KPMG

Generative AI: value, risk and regulation

An exclusive summary based on KPMG survey and analysis showcasing how leaders are approaching Generative AI

kpmg.com/in

—

November 23

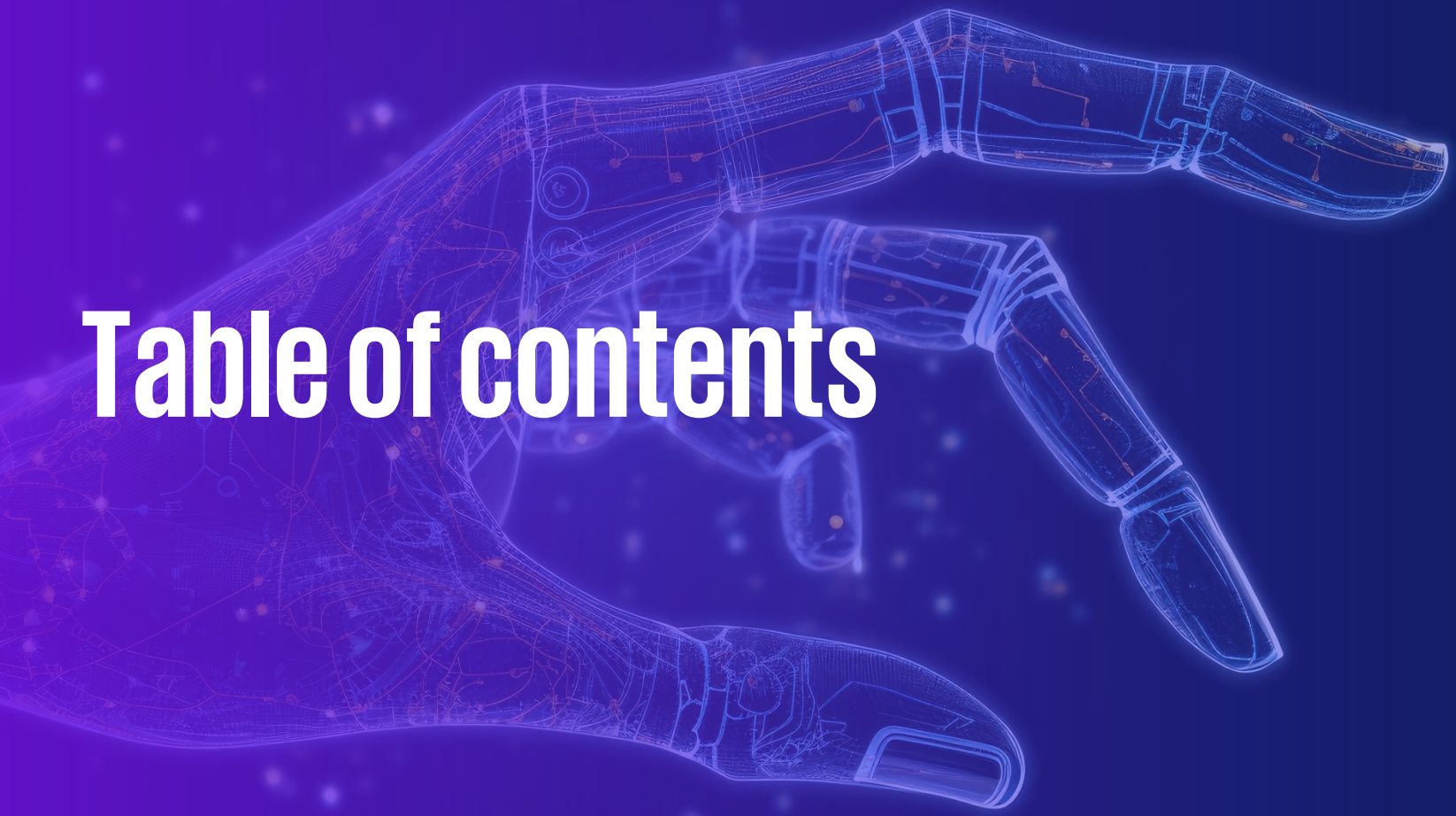


Table of contents

01

Introduction

In last few months, generative artificial intelligence (AI) has become a global sensation. Predictions of its potential impact on society, employment, politics, culture, and business fill the media and the internet. Business leaders are intrigued by the possibilities and are convinced that generative AI is truly a game-changer.

