

- Organizations implementing AI transparency, trust, and security will witness a 50% improvement in AI model adoption, business goal achievement, and user acceptance by 2026.1
- 34% of organizations globally are either using or implementing AI application security tools to mitigate generative Al risks.²
- 26% of organizations are in the process of implementing or using privacy-enhancing technologies (PETs).²
- ModelOps is being implemented or used by 25% of the organizations; model monitoring is adopted or utilized by 24% of the organizations globally.²

Critical Factors for Al Success and Scaling

Leaders must focus on strategies and practices relating to:



Al Risks with Proactive Approaches



Data Risks

- Variations in the quality of the data and the accuracy of the model outputs could have adverse outcomes.
- Unintentional bias in training data leads to undesirable outcomes.

Proactive Approach

- Implement data quality checks, ensure data accuracy, and establish data governance practices.
- Regularly audit and diversify training data, employ bias detection algorithms and implement fairness-aware machine learning techniques.

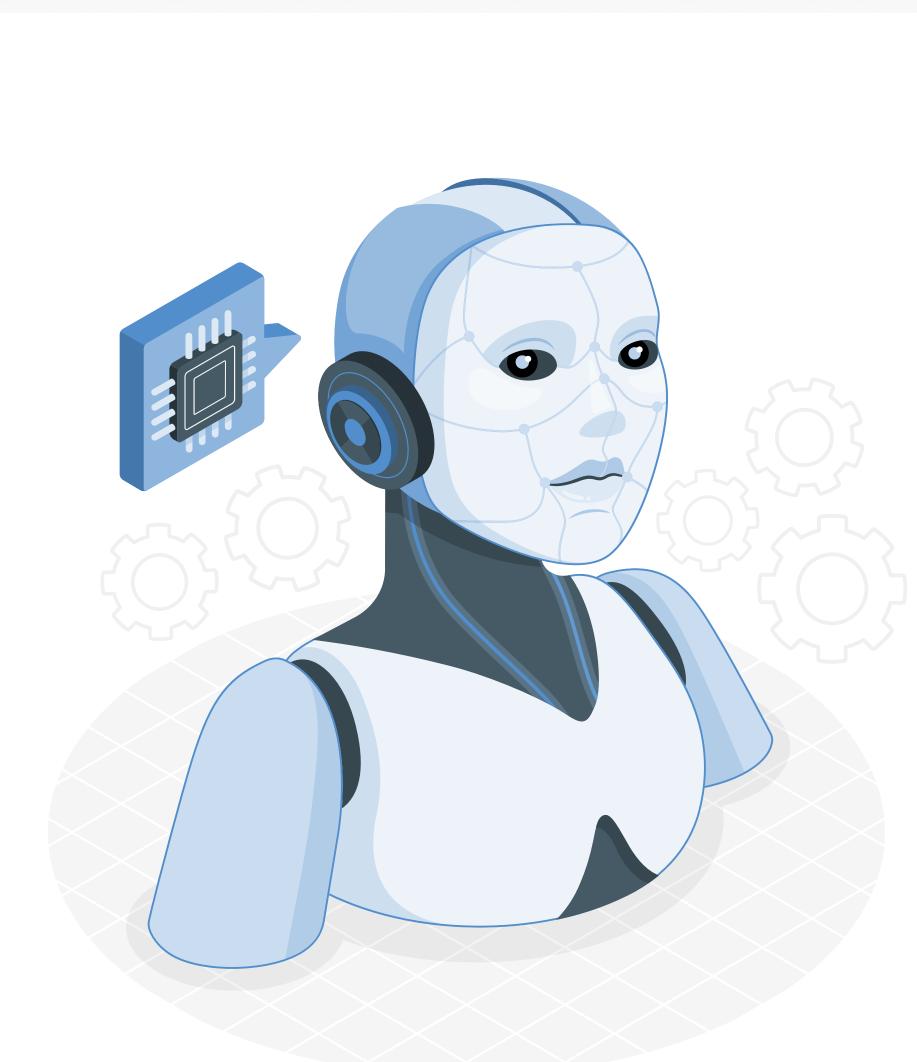
• Al decision-making, especially in sensitive domains, gives rise to ethical

