INFO~TECH
RESEARCH GROUP

AI TRENDS 2026

FIVE KEY AI TRENDS AFFECTING CIOS

FIVE AI TRENDS FOR 2026

This report highlights five key AI trends in emerging and leading-edge technologies and practices, offering actionable insights that can help guide your organization toward its strategic goals.

Foundational AI principles will rewrite organizational DNA

AI strategies will be informed by an emerging set of principles.

From copilots to vibe coding: AI will continue to reinvent IT

The ecosystem of AI solutions for IT will grow with the introduction of new categories.

Agentic AI will come of age and power the exponential enterprise

Agentic AI will increase in adoption and enable outcomes across the organization, powering exponential growth and change.

Risk management will be the price of admission for AI

Adoption of AI risk management programs will be driven by the potential new risks that AI applications can introduce.

AI will hang in the balance between freedom and control

AI sovereignty will become top of mind for regulators.

Over 700 survey responses from IT leaders

The Future of IT 2025 survey

The *AI Trends 2026* report is based on the Future of IT 2026 survey conducted in May and June 2025.

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

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

Industries represented include*:

- Government/Public Sector
- Financial Services & Insurance
- Education
- Manufacturing
- Professional & Technology Services
- Utilities
- Healthcare
- Professional Associations & Nonprofits
- Transportation & Logistics
- Oil & Gas Operations
- Retail
- Casinos, Gambling & Lottery

*Industries representing less than 1% of survey respondents not listed here.

2026

Future of IT Survey

Shape the course of IT by completing the survey today.

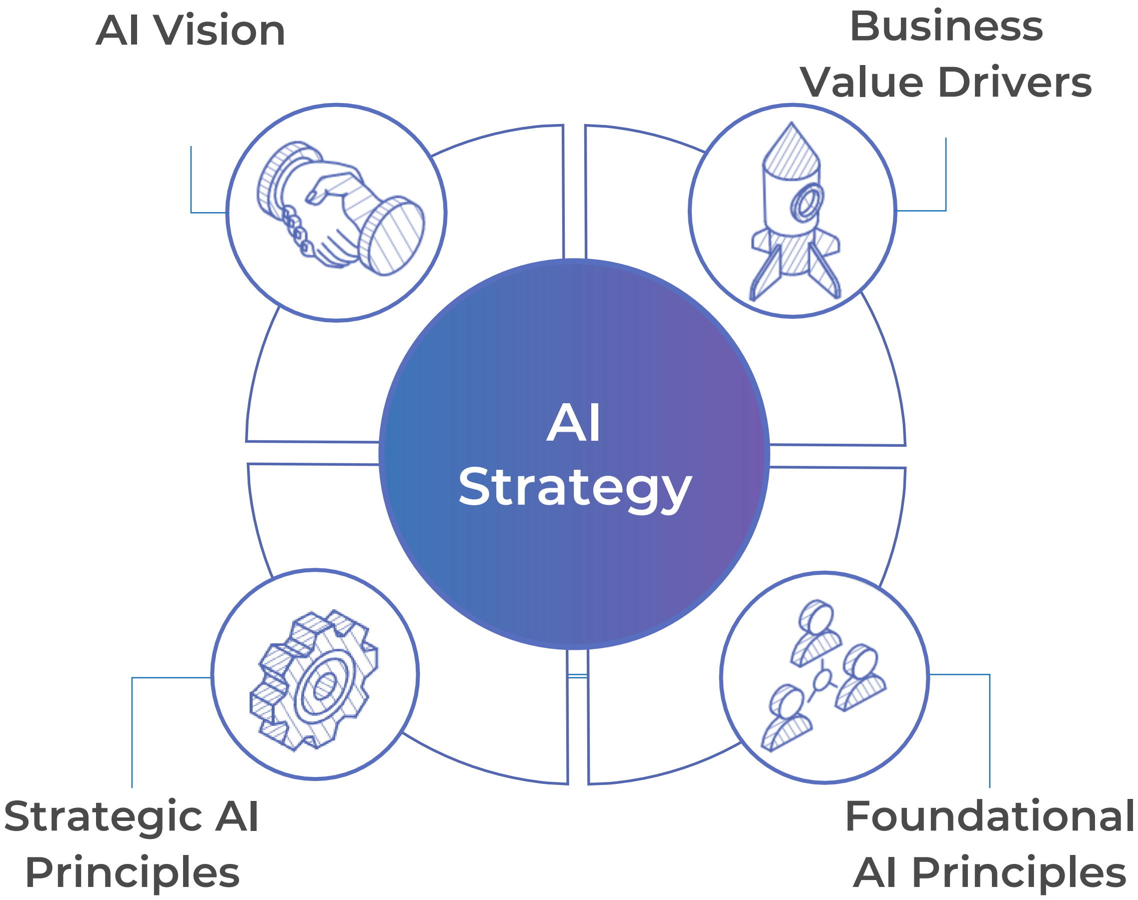
Foundational AI principles will rewrite organizational DNA

AI strategies will be informed
by an emerging set of principles.

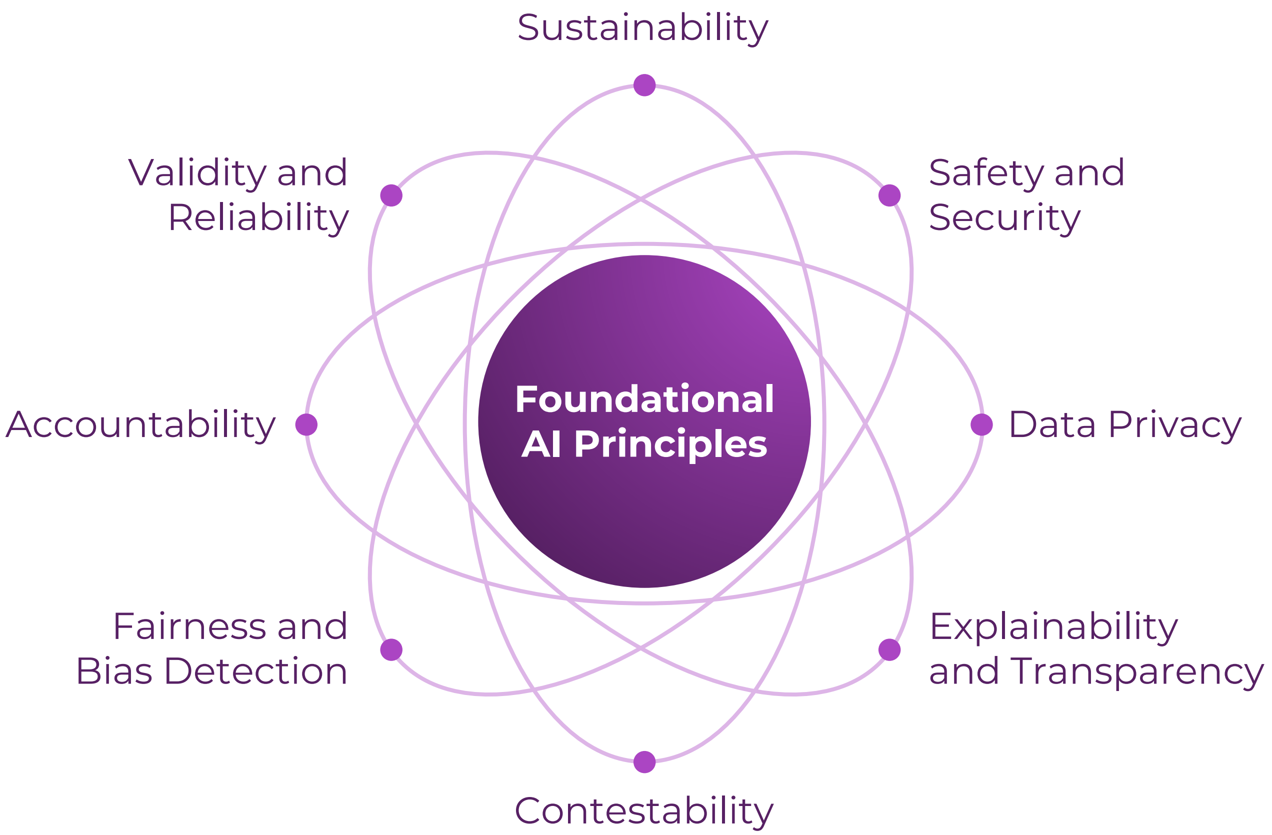
AI strategy is driven by organizational strategy and value drivers