KPMG launched its 2023 KPMG Generative AI Survey to look beyond the hype and understand how enterprises can make progress toward real, meaningful generative AI results.

The chief finding: Across industries and functions, three in four business leaders (74 per cent) rank generative AI as top emerging technology that will impact their businesses over next year. Marketing & sales, Finance & Accounting, Corporate Governance and M&A strategy are priority functions where organisations are envisaged to invest the most on generative AI. Also, increasing prioritisation of Risk Management is seen as a critical aspect for AI adoption. Cyber Security and Data Privacy are the top risks that business leaders are concerned with.

Harnessing the transformative power of generative AI will require a balance of speed with thoughtful planning and careful risk mitigation

The possibilities for using generative AI to transform how enterprises create content, engage users, develop software, and analyse data appear limitless.

But, as with many emerging technologies, the path from buzz to business value while managing risk is not simple or straightforward. Generative AI is still in its infancy and evolving rapidly. Before executives invest in broad adoption, they have many unanswered questions about security, reliability, impact on jobs, regulations and potential value. Executives in our survey cite lack of clarity on regulation, lack of talent and internal cultural resistance as top barriers to implementation.

02

Key highlights

Opportunities

74% of respondents expect generative AI to have the largest impact on their businesses out of all emerging technologies.

73% believe generative AI will increase workforce productivity.

71% will implement their first generative AI solution within the next two years.

64% believe generative AI will help their business gain a competitive advantage over competitors.

67% Of the deployed AI solution have leveraged “off the shelf” solutions and customised them to fit their needs.

Challenges

92% think generative AI implementation introduces moderate to high-risk concerns.

47% are still at the initial stages of evaluating risk and risk-mitigation strategies for generative AI.

Top barriers to implementation

lack of clarity on **regulation**

lack of skilled **talent**

and internal **Cultural resistance**

Top risk focus areas

Cybersecurity and data privacy

03

How Generative AI is capable of creating value

Business leaders are highly interested in the capabilities and opportunities generative AI can unleash and believe it has the potential to reshape how they interact with customers, run their workplaces, and grow their revenue.

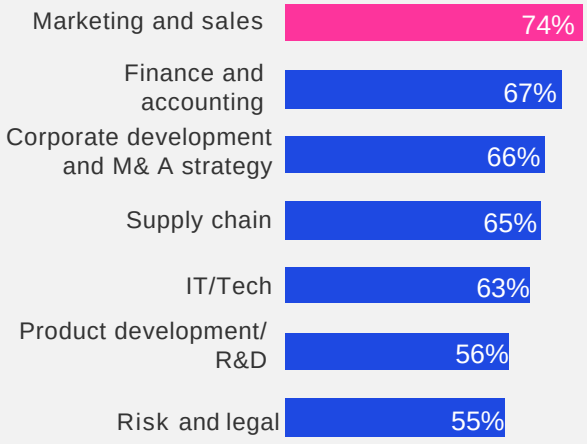
Regardless of sector or function, 74 per cent rank generative AI as the emerging technology that will have the biggest impact on the business over the next 3 to 5 years, ahead of other trending technological capabilities such as advanced robotics, quantum computing, augmented reality/virtual reality (AR/VR), 5G, and blockchain.

Transforming business processes using generative AI precursors like machine learning and automation requires breaking them down into their individual component parts and applying strategic thinking around what components to accelerate or optimise. As such, they mostly impact business processes with point solution approaches designed to solve a single problem.

Generative AI changes the game. Processes do not need to be broken down because generative AI tools can apply the large variety of human knowledge, experiences, and common sense embedded into their models to fill the gaps. This creates immense opportunity to apply and scale the technology across real-world enterprise-wide business processes.

