



Market Insights Report:

# The Essential Role of Governance in Mitigating AI Risk

# Table of Contents

- 3 Letter from Prove AI
- 5 Data Highlights
- 6 Demographics and Methodology
- 7 **Chapter 1** AI's Momentum Continues to Build Across the Enterprise
- 12 **Chapter 2** A Closer Look at the Challenges of Securing Data
- 17 **Chapter 3** The Key to Effective Risk Management: AI Governance
- 24 **Chapter 4** AI Governance Readiness
- 28 Conclusion
- 29 About Prove AI



# Letter from the Founder

## We're standing at a critical inflection point in AI's evolution.

Spurred in no small part by the advent of ChatGPT in late 2022, AI has experienced an unparalleled uptick in adoption in recent years. This evolution has subsequently spurred considerable advancements in database automation, large language models (LLMs) and generative AI that have placed the technology firmly in the mainstream. AI has nearly limitless potential to transform everything from filmmaking to technical workstreams – and significant steps are currently being realized on that journey.

As it evolves beyond the hype cycle, AI is beginning to create efficiencies and value that were once only dreamed about. But these productivity gains come with a significant new level of risk. Risk management has emerged as a paramount concern vis a vis AI: organizations now have a clear onus to better demonstrate how and why a given AI system behaves the way it does, and to demonstrate the ability to better manage it when it deviates from its intended purpose.

It's no surprise that AI governance has emerged as a top focus for both the public and private sectors. Governance is an increasingly critical part of the larger, emerging AI technology stack—and it all starts with the data feeding AI systems. The effectiveness of a machine learning model hinges on the quality of the data

that teaches it, so it stands to reason that verifiable, tamper-proof data is key to realizing AI's potential and unlocking new opportunities.

And yet, current understanding of the data that powers most models remains alarmingly incomplete: many organizations cannot verify and demonstrate that their training data is properly sourced, secured, and maintained. Business leaders agree: nearly half of respondents (**45%**) in this report reported that risk associated with data integrity/security is the top factor discouraging them from employing AI in certain business functions, even with its considerable potential.

This knowledge gap limits the ability to fully train, modify, and ultimately govern AI systems in ways that align with a business' best intentions. Without a robust governance layer, AI models can behave unpredictably, give biased or untrue responses, and damage brand reputation and user trust.

While lawmakers are introducing regulations to address these concerns—the EU AI Act and California's AI Act among them—and businesses are developing their own responsible AI frameworks, both are still in their most nascent stages.

To better understand how businesses today are thinking about and actively deploying AI governance strategies, this study polled 600+ technology leaders from the US, UK and Germany. Their responses show that while the vast majority recognize the importance of AI governance, there remains a long journey ahead to realize broadly accepted standards for responsible AI.

Few organizations feel truly confident in their current capabilities, and most feel a renewed sense of urgency to address the issue. This study found that **85%** of leaders report that they plan for their organization to implement a robust AI governance solution by summer 2025. This consensus underscores the urgency of establishing clear best practices and adopting tools to govern AI's development and deployment.

While regulation is often painted as an antagonist to innovation, such thinking obscures the broader point. Thoughtful regulation is necessary to realize broadly accepted standards that enhance transparency into AI training data—which will in turn spur greater innovation. It's true that careless or overreaching legislation can hinder innovation, but it's equally true that a lack of any real oversight will instill an unacceptable level of risk within AI that makes broader adoption an impossibility. Hence, it's key that the public and private sector work together to develop thoughtful policies that strike the right balance.

The coming years of AI development will be defined by the pursuit of responsible, effective AI. This will require collaboration and communication between both public and private sectors: accomplishing wide recognition of shared ethical standards, as well as cutting-edge tools to enforce those standards. Realizing a truly responsible AI standard will require a thoughtful mix of both regulation and innovation.



Mrinal Manohar,  
Co-founder and CEO, Casper Labs

## Data Highlights:

# AI's Adoption Curve Depends on Developing Good Governance Standards

In a survey of 607 global business decision-makers in the US, UK, and Germany, we found:

**96%**

of respondents plan to increase their investment in AI at their organizations in the next year.

of organizations plan to invest in blockchain technology in the next 12 months.

The **top three** use cases for AI in the enterprise are:

**1.** Customer service and support

**2.** Predictive analytics

**3.** Marketing and advertising optimization

Risk associated with data integrity/security is the top factor discouraging organizations from using AI in their business.

**86%**

of respondents said better explainability in AI models would moderately or significantly impact the likelihood of their choice to use AI in business operations.

**82%**

indicated a somewhat or extremely pressing need for their organization to implement a robust AI governance solution in the next 12 months.

**63%**

believe the integration of AI and blockchain technology has the potential to revolutionize their industry, enabling enhanced data security, transparency, and efficiency.

It's increasingly clear that AI requires strong governance—and that blockchain technology is uniquely suited to support it.

Blockchain already supports a range of AI endeavors. The **top five ways blockchain is used today**, across industries:

**1.** Database automation

**2.** Ensuring security, compliance, or regulatory reporting

**3.** Supporting AI initiatives

**4.** Verifying financial transactions or payments

**5.** Tracking and tracing goods/supply chain management

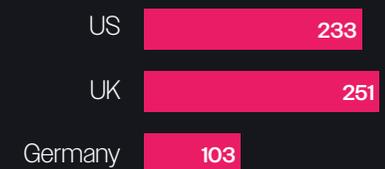
Offering secure, automated data transparency and controls to support AI governance, **blockchain has found its moment.**

# Demographics and Methodology

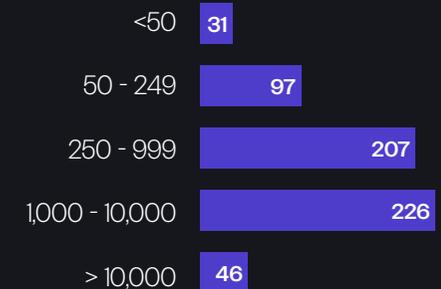
Zogby Analytics conducted an online survey of 607 IT decision-makers in the US, UK, and Germany.

Using internal and trusted interactive partner resources, thousands of technology leaders were randomly invited to participate in this interactive survey. Based on a confidence interval of **95%**, the margin of error for 607 is +/- 4 percentage points.

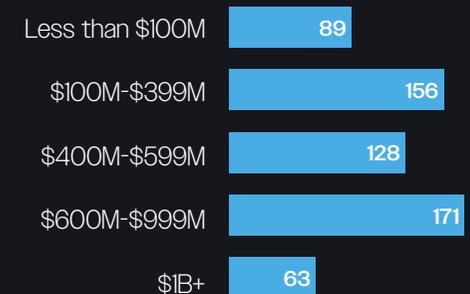
## Company location



## How many total employees are in your organization?



## What is your organization's revenue?



## Chapter 1

# State of the Industry: Blockchain Grows Up

---

AI is now deeply integrated into business operations, with most surveyed companies and industries actively exploring how to leverage it to enhance efficiency, innovation, and decision-making. This widespread adoption reflects the growing recognition of AI's potential to transform various aspects of business, from automating routine tasks to providing insights through advanced data analysis.

