KPMG

Artificial intelligence:

An enabler or a double-edged sword?

Board Leadership Center (India)

What once was a sci-fi fiction shown in movies, has now become today's reality - AI is gradually taking over. Albeit, it is not as apocalyptic as many had imagined it would be. It is rather a powerful tool which can help unlock a world of possibilities when leveraged in the right manner. From improving customer experiences to optimising operations, AI and Machine Learning (ML) have capabilities to revolutionalise the way companies operate and make decisions, while driving innovation and efficiency.

Companies are leveraging these technologies for data analysis, predictive modeling, automation, and intelligent decision-making. AI-powered algorithms can sift through vast amounts of data, uncover patterns and insights, and enable informed business decisions. ML models are being used for personalised marketing, recommendation systems, fraud detection, supply chain optimisation, and more. By harnessing the power of AI and ML, businesses are gaining a competitive edge and driving growth.

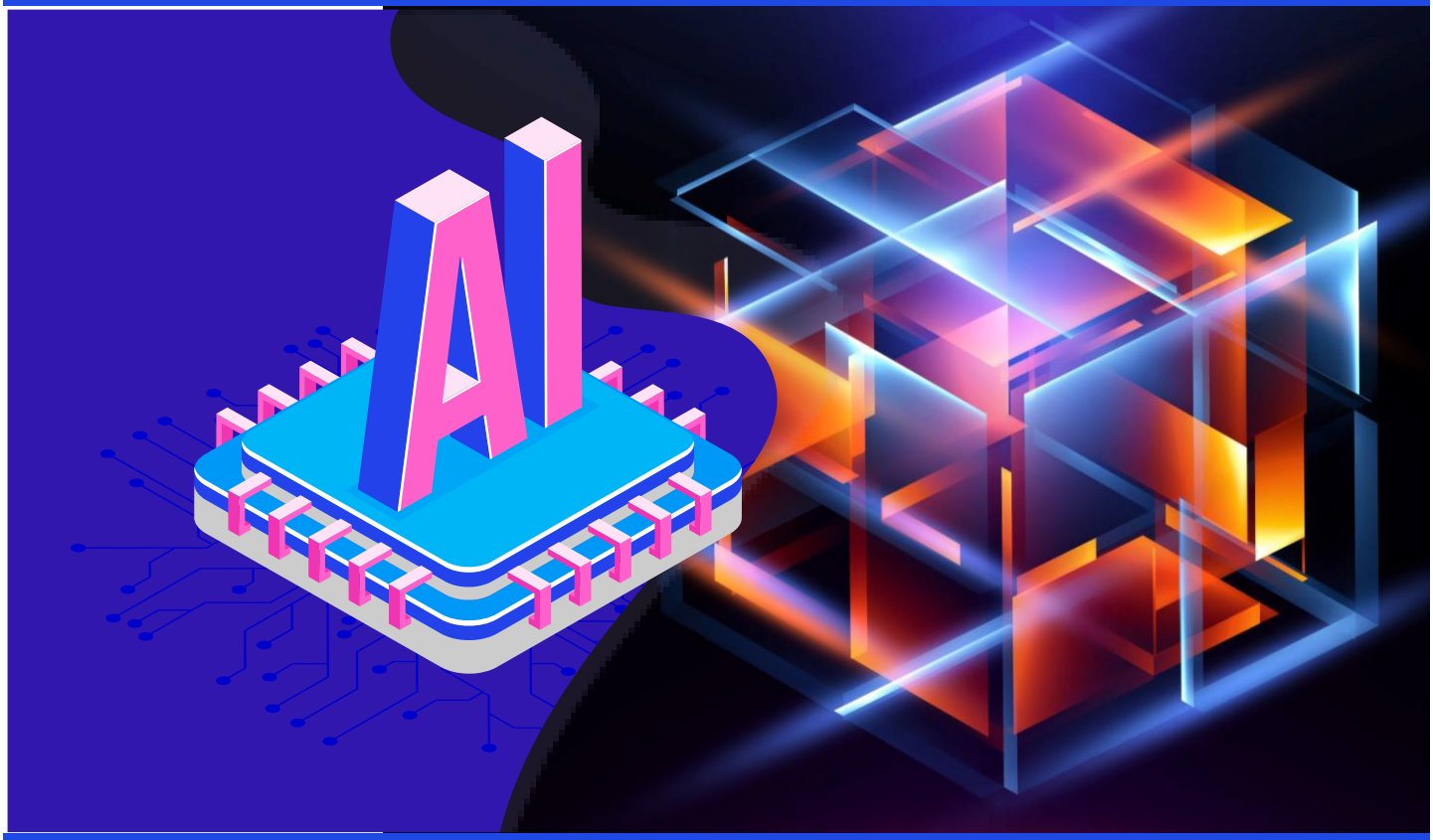
But like any other opportunity, AI has its own risks which need to be effectively managed to go beyond the boundaries of limitations. Companies can face a barrage of AI-related risks in the form of algorithmic biases affecting critical decisions (hiring, loan credit decisions, etc.); cyber threats; issues around false information; deepfakes; etc. In light of these risks, many companies and even some countries have started taking an extremely conscious approach towards AI. Countries such as Italy have expressed concerns that generative AI technology can have severe implications and might possibly violate the European Union's General Data Protection Regulations (GDPR). EU as a whole has prepared an Artificial Intelligence Act which might soon become law and could set a precedent for future risk-based regulatory approaches, as it would rank AI systems according to their risk levels and ban or regulate AI systems based on those risk levels. The US has also developed a Blueprint for an AI Bill of Rights. While India is yet to release any official guidelines in this area, companies will have to keep a close eye on evolving AI legislations/regulations and complying with them. Keeping the legal, regulatory and reputational risks in mind, companies will have to take a more rigorous approach to AI governance and aim for "ethical" or "responsible" AI that aims at making AI systems transparent, fair, secure, and inclusive. As organisations increase its adoption, it becomes essential for the board of directors as well to understand the risks associated with AI systems and to navigate them.

