

# AI TRENDS 2025

Four key AI trends affecting CIOs.

# FOUR AI TRENDS FOR 2025

In this report, we explore four AI trends for emerging and leading-edge technologies and practices that can improve the capabilities needed to meet the ambitions of your organization.

01

AI Strategy

The CIO and IT are the ones asked most often to lead the development of the organization's AI strategy.

02

AI Ecosystem

The ecosystem of AI tools and solutions continues to evolve and grow.

03

AI Regulations

AI regulations and legislation are emerging and continuing to grow.

04

Deepfake  
Threats

Use of AI to create very realistic deepfakes is on the rise and is a threat to individuals and the democratic process.



# Nearly 1,000 survey responses from IT leaders

## The Future of IT 2025 survey

The *AI Trends 2025* report is based on the Future of IT 2025 survey conducted in May and June 2024.

Most respondents were in North America, but countries around the globe were represented.

Over half of respondents held director-level or more senior positions.

### Top industries represented:

- Government/Public Sector
- Financial Services
- Media, Information, Telecom
- Education
- Healthcare



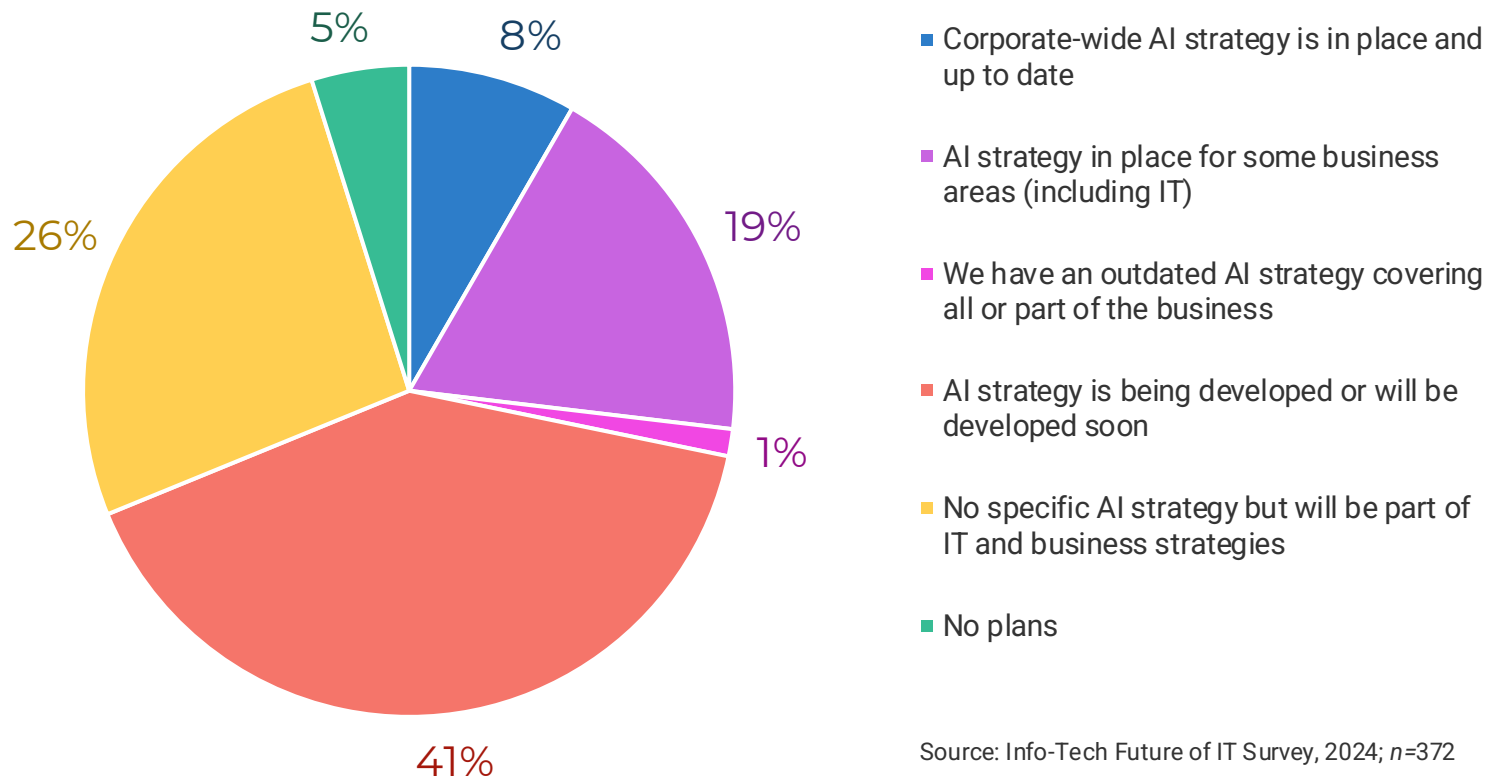
## TREND 1

# IT Takes the Lead for Developing AI STRATEGY



# AI strategy is new for most organizations

What best describes your organization's approach to AI strategy?



Source: Info-Tech Future of IT Survey, 2024; n=372

## INSIGHTS

Developing an AI strategy is new for most organizations.

- 41% of respondents said an AI strategy is being developed or will be developed soon.
- 26% said there is no specific AI strategy, but AI will be part of IT and business strategies.

# Challenge: Creating value

When it comes to harnessing AI to create value, rank the following challenges for how much they hinder the adoption of your AI initiative.

Challenge	Order of average ranking
Lack of AI or data management skills	1
AI governance	2
Data platform not optimized for AI	3
Complexity of integration/selecting use case	4
Lack of budget or executive support	5
Inability to manage AI risks	6
Cultural resistance	7
Lack of automated tools	8
Lack of infrastructure	9

## INSIGHTS

Many business and technical challenges present barriers to successfully deploying and adopting AI initiatives.

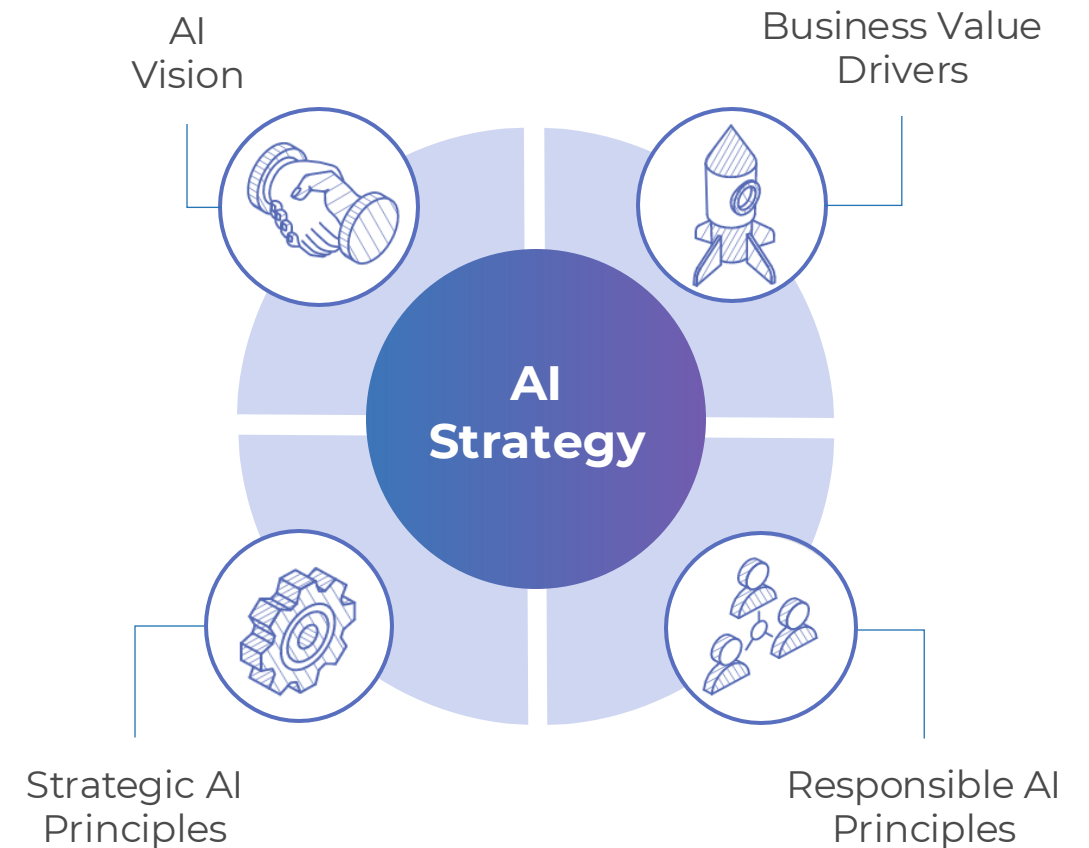
- Lack of skills and AI governance are the most difficult challenges.
- Having the proper data platform and selecting the right AI use case to pursue were also noted as significant challenges.

# AI strategy needs to align with the organization's corporate strategy

Strategy should be driven by the stakeholders of the organization and focused on delivering improved business outcomes

A business-driven AI strategy is aligned with the organizational strategy. Key components of the AI strategy include:

- **AI Vision:** The AI vision statement is usually forward-looking and aspirational and reflects the organization's commitment to leveraging AI to deliver positive and responsible outcomes.
- **Business Value Drivers:** These drivers represent the ways value is recognized by the organization and are used to ensure candidate AI initiatives are aligned to the goals and objectives of the organization.
- **Strategic AI Principles:** These guiding principles align the business strategy with the AI strategy and reflect the organization's overall approach to the use of AI.
- **Responsible AI Principles:** These guiding principles govern the development, deployment, and maintenance of AI applications to mitigate the possible risks from deploying AI-based applications.



# AI strategy is driven by vision, mission, and strategic principles

## AI Vision

Responsibly and securely explore artificial intelligence to build an organization that is digitally enabled, agile, able to grow, and focused on delivering valuable, cost-effective solutions.

## AI Mission

Create groundbreaking product innovations, make our products more sustainable, build a creative and diverse global team, provide a great employee experience, include the human aspect in all that we do, and make a positive impact in communities where we live and work.

## AI Guiding Principles



01

### Leverage AI to Augment Employees' Contribution

We prioritize people at the heart of our AI solutions, ensuring their wellbeing, dignity, and active and equitable involvement in decision-making.



02

### Empower and Enhance (Workforce Wellness)

We empower our team members and enhance their work experience, making it easy to do their best work.



03

### Buy Over Build

We will prioritize the sourcing of existing market solutions over the in-house building of machine learning models.



04

### Be Human-Centric

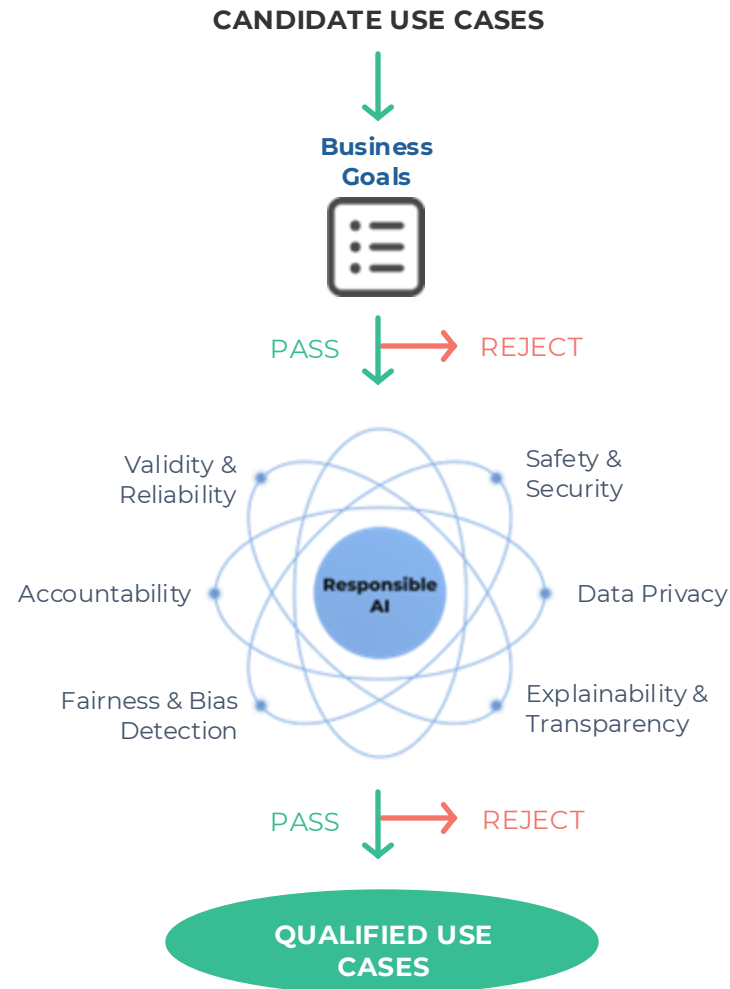
Prioritize the development and adoption of AI solutions that complement and enhance human skills, creativity, and judgment, rather than automating them away.