**96%** of organizations are using AI, and most **94%** are either confident or very confident in the ways they are leveraging genAI models or LLMs in their business. Where reluctance to adopt AI exists, it stems from security concerns, which respondents view as a more significant risk than the potential costs or complexities associated with AI implementation. Risks with data integrity and security are discouraging use at **45%** of companies, and **34%**

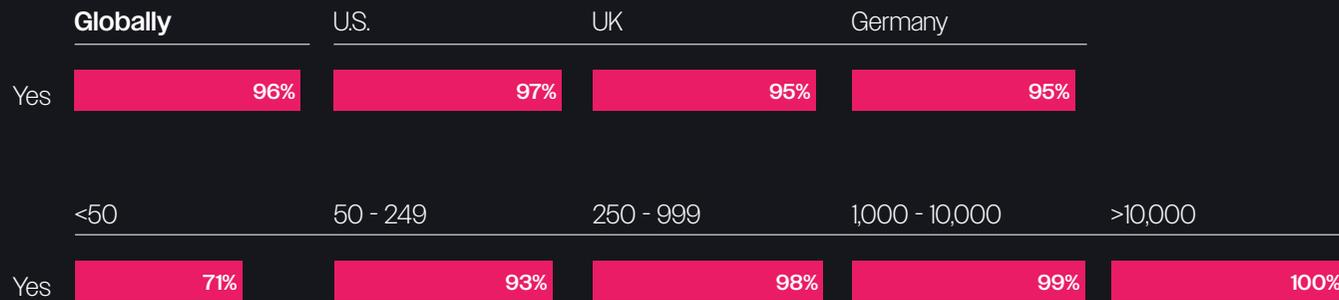
“From what I’ve seen over the last year, executives increasingly understand the opportunities and risks of AI and are closely watching the changes in the regulatory landscape. At the same time, many of them are still unclear about how to get started scaling true AI governance at the enterprise level, taking into consideration regulatory change, ethics and bias, cybersecurity, data privacy and other factors. Getting to scale requires an AI governance approach that encompasses people, processes and technology.”

Shyam Nagarajan | Global Partner, IBM

worry about the vulnerability of AI systems to cyberattacks and data breaches. Meanwhile, **37%** have already had issues with bias detection and unfair algorithmic decisions, raising concern about the ethical implications of using AI in sensitive areas.

Despite these concerns, most businesses see promise in AI and continue investing in the technology. They recognize its potential to drive growth and innovation, but there is still some uncertainty about the effectiveness and value of AI when implemented at scale. Businesses are cautious about whether AI can consistently deliver measurable benefits across all areas of their operation, especially in complex, real-world scenarios. This hesitation highlights the need for robust governance solutions to not only address the aforementioned security concerns but to facilitate improved performance.

# Does your organization currently use AI for its business operations?



Internationally, all geographies reported a high rate of AI adoption. The rate of AI adoption was correlated positively with company size: all enterprises with over 10,000 employees reported AI usage.

Across industries, adoption was lowest in the public sector (**83%**) and staffing and recruiting (**86%**). In the public sector, this reluctance is likely due to budgetary constraints as well as concerns regarding regulatory compliance in the long term. In staffing and recruiting, respondents report equal concern about the lack of transparency in understanding AI behavior, risks associated with data integrity and security, and enforcing shutdowns when AI behaves unpredictably.

# What motivations does your organization have for investing in AI?

82%

Increased productivity

73%

Operational efficiency

65%

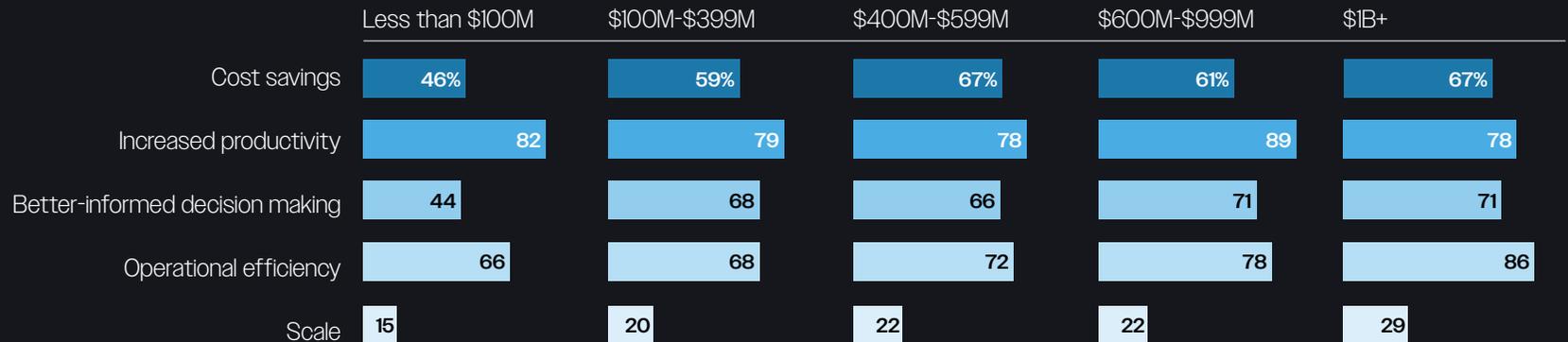
Better-informed decision making

60%

Cost savings

22%

Scale



# When It Comes to AI Priorities, Size Matters

The priorities driving AI adoption varied by company size. Organizations with \$1B+ revenue prioritize increased productivity (**86%**) and better-informed decision-making (**77%**) the most. Smaller companies with less than \$100M in revenue focus more on using AI to fuel business growth, through improvements to operational efficiency (**64%**) and cost savings (**64%**). When responses are broken down by the respondent's role, CEOs and CXOs are particularly focused on increased productivity (**79%** and **79%**) and better-informed decision-making (**71%** and **83%**, respectively).

Use cases are maturing as businesses find more applications for AI. Across sectors and regions, increased productivity stood out as the leading factor driving AI adoption. Scale was ranked decisively the lowest, suggesting that most companies don't yet have faith in the ability of AI infrastructure to support scaling operations.

## The top 5 AI use cases:



Customer service and support continues to be the leading use case driving AI adoption, up **25%** from **61%** last year, while predictive analytics usage is up **20%** from **50%** last year.

Organizations with \$1B+ revenue tend to invest heavily in predictive analytics (**66%**) and process automation (**54%**), indicating a focus on enhancing decision-making and operational efficiency at scale. Smaller companies, particularly those with less than \$100M in revenue, focus more on customer service and support (**71%**) and marketing and advertising optimization (**61%**), aiming to improve customer engagement and marketing ROI.

Larger organizations (with >10,000 employees) emphasize customer service and support (**80%**) and predictive analytics (**67%**). These companies leverage AI to handle large volumes of customer interactions and data-driven decision-making.