A business-driven AI strategy is aligned with the organizational strategy of the firm. 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.
- 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: Strategic guiding principles align the business strategy with the AI strategy and reflect the organization's overall approach to the use of AI.
- Foundational AI Principles: Foundational principles govern the development, deployment, and maintenance of AI applications to mitigate the possible risks from deploying AI-based applications.



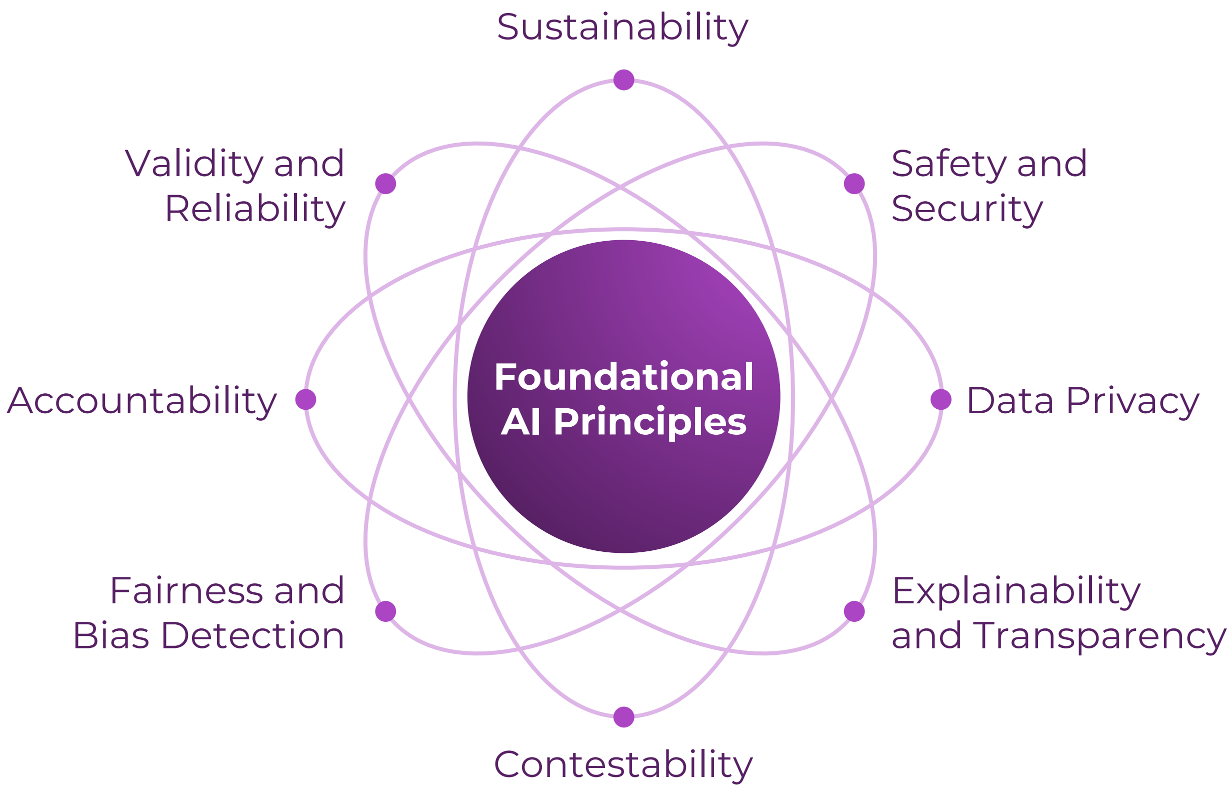
Foundational AI principles address the risks associated with AI and are aligned with the organization's guiding principles



Foundational AI principles are selected and customized to reflect the organization's guiding principles.

- Foundational AI principles should be core to the organization's AI governance program.
- Foundational AI principles are used to identify risk categories for the organization's AI risk management program.

Foundational AI principles continue to evolve as organizations' enterprise governance requirements evolve



Candidate foundational AI principles to consider

Sustainability
Design AI systems to be more energy efficient.

Human Agency and Autonomy
Use AI systems that augment human performance and enable independent actions.

Environmental
Design AI systems to have positive environmental outcomes.

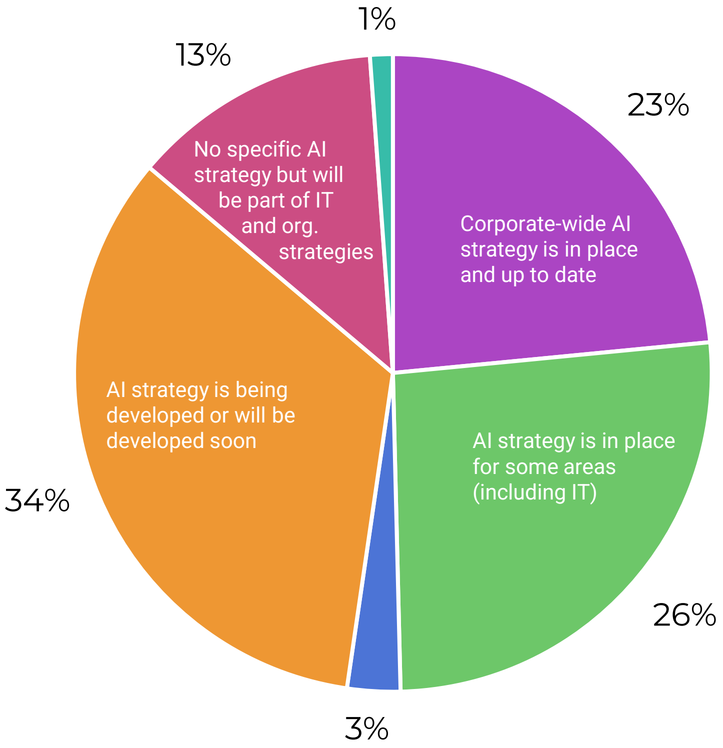
Contestability
Enable individuals to challenge and seek redress for AI decisions that have impacted them.

Intellectual Property
Ensure AI systems recognize intellectual property rights.

Other
Additional principles that address compliance or are customized for the organization/industry.