Businesses recognise generative AI's potential. Generative AI technology is in the midst of a meteoric rise and is now reaching an inflection point. The market has evolved to the point that large companies in basically every industry can no longer ignore it and are now springing into action.

Exhibit 1: Priority functions on which organisation will spend their Gen AI budget



Notes: Sum will not add up to 100% as it is a multi-select question
Source: KPMG Generative AI survey, June 2023

Executives expect the impact of generative AI to be highest in enterprise-wide areas driving innovation, customer success and technology investment. Sales & marketing and finance & accounting are the top two functional areas where respondents are currently exploring to implement generative AI in their businesses.

Generative AI use cases being prioritised	Analysing customer feedback/ improving customer relationships	Identifying new products and use cases	Developing external/ internal chatbots and/or virtual assistants	Automating data governance

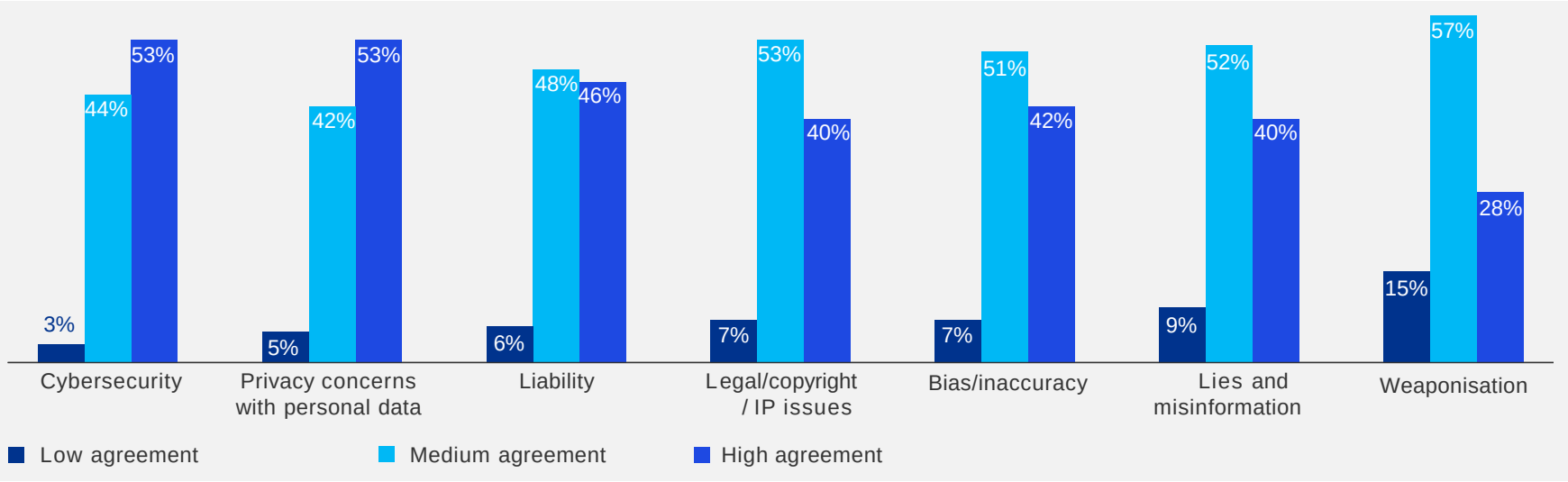
04

Top risks with adoption of Generative AI

The risks posed by generative AI models are broad and complex, spanning multiple areas of the business, from privacy and security to compliance and ethics. Billions of dollars could be wasted if enterprises place bets on wrong tools, applications, or use cases, or fail to weave initial pilot projects into their ways of operating. Customers could be alienated, and brands could be ruined, by an unsupervised generative AI algorithm spewing out immoral or erroneous advice. Anxiety could rise among employees who feel threatened by the possibility of technological displacement or confused by the changes in their normal work routines brought on by generative AI tools. Businesses could run afoul of global laws and regulations if a generative AI bot exposes sensitive or confidential information or intellectual property.

The vast majority of respondents (92 per cent) rank their concerns about the risks of implementing generative AI as moderately to highly significant. The top risk management and mitigation focus areas—those selected by the greatest percentage of survey respondents as high priorities—are cybersecurity (53 per cent), privacy concerns with personal data (53 per cent), and liability (46 per cent).