Most popular LLMs among respondents:

**63%**  
GPT-4

**50%**  
Gemini

**44%**  
Copilot

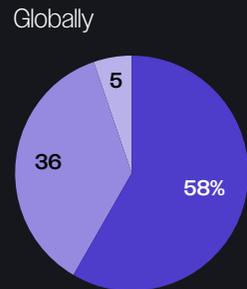
**28%**  
GPT-3.5

**25%**  
AlphaCode

# Confidence in AI is through the roof:

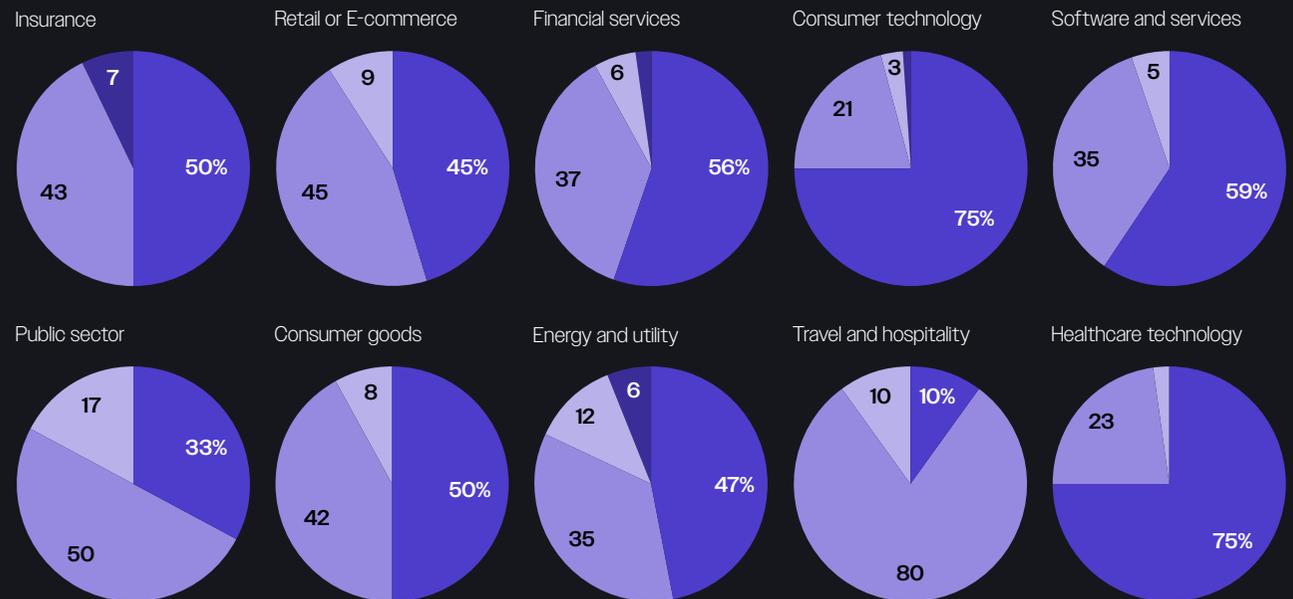
**25%** say there are no factors that discourage them from using AI, up **277%** from **9%** last year. Only a few respondents (less than **1%**) answered that their organization displays a significant or total lack of confidence in AI.

- Very confident
- Confident
- Neutral
- Not very confident
- Not confident at all



## How confident is your organization in leveraging genAI models/LLMs in its business operations?

By industry:



Across sectors, the strength of confidence varied greatly. While **75%** of respondents in both healthcare technology and consumer technology expressed a high level of confidence in using genAI and LLMs, just **33%** of those in the public sector, **30%** of those in the automotive sector, and **10%** of those in travel and hospitality felt the same.

**But high confidence doesn't mean risk has vanished.** Derisking AI is arguably even more imperative in this era of newfound confidence. When humans place greater trust in AI models without understanding how they work, they may miss obvious errors and misinformation when analyzing an AI's output.

## Chapter 2

# A Closer Look at the Challenges of Securing Data

---



“The amount of data being processed by [AI] models is extraordinary. How are we going to make sure all of that data is secure and ‘good’ data? That uncertainty is what’s holding companies back from going all in with AI. AI can be a force for good if we can make it accessible, safe, and trustworthy for both AI developers and end users of all stripes.”

Henry Guo | VP of Product, Prove AI

To solidify confidence in AI, and fully understand and mitigate the risks it entails, look no further than the data.

Among survey respondents, data integrity and security was named the highest area of concern for companies using AI—and for good reason. Without a solid understanding of the data fueling the decisions of machine learning models, it’s difficult (sometimes impossible) to trace how a given model made a certain decision. And the risks of misbehaving AI are real: reputational and financial damages, application disruptions, and customer churn, to name a few.

To build greater confidence among users and lower risk, companies need to thoughtfully consider how they secure and monitor their training data. Achieving data security is a critical component of AI governance strategy.

# What specific performance issues have you experienced with AI deployment in your organization?

82%

Data quality issues (eg inconsistencies or inaccuracies)

73%

Bias detection and mitigation challenges in AI algorithms, leading to unfair or discriminatory outcomes

65%

Difficulty in quantifying and measuring the return on investment (ROI) of AI initiatives, making it challenging to justify investments and prioritize projects

60%

Hallucinations or significant errors in AI-driven systems, resulting in unexpected or incorrect predictions

22%

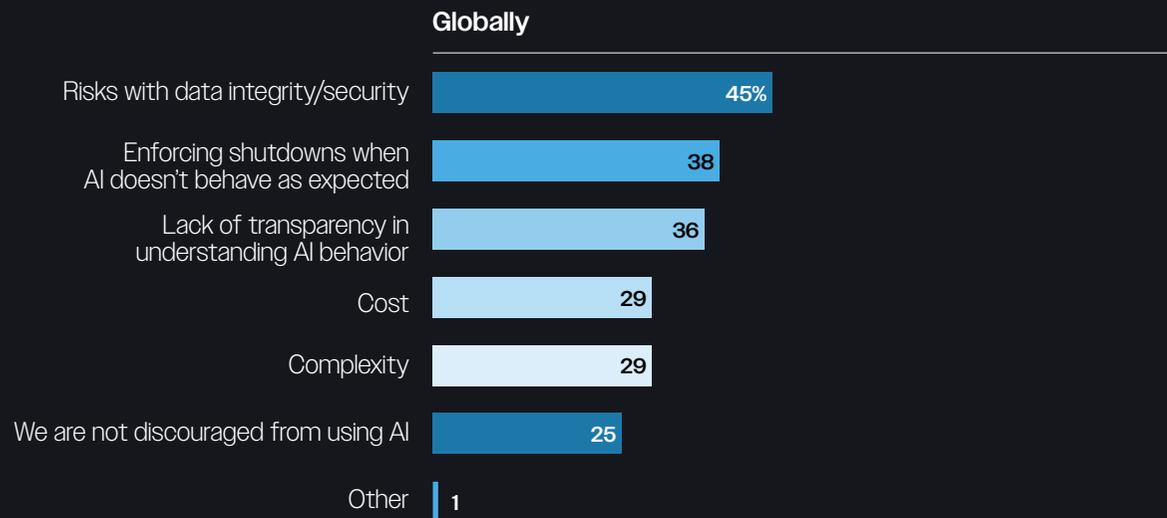
Integration issues with existing systems and workflows, hindering seamless deployment and adoption of AI technologies

The top performance issue (**41%**) that companies have with AI is data quality (inconsistencies or inaccuracies). Bias detection and challenges leading to discrimination in outputs (**37%**) was named as the next most prevalent issue.

Across demographics, company size exerted the largest influence on responses to this question. Of those companies with over 10,000 employees, **60%** identified data quality as a performance issue (as compared to **41%** for the whole sample), while **44%** selected hallucination (compared to **25%**). However, this same class of companies had a much lower rate of issues with performance degradation than other respondents: **7%** compared to **21%**.