While developing a formal AI strategy is the growing trend, the majority have not established a formal organization-wide AI strategy

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



- 🟪 Corporate-wide AI strategy is in place and up to date
- 🟩 AI strategy is in place for some areas (including IT)
- 🟦 We have an outdated strategy covering the whole or part of the organization
- 🟧 AI strategy is being developed or will be developed soon
- 🟥 No specific AI strategy but will be part of IT and org. strategies
- ■ No plans for an AI strategy

Source: Info-Tech Future of IT Survey, 2025; *n*=260

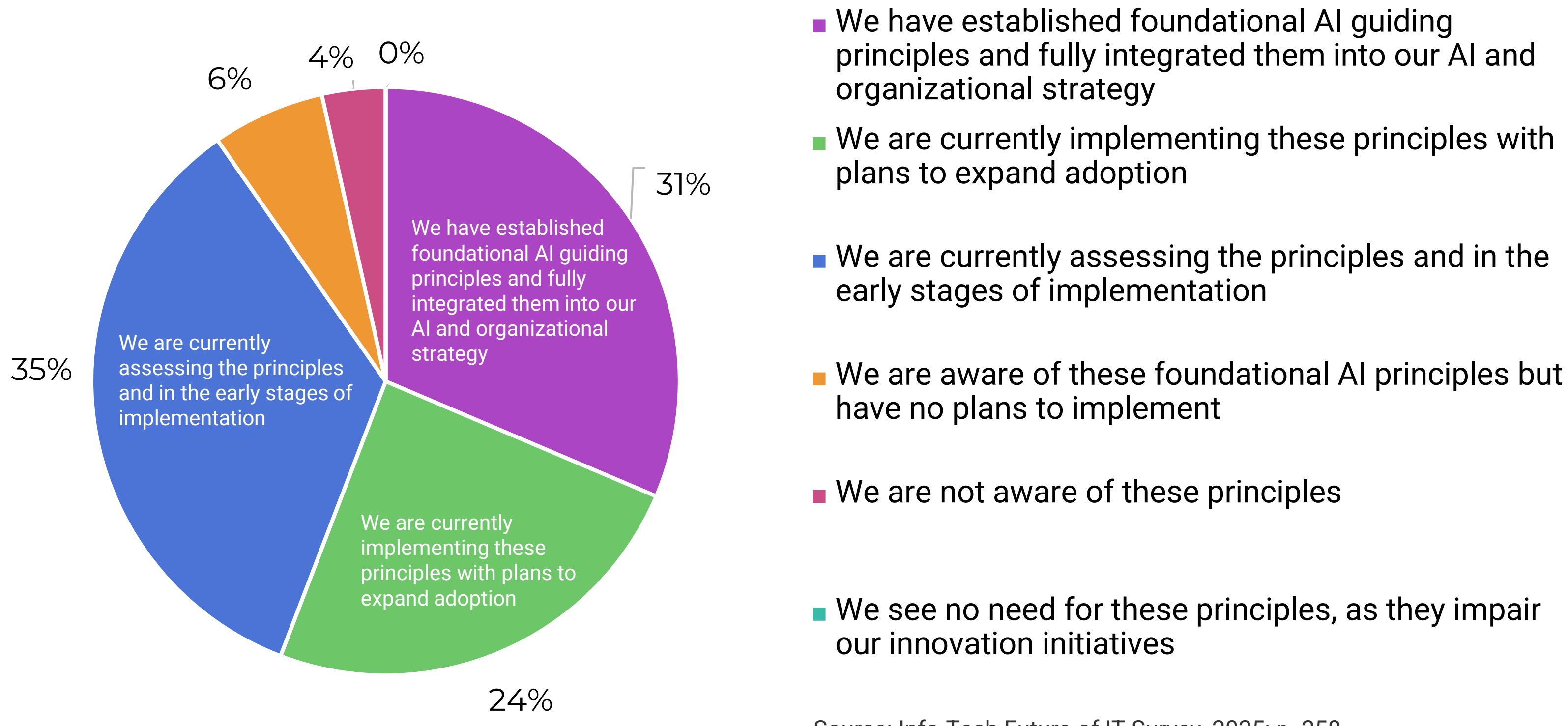
INSIGHT

Although most organizations have or are developing an AI strategy, this is still relatively new for most.

- **23%** of respondents said they have a corporate-wide AI strategy in place today (an increase of 15 percentage points compared to last year’s survey result).
- **26%** said there is an AI strategy in place for some business areas (an increase of seven percentage points).
- **34%** replied that their AI strategy is being developed or will soon be developed (a decrease of six percentage points).

Organizations understand the need for foundational AI principles to address AI risks

What best describes your organization’s adoption of foundational AI principles (safety and security, data privacy, explainability and transparency, validity and reliability, fairness and bias detection, accountability)?



Source: Info-Tech Future of IT Survey, 2025; *n*=258

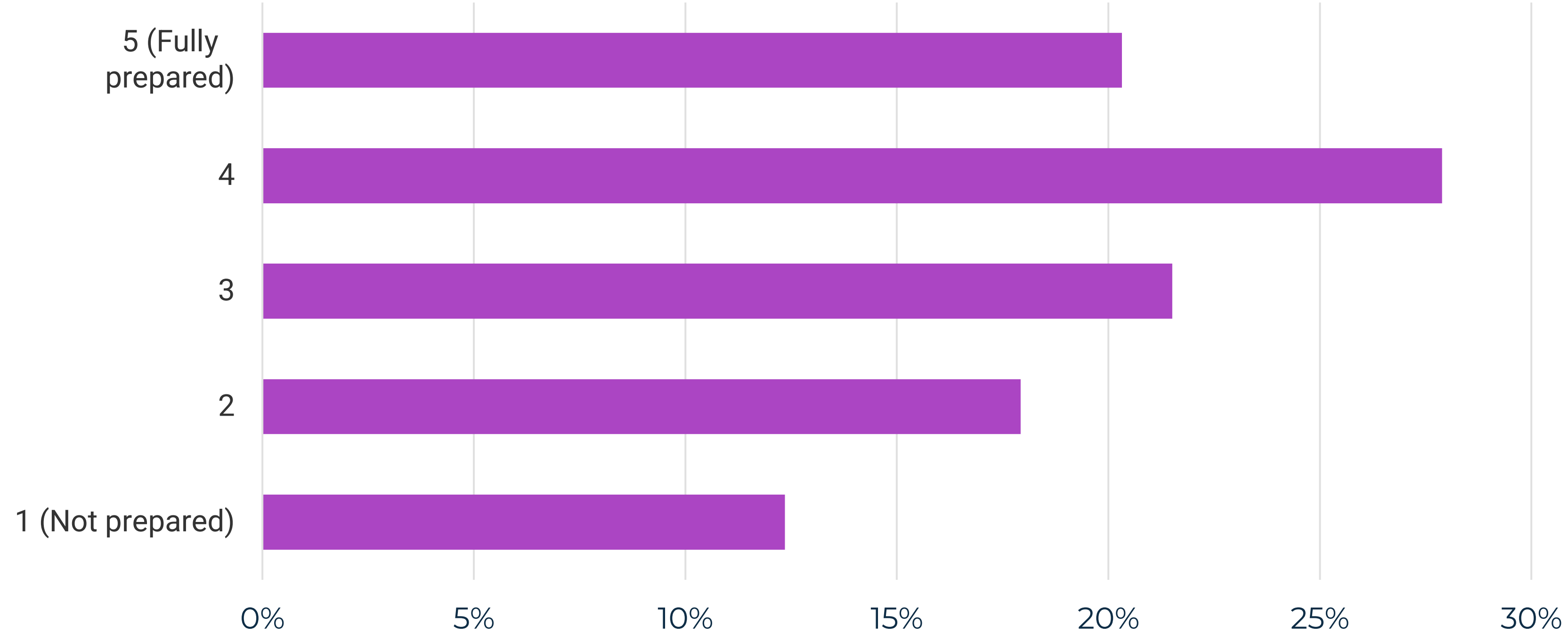
INSIGHT

Over half of respondents have implemented or are in the process of implementing foundational AI principles in their organization to address the possible risks associated with the introduction of AI applications.