Risks associated with AI

While AI and ML offer tremendous benefits, they also introduce unique risks that need to be addressed.

Companies need to proactively identify and mitigate these risks through various measures:

Risk	Problem	Suggested Measures:
Data privacy and security	Evolving technology and AI pose threat to the security of customer data and other sensitive information	By employing privacy by design principles, companies can maintain customer trust and safeguard sensitive information
Algorithmic bias	AI algorithms can lead to discriminatory outcomes, perpetuating societal inequalities	Regular auditing and testing of algorithms can help rectify biases and ensure transparency and fairness
Transparency	The 'black box' nature of AI has raised concerns regarding its decision-making processes	Companies should focus on developing explainable AI models that can provide insights into how decisions are reached
Ethical frameworks and guidelines	Establishing ethical frameworks and guidelines that govern the development and use of AI systems	By adhering to ethical guidelines, companies can ensure that AI is deployed in a manner consistent with social and moral values
Continuous monitoring and auditing	Monitoring the skillset and auditing of AI systems to detect and rectify any anomalies or risks	Continuous monitoring of models will help in identify emerging risks and ensures compliance with regulatory requirement.



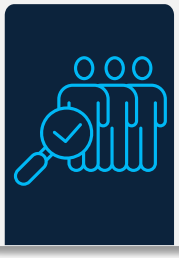
Best practices for boards to ensure ethical and responsible AI

Securing AI pipelines against adverse threats is a critical responsibility for corporate leaders and board members. By conducting comprehensive risk assessments, implementing strong data security measures, guarding against adversarial attacks, ensuring ethical data use, training employees, implementing continuous monitoring and auditing, and engaging external security experts, organisations can effectively protect their AI pipelines.

1

Conduct comprehensive risk assessment: Begin by conducting a thorough risk assessment specific to AI pipelines. Identify potential vulnerabilities, including data breaches, unauthorised access, and insider threats. Assess the potential impact of these risks on the organisation's operations, reputation, and compliance obligations. This assessment will serve as the foundation for developing a robust security strategy.