# Use cases need to align to the business objectives and responsible AI principles

## Business alignment

- Business risk
- Business value
- Regulatory/legal compliance
- Supports organization's value proposition



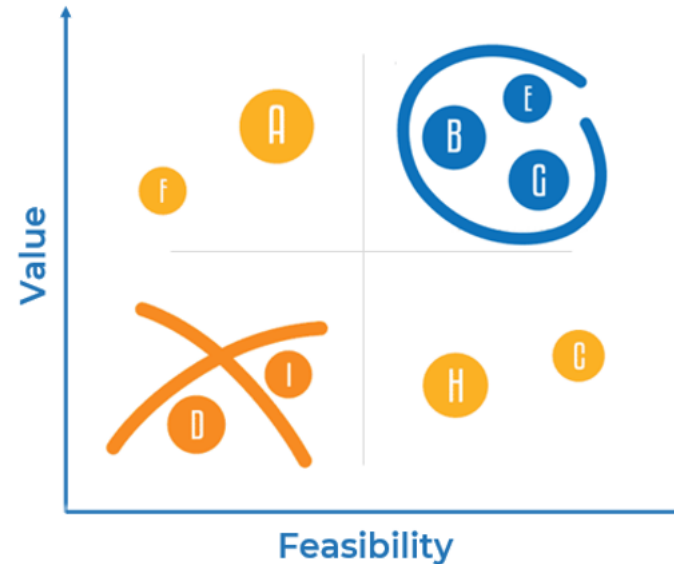
## Responsible AI alignment

- Validity and reliability
- Safety and security
- Data privacy
- Explainability and transparency
- Fairness and bias detection
- Accountability

# Prioritize AI use cases by assessing business value vs. feasibility

## Business value drivers

- Improve customer experience
- Drive revenue
- Improve operational excellence
- Accelerate innovation
- Mitigate risk



## Project feasibility characteristics

- Complexity/integration/risk involved
- Resources (people, process, technology...)
- Costs (acquisition, operational, support...)
- Risk
- Stakeholder support

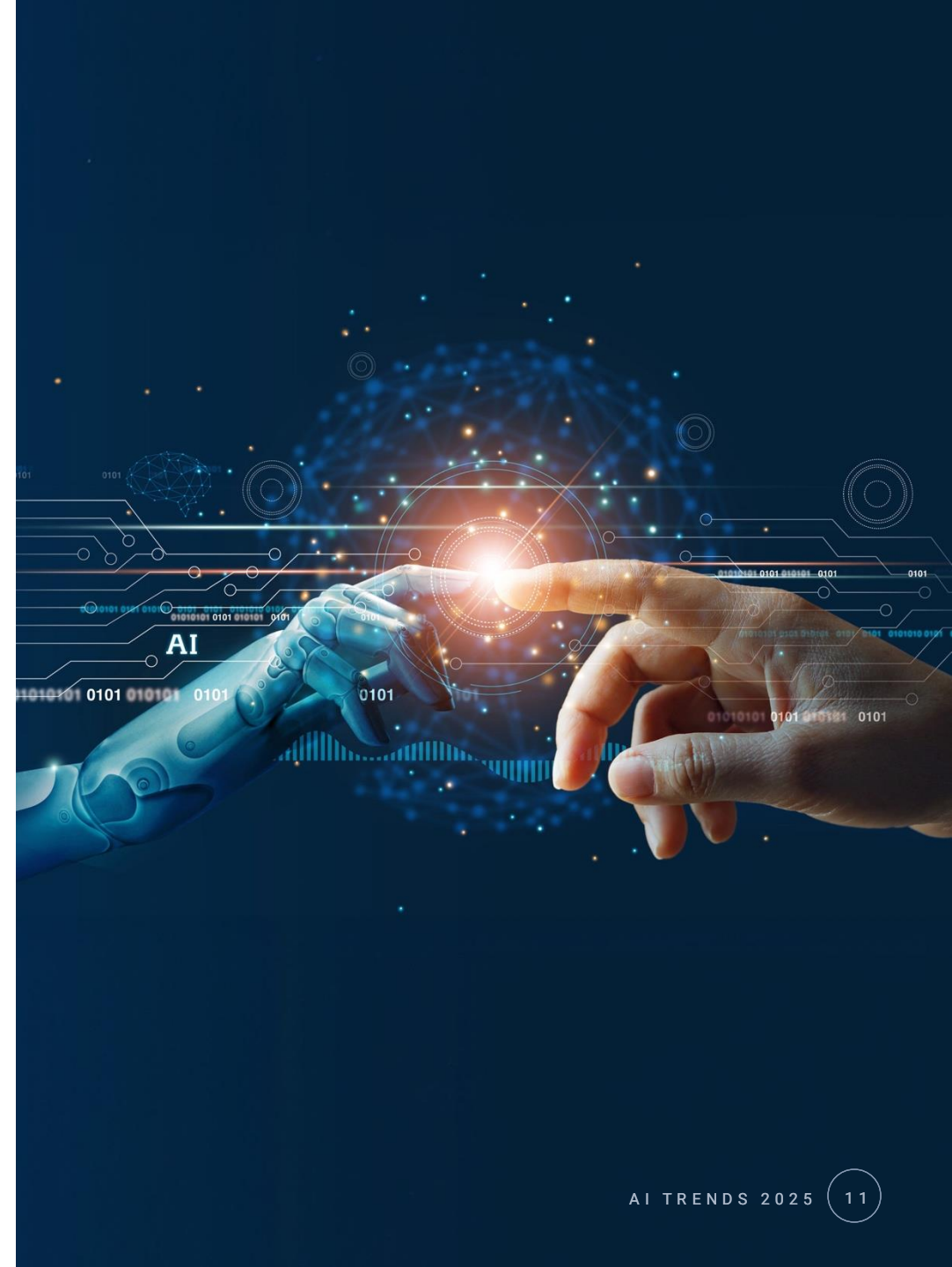
# Opportunities and threats

## Opportunities

- Increase operational efficiencies
- Improve the customer/user experience
- Increase growth initiatives
- Introduce innovation into workflows
- Improve risk mitigation

## Threats

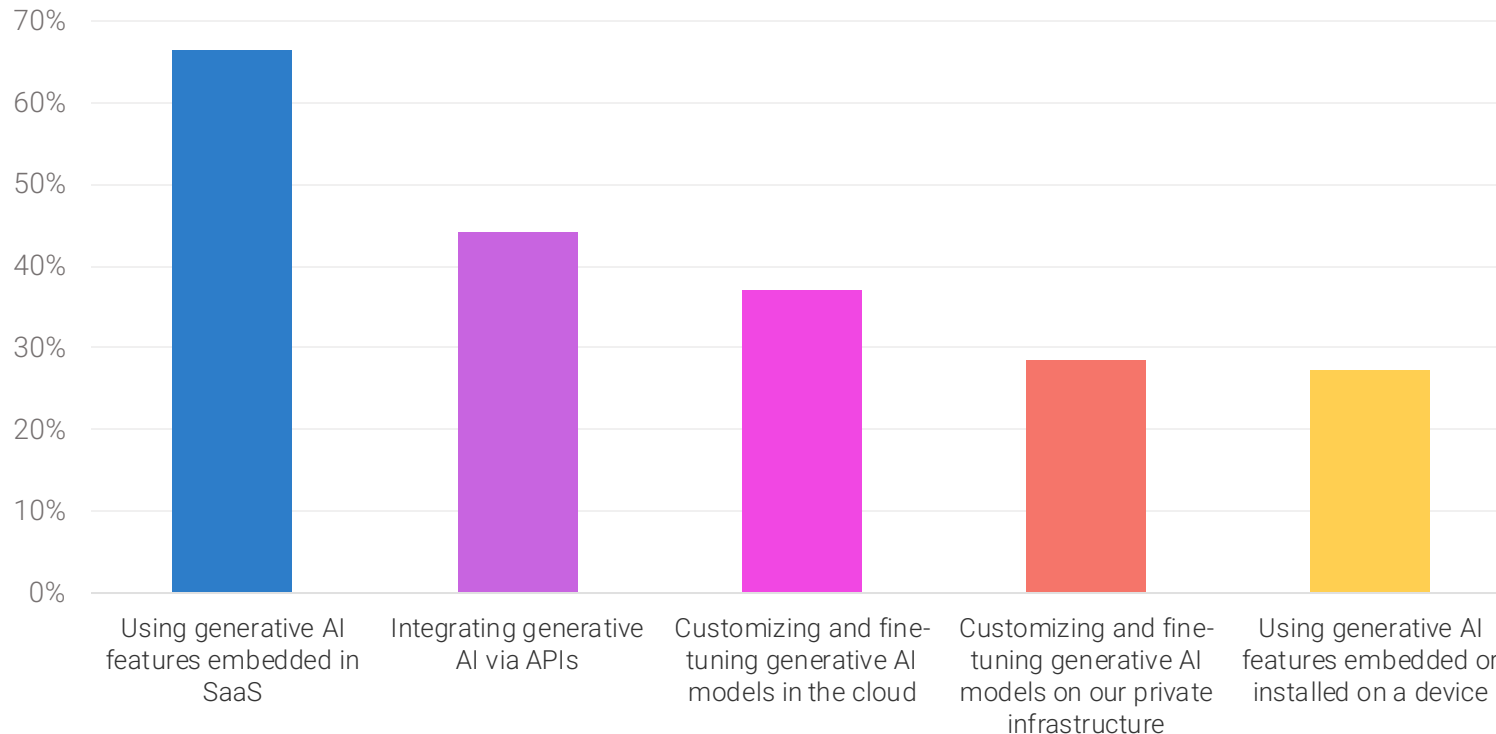
- Work disruption/possible job displacement
- Possible bias in responses
- Creation of misinformation campaigns
- Privacy concerns about the use and sharing of data
- Use of deepfakes for identity theft or fraud





# Organizations prefer to access generative AI through applications

**How does your organization plan to make use of generative AI from now through the end of 2025?**



Source: Info-Tech Future of IT Survey, 2024; n=183

## INSIGHTS

Many organizations want to purchase applications (software as a service) that include generative AI capabilities rather than building generative AI capabilities themselves.

# JPMorgan Chase: The AI industry leader in financial services

## Situation

The financial services sector is an extremely competitive industry, with firms constantly searching for new ways to differentiate their offerings. AI has the potential to augment and transform every banking line of business. At JPMorgan Chase, key business drivers for AI initiatives focus on:

- Improving customer experience.
- Reducing risk.
- Increasing efficiencies.

For the underlying data platform that supports the bank's analytics and AI applications, the bank has adopted a data mesh architecture to produce data products, groups of data from systems that support the business. Product-specific data lakes are built to support the data groups. Each data lake is separated by its own cloud-based storage layer. The bank catalogs the data in each lake using storage and data integration technologies from its cloud platform.

Jamie Dimon, JPMorgan Chase chairman and CEO, has stated: *"Over time, we anticipate that our use of AI has the potential to augment virtually every job, as well as impact our workforce composition. It may reduce certain job categories or roles, but it may create others as well. As we have in the past, we will aggressively retrain and redeploy our talent to make sure we are taking care of our employees if they are affected by this trend"* ("Chairman and CEO Letter," JPMorgan Chase, 2024).

## Action

The bank leads the industry in several areas:

- It invests \$12 billion annually in technologies, which include AI.
- It employs more than 2,000 AI/machine learning experts and data scientists.
- The bank employs over 200 AI researchers and decisively leads the pack in AI research, representing 35% of all AI researchers affiliated with banks in the Evident AI Index – greater than the next seven largest teams combined (Evident AI, 2024).
- A prompt engineering course is mandatory for new hires.

The organization has plans to deploy AI across the entire enterprise. Its more prolific AI applications include the following:

- LLM Suite, available to more than 60,000 employees, acts as a portal to external large language models to provide productivity assistance for users writing reports or drafting emails.
- Quest IndexGPT is JPMorgan's first client-facing offering leveraging generative AI. This uses GPT-4 to deliver greater efficiency, accuracy, and speed when constructing an investment index. It allows a more representative selection of keywords as search parameters when researching prospective companies to be part of the index.
- The COIN (Contract Intelligence) Platform for Legal Documents Analysis processes approximately 12,000 commercial credit agreements annually with a near-zero error rate, saving upwards of 360,000 hours of human work (JP Morgan Journal of Machine Learning, 2021, as cited in AtliQ, 2024).

## Results

- In 2024, JPMorgan Chase recorded the highest annual profit for a US bank, with a revenue of \$155.29 billion.
- JPMorgan Chase increased its share of new banking industry AI research from 30% in 2018 to 45% in 2023 ("The Dispatch," Evident AI, 2024).
- Regarding the AI use cases deployed, according to the CEO in May 2024: *"So, I think we said that there are 400 use cases probably, by the end of this year maybe 800"* ("Bernstein Strategic Decisions Conference," JPMorgan Chase, 2024).
- Regarding the business value of AI, Daniel Pinto, JPMorgan Chase president and chief operating officer, stated, *"[R]oughly the value that we assign to our artificial intelligence use cases is around between \$1 billion to \$1.5 billion and is in the fields of customer personalization, trading, operational efficiencies, fraud manager, credit decisioning"* ("2024 Investor Day," JPMorgan Chase, 2024).

While the overriding trend is to have the CIO and the IT department lead in the development of the organization's AI strategy, JPMorgan Chase stands out as an exception because it is the CEO who is leading and driving the organization's AI strategy. JPMorgan Chase's dominance in financial services is a direct result of its investment in AI and elevation of AI strategy as being an integral part of its corporate strategy and driven from the office of the CEO.