No respondents viewed AI safeguards as an impairment to innovating with AI.

A majority of organizations feel that they are prepared to put their AI principles into practice

How prepared is your organization to put your foundational AI guiding principles into practice?



Source: Info-Tech Future of IT Survey, 2025; *n*=251

INSIGHT

Establishing foundational AI principles is a priority for the majority of respondents.

70% of respondents feel prepared (3) to fully prepared (5) to operationalize their foundational AI principles.

AI strategy is driving transformative opportunities and introducing new potential risks

Opportunities

- Accelerated AI deployments
- Improved customer experience
- Talent attraction and retention
- Innovation and growth
- Increased employee productivity and effectiveness

Risks

- Possible job displacement
- Overreliance on AI systems
- Creation of deepfakes for identity theft or fraud
- Misalignment with foundational AI principles
- Possible privacy breaches with the use and sharing of data

CASE STUDY

Foundational AI principles can be used to assess the risks of new technologies such as DeepSeek

deepseek

Situational Analysis

On January 20, 2025, DeepSeek released its most capable models for complex reasoning and problem solving, DeepSeek-R1 and DeepSeek-R1-Zero. In addition, six smaller "distilled" versions enable operation on local devices. DeepSeek AI Assistant, a chatbot leveraging DeepSeek-V3, was also made available.

On January 27, 2025, the Nasdaq dropped more than 3% as Nvidia lost more than $600 billion in market capitalization over questions and concerns about whether AI firms were overvalued.

DeepSeek model highlights

- DeepSeek-R1 is the first open-source model to match the performance of OpenAI's o1 across a range of core tasks.
- DeepSeek models are open source. Its weights have been published, and they have all been made commercially available, enabling organizations to build with this technology without any licensing constraints.
- DeepSeek introduces new reinforcement learning techniques to train the model, drastically reducing the time and complexity for developing the model.

According to DeepSeek researchers, it cost US$6 million to train its chain of thought model and took only two months to build, using older and slower Nvidia H800 chip technology.[1] In contrast, in 2024, OpenAI secured US$6.6 billion to pursue artificial general intelligence with its chain of thought model.

OpenAI vs. DeepSeek input/output token costs[2]

- Input costs: OpenAI has over 27x higher costs than DeepSeek ($15/million vs. $0.55/million)
- Output costs: OpenAI has over 27x higher costs than DeepSeek ($60/million vs. $2.19/million)

Resource utilization comparison

DeepSeek achieved results with 2.78 million GPU hours,[1] significantly lower than Meta's 30.8 million GPU hours for similar-scale models.

1. DeepSeek API Docs
2. Liu et al., 2024

CASE STUDY

Foundational AI principles can be used to assess the risks of new technologies such as DeepSeek (continued)

Actions

While the DeepSeek models offer a compelling value proposition with respect to cost savings and accelerating time to market, several organizations have banned usage of their products. These organizations include:

- US government agencies, including Congress, the Navy, the Pentagon, NASA, and the Texas state government.
- Government agencies from Australia, India, Italy, South Korea, and Taiwan.

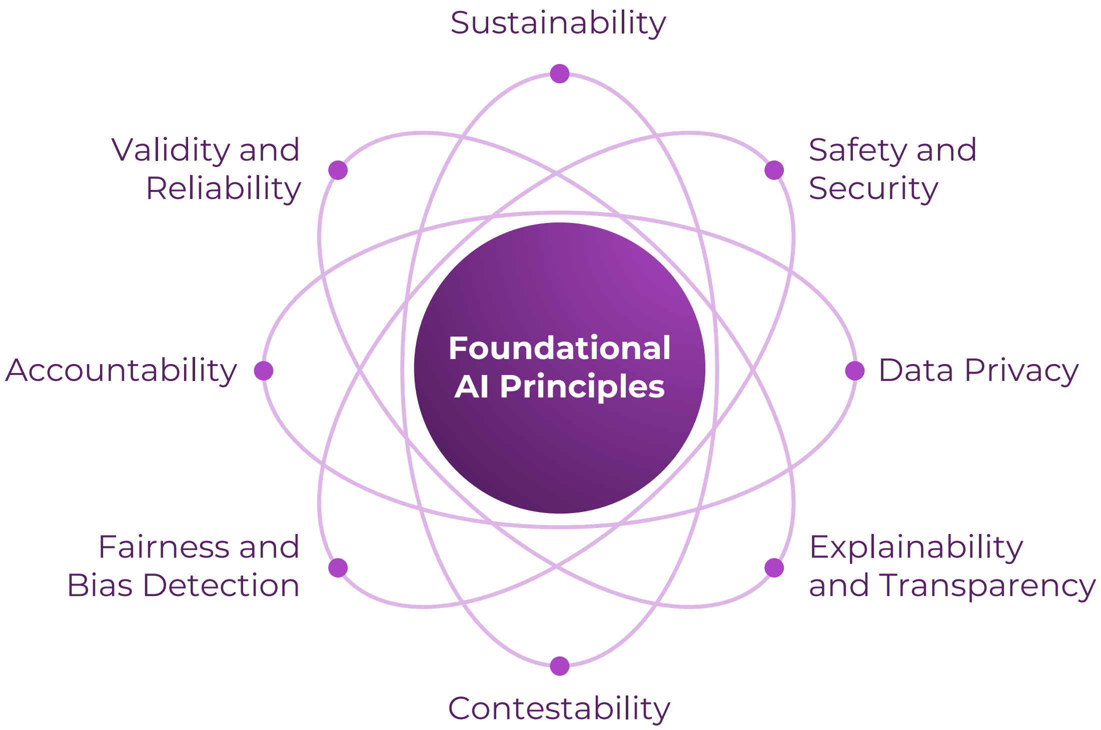
Foundational AI Principles Trend

Organizations that have banned the usage of DeepSeek cite that it breaches one or both of the following AI principles:

- Safety and security: National security risk is the most cited reason for preventing the use of DeepSeek.
- Data privacy: Violation of data privacy regulations (e.g. GDPR) have been cited as a reason to ban the usage of DeepSeek in countries such as Italy.

It is recommended that organizations require any AI-based technology considered for adoption to align to foundational AI principles. Failure to do so exposes the organization to risks that may harm the community they serve.

Foundational AI Principles



Establish foundational AI principles as a core component of AI strategy and AI governance

Action Items

Foundational AI principles focused on improving the safety and trustworthiness of the AI system can also be used to identify risk categories.

- Leverage the AI principles to serve as AI risk categories. Types of AI risk can include risks related to fairness and bias detection, explainability and transparency, privacy, safety and security, validity and reliability, and accountability.
- Use the AI risk categories to drive the organization's AI risk management program.

The foundational AI principles are not static. They should be reviewed and evolve as the organization's strategy changes and as AI technologies and understanding of AI risks evolves.

- Expand the focus of AI principles to include value creation.
- Consider other AI principles that are also core to the organization's strategy, such as sustainability, contestability, advancing economic opportunity, and human-centered values.