Exhibit 2: Cybersecurity and data privacy are the top risk-management focus areas



Source: KPMG Generative AI survey, March 2023

05

Regulations evolving around AI

To steer industries toward responsible action around AI broadly, governments around the world have proposed regulations such as EU AI Act and the US AI Bill of Rights that require businesses to consider consequences of adopting AI technology alongside opportunities. Given the rapid adoption of generative AI and the predicted massive impact across business and operational models, attention on AI regulatory guidelines is growing and compliance is becoming increasingly important to reputation and trust.

Non-compliance could have significant monetary impacts. For example, the proposed EU AI Act—which will require organisations to determine AI system risk and monitor high-risk systems has provision of administrative fines of up to €40M or, if the offender is a company, up to 7 per cent of its total worldwide annual turnover for the preceding financial year, whichever is higher for using prohibited AI practices.

Other countries have also introduced draft laws such as Canada's The Artificial Intelligence and Data Act (AIDA)[2] which will require high impact AI systems to meet requirements of existing Canadian consumer protection and human rights laws. It also empowers Ministry of Innovation, Science and Industry to administer and enforce the act. Key guiding principles covered in the act are: Human Oversight & Monitoring, Transparency, Fairness and Equity, Safety, Accountability, Validity & Robustness.

President Biden issued an Executive Order[1] on Safe, Secure and Trustworthy Artificial Intelligence on 30 October 2023. The Executive Order aims to establish new standards for AI safety and security, protect Americans' privacy, advance equity and civil rights, stands up for consumers and workers, promote innovation and competition and advance American leadership around the world.

The EU is paving the way with its EU AI Act, which will require organisations to:

- **Determine the level of risk embedded in their AI Systems**
- **Conduct conformity assessments on high-risk AI systems**
- **Implement post-market monitoring systems on high-risk AI systems**

Non-compliance brings major penalties:

Administrative fines of up to €40M or, if the offender is a company, up to 7 per cent of its total worldwide annual turnover for the preceding financial year, whichever is higher

1. White house – Briefing room – Statements and releases President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence
2. The Artificial Intelligence and Data Act – Companion document (Government of Canada)