# Trend summary

## Trend scenario

Organizations will continue to be pressured to implement AI solutions quickly to drive improved business outcomes.

- Many are proceeding without a full business case.
- Safeguards and governance are lacking.

## Next steps

Enable the organization to leverage generative AI.

**Assemble a strong team.**

- Consider involving partners.

**Focus on driving business value.**

- Improve operational excellence.
- Improve the human/AI experience.

**Prepare to upgrade your organization's AI maturity.**

- Data management and AI governance will often require focus.





The background is a vibrant, futuristic scene. It features several glowing circular elements, possibly representing data or energy, with bright blue and purple light streaks radiating from them. The overall color palette is dominated by deep blues, purples, and bright whites from the light effects.

TREND 2

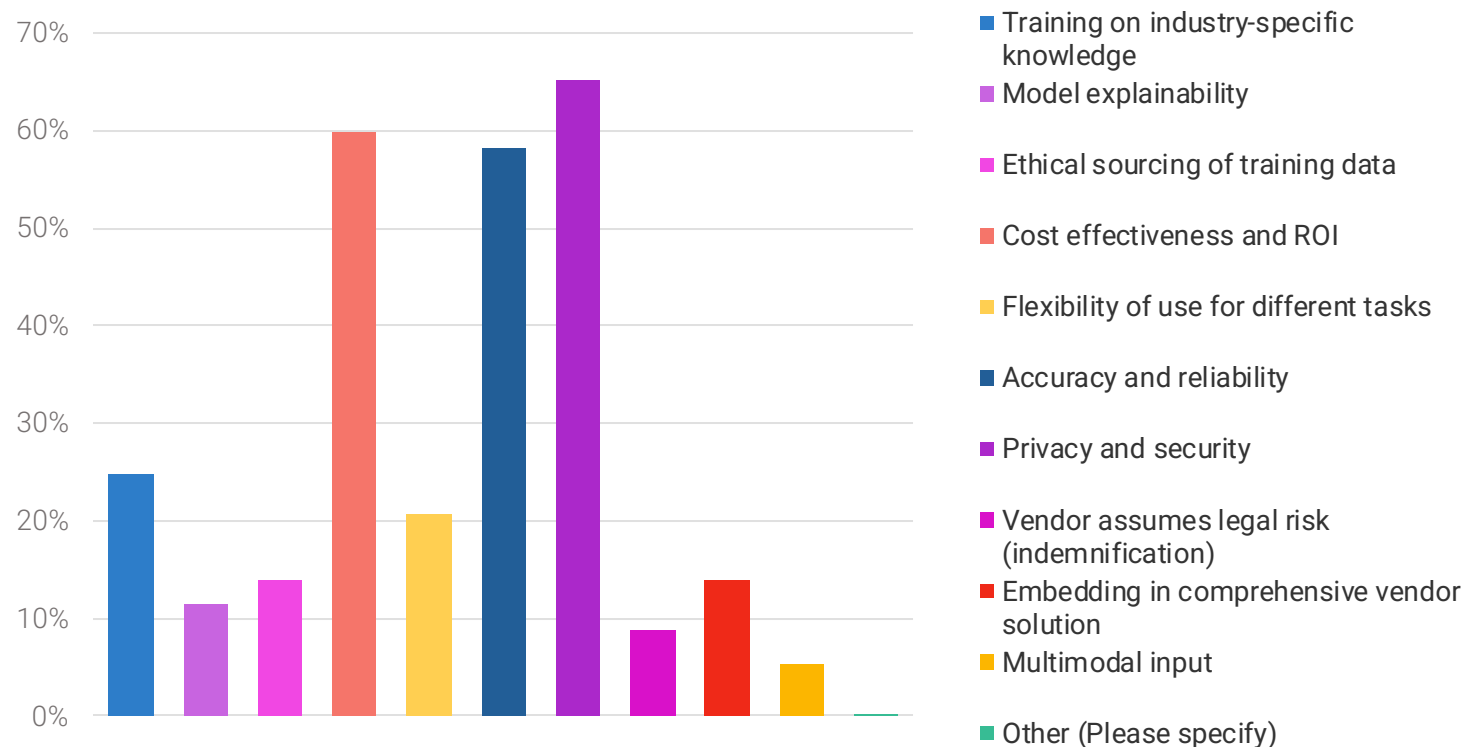
# AI ECOSYSTEM

Solution-Based Offerings  
Are Leading Assessments



# Privacy and security are the top requirement when selecting an AI vendor solution

**What are the most important factors that will determine what generative AI solutions you invest in? (Select up to 3)**



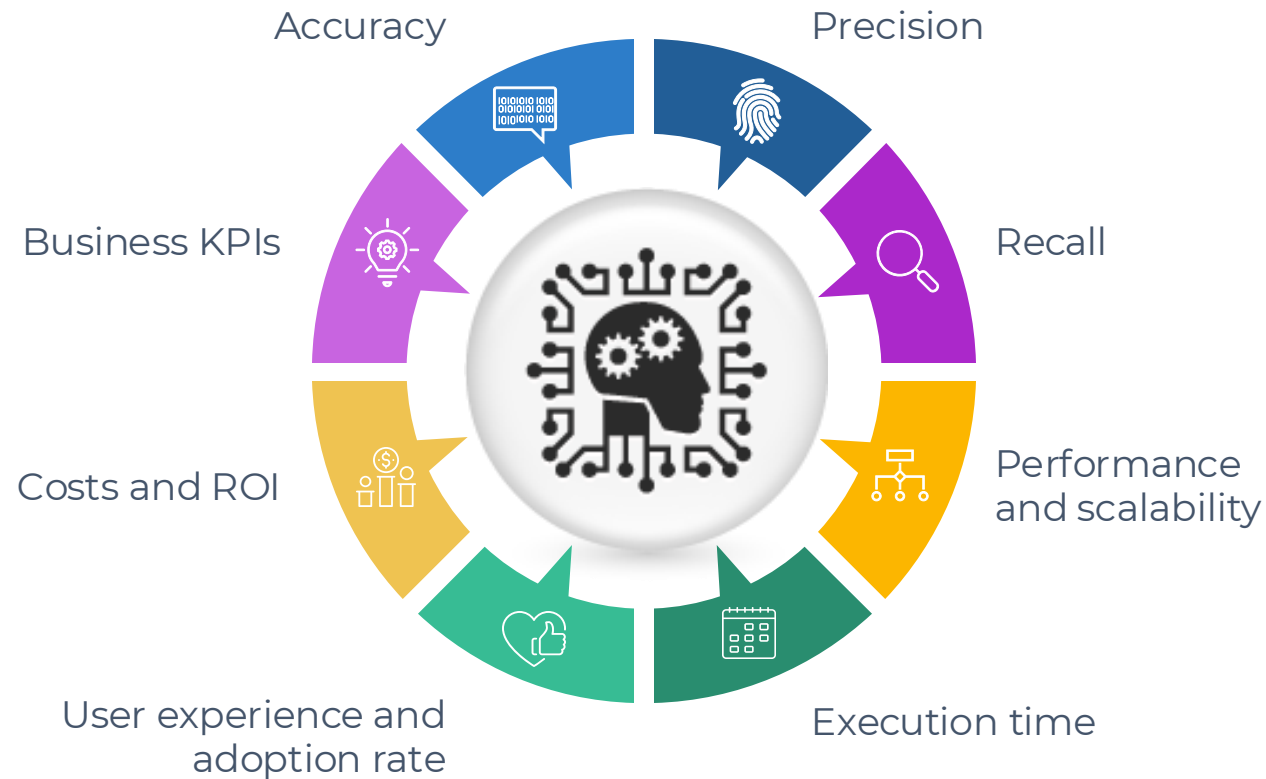
Source: Info-Tech Future of IT Survey, 2024; n= 339

## INSIGHTS

### Top considerations

- Privacy and security (65.19%)
- Cost-effectiveness and ROI (59.88%)
- Model accuracy and reliability (58.11%)

# Solution vendor selection criteria – candidate capabilities to evaluate



































































## INSIGHTS

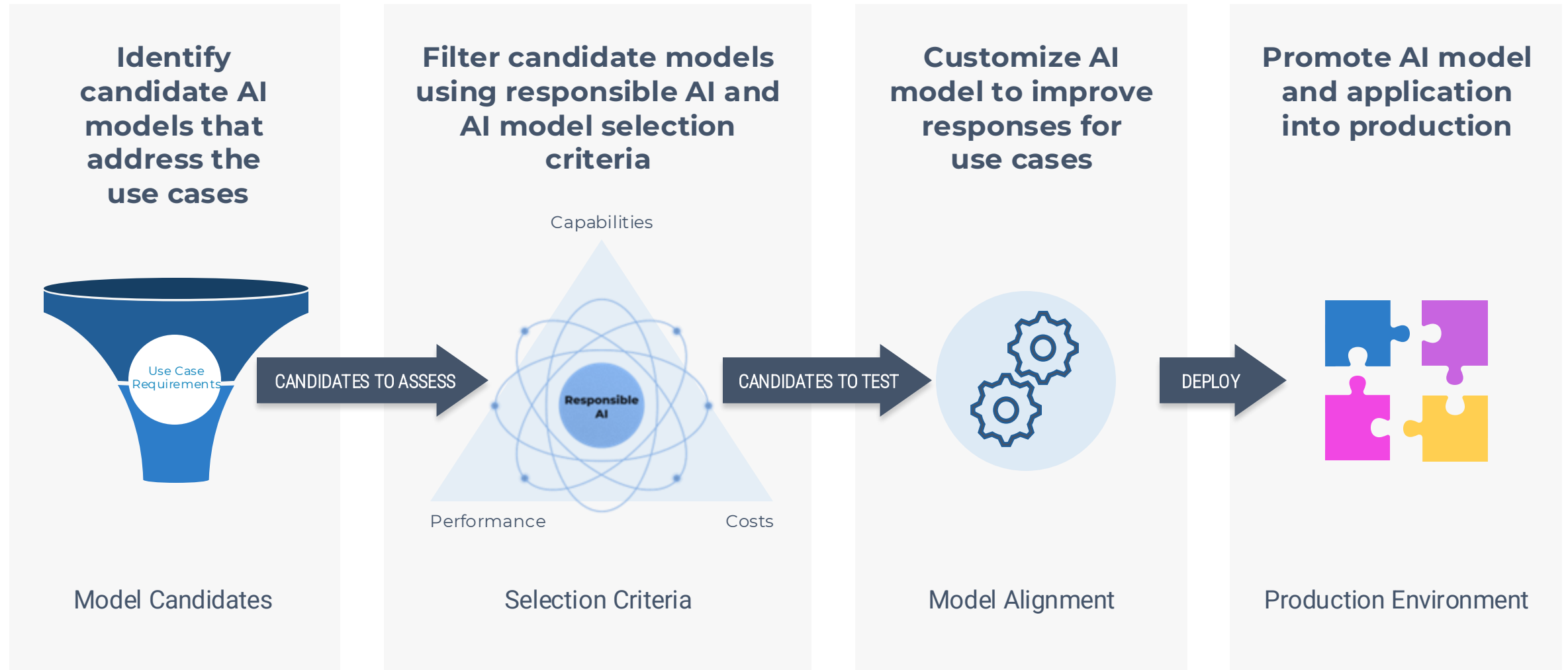
In addition to functional capabilities, assess any potential AI solution's compliance with policies your organization has established to mitigate AI risks and ensure privacy, validity, reliability, and security.