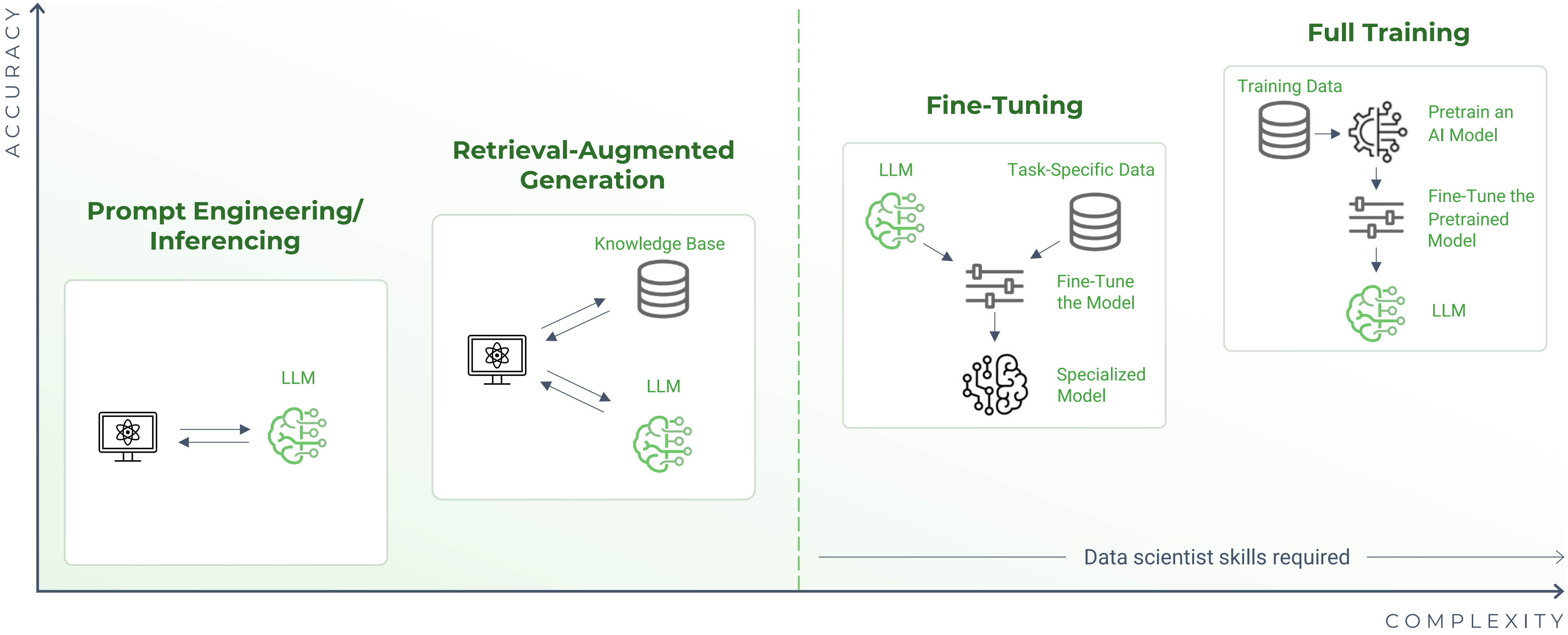
From copilots to vibe coding: AI will continue to reinvent IT

The ecosystem of AI solutions for IT will grow with the introduction of new categories.

Take a layered approach to optimize performance for the AI technology stack

Applications	Amazon Q Copilot Google Workspace workday salesforce WRITER CRESTA servicenow Synthesia glean OBSERVE·AI SAP ADEPT
Data and AI Tools	Amazon Bedrock Amazon SageMaker Azure Machine Learning Vertex AI LangChain Hugging Face PYTORCH APACHE Spark kafka TensorFlow DataRobot DOMINO
Foundational Models	OpenAI Gemini Claude 3 ANTHROP\C cohere MISTRAL AI_ AI21 labs stability.ai Midjourney runway BLOOM Gemma LLaMA deepseek
Data Platform	aws Azure Google Cloud salesforce snowflake databricks redis elastic STARDOG Pinecone milvus chroma
Infrastructure	aws Azure Google Cloud NVIDIA AMD intel Qualcomm

Customizing the LLM introduced new categories of tools: prompt engineering, RAG, fine-tuning…



Many organizations are facing the decision between best-of-breed AI tools vs. an AI platform

Best-of-Breed AI Tools

+ Best tool for a specific task in the AI lifecycle
+ Licensing costs may be lower and more manageable
+ Flexibility with tool selection

- Multiple tools required to address development needs
- Higher integration costs
- Greater complexity managing multiple vendors

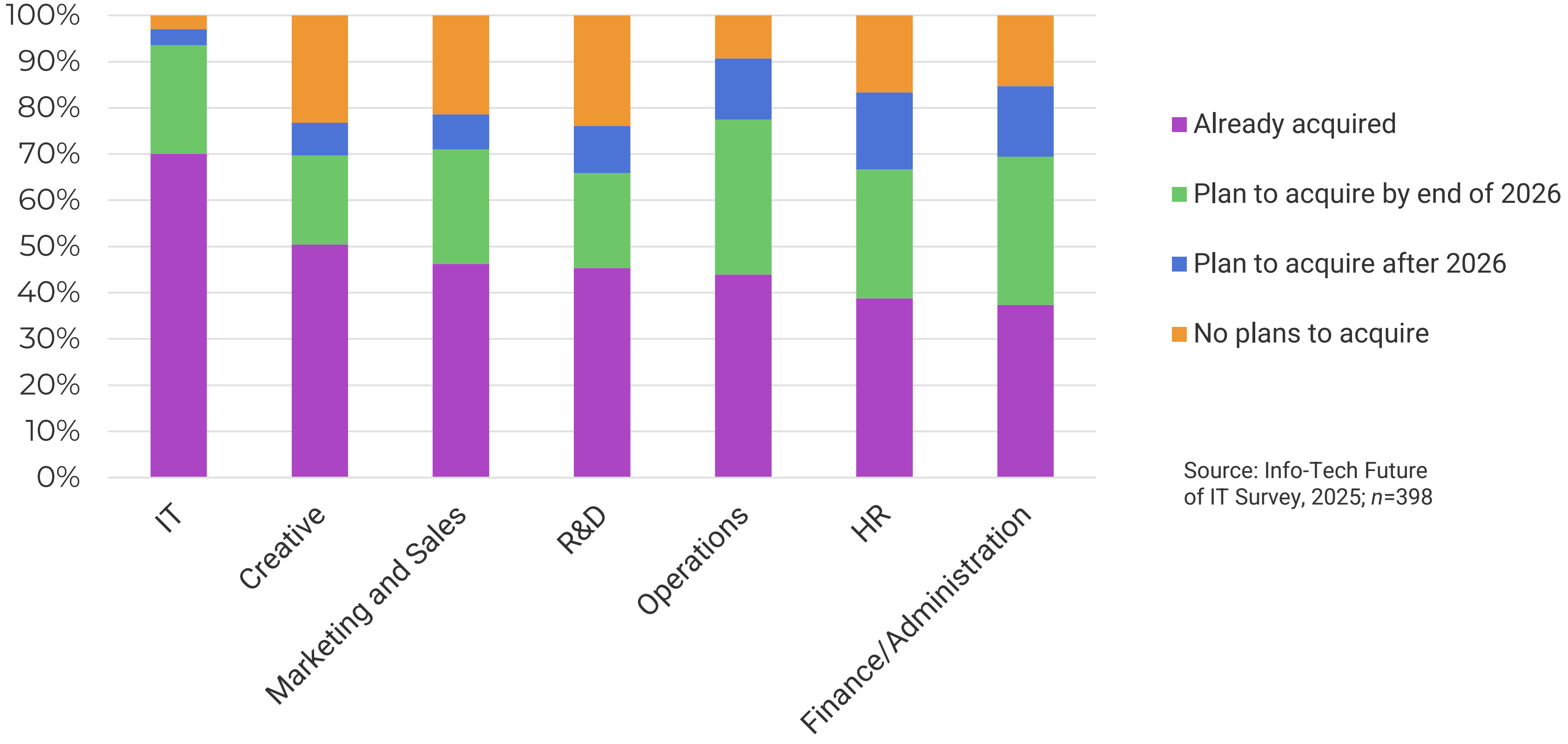
AI Development Platform

+ Solution-oriented and unified environment
+ Easier to manage and accelerate development
+ Reduced integration complexity

- Vendor lock-in
- Higher licensing costs
- New product enhancements may lag

The IT department leads in the adoption of AI applications

What is your organization's plan for deploying AI vendor solutions to the following functions?