2



Establish and implement AI risk management framework: Given the critical importance of AI risk management, boards should have their management teams assess whether the AI Framework can provide helpful guidance in building or enhancing the company's AI risk management structure and processes. There are now a number of frameworks available to guide companies on this area including National Institute of Standards and Technology (NIST)'s Risk Management framework, BSA framework, GAO framework, etc.

3

Implement strong data security measures: Data is the lifeblood of AI pipelines, and securing it is crucial. Start by implementing strict access controls to ensure that only authorised personnel can access sensitive data. Encrypt data at rest and in transit to protect it from unauthorised interception. Regularly update and patch software and systems to address potential vulnerabilities. Establish secure data storage practices, including regular backups and disaster recovery plans.

4

Guard against adversarial attacks: Adversarial attacks aim to deceive or manipulate AI systems by introducing malicious inputs or exploiting vulnerabilities. Implement defence mechanisms, such as robust input validation, anomaly detection, and outlier rejection, to detect and mitigate adversarial attacks. Regularly monitor and analyse system behaviour to identify and respond to potential anomalies.

5

Train and educate employees: Human error and insider threats can pose significant risks to AI pipelines. Train employees on security best practices, emphasising the importance of data protection, secure coding, and adherence to security policies. Conduct regular awareness programmes to keep employees informed about emerging threats and security protocols. Foster a culture of vigilance and encourage reporting of potential security incidents promptly.

6

Engage external security experts: Consider engaging external security experts to conduct penetration testing and security audits. Independent assessments can provide valuable insights into potential vulnerabilities and recommend targeted mitigation strategies. External experts can also help organisations stay updated on the latest security practices and emerging threats, enabling proactive security measures.

Eight core governing principles to guide responsible AI

1. Fairness
Ensure models are free from bias and equitable.

2. Explainability
Ensure AI can be understood, documented, and open for review

3. Accountability
Ensure mechanisms are in place to drive responsibility across the lifecycle.

4. Security
Safeguard against unauthorised access, corruption, or attacks

5. Privacy
Ensure compliance with data privacy regulations and consumer data usage.

6. Safety
Ensure AI does not negatively impact humans, property, and environment.

7. Data integrity
Ensure data quality, governance, and enrichment steps embed trust.

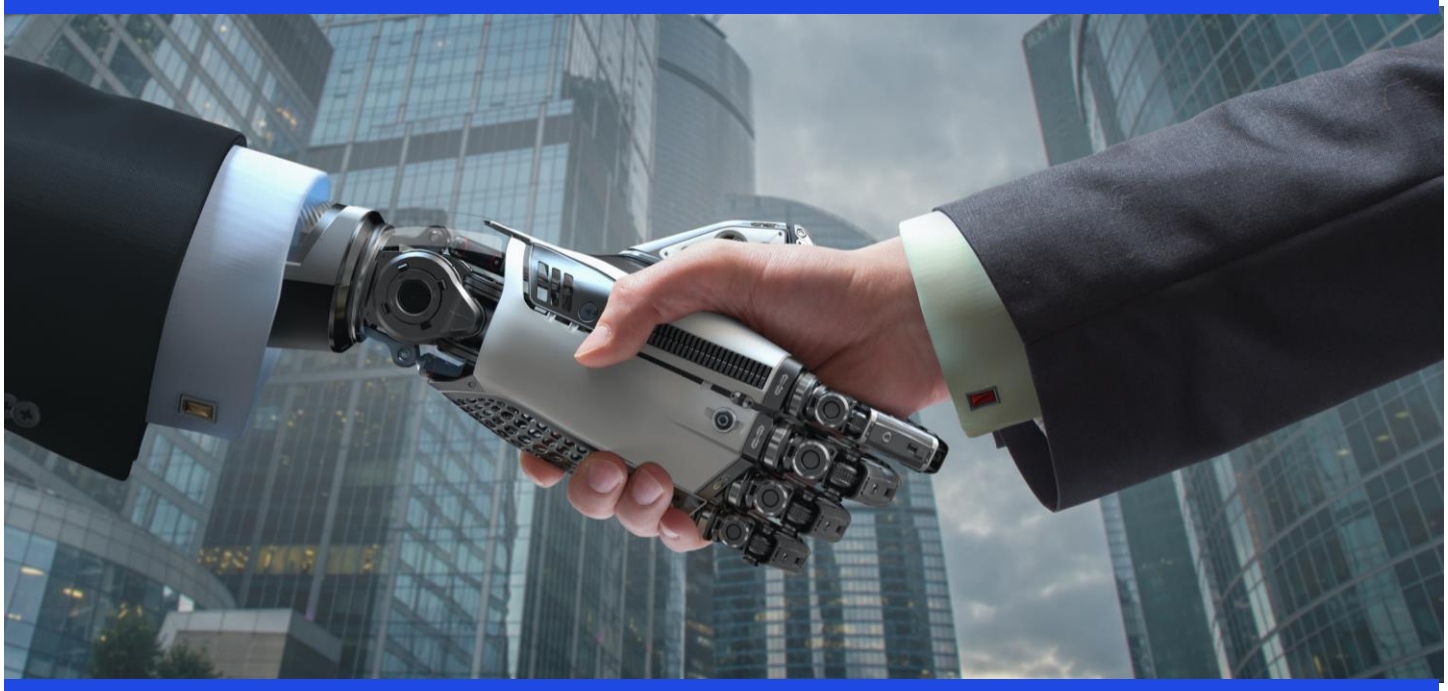
8. Reliability
Ensure AI systems perform at the desired level of precision and consistency.