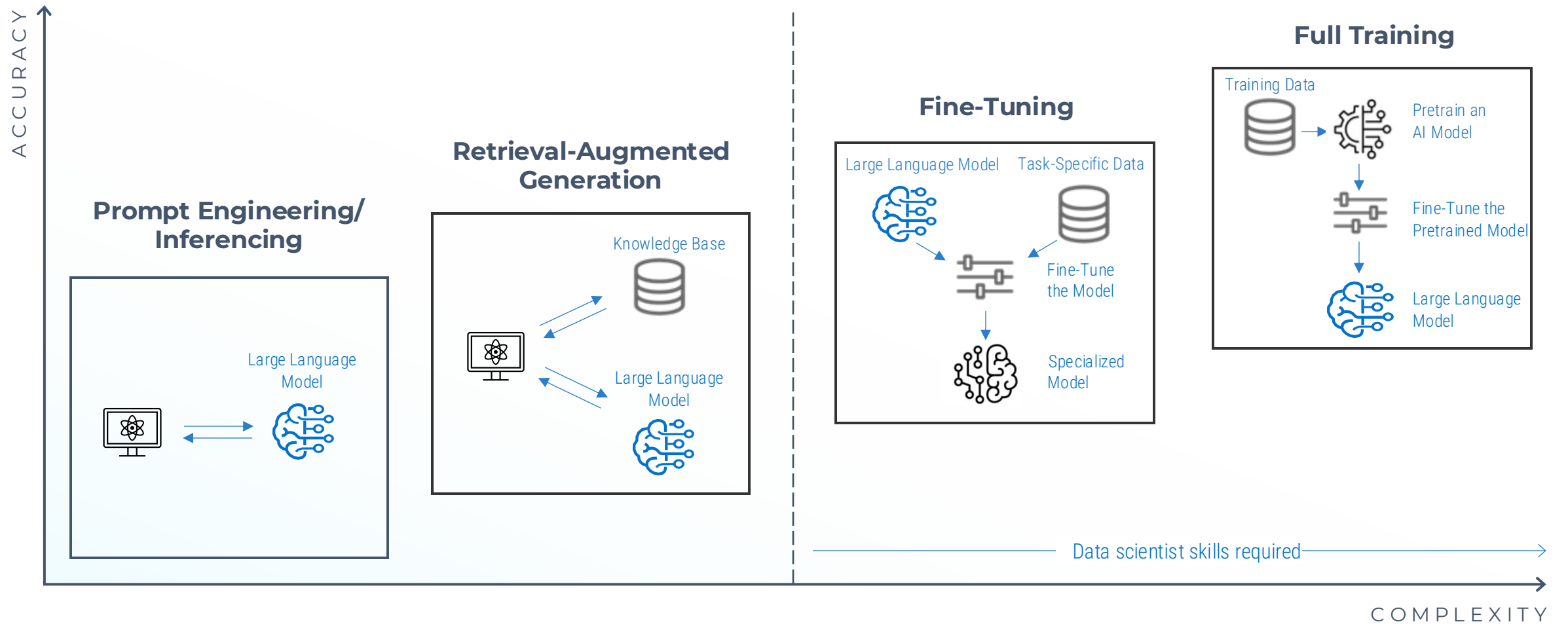
# The AI ecosystem continues to grow

<b>Applications</b> (the fastest growing category)	 Copilot         Your generative AI assistant for work     
<b>Foundational Model Platforms</b>	               
<b>Data Platforms</b>	           
<b>Systems Software</b>	        
<b>Infrastructure</b>	             <ul style="list-style-type: none"> <li>• Spectrum-X</li> <li>• BlueField-2</li> </ul>

# Challenge: AI model selection is complex



# Customizing the large language model can be complex and introduces a new ecosystem of tools





# Foundation Model Ops, MLOps, and DataOps tools are evolving

	AWS	Azure	Google	Third-Party	Open-Source
FMOps					
Foundation Model	Anthropic, AI21 labs, Cohere, Meta, Mistral, Stability AI	GPT-4, GPT-4o, OpenAI o1, Cohere, Meta, Mistral	Gemini, Gemma, Anthropic, Meta, Mistral	Hugging Face Transformers	BLOOM
Model Deployment	Amazon SageMaker, Amazon Bedrock	Azure ML	Vertex AI	LangChain	TensorFlow
Fine-Tuning	Amazon SageMaker, Amazon Bedrock	Azure OpenAI	Vertex AI	Mosaic	Stability AI
Low-Code Development	Amazon SageMaker Canvas, AWS App Studio	Power Apps	Gen App Builder	Dataiku	Budibase
Vector Database	Amazon OpenSearch/Aurora/RDS/DocumentDB, Vector Search for Amazon MemoryDB	Cosmos DB	Cloud SQL	Pinecone	Milvus
Code Completion	Amazon Q Developer	GitHub Copilot	Duet AI	Tabnine	Jedi
MLOps					
ML Platform	Amazon SageMaker	Azure ML	Vertex AI	DataRobot	Kubeflow
Bot	Amazon Q Business, Amazon Lex	Microsoft Bot Framework	Dialogflow	Chatfuel	Botpress
Speech	Amazon Polly, Amazon Transcribe	Azure AI Speech	Speech-to-Text/Text-to-Speech	Verint	SpeechBrain
Video	Amazon Rekognition Video	Video Indexer	Video AI	Final Cut Pro	OpenCV
NLP	Amazon Comprehend	Text Analytics	Natural Language AI	Sentiment Analysis	Natural Language Toolkit
Translation	Amazon Translate	Translator	Translation AI	DeepL Translate	OpenNMT
DataOps					
Relational Database	Amazon RDS	SQL Database	Cloud SQL	Snowflake	PostgreSQL
NoSQL	Amazon DynamoDB	Cosmos DB	Firestore, Bigtable	MongoDB	Apache Cassandra
Caching	Amazon RDS, DynamoDB, MongoDB, Apache Cassandra	Cache for Redis	Memorystore	Redis	Memcached
Big Data	Amazon EMR	Data Lake Storage	Dataproc	Databricks	Apache Hadoop
Data Integration	AWS Glue	Synapse Studio	Cloud Data Fusion	Informatica	Apache Camel

The tools presented are illustrative examples and do not represent a comprehensive list.

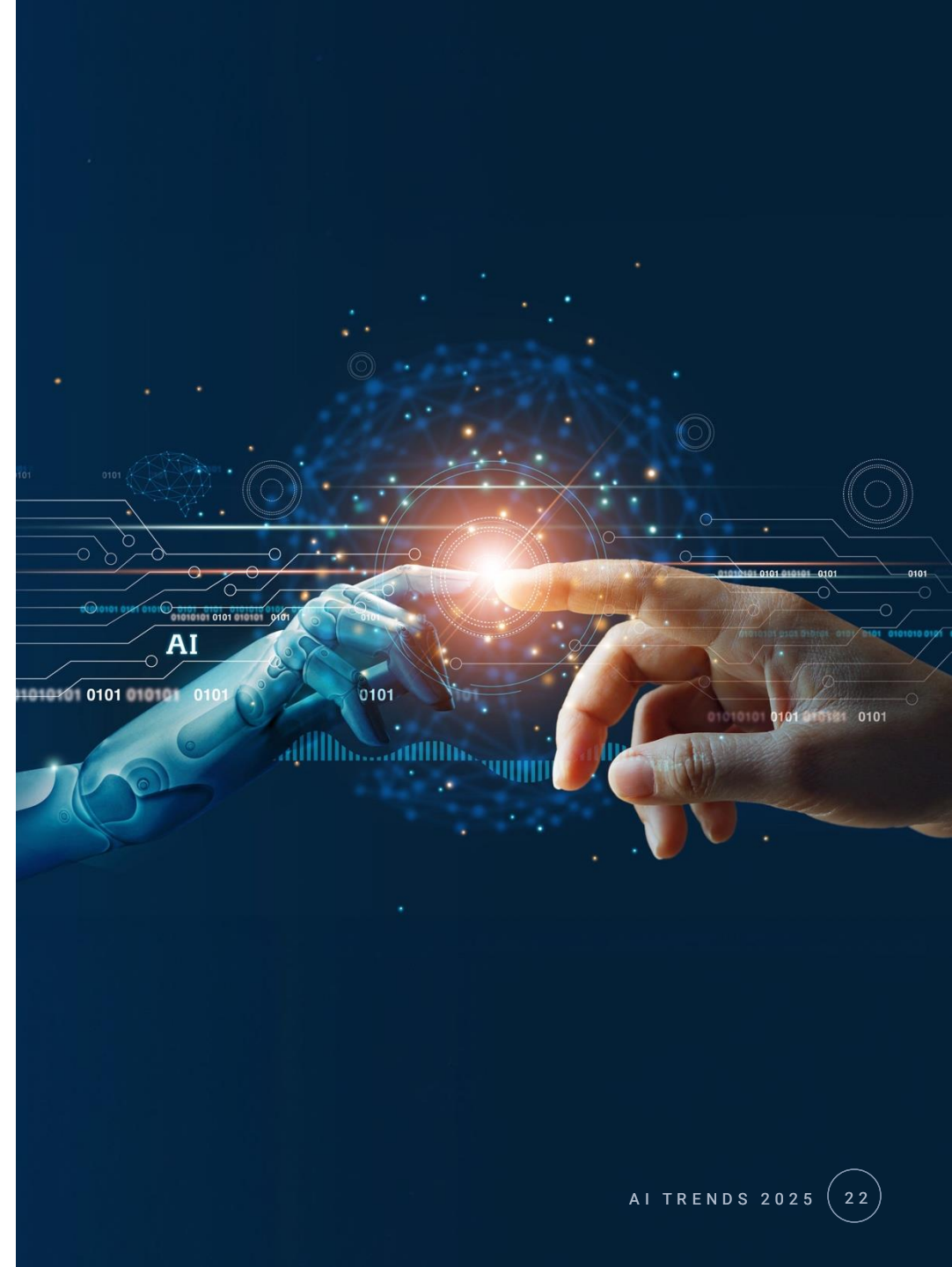
# Opportunities and threats

## Opportunities

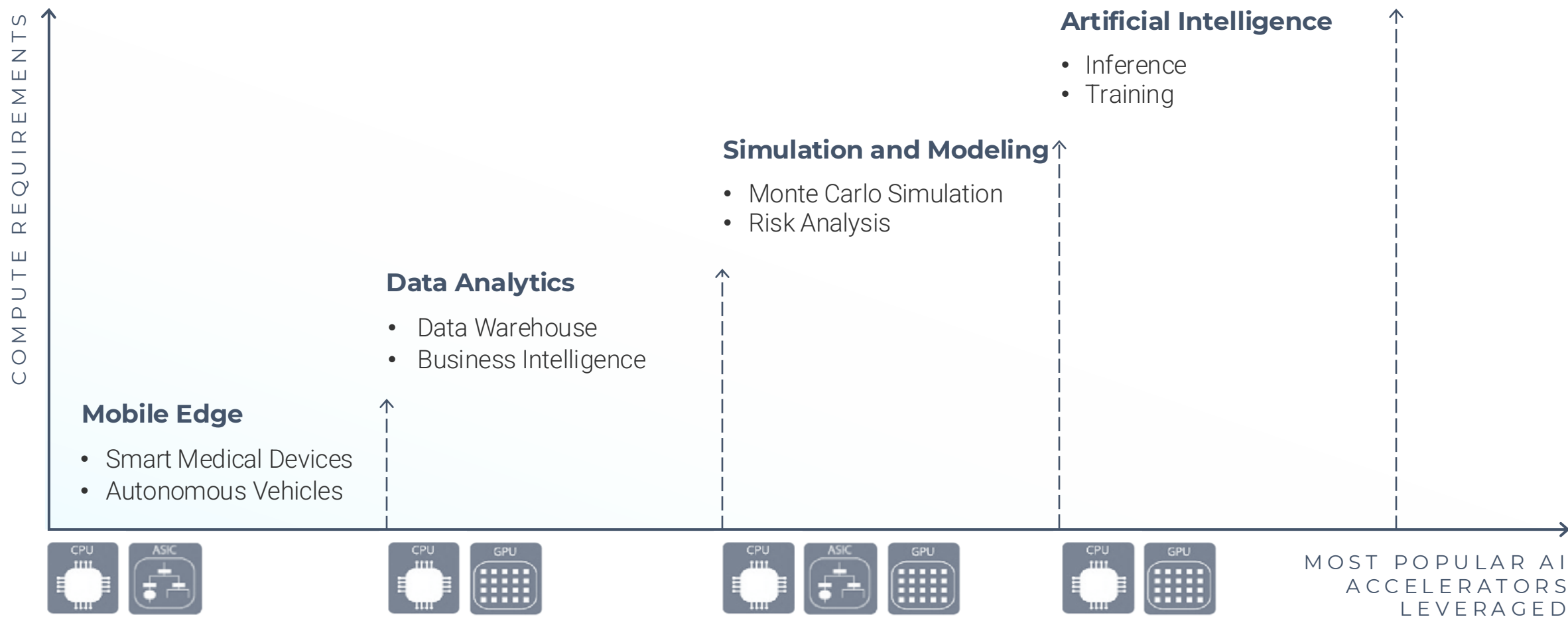
- Improve productivity
- Drive innovation and creativity
- Personalize the user experience
- Improve decision-making
- Introduce new business models

## Threats

- Possible copyright issues with content created
- Possible lack of guardrails for recommendations generated
- Increased negative environmental impact
- Overreliance on technology
- Privacy concerns regarding the use of personal data



# Optimize your hardware infrastructure based on the workload





# The rise of small language models and AI agents has the potential to further transform business outcomes

## Situation

Small/specialized language models (SLMs) are foundation models designed to be smaller and more efficient than large language models (LLMs). Some of the reasons organizations are adopting SLMs include:

- **Efficiency:** Smaller AI models require less compute power to train and execute.
- **Accessibility:** SLMs can execute on a range of devices, including smartphones, Internet of Things devices, and laptops, as well as large compute platforms.
- **Flexibility:** SLMs can be customized for specialized tasks.

AI agents are autonomous systems designed to interact with their environment, perceive information, and take actions to achieve specific goals. They are software programs that can reason, learn, and make decisions independently. Key characteristics of AI agents include:

- **Autonomous:** They can take actions to achieve their goals by interacting with their environment, without human supervision or interaction.
- **Goal-oriented:** They can process information, make decisions autonomously, and plan actions based on their goals and the current situation.
- **Adaptive:** They can improve their performance over time through experience and by acquiring new knowledge or skills.

This next evolution of AI technologies will enable organizations to drive value from a variety of complex, multistep workflows across various platforms.

## Action

Organizations across all industries are deploying agent-based AI applications. The use cases include:

- **Chatbots:** These agents can engage in conversations with humans, providing information or assistance and potentially resolving issues.
- **Autonomous vehicles:** These vehicles use AI agents to process data from sensors (e.g. cameras, LiDAR) to navigate roads, detect obstacles, and select the optimal route.
- **Virtual assistants:** These agents can help users with tasks like scheduling appointments, setting reminders, or finding information.
- **Building management systems:** AI agents can use the data from sensors and IoT devices to collect data to optimize energy consumption and improve security.