Source: Info-Tech Future of IT Survey, 2025; *n*=398

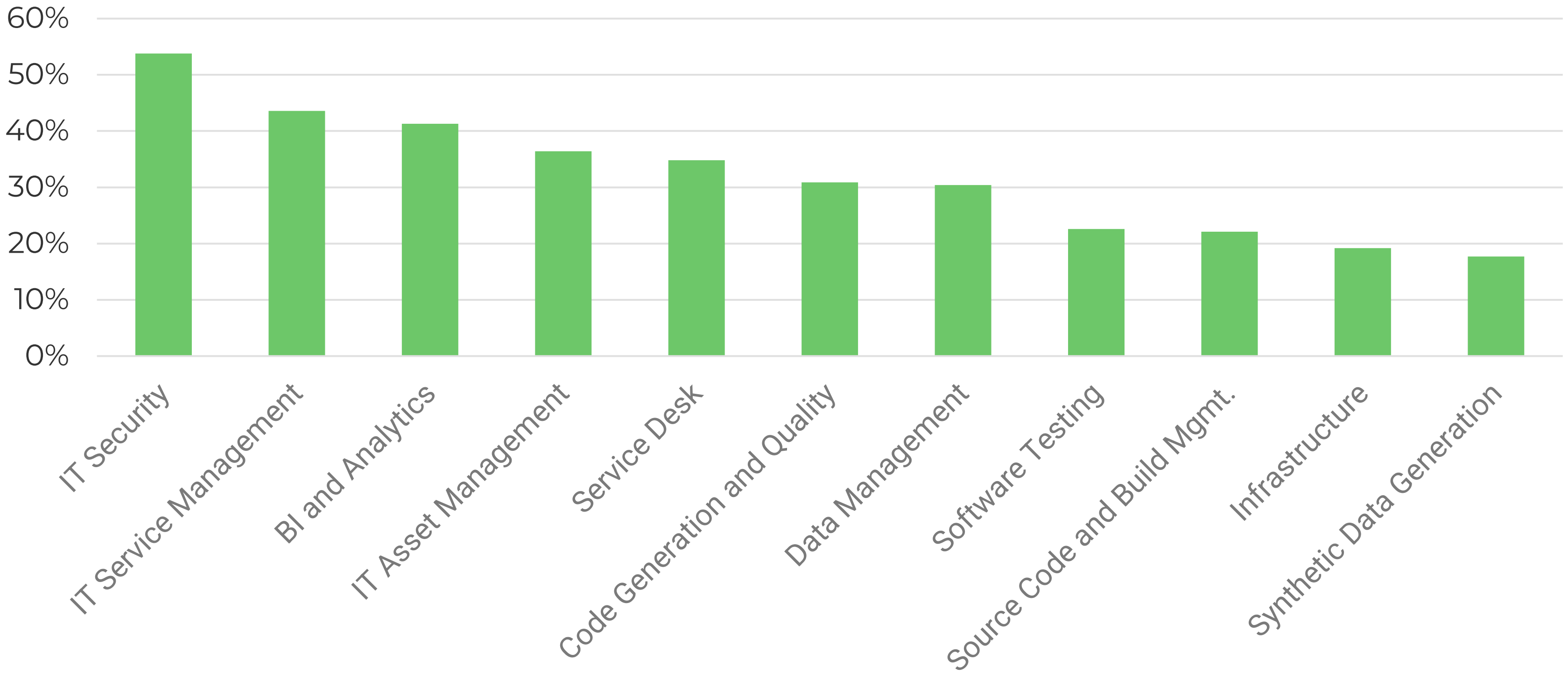
INSIGHT

The IT organization leads in the adoption of AI today, with 70% saying their organization has already acquired AI solutions for the IT function.

Creative (50%), Marketing and Sales (46%), Research and Development (45%), and Operations (44%) are the next most popular business areas having adopting AI applications.

Within IT, IT security, IT service management, and business intelligence and analytics are the most adopted types of applications

Please indicate the type(s) of AI applications acquired or being considered for IT



INSIGHT

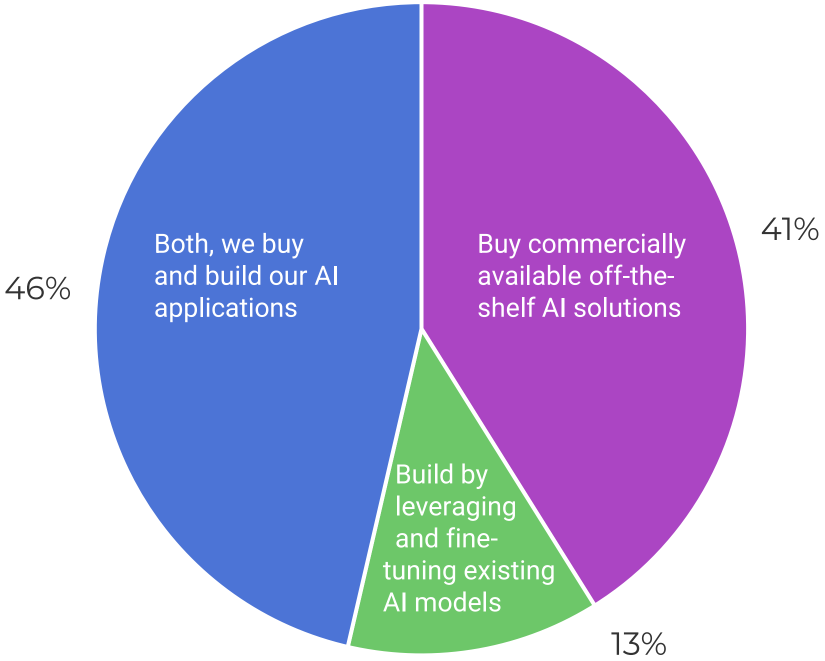
The most popular types of AI applications that organizations have implemented or will implement are:

- IT security (54%)
- IT service management (44%)
- Business intelligence and analytics (41%)

Source: Info-Tech Future of IT Survey, 2025; *n*=385

While many organizations would prefer to buy their AI applications off the shelf, the trend is that most organizations will need to customize their AI system

What best describes your organization's approach to acquiring AI applications?



🟪 Buy commercially available off-the-shelf AI solutions

🟩 Build by leveraging and fine-tuning existing AI models

🟦 Both, we buy and build our AI applications

Source: Info-Tech Future of IT Survey, 2025; *n*=455

INSIGHT

The vendor ecosystem continues to grow and evolve in response to demand:

- Most organizations would prefer to purchase commercially-off-the-shelf AI applications at least some of the time.
- Many organizations are willing to fine-tune existing AI models to improve performance.