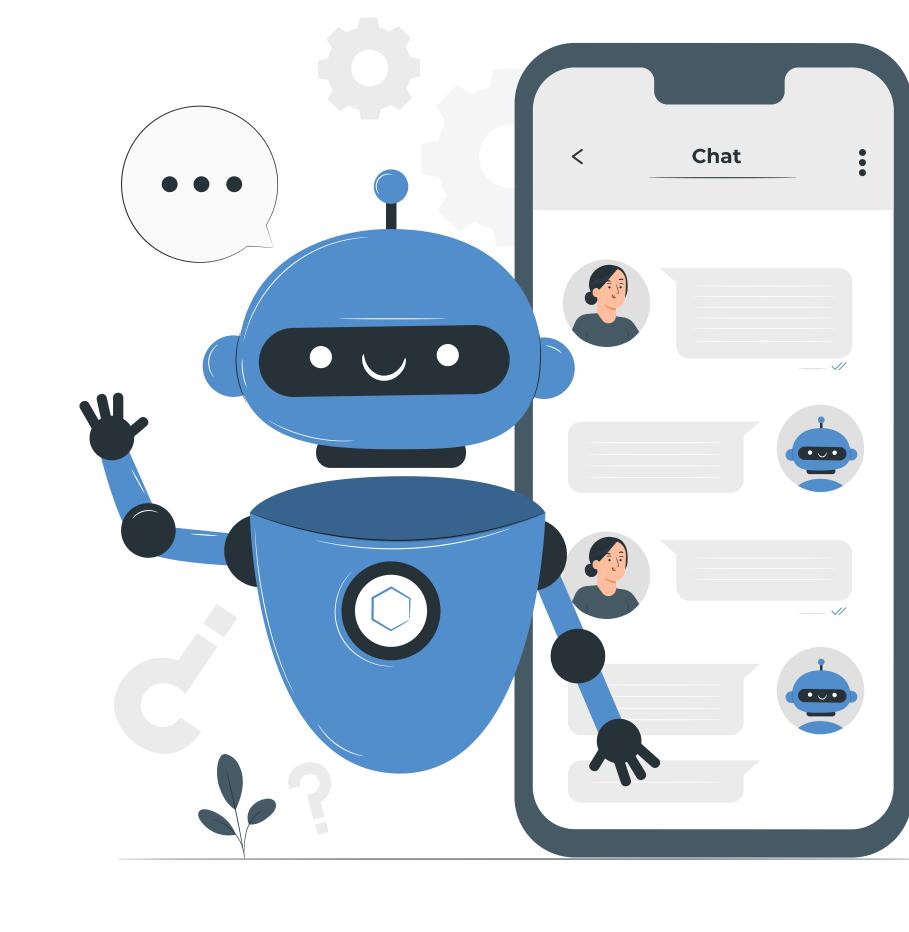
Ethical and Transparency Concerns

- dilemmas.
- The lack of transparency in AI decision-making processes makes understanding and interpreting outcomes challenging.

Proactive Approach

- Establish ethical guidelines and integrate ethical considerations into the design process.
- Use interpretable models, explain AI decisions, and prioritize transparency in algorithmic processes.





Regulatory Compliance • Failure to comply with evolving AI regulations and standards.

Proactive Approach

- Stay updated on regulations, engage with regulatory bodies, and establish internal compliance checks.
- check of AI applications used in the organization. Initiate a formal organization-wide program to educate employees about Al

Determine the extent of AI exposure by performing an exhaustive inventory

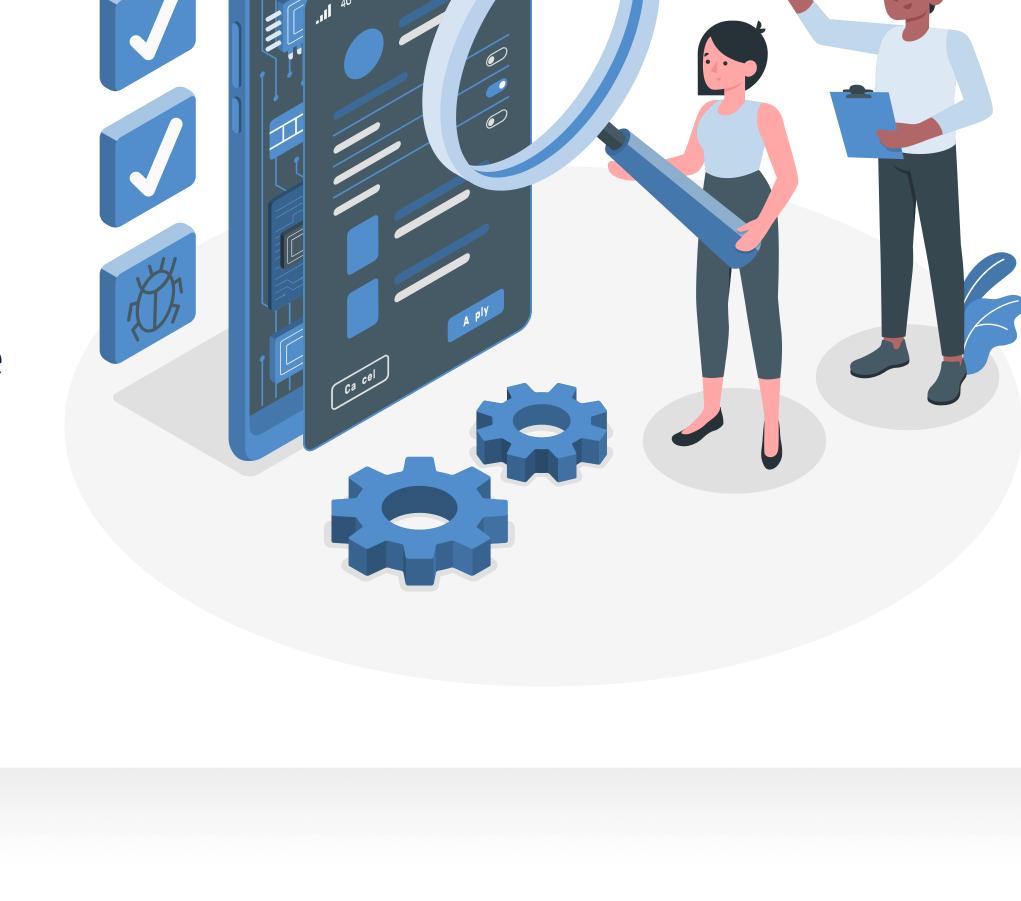
- compliance and risks. Avoid internal and shared AI data vulnerabilities by establishing strong data
- protection and privacy policies.