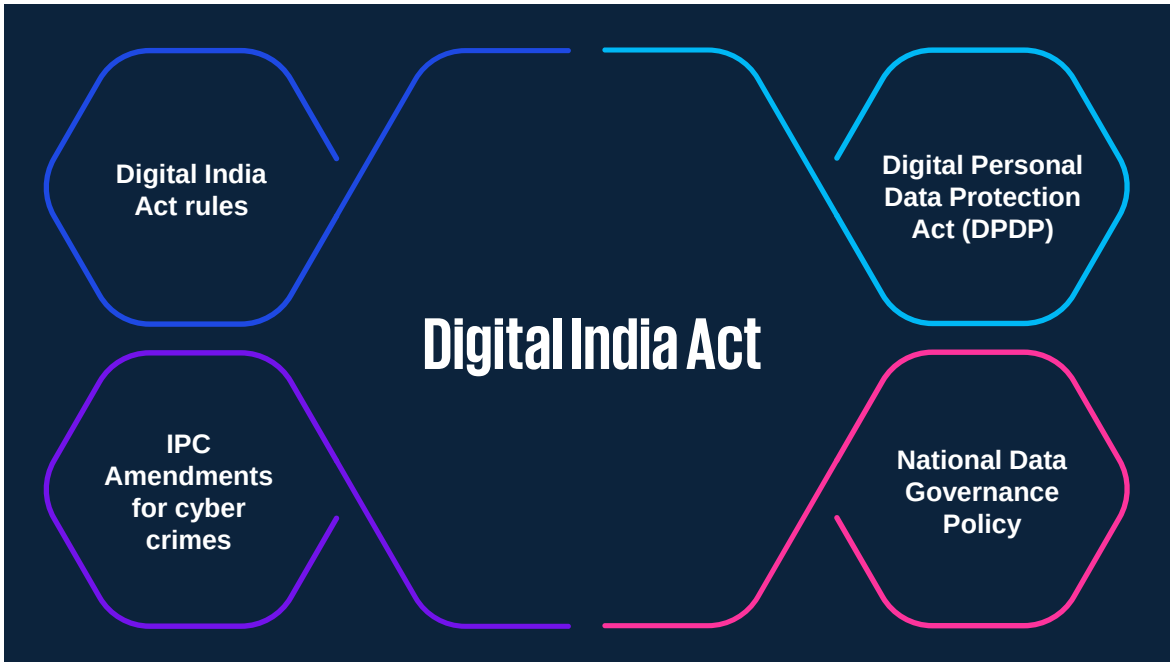
06

Regulations around AI in India

In India, Ministry of Electronics and Information Technology (MEITY) has proposed Digital India Act (DIA) 2023 aimed to replace IT Act 2000. In this proposed act, AI has been identified as one of the intermediaries alongside other intermediaries such as eCommerce, search engines, gaming, digital media etc. This means AI is going to be one of the focus areas in Digital India Act and there will be separate rules for AI as well..

To ensure online safety and trust, it is expected that the proposed act shall define and regulate hi-risk AI systems through legal, institutional quality testing framework to examine regulatory models, algorithmic accountability, zero-day threat & vulnerability assessment, examine AI based ad-targeting, content moderation etc.

It is envisaged that the proposed act will have measures for ethical use of AI based tools. In order to establish accountable internet through this proposed act, it is expected that a dedicated inquiry agency and a specialised dispute resolution /adjudication framework will get established which will be applicable to AI solutions as well.



Source: Ministry of Electronics and Information Technology, (meity.gov.in) – Proposed Digital India Act – Digital India Dialogues presentation dated 09.03.2023

Acts/frameworks in India which may impact AI regulation

DPDP Act –
Aims at protecting the individual's privacy by empowering them with rights over the manner in which their data is processed.

National Data Governance Policy -
Aims to transform and modernise Government's data collection and management processes and systems

IPC Amendments for cyber crimes –
Aims to provide legal framework for investigation and prosecution of cyber crimes.

Digital India Act rules:
Aims to create separate rules for each class of identified intermediaries in DIA including AI

07

How KPMG in India can help

Generative AI is poised to transform the future of enterprise. Businesses will increasingly rely on generative AI to gain insights, make critical decisions, alleviate skills shortages, create new products, and engage with customers.

We believe, however, that many businesses do not fully understand or account for the risks and challenges generative AI poses. Successful generative AI adoption requires a holistic approach across AI lifecycle encompassing designing, building, deploying and improving systems in a safe, trustworthy, and ethical manner.

KPMG in India can help organisations in their AI journey by managing risks that manifest at each layer of the AI lifecycle. Key risks that need to be addressed at each layer may include the following:

1. Data layer (ingestion, data exploration, data processing and feature selection): data privacy breach, data bias, IP protection, attribution and consent, data exfiltration, etc.
2. Model Layer (model training, model tuning, model adaptation, model deployment and model maintenance): training data poisoning, model bias, model drift, model induced breach, sensitive information disclosure, model underfitting and overfitting, hallucination, etc.
3. Compute Layer (IT infrastructure such as GPUs, storage, firewall, etc.): model denial of service, model theft, data exfiltration, enhanced training time, conflict with E goals in ESG, etc.
4. Process Layer (governance, supply chain, regulation, compliance etc.): regulatory Risks, explainability, overreliance, etc.

We, at KPMG in India, have combined our deep industry experience and modern technical skills to develop a Responsible AI Framework, which can help business leaders harness the power of AI to accelerate value in a trusted manner – from strategy and design through to implementation and ongoing improvement.

Our Responsible AI Framework provides a set of controls, processes and tools to help ensure AI systems are designed and deployed in a trustworthy and ethical manner so that organisations can accelerate value while managing risks.

Eight core principles guide our approach to Responsible AI

Fairness
Ensure models are free from bias and equitable.