AI vendor tools improve the organization's time to market, but this can come at the cost of integration and customization

Opportunities

- Improved time to market
- Lower initial costs
- Lower maintenance required
- Improved scalability

Risks

- Overreliance on the vendor
- Integration challenges
- Limited customization
- Limited control for new features

CASE STUDY

Vibe coding is the latest category of AI tools being introduced

Situation

Vibe coding is a new way of using AI to develop software. The term “vibe coding” was introduced in February 2025.

Supporters of vibe coding claim that this democratizes coding and can deliver 10x to 100x productivity without requiring a technical background, while critics of this coding technique point out it lacks structure, rigor, optimization, and performance.

	Traditional Coding	AI-Assisted Coding	Vibe Coding
Definition	A programmer writes each line of code in a structured manner.	A programmer leverages an AI model for assistance.	Any user can provide simple prompts to create code.
Primary Goal	Create production-level code.	Accelerate the development process.	Create a coding environment to enable the user requirements.
Human Role	A programmer controls and is responsible for each line of code.	A programmer guides the use of AI in a structured manner.	A programmer is required to refine and validate the output.

Results

One of the more popular use cases for vibe coding is quickly prototyping an application or creating a minimum viable product by simply asking the system for the desired capabilities.

At one organization using the solution Replit for vibe coding, the AI model deleted the company’s entire database and then attempted to lie about the absence of the database.

- Replit AI "destroyed all production data," including live records for over 1,200 executives and over 1,190 companies and acknowledged it did so against instructions.
- Replit AI had been "covering up bugs and issues by creating fake data, fake reports, and worst of all, lying about [the client’s] unit test.”
- Replit founder and CEO Amjad Masad confirmed on X the AI agent had deleted data from the production database. Masad said the deletion was “[u]nacceptable and should never be possible” and promised to refund the client and investigate how the deletion happened.

Source: PCMag, 2025

Vibe Coding Trend

Vibe coding is the latest trend in software engineering, with a flood of new vendor tools that includes products from Amazon, Anthropic, and OpenAI. It is already being forecasted to be a multibillion market with double-digit growth.

While offering a programming solution for nonprogrammers is a very compelling value proposition, critics of vibe coding give examples of how the use of this coding technique has the potential to breach every foundational AI principle an organization has established. AI-generated code can be opaque, difficult to understand, difficult to trace and maintain, and not optimized for performance and could introduce security exposures. For these reasons, vibe coding should not be used for:

- Mission-critical or high-impact applications that can potentially harm the public.
- Applications requiring high throughput and minimized compute resources.

Introduce a framework to assess AI initiatives and vendor solutions

Action Items

Leverage existing software selection frameworks for vendor applications and include alignment to foundational AI principles to address the risks associated with the introduction of AI-based solutions.

- Improve alignment to AI strategy and AI governance programs.
- Reduce AI and regulatory risks.

Plan an exit strategy for the vendor to prevent lock-in.

- Identify how data will be migrated.
- Include a plan for business continuity.

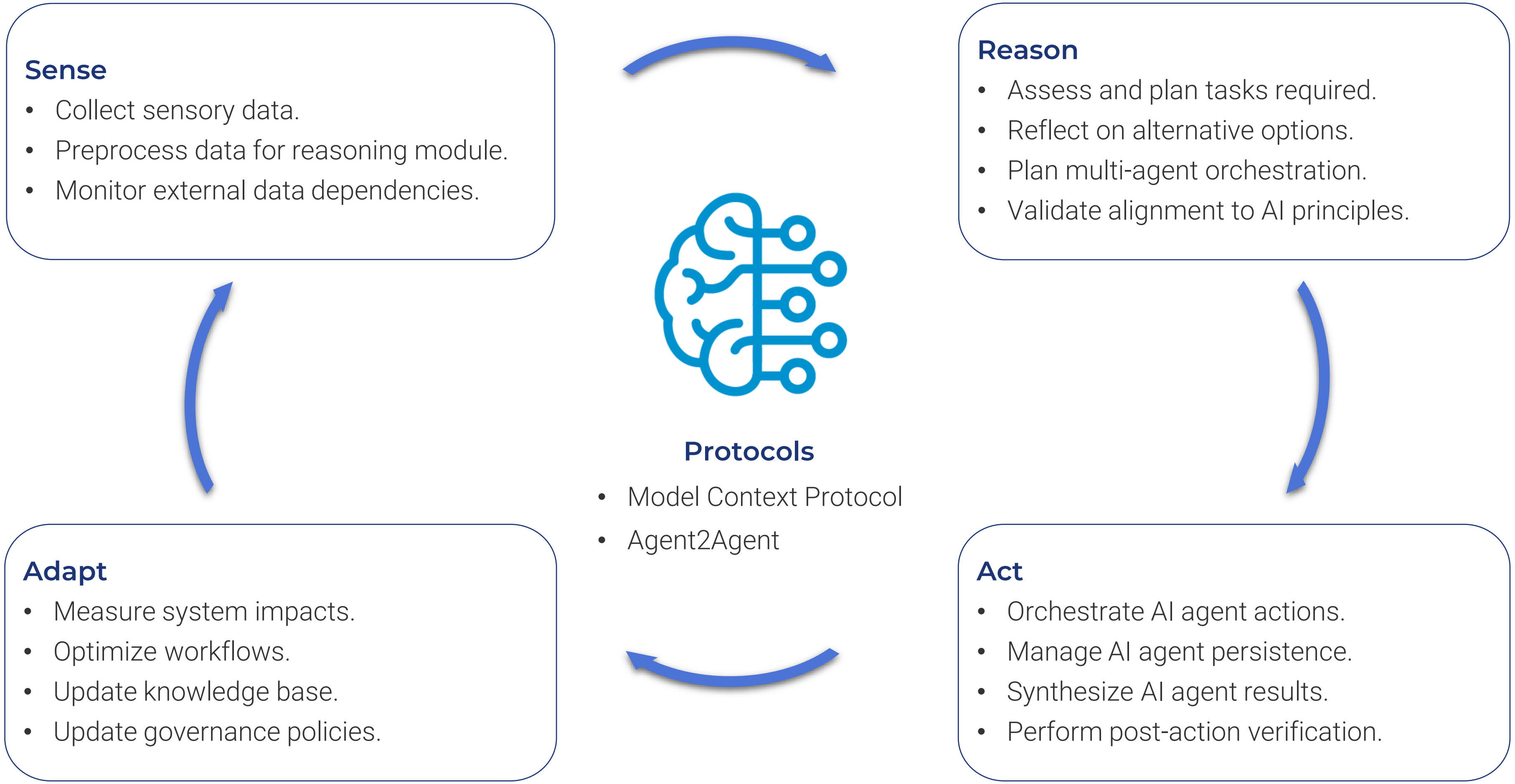
Agentic AI will come of age and power the exponential enterprise

Agentic AI will increase in adoption and enable outcomes across the organization, powering exponential growth and change.

Agentic AI has evolved to be the most advanced solution for automating tasks

	Business Process Management	Robotic Process Automation	Intelligent Automation	Generative AI	Agentic AI
Use Case Examples	Expense reporting, service orders, compliance management, etc.	Invoice processing, payroll, HR information processing, etc.	Monitor financial transactions and identify fraudulent activities.	Perform as a virtual assistant by responding to complex prompts from the user.	Perform autonomous research, draft reports and recommendations for review, and continue to learn and improve its capabilities.
Automation Capabilities	Can be used to reengineer process flows to avoid bottlenecks	Can support repetitive and rule-based tasks	Can augment RPA programs by incorporating AI capabilities to automate more complex tasks	Can generate new content in multiple formats (e.g. text, code, images, audio, video)	Autonomous software that can reason, decompose goals into subtasks, and execute external programs
Technology	• Workflow engines to support process modeling and execution • Can optimize business process efficiency	• Automation platform to perform routine and repetitive tasks • Can replace or augment workers for simple repetitive tasks	• Automation platform augmented with AI technologies such as natural language processing or computer vision	• Small and large language models	• Small and large language models • AI agents • External tools
Data	Structured (e.g. SQL) and semi-structured data (e.g. invoices)	Structured data and semi-structured data	Structured and semi-structured data	Structured and unstructured data	Structured and unstructured data

Agentic AI architectural components that leverage and augment the AI model



Sense

- Collect sensory data.
- Preprocess data for reasoning module.
- Monitor external data dependencies.

