30. Hamjen, H., Rumata, V. M., & Damanik, M. P. (2023). The Trading Robot Regulatory Naratives: AI Implications in Indonesia. In *Handbook of Research on AIand Knowledge Management in Asia's Digital Economy* (pp. 81-96). IGI Global.
31. Hamon, R., Junklewitz, H., & Sanchez, I. (2020). Robustness and explainability of artificial intelligence. *Publications Office of the European Union*, *207*.
32. Hickok, M. (2022). Public procurement of AI systems: new risks and future proofing. *AI & society*, 1-15.
33. Horgan, D., Romao, M., Morré, S. A., & Kalra, D. (2019). Artificial intelligence: power for civilisation–and for better healthcare. *Public health genomics*, *22*(5-6), 145-161.
34. Jakka, G., Yathiraju, N., & Ansari, M. F. (2022). AI in Terms of Spotting Malware and Delivering Cyber Risk Management. *Journal of Positive School Psychology*, *6*(3), 6156-6165.
35. Janiesch, C., Zschech, P., & Heinrich, K. (2021). Machine learning and deep learning. *Electronic Markets*, *31*(3), 685-695.
36. Jarrahi, M. H., Askay, D., Eshraghi, A., & Smith, P. (2023). AIand knowledge management: A partnership between human and AI. *Business Horizons*, *66*(1), 87-99.
37. Javaid, M., Haleem, A., Singh, R. P., & Suman, R. (2022). AI applications for industry 4.0: A literature-based study. *Journal of Industrial Integration and Management*, *7*(01), 83-111.
38. Kallini, J. R., & Moriarty, J. M. (2022, June). AIin Interventional Radiology. In *Seminars in Interventional Radiology* (Vol. 39, No. 03, pp. 341-347). Thieme Medical Publishers, Inc..
39. King, M. R. (2023). The future of AI in medicine: a perspective from a Chatbot. *Annals of Biomedical Engineering*, *51*(2), 291-295.
40. Khan, H. U., Malik, M. Z., Alomari, M. K. B., Khan, S., Al-Maadid, A. A. S., Hassan, M. K., & Khan, K. (2022). Transforming the Capabilities of AIin GCC Financial Sector: A Systematic Literature Review. *Wireless Communications and Mobile Computing*, *2022*.
41. Kobilov, A. U. (2023). Development of Artificial Intelligence:Characteristics of research Directions. Экономика и социум, (2 (105)), 152-156.
42. Kochura, Y., Gordienko, Y., Taran, V., Gordienko, N., Rokovyi, A., Alienin, O., & Stirenko, S. (2020). Batch size influence on performance of graphic and tensor processing units during training and inference phases. In *Advances in Computer Science for Engineering and Education II* (pp. 658-668). Springer International Publishing.

43. Lampropoulos, G. (2023). Artificial Intelligence, Big Data, and Machine Learning in Industry 4.0. In *Encyclopedia of Data Science and Machine Learning* (pp. 2101-2109). IGI Global.
44. Li, T., Chang, X., Wu, Z., Li, J., Shao, G., Deng, X., ... & Wang, J. (2017). Autonomous collision-free navigation of microvehicles in complex and dynamically changing environments. *Acs Nano*, *11*(9), 9268-9275.
45. Loza de Siles, E. (2021). AIBias and Discrimination: Will We Pull the Arc of the Moral Universe Towards Justice?. *J. Int'l & Comp. L.*, *8*, 513.
46. Lu, H., Li, Y., Chen, M., Kim, H., & Serikawa, S. (2018). Brain intelligence: go beyond artificial intelligence. *Mobile Networks and Applications*, *23*, 368-375.
47. Manab, N., & Aziz, N. A. A. L. (2019). Integrating knowledge management in sustainability risk management practices for company survival. *Management Science Letters*, *9*(4), 585-594.
48. Margetis, G., Ntoa, S., Antona, M., & Stephanidis, C. (2021). Human-centered design of artificial intelligence. *Handbook of human factors and ergonomics*, 1085-1106.
49. Masys, A. J. (2021). The security landscape—Systemic risks shaping non-traditional security. In *Sensemaking for Security* (pp. 1-14). Cham: Springer International Publishing.
50. Mazurek, G., & Małagocka, K. (2019). Perception of privacy and data protection in the context of the development of artificial intelligence. *Journal of Management Analytics*, *6*(4), 344-364.
51. Mishra, B. K., Rolland, E., Satpathy, A., & Moore, M. (2019). A framework for enterprise risk identification and management: the resource-based view. *Managerial Auditing Journal*.
52. Mudditt, J. (2022). Policing the risk landscape. *Company Director*, *38*(2), 58-59.
53. Naik, B., Mehta, A., Yagnik, H., & Shah, M. (2022). The impacts of AI techniques in augmentation of cybersecurity: a comprehensive review. *Complex & Intelligent Systems*, *8*(2), 1763-1780.
54. Oguntola, I. O., & Ülkü, M. A. (2023). AI for Sustainable Humanitarian Logistics. *Encyclopedia of Data Science and Machine Learning*, 2970-2983.