	50 - 249	250 - 999	1,000 - 10,000	>10,000
Data quality issues (eg inconsistencies or inaccuracies)	34%	43%	39%	60%
Bias detection and mitigation challenges in AI algorithms, leading to unfair or discriminatory outcomes	34	38	40	33
Difficulty in quantifying and measuring the return on investment (ROI) of AI initiatives, making it challenging to justify investments and prioritize projects	28	26	30	33
Performance degradation over time, where AI models lose accuracy or effectiveness as they age or encounter changing data patterns	23	24	23	7
Hallucinations or significant errors in AI-driven systems, resulting in unexpected or incorrect predictions	20	27	22	44
Compliance and regulatory challenges related to data privacy and security	18	20	25	18
We don't experience any performance issues	18	19	17	13
Integration issues with existing systems and workflows, hindering seamless deployment and adoption of AI technologies	16	23	26	20
Challenges in validating the accuracy and reliability of AI models, particularly in complex or dynamic environments	16	21	24	13

# What discourages your organization's use of AI in business operations?



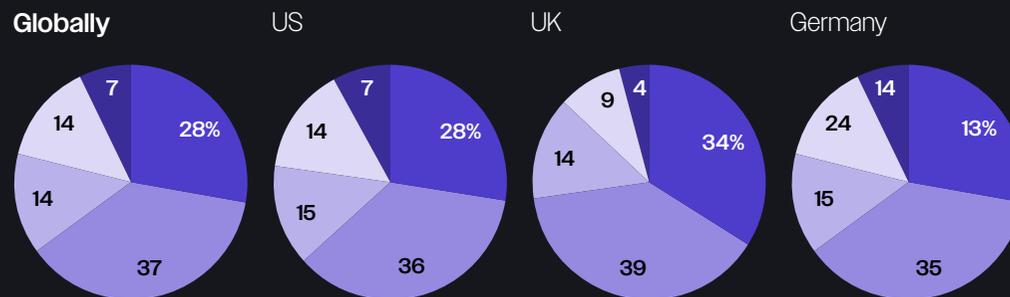
**AI usage is maturing, and so are concerns about its use.** The top obstacle to AI usage was named as risks around data integrity and security (**45%**), followed by enforcing shutdowns in the event of AI misbehavior (**38%**).

As AI becomes table stakes in business operations, companies have pivoted from simply trying to use AI, to trying to use it *well*: securing data, preventing misbehavior, and ensuring transparency in understanding AI behavior all outranked cost and complexity as deterrents from AI use.

A blanket statement about data safety and integrity is no longer enough to assure companies that an AI model is founded on solid data: companies are increasingly interested in seeing proof of data security. If AI was perceived as being more secure, more companies would use it across their business operations. To boost security and trust, companies should focus on governance solutions that specifically alleviate concerns around data integrity.

# When deploying AI applications within your organization, how concerned are you about potential issues related to copyright infringement and data security?

- Very concerned
- Somewhat concerned
- Neutral
- Not very concerned
- Not concerned at all



Across geographies, most respondents were somewhat (**37%**) or very concerned (**28%**) about copyright infringement and data security issues in AI deployment. However, the urgency and prevalence of this concern were much lower in Germany (**13%** of respondents marked very concerned, compared to **28%** in the US and **34%** in the UK). Contributing factors include regionally-specific copyright law as well as the enforcement of the EU AI Act in Germany, which—in its acknowledgment of the importance of copyright protection—may create an extra layer of confidence for German organizations.

# What governance-related challenges do you anticipate your organization encountering when deploying AI?

	Globally	U.S.	UK	Germany
Ensuring compliance with evolving regulatory frameworks	53%	54%	55%	47%
Ensuring the reliability and accuracy of AI model predictions	50	51	47	52
Understanding and explaining how AI models make decisions	37	36	41	30
Navigating complex and ambiguous legal requirements	37	40	36	34
Detecting and mitigating vulnerabilities and data breaches	34	37	32	30

All three geographies surveyed equally identified their top governance challenge as being able to remain compliant with evolving regulatory frameworks. But ensuring the reliability and accuracy of AI model predictions followed close behind.

Just as organizations have moved from simply wanting to use AI to wanting to use it well, they've also shifted from wanting

governance safeguards to wanting those governance safeguards to work effectively and provide a return on investment. A robust governance model aims not only to achieve compliance but to create security, transparency, and accountability in AI use from the ground up—leading in turn to improved model performance and explainability.

## Defining AI Risk Management and Governance

What are AI risk management and governance, and how do they overlap? As outlined below, AI risk management is one important priority concern addressed by AI governance:

AI risk management refers to the process of identifying, assessing, and mitigating the potential risks associated with the development and deployment of AI systems. These risks can include data security vulnerabilities, algorithmic bias, regulatory compliance issues, and ethical concerns.

AI governance refers to the total framework of policies and procedures that guide the ethical and responsible development, deployment, and utility of AI systems. Governance involves setting standards for data management, ensuring transparency in AI operations, and enforcing accountability for decisions made by AI systems.

That means governance is crucial for aligning AI initiatives with an organization's values, legal requirements, and societal expectations—and to help lower risk. By implementing strong AI governance, organizations can build trust with stakeholders, enhance the quality of their AI outputs, and ensure that their AI systems contribute positively to both business goals and broader social outcomes.

## Chapter 3

# The Key to Effective Risk Management: AI Governance

---



“AI regulation: It’s not an abstract possibility, it’s a concrete reality. When we’re thinking about governance, we really need to think about multi-party access and an independent certification.”