AI agents proceed in executing the next steps in a workflow autonomously via a single prompt by creating tasks, executing them, collecting any feedback from the environment, and then planning and prioritizing the remaining tasks until the objective has been completed. SLMs can be used as the reasoning and planning component for the AI agent to make the agent more efficient and responsive.

	Agentic AI	Generative AI
Primary Goal	To perform tasks autonomously to achieve a specific objective	To generate new content
Capabilities	Makes plans and decisions, can interact with the environment	Demonstrates creativity and can generate novel responses
Autonomy	Very autonomous	May require user prompts
Focus	Goal-directed behavior and problem solving	Content generation and creativity

## Results

The entire tech industry will be reengineering products and introducing new products to leverage agentic AI architectures and SLMs. For example:

- **Amazon Bedrock Agents** orchestrate interactions between foundation models, data sources, software applications, and user conversations. In addition, agents automatically call APIs to take actions and invoke knowledge bases to supplement information for these actions. Regarding the future of the SLM and LLM landscape, Matt Wood, AWS VP of AI Products, sums it up: [“There is no one model to rule them all”](#) (AWS Events, 2024).
- **Microsoft 365 Copilot Agents** act as intelligent assistants. Regarding the future of Copilot Agents, Charles Lamanna, VP Business & Industry Copilot, forecasts: [“Every employee will have a Copilot, their personalised AI agent, and then they will use that Copilot to interface and interact with the sea of AI agents that will be out there”](#) (Reuters, 2024).
- **Google Vertex AI Agent Builder** brings together foundation models, Google Search and other developer tools for partners to build and deploy agents, alongside orchestration and augmentation capabilities.
- **Salesforce Agentforce** is a contact center platform that enables businesses to deliver and manage customer interactions to gain valuable insights into customer behavior. Marc Benioff, Salesforce chair and CEO, states: [“Agentforce enables companies to scale their workforces on demand with a few clicks. The future of AI is agents, and it’s here”](#) (Salesforce, 2024).

# Trend summary

## Trend scenario

Organizations will continue to favor adopting solutions vs. building solutions.

- Larger LLMs may not always be the best choice.
- Agent-based AI applications and fit-for-purpose SLMs will grow in adoption.

## Next steps

Focus on high-value use cases for your organization.

Ensure candidate solutions have the AI capabilities you require:

- Accuracy
- User experience
- Use case requirements

Test the solution with your data.

Assess potential risk involved and develop a plan to monitor and mitigate risk.







TREND 3

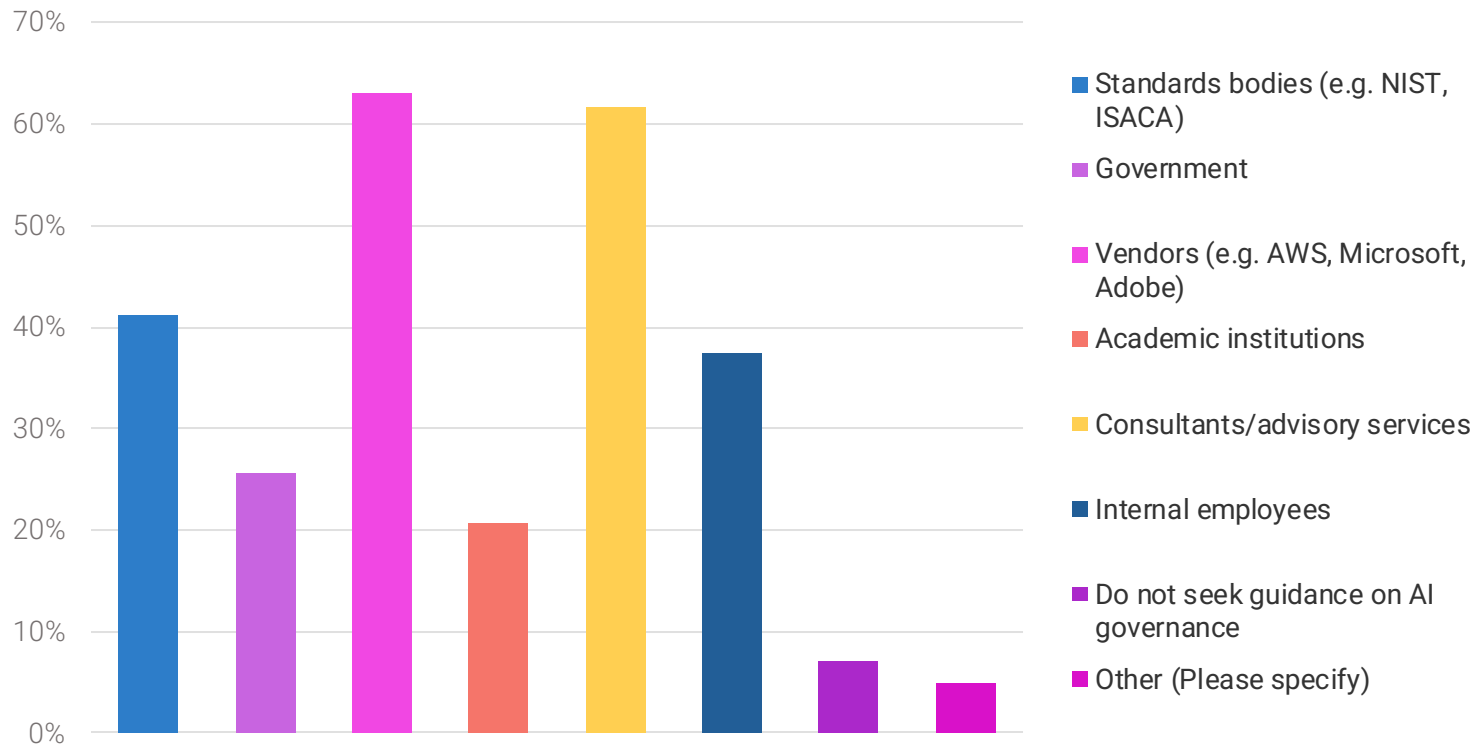
# AI REGULATIONS

Are Driving Responsible AI Frameworks



# AI governance guidance is often sought from external sources

## Where does your organization seek guidance on its approach to AI governance?



Source: Info-Tech Future of IT Survey, 2024; n= 371

## INSIGHTS

Vendors and external consultants are often used to provide guidance on AI governance to organizations.

# Challenge: Balancing safety and innovation

## Safety

- Protect users/citizens from unintended consequences from AI applications by requiring organizations to ensure applications are developed/deployed in a way that addresses data privacy, safety and security, explainability and transparency, fairness and bias detection, validity and reliability, and accountability.
- Deliver a framework where users/citizens have the right to file complaints against AI providers and compensation can be enforced.

## Innovation

- Promote and enable rapid and agile development and deployment of AI applications.
- Minimize bureaucratic oversight and compliance costs.
- Deliver an AI ecosystem/framework that promotes innovation and competition.



# AI regulatory initiatives around the world

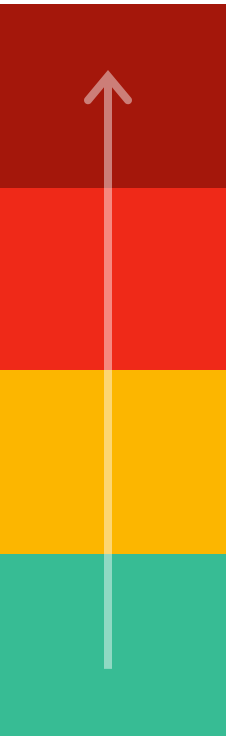


	European Union	United States	United Kingdom	China	Canada	Australia
Regulatory Approach	Risk- and rights-based	Market-driven	Innovation-driven	State-driven	Risk- and rights-based	Risk- and rights-based
AI Regulations/ Initiatives	<ul style="list-style-type: none"> <li>• EU AI Act</li> <li>• General Data Protection Regulation</li> <li>• Product Liability Directive</li> <li>• EU Data, Digital Services, Digital Markets, and Data Governance Acts</li> </ul>	<ul style="list-style-type: none"> <li>• White House AI Executive Order 14110 (federal agencies)</li> <li>• AI Foundation Model Transparency, Algorithmic Accountability, Federal AI Risk Management, and AI Research, Innovation, and Accountability Acts (proposed)</li> </ul>	<ul style="list-style-type: none"> <li>• Context and principle-based framework</li> <li>• UK Online Safety Act</li> <li>• UK Data Protection Framework and Digital Information Bill</li> </ul>	<ul style="list-style-type: none"> <li>• Generative AI Regulation</li> <li>• Personal Information Protection Law</li> <li>• Deep Synthesis Regulation</li> <li>• Algorithm Recommendation Regulation</li> </ul>	<ul style="list-style-type: none"> <li>• AI and Data Act (proposed, part of Bill C-27, the Digital Charter Implementation Act) focused on responsible AI guidelines for development/ deployment</li> </ul>	<ul style="list-style-type: none"> <li>• AI Ethics Principles (voluntary guidelines)</li> <li>• Australia's AI Action Plan</li> </ul>
Enforcement	<ul style="list-style-type: none"> <li>• European AI Office</li> <li>• National Data Protection Authorities</li> </ul>	<ul style="list-style-type: none"> <li>• Federal Trade Commission (FTC)</li> <li>• Consumer Financial Protection Bureau (CFPB)</li> <li>• Sector-specific agencies</li> </ul>	<ul style="list-style-type: none"> <li>• Information Commissioner's Office</li> <li>• Competition and Markets Authority</li> <li>• Department for Science, Innovation and Technology</li> <li>• Sector-specific regulators</li> </ul>	<ul style="list-style-type: none"> <li>• Ministry of Science and Technology</li> <li>• National Development and Reform Commission</li> <li>• Sector-specific regulators</li> </ul>	<ul style="list-style-type: none"> <li>• Innovation, Science and Economic Development Canada (ISED)</li> <li>• Sector-specific regulators</li> </ul>	<ul style="list-style-type: none"> <li>• Office of the Australian Information Commissioner (OAIC)</li> <li>• Australian Competition and Consumer Commission (ACCC)</li> </ul>



# The EU AI Act will influence proposed AI legislation around the world

## The AI Act classifies AI according to its risk



### Unacceptable Risk

Prohibited (e.g. social scoring systems and manipulative AI).

### High Risk

The focus of the AI Act; regulated systems that categorize individuals.

### Limited Risk

Subject to lighter transparency obligations: Developers and deployers must ensure that end users are aware that they are interacting with AI (chatbots and deepfakes).

### Minimal Risk

Unregulated. This includes the majority of AI applications currently available on the EU single market, such as AI-enabled video games and spam filters.

## INSIGHTS

The **EU AI Act** is the world's first comprehensive AI risk-based regulation. It introduces new agencies, including the **EU AI Office**, and **fin**es as a percentage of sales.

# The AI Executive Order is directing US federal agencies to implement AI in a safe and secure manner

## AI Executive Order Summary

- New Standards for AI Safety and Security
- Protecting Americans' Privacy
- Advancing Equity and Civil Rights
- Standing Up for Consumers, Patients, and Students
- Supporting Workers
- Promoting Innovation and Competition
- Advancing American Leadership Abroad
- Ensuring Responsible and Effective Government Use of AI

Source: The White House, 2023

## INSIGHTS

The White House has mandated its federal agencies to implement recommended AI policies for the safe use of AI. The government is not introducing any new legislation and is promoting self-regulation with AI principles.