55. Pagèsa, G. (2023). Introduction to Part V Machine Learning and Applied Mathematics: a Game of Hide-and-Seek?. *Machine Learning and Data Sciences for Financial Markets: A Guide to Contemporary Practices*, 343.
56. Peres, R. S., Jia, X., Lee, J., Sun, K., Colombo, A. W., & Barata, J. (2020). Industrial AIin industry 4.0-systematic review, challenges and outlook. *IEEE Access*, *8*, 220121-220139.
57. Rodríguez-Espíndola, O., Chowdhury, S., Dey, P. K., Albores, P., & Emrouznejad, A. (2022). Analysis of the adoption of emergent technologies for risk management in the era of digital manufacturing. *Technological Forecasting and Social Change*, *178*, 121562.
58. Sadiku, M. N., Ajayi-Majebi, A. J., & Adebo, P. O. (2023). AIin Manufacturing. In *Emerging Technologies in Manufacturing* (pp. 13-32). Cham: Springer International Publishing.
59. Saeidi, P., Saeidi, S. P., Sofian, S., Saeidi, S. P., Nilashi, M., & Mardani, A. (2019). The impact of enterprise risk management on competitive advantage by moderating role of information technology. *Computer standards & interfaces*, *63*, 67-82.
60. Saravi, B., Hassel, F., Ülkümen, S., Zink, A., Shavlokhova, V., Couillard-Despres, S., ... & Lang, G. M. (2022). Artificial intelligence-driven prediction modeling and decision making in spine surgery using hybrid machine learning models. *Journal of Personalized Medicine*, *12*(4), 509.
61. Schwalbe, N., & Wahl, B. (2020). AIand the future of global health. *The Lancet*, *395*(10236), 1579-1586.
62. Sharma, S., Islam, N., Singh, G., & Dhir, A. (2022). Why Do Retail Customers Adopt AI(AI) Based Autonomous Decision-Making Systems?. *IEEE Transactions on Engineering Management*.
63. Singh, K. (2023). Evaluation Planning for Artificial Intelligence-based Industry 6.0 Metaverse Integration. *Intelligent Human Systems Integration (IHSI 2023): Integrating People and Intelligent Systems*, *69*(69).
64. Smith, P. G., & Merritt, G. M. (2020). *Proactive risk management: Controlling uncertainty in product development*. CRC Press.
65. Soukup, V. (2022). Industry 4.0: From Smart Factories to Artificial Intelligence. In *Industry 4.0 Challenges in Smart Cities* (pp. 95-105). Cham: Springer International Publishing.
66. Stahl, B. C., Antoniou, J., Bhalla, N., Brooks, L., Jansen, P., Lindqvist, B., ... & Wright, D. (2023). A systematic review of AIimpact assessments. *AIReview*, 1-33.
67. Suwarno, I., Cakan, A., Raharja, N. M., Baballe, M. A., & Mahmoud, M. S. (2023). Current trend in control of AIfor health robotic manipulator. *Journal of Soft Computing Exploration*, *4*(1).
68. Tarafdar, M., Beath, C. M., & Ross, J. W. (2019). Using AI to enhance business operations. *MIT Sloan Management Review*, *60*(4).
69. Todorova, M. (2020). " Narrow AI" in the Context of AI Implementation, Transformation and the End of Some Jobs. *Nauchni trudove*, (4), 15-25.
70. Truby, J. (2020). Governing AIto benefit the UN sustainable development goals. *Sustainable Development*, *28*(4), 946-959.
71. Umamaheswari, S., & Valarmathi, A. (2023). Role of AIin The Banking Sector. *Journal of Survey in Fisheries Sciences*, *10*(4S), 2841-2849.
72. Vilone, G., & Longo, L. (2021). Notions of explainability and evaluation approaches for explainable artificial intelligence. *Information Fusion*, *76*, 89-106.

73. Wartman, S. A., & Combs, C. D. (2018). Medical education must move from the information age to the age of artificial intelligence. *Academic Medicine*, *93*(8), 1107-1109.
74. Wilson, R. S., Zwickle, A., & Walpole, H. (2019). Developing a broadly applicable measure of risk perception. *Risk Analysis*, *39*(4), 777-791.
75. Woods, M. (2022). *Risk management in organisations: An integrated case study approach*. Routledge.
76. Yu, X., Xu, S., & Ashton, M. (2023). Antecedents and outcomes of AIadoption and application in the workplace: The socio-technical system theory perspective. *Information Technology & People*, *36*(1), 454-474.
77. Završnik, A. (2023). In Defence of Ethics and the Law in AI Governance: The Case of Computer Vision. In *Artificial Intelligence, Social Harms and Human Rights* (pp. 101-139). Cham: Springer International Publishing.
78. Zhu, L., Xu, X., Lu, Q., Governatori, G., & Whittle, J. (2022). AI and ethics—Operationalizing responsible AI. *Humanity Driven AI: Productivity, Well-being, Sustainability and Partnership*, 15-33.