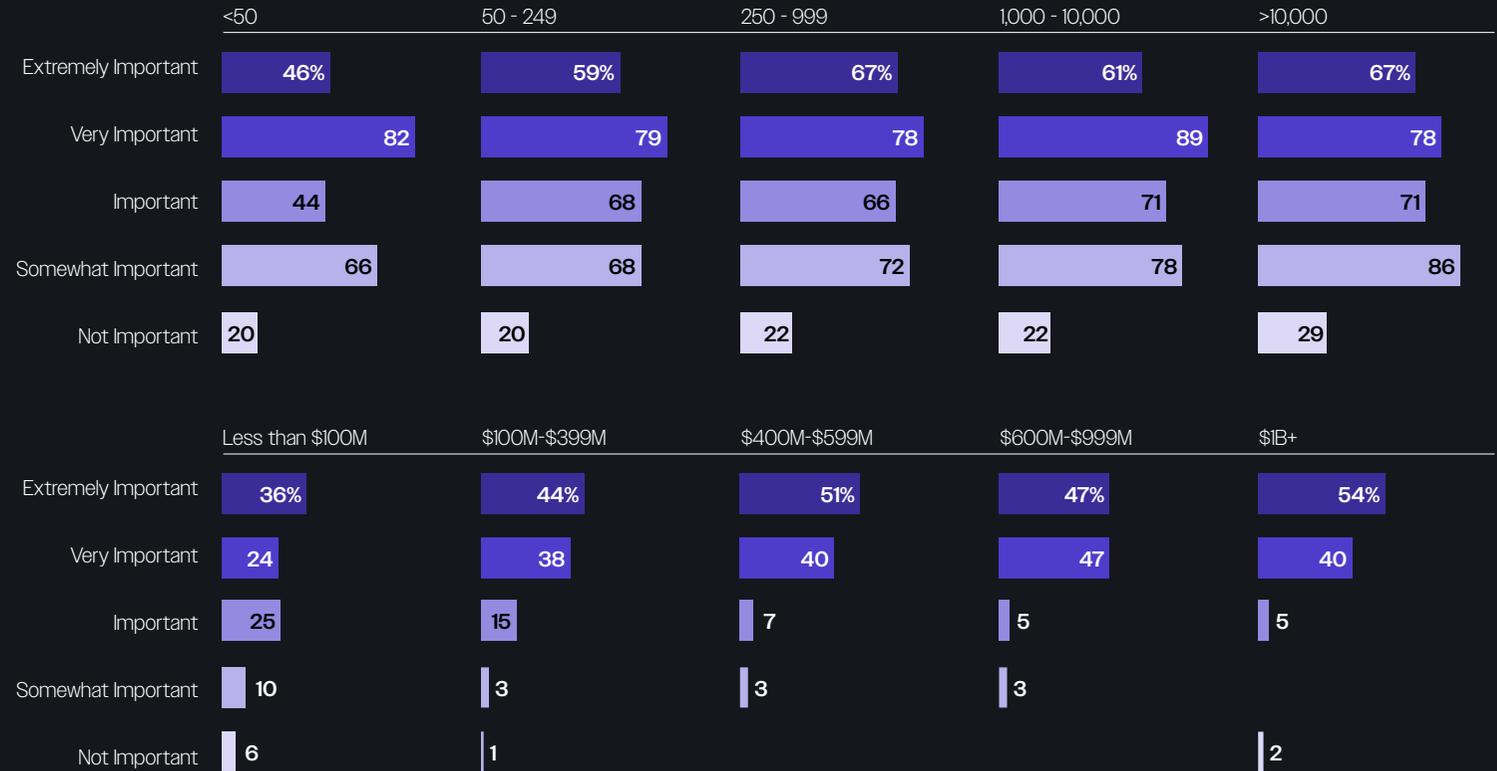
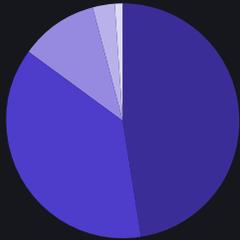
Kay Firth-Butterfield | CEO, Good Tech Advisory

There’s no doubt about the importance of AI governance: companies agree that it’s essential to ensure their technology is safe, compliant, and dependable. But governance will benefit AI growth, too. By allowing companies to develop and deploy AI technology with confidence, governance will accelerate the pace of AI innovation.

To achieve solid AI governance, companies need to lean on emerging technologies that will help better secure and handle data—creating transparency for critical stakeholders. The visibility and control that come from version control and a tamper-proof, immutable ledger—the main advantages of blockchain technology—go a long way toward putting companies in a position to strictly govern their AI data and applications, and ensure the responsibility and compliance of their AI initiatives.

# How important do you believe it is for your organization to prioritize AI governance?

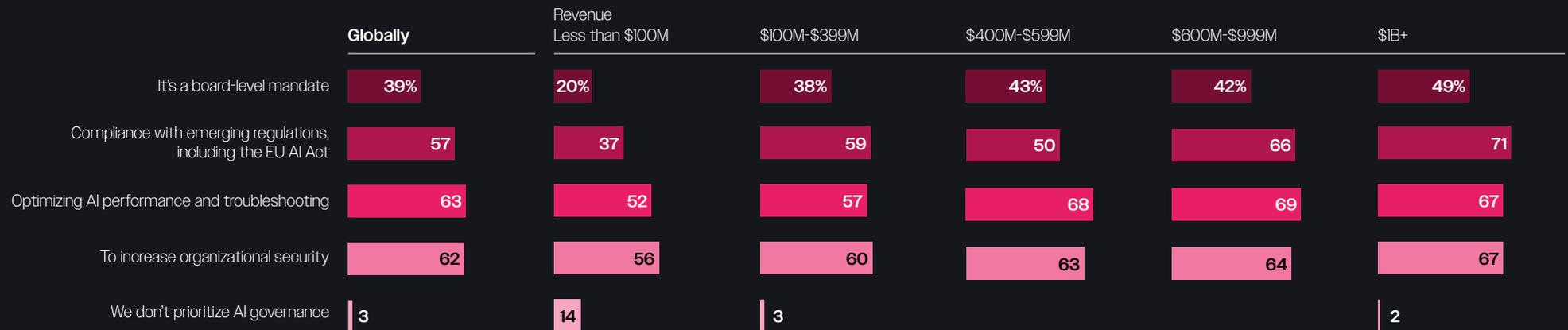
- Extremely Important
- Very Important
- Important
- Somewhat Important
- Not Important



The larger the company (in terms of both employee size and revenue), the more important prioritizing AI governance becomes. For companies with more than 10,000 employees, governance is over **60%** more likely to be considered extremely important (**57%**) than for those with fewer than 250 employees (**35%**). Smaller and lower-earning companies were more likely to consider governance

somewhat important or not important at all. Given that AI adoption is also lower at these companies, the data suggests that wider adoption of AI elicits greater concern over its governance: as users interact more with AI, they're seeing both its risk and the need for safeguards.

# Which of the following rationales best categorizes your organization's motive(s) for AI governance?



The top rationale driving AI governance was the optimization of performance and troubleshooting (**63%**), reinforcing the widespread recognition of the power of AI governance to improve AI model output. For companies with higher revenue, compliance was ranked as more important—almost twice as important to companies with revenue >\$1B+ (**71%**) as to companies with a revenue under \$100M (**37%**). However, other motivating factors seem to increase in priority at higher revenue companies, albeit to a lesser degree.

# Does explainability in AI models impact the likelihood of your organization using the technology in its operations?

Globally

55%

It significantly impacts the likelihood of use

31%

It moderately impacts the likelihood of use

10%

It slightly impacts the likelihood of use

4%

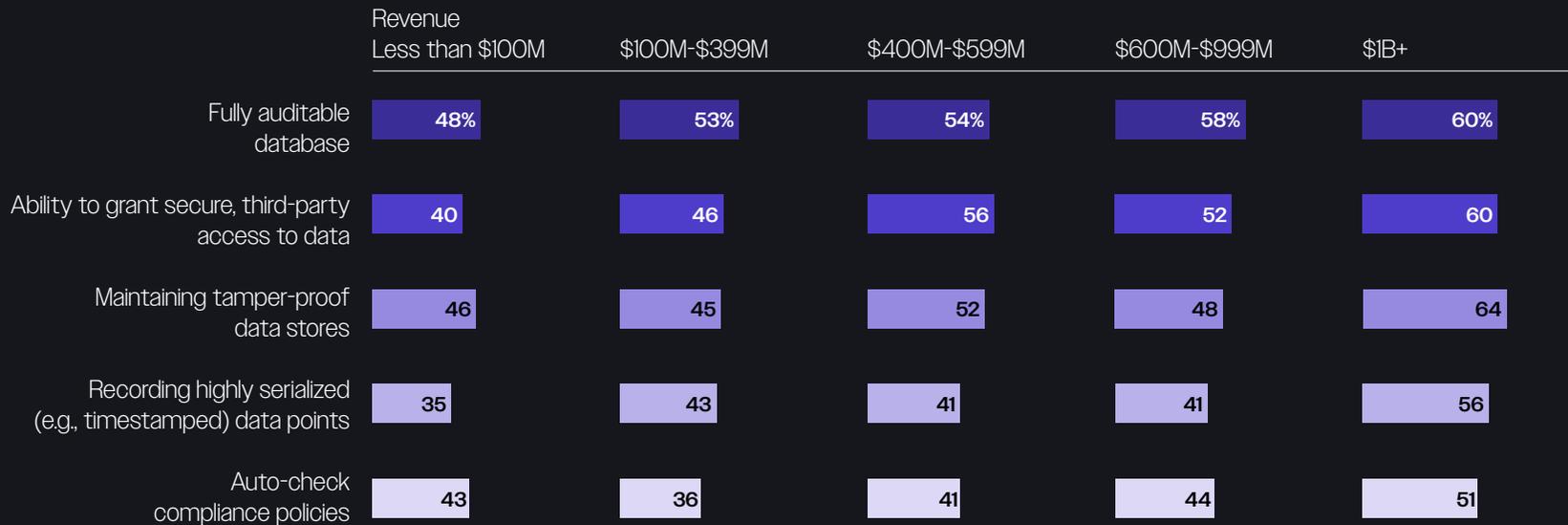
It does not impact the likelihood of use