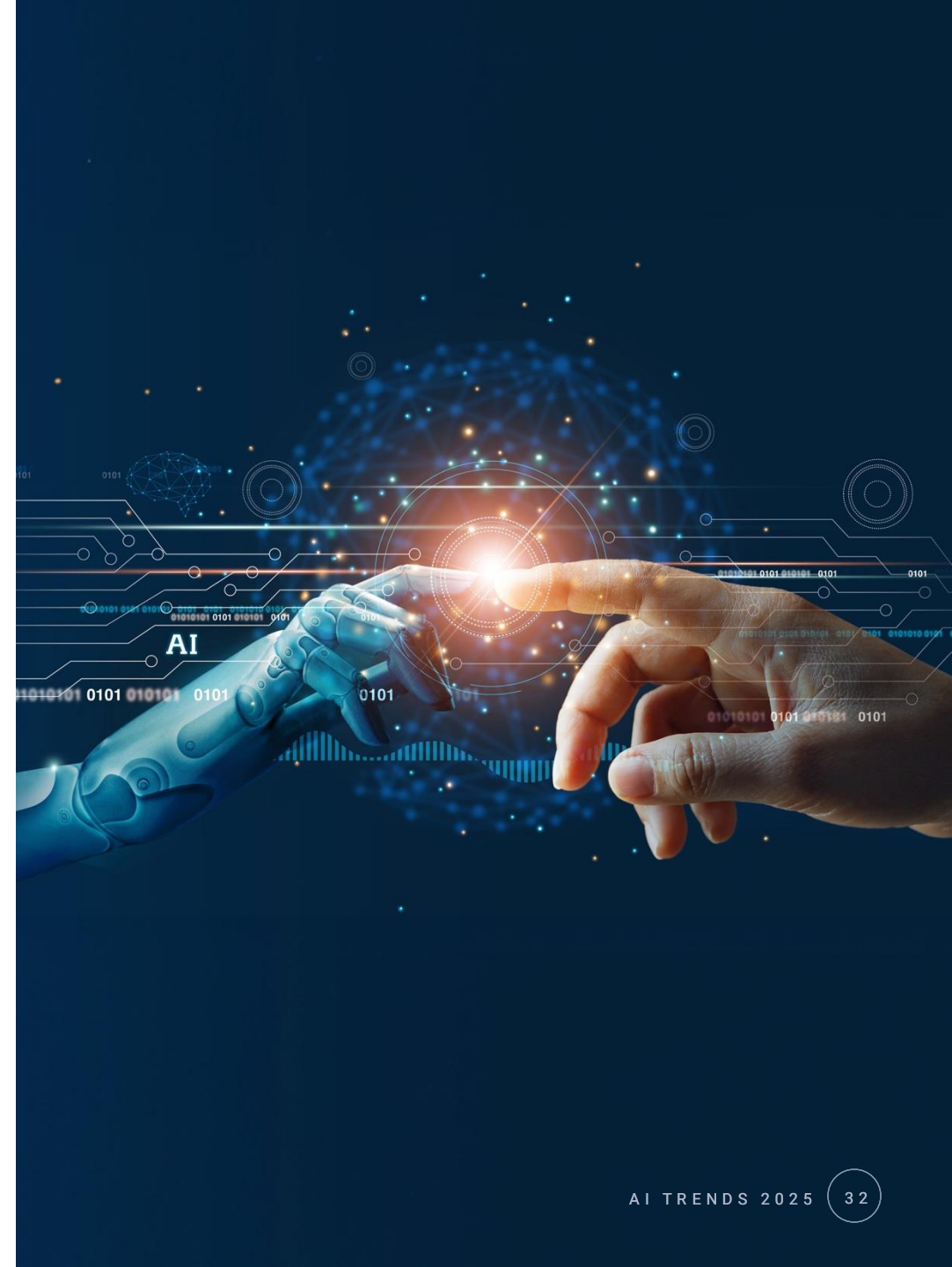
# Opportunities and threats

## Opportunities

- Increase trust and adoption
- Increase fairness and decrease bias
- Improve data privacy compliance
- Improve transparency
- Improve accountability

## Threats

- Stifled innovation
- Reduced competitiveness
- Increased government bureaucracy
- Excessive reporting and compliance requirements
- Increased costs





# US (pro-innovation) vs. EU (pro-safety) AI regulatory comparison



## United States

## European Union

Key Driver	Innovation	Safety and mitigating risk
Approach	Policy	Legislation and regulation
AI Regulatory Framework	<ul style="list-style-type: none"><li>• No legislation at the federal level</li><li>• Legislation exists at the state and municipal level</li><li>• White House AI Executive Order 14110 (policies for federal agencies)</li></ul>	<ul style="list-style-type: none"><li>• EU AI Act</li><li>• General Data Protection Regulation</li><li>• Product Liability Directive</li><li>• EU Data, Digital Services, Digital Markets, Data Governance Act</li></ul>
Enforcement Agencies	<ul style="list-style-type: none"><li>• Federal Trade Commission (FTC)</li><li>• Consumer Financial Protection Bureau (CFPB)</li><li>• Sector-specific regulators</li></ul>	<ul style="list-style-type: none"><li>• European AI Office</li><li>• European AI Board</li><li>• National Data Protection Authorities</li></ul>
AI System Classification	Emphasizes responsible use, no reporting/classification requirements	<ul style="list-style-type: none"><li>• Unacceptable risk: any system leveraging personal biometric data</li><li>• High risk: any system that categorizes or profiles individuals</li></ul>
Regulatory Focus	Vertical/sector/risk-based, will depend on context	Horizontal-based, same rules apply to all industries
Penalties	No new penalties; leverages existing laws	Fines based on a percentage of revenue
Obligations	Compliance with AI principles	Based on requirements for high-risk AI systems (Section 2) <ul style="list-style-type: none"><li>• Risk Management System, Data Governance, Documentation, Record-keeping, Transparency to Deployers, Human Oversight, Accuracy, Robustness and Cybersecurity</li></ul>

# The responsible AI tools ecosystem is growing

## Validity & Reliability

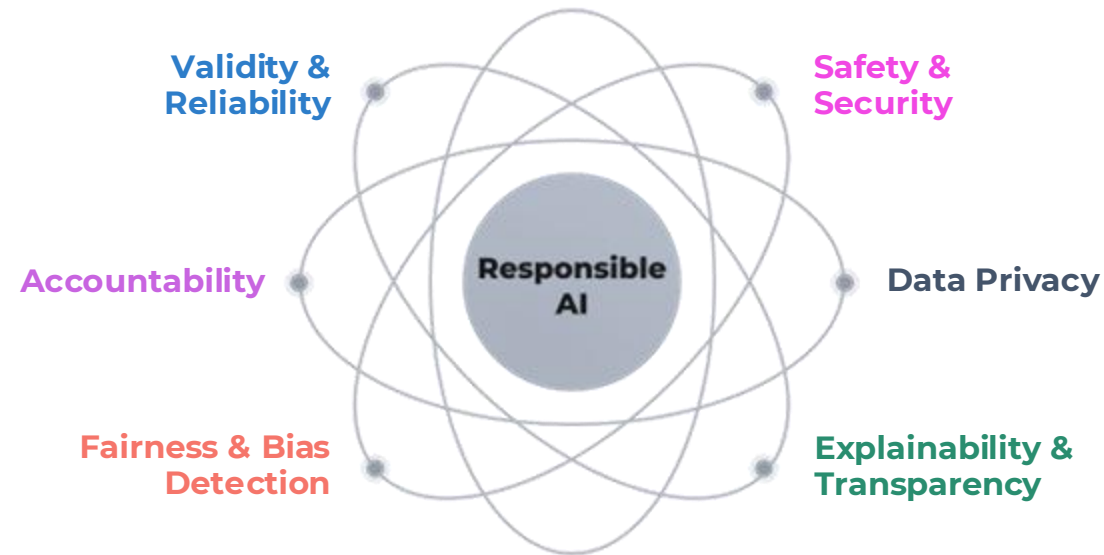
WhyLabs
Arize AI
Deepchecks
Evidently AI
Alibi Detect

## Accountability

Accountability Principles for Artificial Intelligence (AP4AI)
Artificial Intelligence Risk Management Framework (AI RMF 1.0)

## Fairness & Bias Detection

TensorFlow Fairness Indicators	FAT Forensics
Google What-If Tool	Themis-ml
Amazon SageMaker Clarify	FairTest
AI Fairness Checklist	Aequitas
Microsoft Fairlearn	Trusted-AI/AIF360



## Responsible AI Platforms

AWS Bedrock Guardrails
Microsoft Responsible AI Dashboard
Google Cloud Responsible AI
TensorFlow Responsible AI Toolkit

## Safety & Security

TensorFlow Federated
Saidot
Securiti
DynamoAI
Mithril Security

## Data Privacy

TensorFlow Data Validation
TensorFlow Privacy
Microsoft Presidio
Google Differential Privacy
IBM Privacy Toolkit
Privacy Meter

## Explainability & Transparency

Activation Atlases
Google What-If Tool
LIME
Skater
ELI5
Shapley SHAP
IBM AI Explainability 360
Alibi

# The United Nations proposes the first global framework for AI governance

## Situation

Artificial intelligence represents an immense opportunity to transform and drive innovation in all industries by improving operational excellence and solving complex problems that were out of reach using traditional computing solutions. In the pursuit of the benefits of AI-based solutions, organizations around the world are being challenged with how to govern AI. Many are just becoming aware of what responsible AI principles are and how they can help mitigate AI risks. In today's environment, without any legislation or coordination, the benefits of AI will likely be limited to a handful of countries, companies, and individuals. In addition, left ungoverned, AI will continue to disrupt the workplace and be leveraged to create deepfakes, create autonomous weapons, and pose risks to peace and security.

The United Nations is proposing the first global framework for AI governance to mitigate AI risks and address the inequities in accessing AI resources. The multi-stakeholder UN High-level Advisory Body on Artificial Intelligence released its findings on the need for global AI governance and stressed that [“The technology is too important, and the stakes are too high, to rely only on market forces and a fragmented patchwork of national and multilateral action.”](#)

## Action

In the UN report *Governing AI for Humanity*, the AI Advisory Body shared seven recommendations:

1. The establishment of an International Scientific Panel on AI to provide impartial information.
2. A new policy dialogue on AI governance at the UN, featuring intergovernmental and multi-stakeholder meetings.
3. An AI standards exchange to ensure technical interoperability of AI systems.
4. The creation of a global AI capacity development network to boost AI governance capacities and access to AI resources.
5. The establishment of a global AI fund to address gaps in capacity and collaboration, empowering local efforts to further the Sustainable Development Goals (SDGs).
6. The fostering of a global AI data framework to standardize data-related definitions, principles, and stewardship.
7. Formation of a small AI office within the UN Secretariat to support and coordinate the implementation of these proposals.

## Results

New regulations to govern AI are coming. It will take time, collaboration, and coordination for the UN initiatives to be adopted and implemented across the world. In preparation for new regulations, it is useful to understand the principles that will guide the UN in its development of these new agencies. As *Governing AI for Humanity* states:

- AI should be governed inclusively, by and for the benefit of all.
- AI must be governed in the public interest.
- AI governance should be built in step with data governance and the promotion of data commons.
- AI governance must be universal, networked and rooted in adaptive multi-stakeholder collaboration.
- AI governance should be anchored in the Charter of the United Nations, international human rights law and other agreed international commitments, such as the SDGs.

Take the above principles into consideration when establishing and customizing your responsible AI guiding principles for your organization.

# Trend summary

## Trend scenario

Expect AI regulations to increase. As a result, organizations will increase their adoption of responsible AI frameworks to mitigate the risks of AI and self-regulate to minimize disruption from future legislation. Ongoing challenges will center on:

- Innovation vs. safety
- Enforcement

## Next steps

Establish responsible AI principles.

**Implement an AI risk management framework.**

- Schedule risk assessments on a regular basis.
- Operationalize responsible AI principles.
  - Consider tools to automate monitoring and mitigating risk.

**Cultivate a culture of risk management.**

- Educate your workforce on AI risk and benefits.

## INSIGHTS

“Leadership should establish responsible AI—the human-based principles that organizations need to guide their developers in the development and deployment of this technology to minimize unintended consequences that may occur.”

**Bill Wong,**  
Info-Tech’s AI Research Fellow,  
in Harvard Business Review, 2024



TREND 4

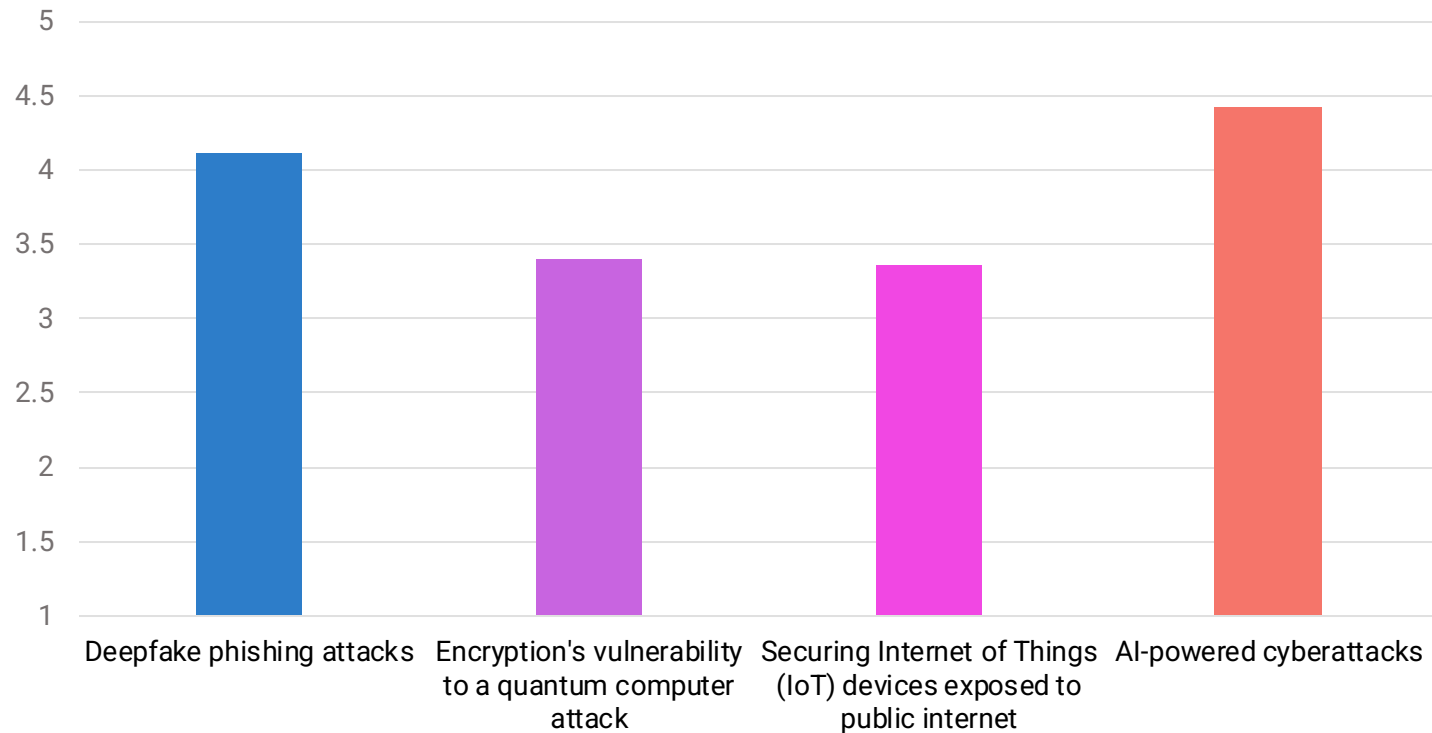
# DEEPPFAKE THREATS

Continue to Rise



# AI-based cyberattacks and deepfakes are the top cybersecurity threats

**How concerned are you about the following external cybersecurity threats? Rate 1 (Not concerned) to 5 (Very concerned)**