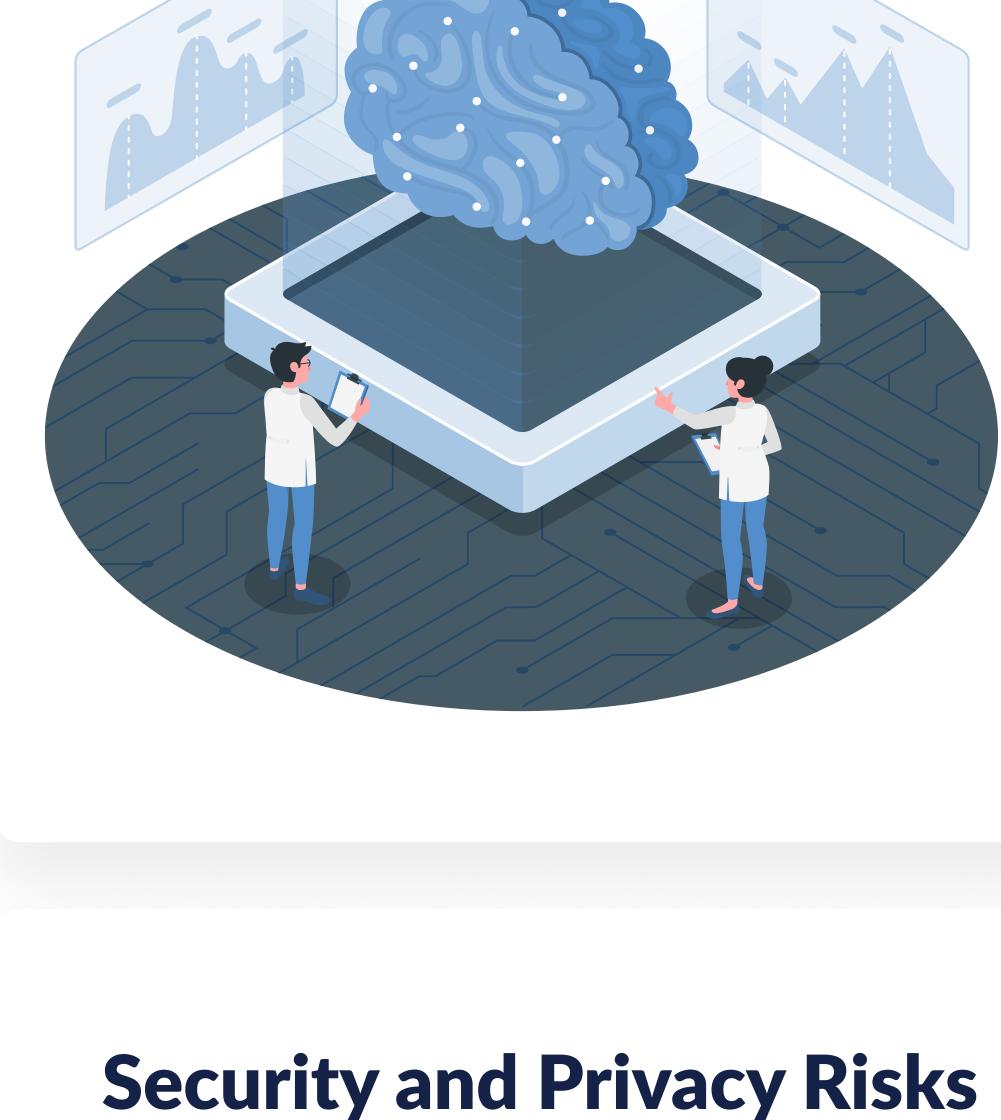
Model Integrity Lack of robustness makes models susceptible to conflicts and unforeseen scenarios.