## 5 Ways Blockchain Helps Govern GenAI

- 1 Understanding training data's origin and history.** To effectively govern genAI systems, it's crucial to know the origin, quality, and characteristics of the data being used by the systems. Understanding this data helps ensure that AI-generated outputs are accurate, unbiased, and reliable, reducing the risk of unintended consequences. Distributed ledger offers a traceable, immutable record of data and data transactions, helping all stakeholders ensure that training data is rock-solid.
- 2 Setting permissions on datasets to address compliance and privacy needs.** Permissions on datasets are vital for maintaining compliance with regulations and protecting sensitive information. By using blockchain to govern multi-party access to training data, companies can safeguard against unauthorized use and ensure that AI systems operate within legal and ethical boundaries.
- 3 Ensuring high-quality input and output data with real-time monitoring measures.** Real-time monitoring of input and output data allows companies to maintain high data quality throughout AI operations. This continuous oversight helps detect and address any anomalies or errors quickly, ensuring the integrity and reliability of AI-driven decisions.
- 4 Enabling version control with a transparent, trustworthy record-keeping system.** Version control is essential for tracking changes to AI models and datasets over time. Blockchain's transparent, tamper-proof record-keeping system ensures that every modification is documented, providing accountability and making it easier to audit AI processes.
- 5 Rooting out performance issues by reviewing time-stamped updates or transactions.** Time-stamped updates and transaction records enable companies to trace the history of AI system performance. This detailed tracking allows for the identification and resolution of performance issues, ensuring that AI systems continue to operate efficiently and effectively.

# Which of the following features do you see as most important when assessing an AI governance solution?



Companies are looking for governance solutions that create auditability, help control third-party access, and tamper-proof data—all strengths of blockchain technology. As a result, blockchain is now poised to meet a key need in the AI governance market.

**Respondents say they're most excited about using blockchain in AI governance to...**

**63%**

Increase the transparency of their AI platform

**58%**

Increase the trustworthiness and reliability of their AI platform

**42%**

Enhance the quality of data outputs in their AI platform

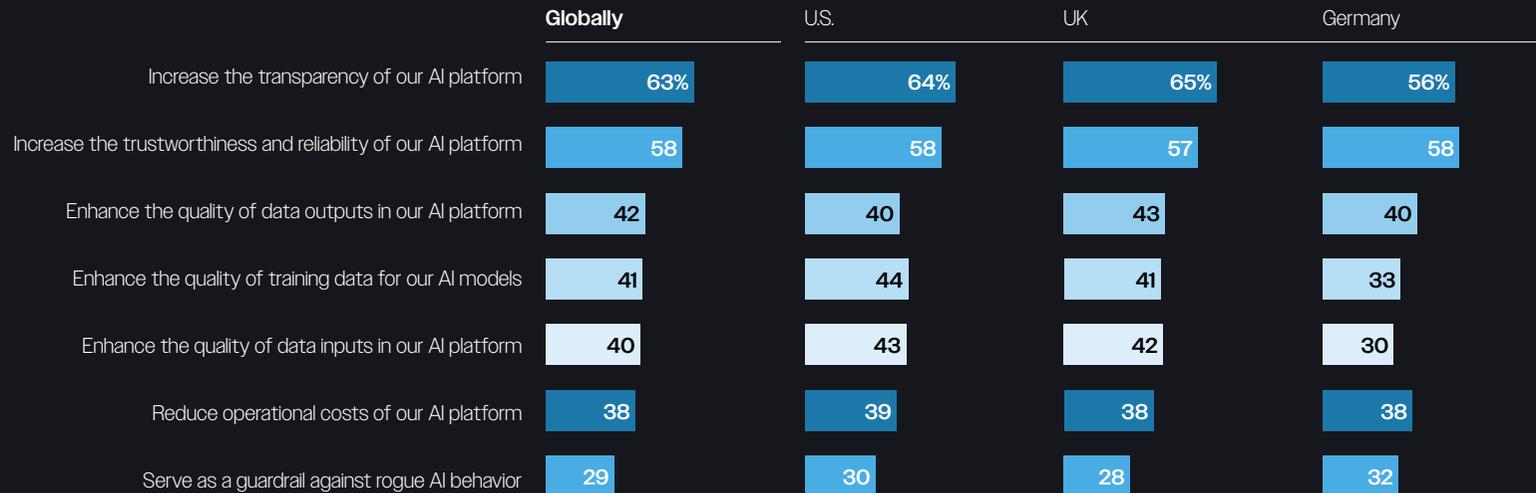
# Which of the following best describes how your organization uses blockchain technology?



More organizations are using blockchain to support their AI initiatives: **57%** of respondents, compared to only **31%** last year.

As distributed ledger technology continues to move away from cryptocurrency applications, it is increasingly being used in a variety of ways across the enterprise. Database automation is the top use case (**67%**), up from **44%** last year.

# Respondents would consider adopting blockchain technology to enhance/strengthen their organization's AI platform if they knew blockchain could:



Executives would be more likely to utilize blockchain-powered solutions if they were proven to address their most pressing AI priorities, including increasing the transparency of their AI platform (**63%**), improving its trustworthiness and reliability (**58%**), and enhancing the quality of data outputs in their AI platform (**42%**).

A growing number—nearly two-thirds—of respondents believe that using AI and blockchain together can revolutionize their industry through better data security, transparency, and efficiency: **63%** compared to only **48%** last year.