Source: Info-Tech Future of IT Survey, 2024; n=190

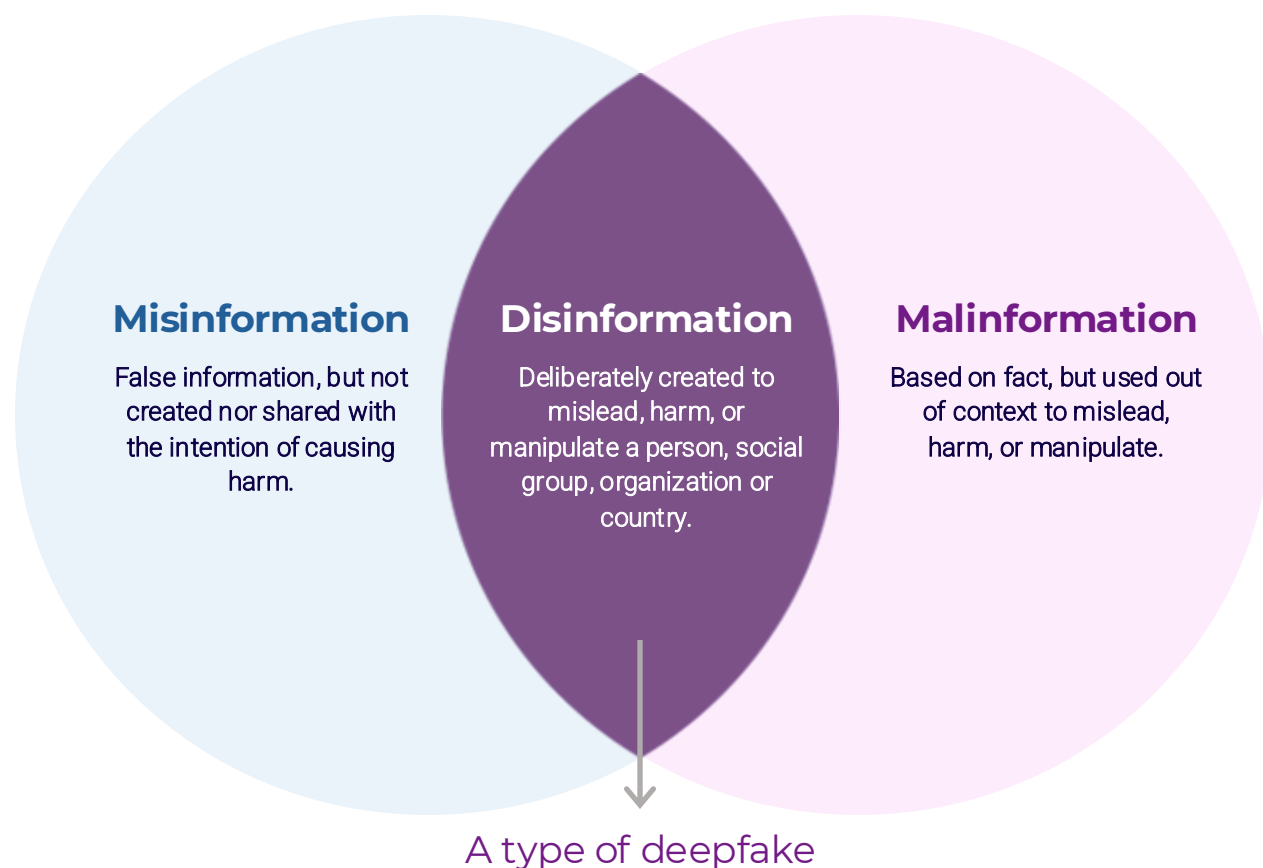
## INSIGHTS

AI introduces improved cybersecurity defenses as well as AI-powered cyberattacks and the creation of deepfakes. A recent survey of security leaders from the US and UK found that:

- 65% anticipate AI will be used in the majority of cyberattacks.
- 93% predict that AI-based cyberattacks will be a daily occurrence by 2025.

Source: Netacea, 2024

# Misinformation and disinformation represent the world's greatest risk



Source: Cybersecurity and Infrastructure Security Agency

## INSIGHTS

This year's Global Risks Report has ranked misinformation and disinformation as the most severe short-term risk the world faces over the next two years.

"Misinformation and disinformation may radically disrupt electoral processes in several economies," according to the report. The report states this threat will "deepen polarized views" and "could trigger civil unrest and confrontation."

Source: World Economic Forum, 2024

# What is a deepfake?

## Definition

Digital media created using deep learning technology so that it appears authentic despite being totally fabricated (not authentic and never occurred).

## Types of deepfakes

- Image deepfakes, face swapping, face manipulation, body swapping
- Voice cloning, lip-synching, audio editing
- Text synthesis, fake news, phishing attacks
- Real-time video

## Deepfake detection technologies

- Speaker recognition, voice liveness detection, facial recognition, facial feature analysis, blink rate analysis, microexpressions
- Temporal inconsistencies, frame-by-frame video analysis, lip-sync mismatches





# Use of deepfakes to manipulate and commit fraud is on the rise and creates threats around the world



## **Election Fraud – Disinformation to manipulate voters**

Deepfake audio/robocall of President Joe Biden created to tell New Hampshire residents not to vote in an upcoming election.

## **Financial Fraud/Social Disruption – Dow Jones drops nearly 80 points**

Deepfake of fire at the Pentagon tweeted by Bloomberg Feed and amplified by media firm Russia Today caused brief panic as the stock market briefly dropped \$500 billion.



## **Financial Fraud – In the EU, deepfakes now represent 6.5% of total fraud attempts (“AI-Driven Identity Fraud,” Signicat, 2024)**

In a 2024 survey, European digital identity company Signicat estimates that 42.5% of detected fraud attempts now use AI, and of these, 29% are successful (“Over a Third,” Signicat, 2024).

## **Election Fraud – Disinformation to manipulate voters**

A fake recording portraying Starmer verbally abusing staff was released on the X social media platform and received 1.5 million views. X ignored requests to take down the content.



## **Financial Fraud – US\$25 million**

Arup has confirmed it was the victim of a deepfake fraud after an employee was duped into sending \$25 million to criminals by a video call where all participants were fake.

## **Data Breach – Business disruption**

Yum! Brands was the victim of hackers using AI-augmented ransomware to breach businesses. The company was forced to close nearly 300 restaurants for a day.

# Challenge: Preventing deepfakes

## **Deepfakes are getting better and harder to detect.**

Bad actors are using this technology to facilitate financial fraud, manipulate public opinion, and erode trust in individuals and institutions.

## **Open-source software has enabled easy access to the technology**

- DeepFaceLab: Leading software to create deepfake videos
- Faceswap: User-friendly tool to develop deepfake videos
- FFmpeg: Known for its speed and processing of large media files

## **Deepfakes may not be considered illegal**

Creating and distributing deepfakes may not be illegal depending on the jurisdiction and social media platform.

## **Humans are easy to fool**

Past elections and inexperience with more sophisticated phishing schemes powered by AI demonstrate that it is not difficult to manipulate voters and undermine the democratic process.



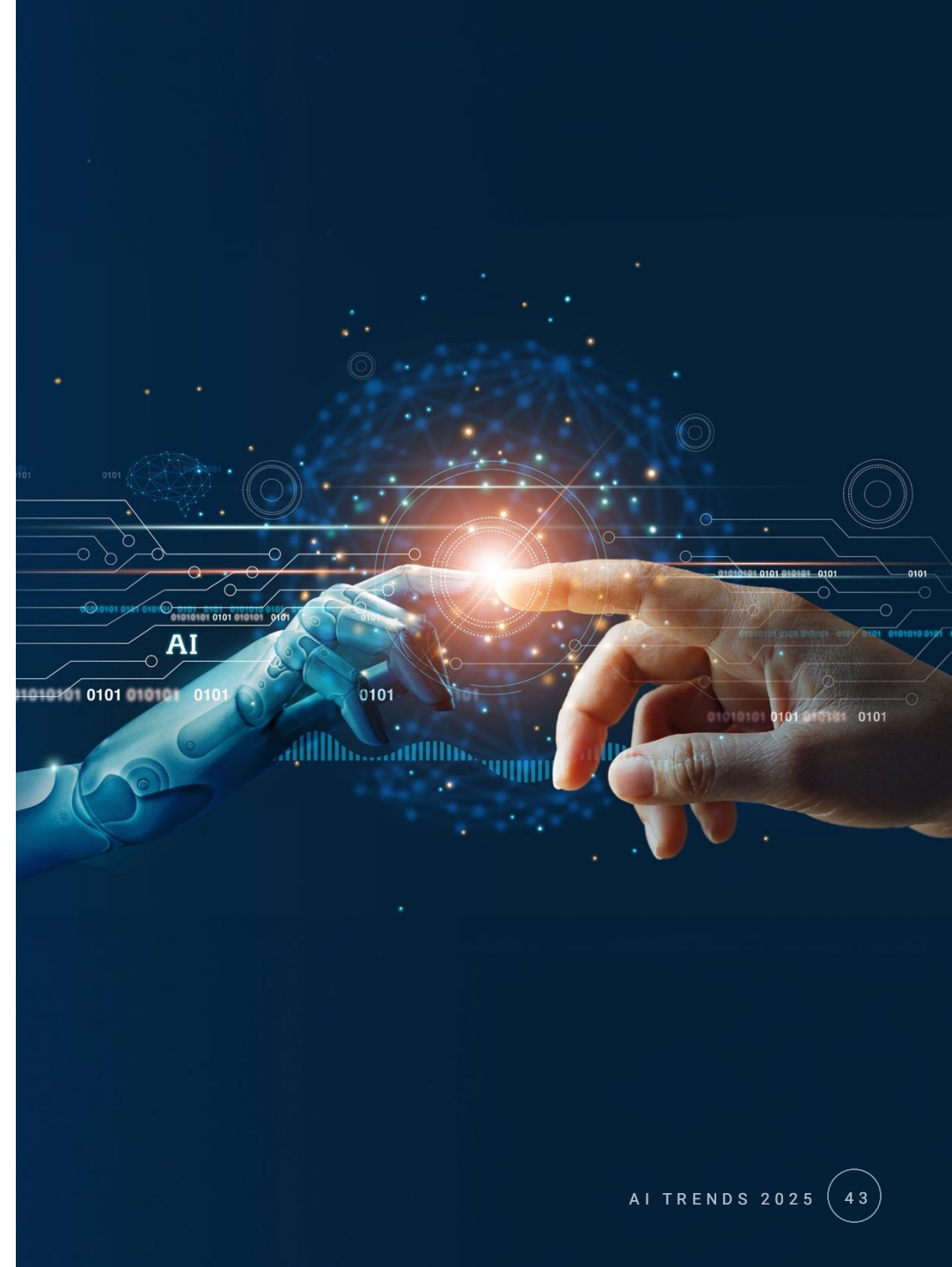
# Opportunities and threats

## Opportunities

- Create personalized marketing campaigns
- Create realistic product demonstrations
- Generate video in multiple languages with synchronized dubbing
- Reduce reliance on personal data
- Animate historical figures for engaging learning