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

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

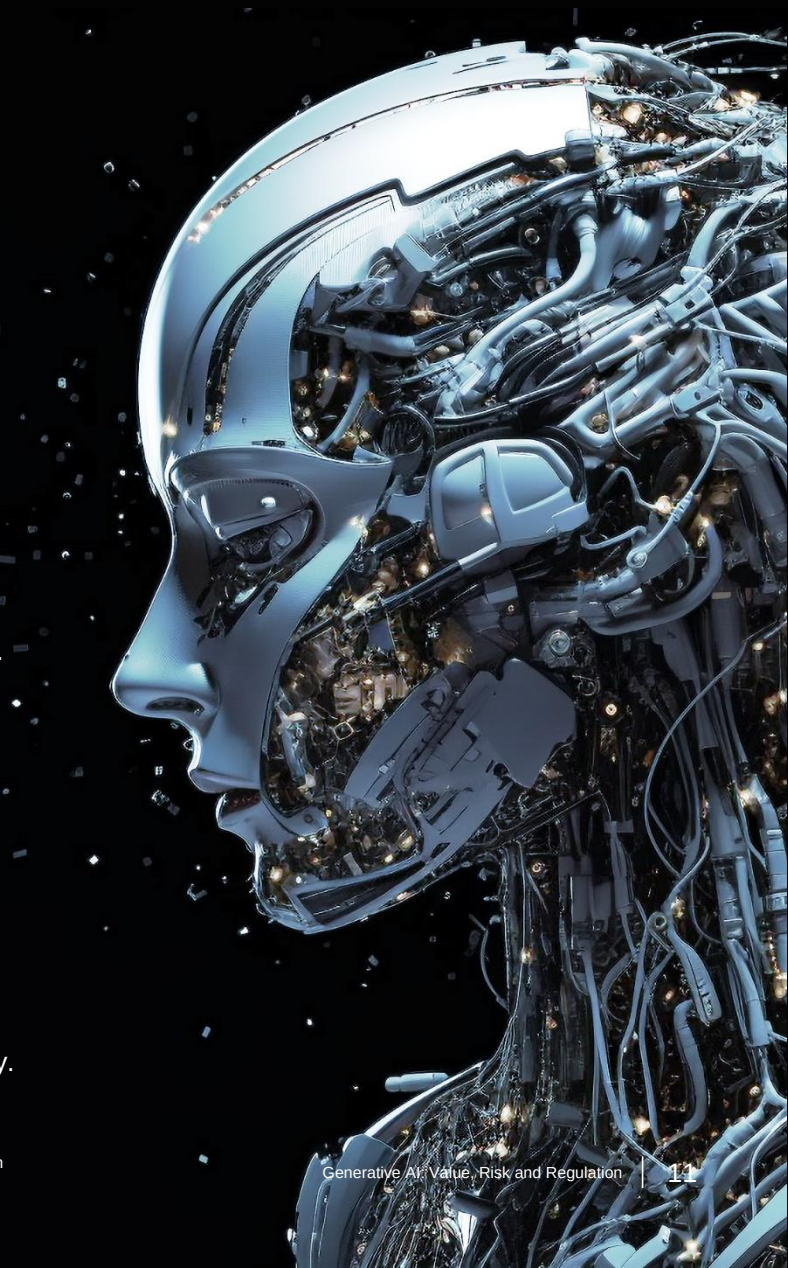
Security
Safeguard against unauthorised access, corruption, or attacks.

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

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

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

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



KPMG in India contacts:

Akhilesh Tuteja
Head – Clients & Markets
Global Head – Cyber Security
E: atuteja@kpmg.com

Atul Gupta
Partner, Head of function – Digital Trust
E: atulgupta@kpmg.com

Rahul Singhal
Partner, Leader- Cyber Assurance – Digital Trust
E: rahulsinghal@kpmg.com

Annapurna Alladi
Partner – Digital Trust
E: aalladi@kpmg.com

Akashdeep Prasad
Technical Director – Digital Trust
E: akashdeepprasad@kpmg.com

kpmg.com/in

Follow us on:

kpmg.com/in/socialmedia

30 years and beyond