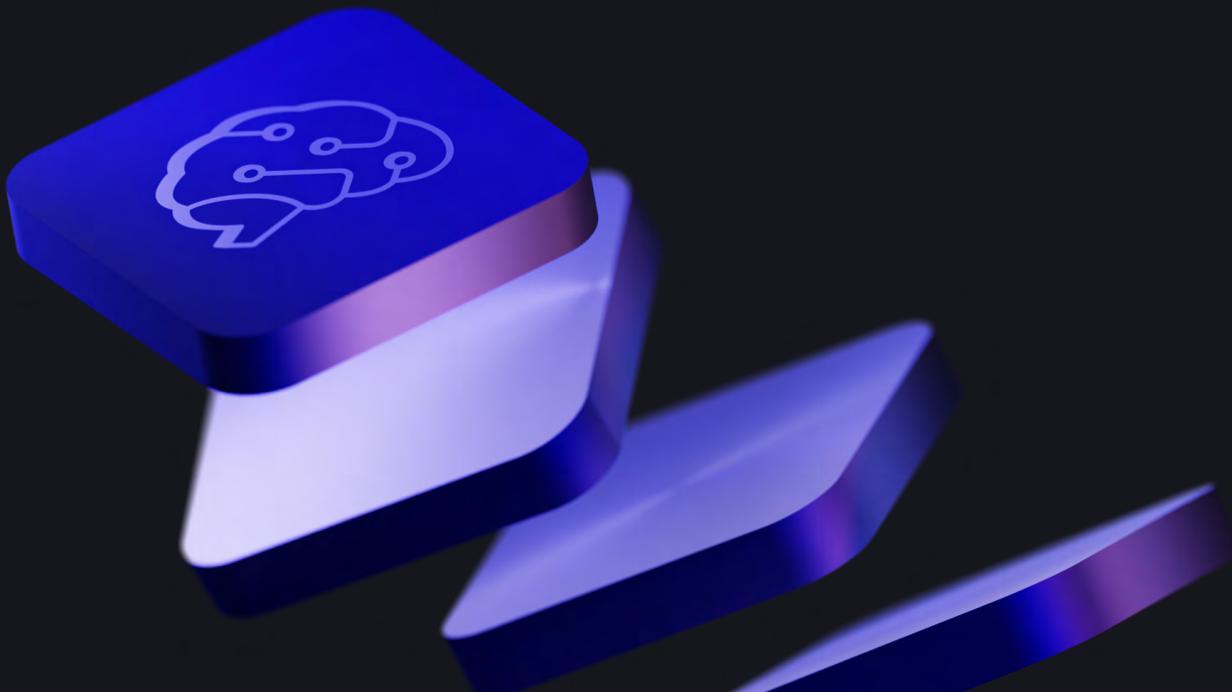
## Chapter 4

# AI Governance Readiness

---

“Lorem ipsum.”

First Last | Title, IBM

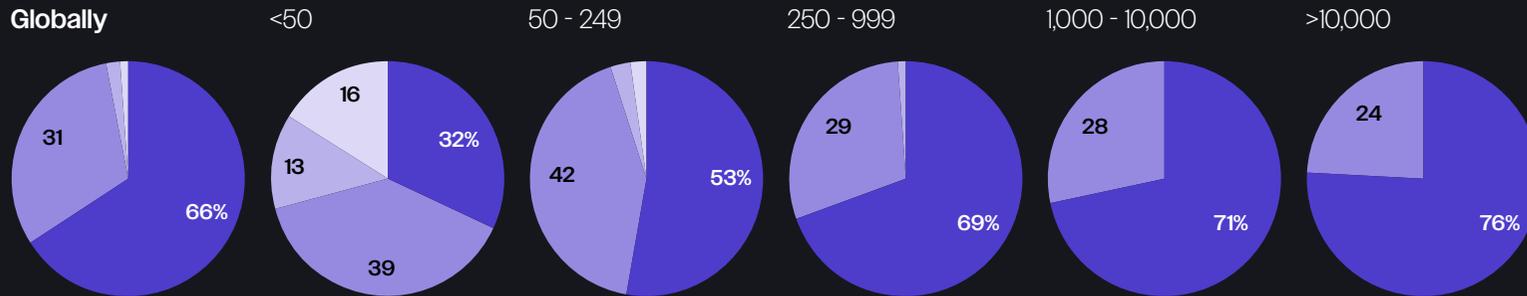


Companies know that more AI regulation is on the horizon. And while they might welcome it, some may be blissfully unaware of their lack of preparedness for upcoming regulations. In fact, some may be overestimating their current ability to adapt and remain compliant in a changing regulatory landscape.

This survey's results suggest there is an opportunity to educate companies about AI governance as a core part of risk management for their businesses. While confident in their current risk management capacity, few have put a comprehensive governance solution into production. There's a pressing need for AI governance—and an opportunity for blockchain to answer the call.

As organizations develop a better understanding of AI and AI governance, confidence is high in current governance capabilities.

# Does your organization believe its AI governance strategy is sufficient to keep up with evolving regulations?



- Yes, our AI governance strategy is adequately equipped to keep up with evolving regulations.
- Somewhat, our AI governance strategy may need adjustments to align with evolving regulations.
- No, our AI governance strategy is not sufficient to keep up with evolving regulations.
- I don't know.

Two-thirds (**66%**) of respondents believe their AI governance strategy is equipped to handle an evolving regulatory landscape. This number is even higher for those with over 10,000 employees (**76%**), while those with fewer than 250 employees are more likely to consider themselves unprepared and even uninformed.

# My organization is doing a good job with AI risk management today.

## Globally

**55%** **31%**

Strongly Agree

Agree

**10%** **4%**

Disagree

Strongly Disagree

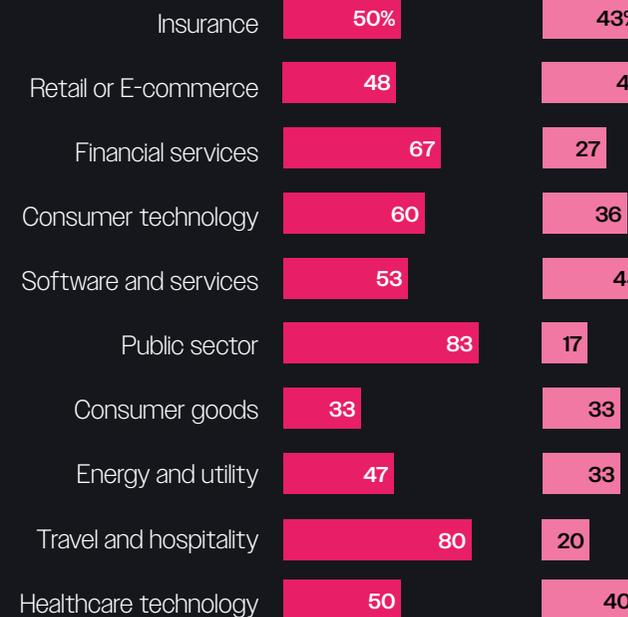
Nearly all (**95%**) respondents agreed or strongly agreed that their organization is doing well with AI risk management today and compliant with all industry and regulatory standards.

Just as in governance, larger companies display greater confidence in AI risk management, with **72%** of respondents at companies with over 10,000 employees indicating that they strongly agreed. While smaller companies display more hesitance in their risk management, they're still largely optimistic: **87%** of companies with fewer than 50 employees and **89%** of companies between 50 and 249 employees agreed they were doing a good job at risk management.

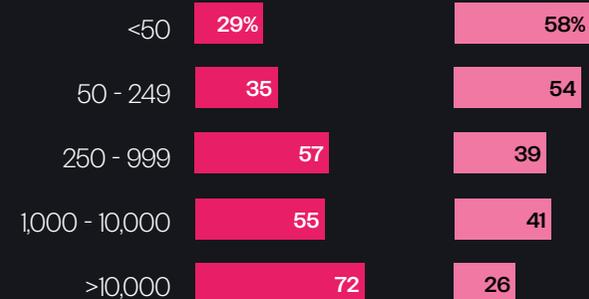
Across industries, confidence is lower among respondents in insurance, consumer goods, and staffing and recruiting. Confidence is highest among the respondents in the public sector, travel and hospitality, and automotive sectors.