Source: The flip side of generative AI: Challenges and risks around responsible use | KPMG US | 2023.

Implementing emerging AI risk management frameworks is crucial for companies to navigate the complex landscape of AI technologies. By understanding the risks, establishing a robust risk governance structure, embedding ethical principles, implementing data governance practices, continuously monitoring AI systems, fostering a culture of learning, and engaging in external collaborations, companies can effectively manage AI-related risks and ensure responsible AI adoption. Corporate leaders and board of directors play a critical role in providing strategic guidance and oversight to drive successful AI risk management initiatives that align with the organisation's objectives and protect the interests of all stakeholders.

Key considerations

- What are the specific business objectives and goals that the organisation aims to achieve through the implementation of artificial intelligence?
- Are the broad, potentially game-changing implications of AI—for the company's industry, business model, and long-term viability and competitiveness—being factored into strategy discussions?
- How does the organisation plan to address potential risks associated with AI implementation, such as algorithmic biases, data security breaches, and regulatory compliance?
- How will the organisation handle ethical considerations related to AI, such as privacy concerns and potential job displacement?
- How will the organisation ensure that AI systems are aligned with legal and regulatory requirements, including data protection and intellectual property rights?
- What data governance practices are in place to ensure the quality, integrity, and security of data used in AI systems?
- What measures are being taken to educate and train employees about AI technologies, their implications, and ethical use?
- What steps have been taken to ensure transparency in AI decision-making processes?
- How will the organisation monitor and evaluate the performance of AI systems to ensure their effectiveness and alignment with business objectives?
- What mechanisms are in place to track and manage potential bias in AI algorithms and decision-making processes?
- How will the organisation ensure that AI implementation complies with industry standards and best practices?
- What AI systems and processes has the company deployed, and which are the most critical?
- How will the organisation ensure the responsible and accountable use of AI, including clear ownership and oversight of AI initiatives?
- What contingency plans are in place to address potential disruptions or failures in AI systems and minimise their impact on business operations?
- How will the organisation balance the benefits of AI implementation with potential risks and challenges, and ensure a favourable risk-reward balance?
- How will the organisation communicate AI-related initiatives, risks, and outcomes to shareholders, customers, and other relevant stakeholders?
- How will the board of directors actively monitor and review the progress of AI implementation, assess its impact on the organisation, and adapt the governance structure and processes accordingly?



KPMG in India contact:

Ritesh Tiwari
Partner
Board Leadership Center
E: riteshtiwari@kpmg.com

kpmg.com/in

kpmg.com/in/socialmedia

30 years and beyond

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.