Proactive Approach

Conduct robustness testing, use adversarial training techniques, and ensure models perform reliably in diverse conditions.

 Incorporate risk management techniques into model operations to enhance model security, dependability, and credibility.





consequences. • Difficulty in explaining AI decisions, especially in crit ical applications.

clear communication of AI outcomes.

Human Oversight and Explainability

Proactive Approach • Incorporate human-in-the-loop systems, establish mechanisms for human

Overreliance on Al without human intervent ion leads to unintended

override, and ensure continuous human monitoring. • Use interpretable models, generate explanations for predictions, and prioritize

Proactive Approach

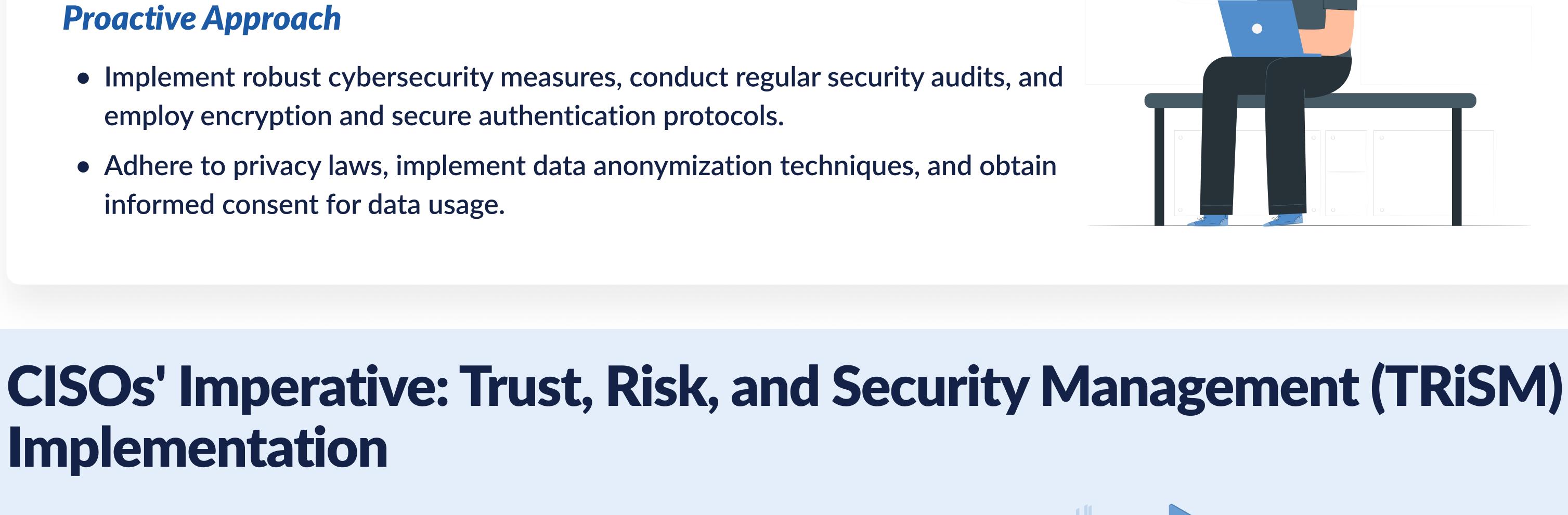
• Implement robust cybersecurity measures, conduct regular security audits, and

• Exposure to cyber threats, data breaches, and adversarial attacks.

employ encryption and secure authentication protocols.

Implementation of AI TRISM allows organizations to:

Violation of privacy regulations and standards.



informed consent for data usage.

Implementation

Assess alignment with original intentions.

Understand AI model behavior.

Driving Al Governance through TRiSM Leadership

Anticipate performance and business value outcomes.



- Chief Information Security Officers (CISOs) must advocate for new forms of Trust, Risk, and Security Management (TRiSM) to prevent AI from taking over their organization.¹
- Accelerating the process of AI model development to production.

• Promoting AI TRiSM has the potential to remove up to 80% of false and fraudulent data and can improve AI



outcomes by¹:

Streamlining AI model portfolios.

Promoting better governance.

Optimize Your Organization's Analytics and Al Management with LatentView