Strongly Agree Agree

## By industry:

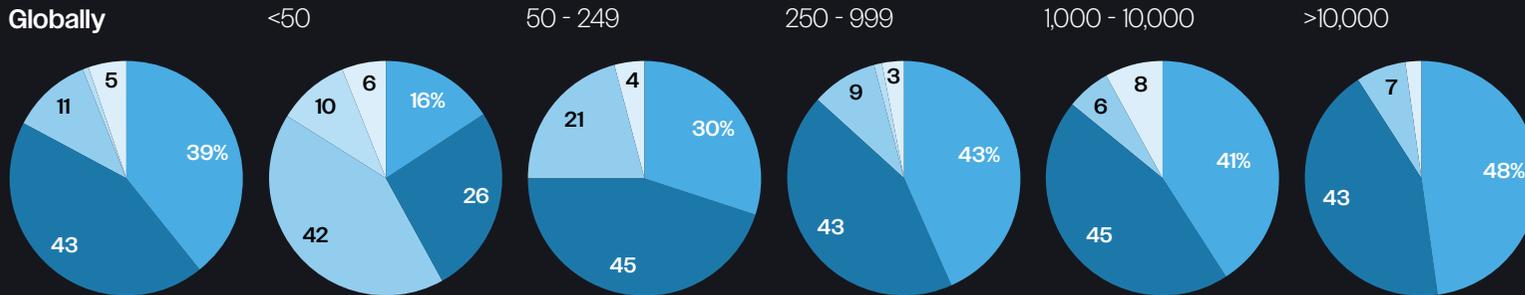


## By Company size:



But is this confidence unearned?

# Based on your current, 12-month outlook for working with AI technologies, how pressing is the need for your organization to implement a robust AI governance solution?



- Extremely pressing
- Somewhat pressing
- Not pressing
- N/A - my organization isn't currently using AI in a meaningful way
- N/A - my organization has already deployed a comprehensive AI governance solution

Just 5% of respondents said they have already deployed a comprehensive AI governance solution. And 82% believe their organization has a somewhat or extremely pressing need to implement a robust AI governance solution.

Likely, many companies don't fully understand how AI governance serves as an essential—and increasingly important—component of risk management. As AI capabilities proliferate, AI governance will help bake in risk management from the ground up, ensuring that all elements of AI risk are addressed.

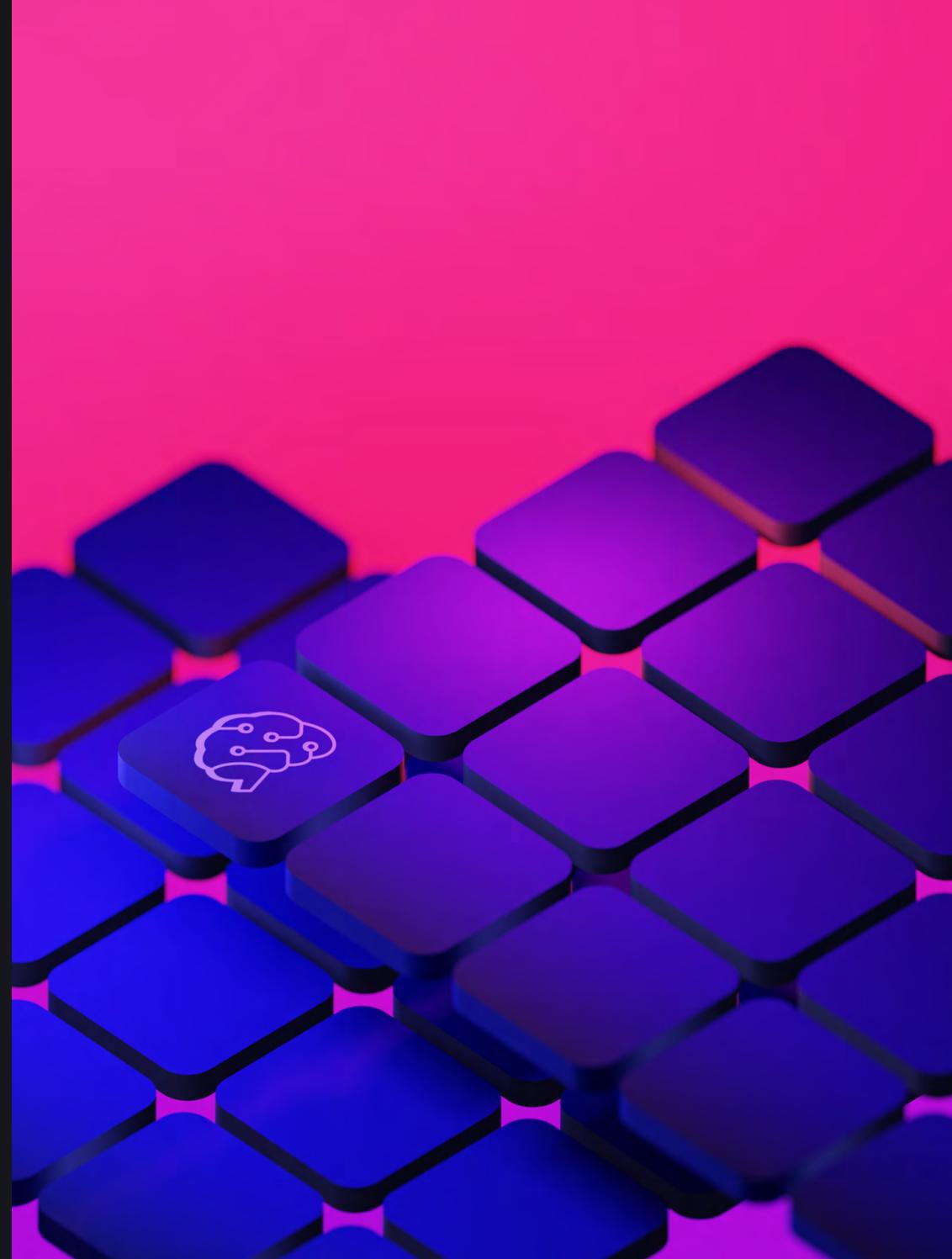
# Conclusion

AI is a transformative force reshaping industries, redefining business processes and challenging long-established norms for organizational decision-making. The potential of AI is vast, but so are the challenges that come with harnessing its power responsibly.

The results of this survey are clear: business leaders recognize the risk inherent in AI, and the resulting need for robust governance and overall data transparency. The systems built today will shape the future of AI for years to come.

The responsibility for navigating this complex landscape doesn't lie with a single player. It will take businesses, regulators, and technologists working hand in hand to build the frameworks that will optimally govern AI and drive improvements in performance and utility. Only through joint efforts can organizations develop the robust governance structures needed to ensure that AI remains a tool for progress and innovation, rather than a source of inherent risk.

Looking ahead, organizations must continue to prioritize AI governance as a foundational element of their AI strategies. This involves not only adhering to regulatory requirements, but also taking proactive steps to ensure that AI systems are transparent, fair, and accountable using the best-emerging technologies available today. Doing so will increase trust in AI, mitigate risks and unlock its full potential.





# About Prove AI

Through distributed ledger technology, Casper Labs has created a governance solution for AI data management that is the first of its kind. Prove AI supports auditability, offers version control, governs multiparty access, and creates an immutable record of data transactions—making data tamperproof.