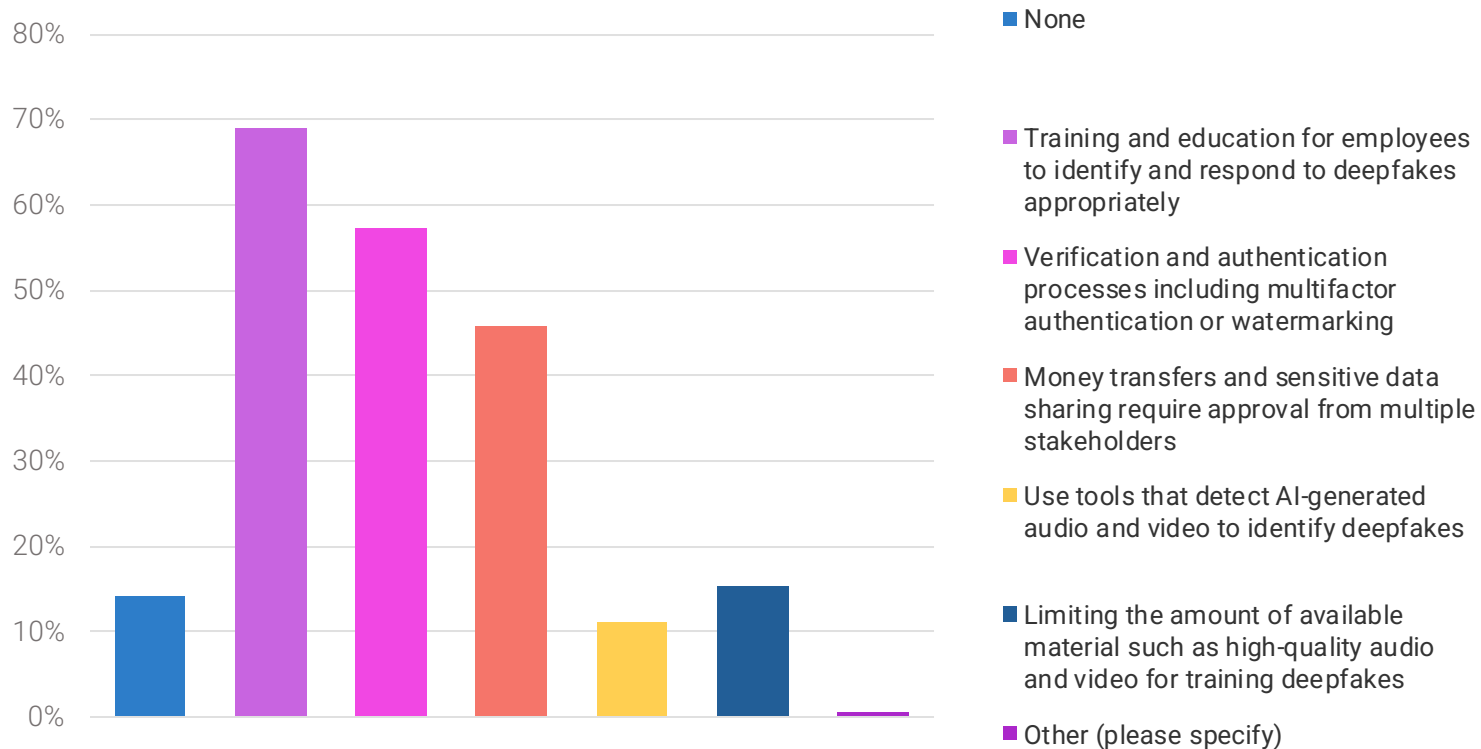
## Threats

- Fake news and political propaganda
- Impersonation for fraud
- Damaged reputations and social unrest
- Deepfakes created and distributed without consent
- Identity theft



# Tactics used today to battle deepfakes

**What tactic(s) does your organization use to protect against deepfake-powered phishing attacks, including phone calls or videoconference calls where AI is used to imitate decision-makers?**



Source: Info-Tech Future of IT Survey, 2024; n=190

## INSIGHTS

Opportunities to enhance cybersecurity defenses:

- The first best practice to adopt against deepfakes is educating and training employees to understand the risks from deepfakes, the techniques used to deploy deepfakes, and steps to mitigate the spread of deepfakes.
- Leverage new detection technologies to detect deepfakes (these can implement zero trust at the application level).
- Implement robust authentication measures, including multifactor authentication, which requires multiple forms of identification like passwords, biometrics, or mobile app codes.



# Deepfake legislative counterinitiatives



## EU

The EU is criminalizing non-consensual explicit deepfakes, making it illegal to create or share sexually explicit deepfakes without the consent of the person depicted.



## United States

- California recently passed legislation making it illegal to create and distribute sexually explicit images of a real person that appear authentic, when intended to cause harm.
- California and Texas have passed laws that criminalize the publishing and distributing of deepfake videos that intend to influence the outcome of an election.
- Virginia Code 18.2-386.2 prohibits the “malicious dissemination or sale” of any image or video created by any means (including deepfakes) that depicts another person in a sexually explicit manner without their consent.
- In just the first three weeks of 2024, lawmakers from both major parties introduced legislation in at least 14 states to combat the kind of misinformation and disinformation AI and deepfakes can create in elections.



## United Kingdom

The UK Online Safety Act criminalizes the sharing of intimate deepfake images on social media without the person’s consent.



## Canada

The province of British Columbia is the first to introduce a law, the Intimate Images Protection Act, that makes it illegal to distribute intimate deepfake images without the person’s consent.



## Australia

Former Australian Competition and Consumer Commission (ACCC) deputy chair Delia Rickard is leading a proposal to update the Online Safety Act. The Basic Online Safety Expectations (BOSE) system, which applies to tech and social media companies, is also intended to be amended.

## INSIGHTS

In 2024, at least 64 countries (plus the European Union) – representing a combined population of about 49% of the people in the world – are planning national elections.

Governments are concerned about the possible risk from deepfakes and misinformation.

# Election Tech Accord to fight deepfakes in elections

## Situation

In 2024, at least 64 countries (plus the European Union) – representing a combined population of about 49% of the people in the world – are planning national elections.

Industry experts warn of the AI risks that are likely to occur through the use of deepfakes and misinformation campaigns in the upcoming elections. Some of the actions taken include:

- In the US, the FCC outlawed AI-generated robocalls aimed to discourage voters.
- At the Munich Security Conference (MSC) this year, 20 leading tech companies signed the Tech Accord to Combat Deceptive Use of AI in 2024 Elections, an accord to prevent AI from being used to disrupt democratic elections worldwide. The industry is specifically targeting deepfakes (audio, image, video) that fabricate deceptive media to fuel misinformation and disinformation campaigns.

The Chair of the Munich Security Conference, Christoph Heusgen, stated: “[The Tech Accord to Combat Deceptive Use of AI in 2024 elections is a crucial step in advancing election integrity, increasing societal resilience, and creating trustworthy tech practices. MSC is proud to offer a platform for technology companies to take steps toward reigning in threats emanating from AI while employing it for democratic good at the same time](#)” (Munich Security Conference, 2024).

Source: AI Elections Accord, 2024

## Action

The voluntary framework consists of principles and actions to advance seven principal goals, as stated on the AI Elections Accord website:

1. Prevention: Researching, investing in, and/or deploying reasonable precautions to limit risks of deliberately Deceptive AI Election Content being generated.
2. Provenance: Attaching provenance signals to identify the origin of content where appropriate and technically feasible.
3. Detection: Attempting to detect Deceptive AI Election Content or authenticated content, including with methods such as reading provenance signals across platforms.
4. Responsive Protection: Providing swift and proportionate responses to incidents involving the creation and dissemination of Deceptive AI Election Content.
5. Evaluation: Undertaking collective efforts to evaluate and learn from the experiences and outcomes of dealing with Deceptive AI Election Content.
6. Public Awareness: Engaging in shared efforts to educate the public about media literacy best practices, in particular, regarding Deceptive AI Election Content, and ways citizens can protect themselves from being manipulated or deceived by this content.
7. Resilience: Supporting efforts to develop and make available defensive tools and resources, such as AI literacy and other public programs, AI-based solutions (including open-source tools where appropriate), or contextual features, to help protect public debate, defend the integrity of the democratic process, and build whole-of-society resilience against the use of Deceptive AI Election Content.

## Results

The accord included the following major tech companies: Adobe, Amazon, Anthropic, Arm, ElevenLabs, Gen, GitHub, Google, IBM, Inflection, Intuit, LG AI Research, LinkedIn, McAfee, Microsoft, Meta, NetApp, Nota, OpenAI, Snap Inc., Stability AI, TikTok, Trend Micro, TrueMedia.Org, Truepic, and X.

The accord represents a symbolic gesture in combatting deepfakes. The voluntary framework does not require any of the technology firms to ban or remove deepfakes. The focus of the accord is to outline methods to detect and label deceptive AI content when it is created or distributed on their platform. It asks that companies share best practices with each other and is vague on what “swift and proportionate responses” should entail.

A few months after the accord was signed, several of the organizations reported on their progress, typically citing updates to their policies and procedures. There was no evidence of any active collaboration to develop improved technology to detect deepfakes (such as digital watermarking). Also, there was no commitment for any of the social media organizations to combat misinformation by building content recommendation systems that do not prioritize engagement above all else.

Unfortunately, the lack of any accountability to produce any measurable deliverable demonstrates that the industry has a long way to go before effectively mitigating the risks from deepfakes.

# Trend summary

## Trend scenario

The threat of deepfakes will continue to grow.

- Realism will continue to improve, and deepfakes will continue to be more difficult to detect.
- Legislative initiatives continue to be slow and are not coordinated with technology initiatives to address deepfakes.

## Next steps

Upgrade your cybersecurity defenses.

- Educate and raise awareness on the risks and latest exploits of deepfake technologies.
- Introduce technologies to detect deepfakes and detect and ensure integrity of content (e.g. digital watermarking).
- Enhance verification procedures for media used in critical business processes and develop an incident response plan to address deepfake-related crises effectively.





# 2025 AI trends summary for the CIO

## **AI strategy**

Develop the organization's AI strategy jointly with business stakeholders.

## **AI ecosystem**

Adopt a solution-centric approach and focus on driving business value in candidate AI proofs of concepts.

## **AI regulations**

Establish a responsible AI framework to provide safeguards and ensure the safe and secure development and deployment of AI-based solutions.

## **Deepfake threats**

For business-critical processes, adopt zero trust processes with a human in the loop to minimize the risks from deepfakes. Introduce upgraded authentication processes to verify requests for any critical resources.





# Expert contributors

## EXTERNAL

### **Tom Godden**

Enterprise Strategist & CxO Advisor  
AWS

### **Amol Shah**

Americas Data & AI GTM Lead  
Microsoft

### **Rob Katz**

VP of Product for Responsible AI & Tech  
Salesforce

## INTERNAL

### **Rob Garmaise**

VP, AI Research

### **Mark Tauschek**

VP, Research Fellowships

### **Jay Elie**

VP, Vendor Partnerships

### **Brian Jackson**

Principal Research Director



# Bibliography

*AI Elections Accord*. AI Elections Accord, 2024, [www.aielectionsaccord.com](http://www.aielectionsaccord.com)

"Australia's AI Action Plan." *Australian Government*, June 2021. Web.

"Banking on Artificial Intelligence: How JP Morgan Uses AI to Lead the Banking Industry." *AtliQ*, 20 May 2024. Web.

"The Battle Against AI-Driven Identity Fraud." Signicat, 28 May 2024. Web.

Benioff, Mark. "Dreamforce 2024 Main Keynote with Marc Benioff | Welcome to Agentforce | Salesforce." *YouTube*, uploaded by Salesforce, 17 Sept. 2024. [www.youtube.com/watch?v=\\_Cs-xTQeGfo](http://www.youtube.com/watch?v=_Cs-xTQeGfo)

Bishop, Todd. "The rise of AI at JPMorgan Chase — and how Jamie Dimon used a chatbot to prepare for Elon Musk." *GeekWire*, 4 June 2024. Web.

Cavaciuti-Wishart, Ellissa, et al. "Global Risks Report 2024." *World Economic Forum*, 10 Jan. 2024. Web.

"Cyber Security in the Age of Offensive AI." *Netacea*, 24 April 2024. Web.

Dimon, Jamie, and John McDonald. "JPM at the Bernstein Strategic Decisions Conference: Transcript." *JPMorgan Chase*, 29 May 2024. Web.

Dimon, Jamie. "Chairman and CEO Letter to Shareholders." *JPMorgan Chase*, 8 April 2024. Web.

"The Dispatch: AI Research." *Evident AI*, Feb. 2024. Web.

"Evident AI Index." *Evident AI*, Oct. 2024. Web.

"Fact Sheet: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence." *The White House*, 30 Oct. 2023. Web.

"Governing AI for Humanity." *United Nations*, 2024. Web.

Grubb, Mikael, et al. "2024 Investor Day: Transcript." *JPMorgan Chase*, 20 May 2024. Web.

Jadhav, Bhushan. "Agentic AI: The Next Frontier of Generative AI." *Aisera*, n.d. Web.

Jain, Anu, et al. "How JPMorgan Chase Built a Data Mesh Architecture to Drive Significant Value to Enhance Their Enterprise Data Platform." *AWS*, 5 May 2021. Web.

"The Launch of the AI Elections Accord at the Munich Security Conference 2024." Munich Security Conference, 2024. Web.

"Mis-, Dis-, and Malinformation: Planning and Incident Response Guide for Election Officials." *Cybersecurity & Infrastructure Security Agency*, n.d. Web.

# Bibliography

"Operationalizing Generative AI for Better Business Outcomes." *Harvard Business Review*, 2024. Web.

"Quest IndexGPT: Harnessing generative AI for investable indices." *J.P. Morgan*, 22 July 2024. Web.

"Salesforce Unveils Agentforce—What AI Was Meant to Be." *Salesforce*, 12 Sept. 2024. Web.

Soni, Aditya. "Microsoft to Let Clients Build AI Agents for Routine Tasks From November." *Reuters*, 21 Oct. 2024. Web.

Stebbing, Harry (host). "Aidan Gomez: What No One Understands About Foundation Models | E1191." *YouTube*, uploaded by 20VC with Harry Stebbings, 19 Aug. 2024, [www.youtube.com/watch?v=FUGosOgiTel](https://www.youtube.com/watch?v=FUGosOgiTel)

Wood, Matt, "AWS Summit New York City 2024 – Keynote with Matt Wood." *YouTube*, uploaded by AWS Events, 11 July 2024, [www.youtube.com/watch?v=hVy1clpu6II](https://www.youtube.com/watch?v=hVy1clpu6II)

Zaragoza, Alba. "Over a Third of Fraud Attempts Targeting Financial Institutions Now Use AI." *Signicat*, 30 May 2024. Web.