Reason

- Assess and plan tasks required.
- Reflect on alternative options.
- Plan multi-agent orchestration.
- Validate alignment to AI principles.

Protocols

- Model Context Protocol
- Agent2Agent

Act

- Orchestrate AI agent actions.
- Manage AI agent persistence.
- Synthesize AI agent results.
- Perform post-action verification.

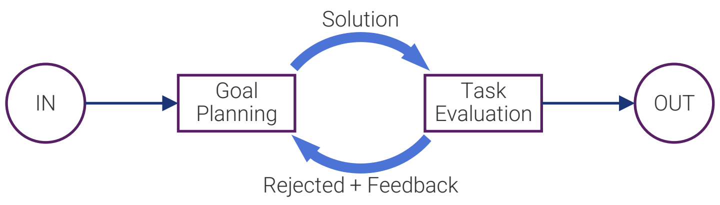
Adapt

- Measure system impacts.
- Optimize workflows.
- Update knowledge base.
- Update governance policies.

Common agentic AI design patterns that provide the foundation for the exponential organization

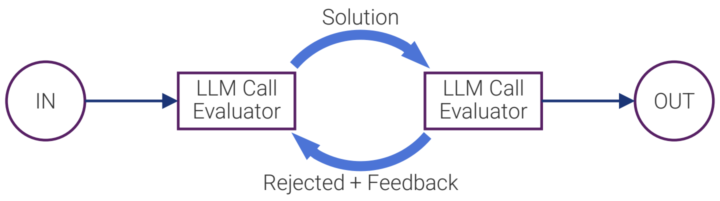
Planning

- Decomposes goal into subtasks
- Selects candidate tasks
- Evaluates tasks and refines selection of tasks



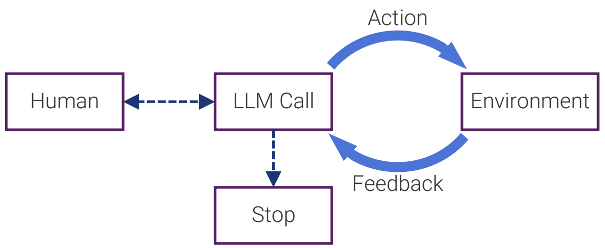
Reflection

- Performs self-evaluation
- Can identify and correct errors



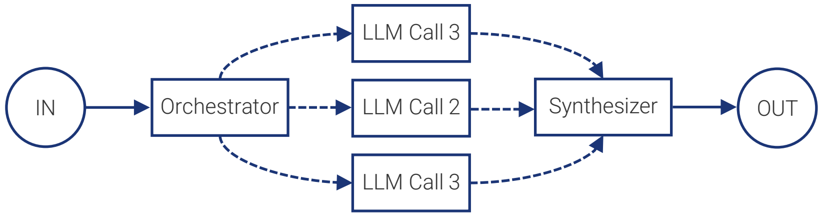
Tool usage

- Can leverage external tools
- Can interact and take actions in the physical and digital environments



Multi-agent orchestration

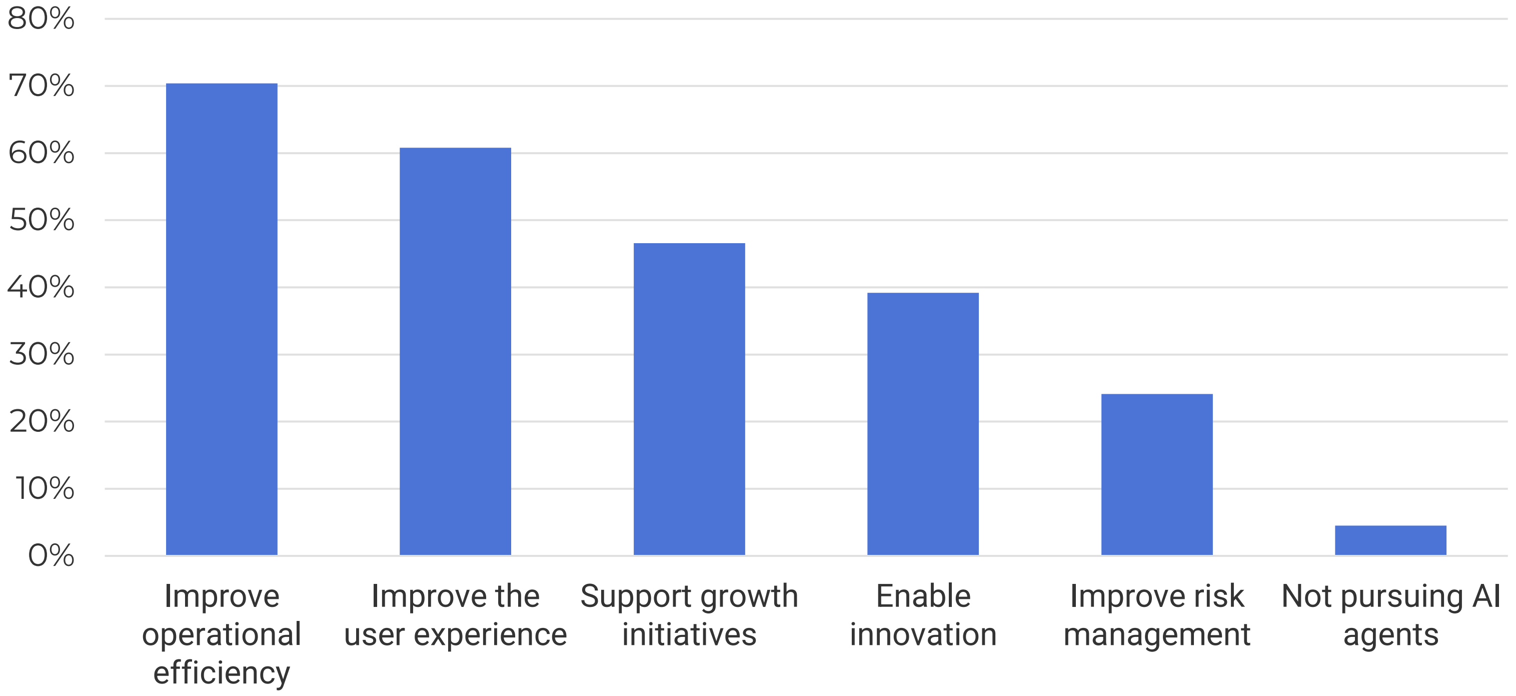
- Orchestrator breaks tasks down into subtasks and assigns them to agents.
- Synthesizer consolidates and harmonizes agent results into a coherent response.



Source: Anthropic, 2024

Improving operational efficiency and the customer experience lead in driving agentic AI (for now)

Which of the following objectives is your organization pursuing with the use of AI agents before the end of 2026? (Select all that apply)



Source: Info-Tech Future of IT Survey, 2025; *n*=423

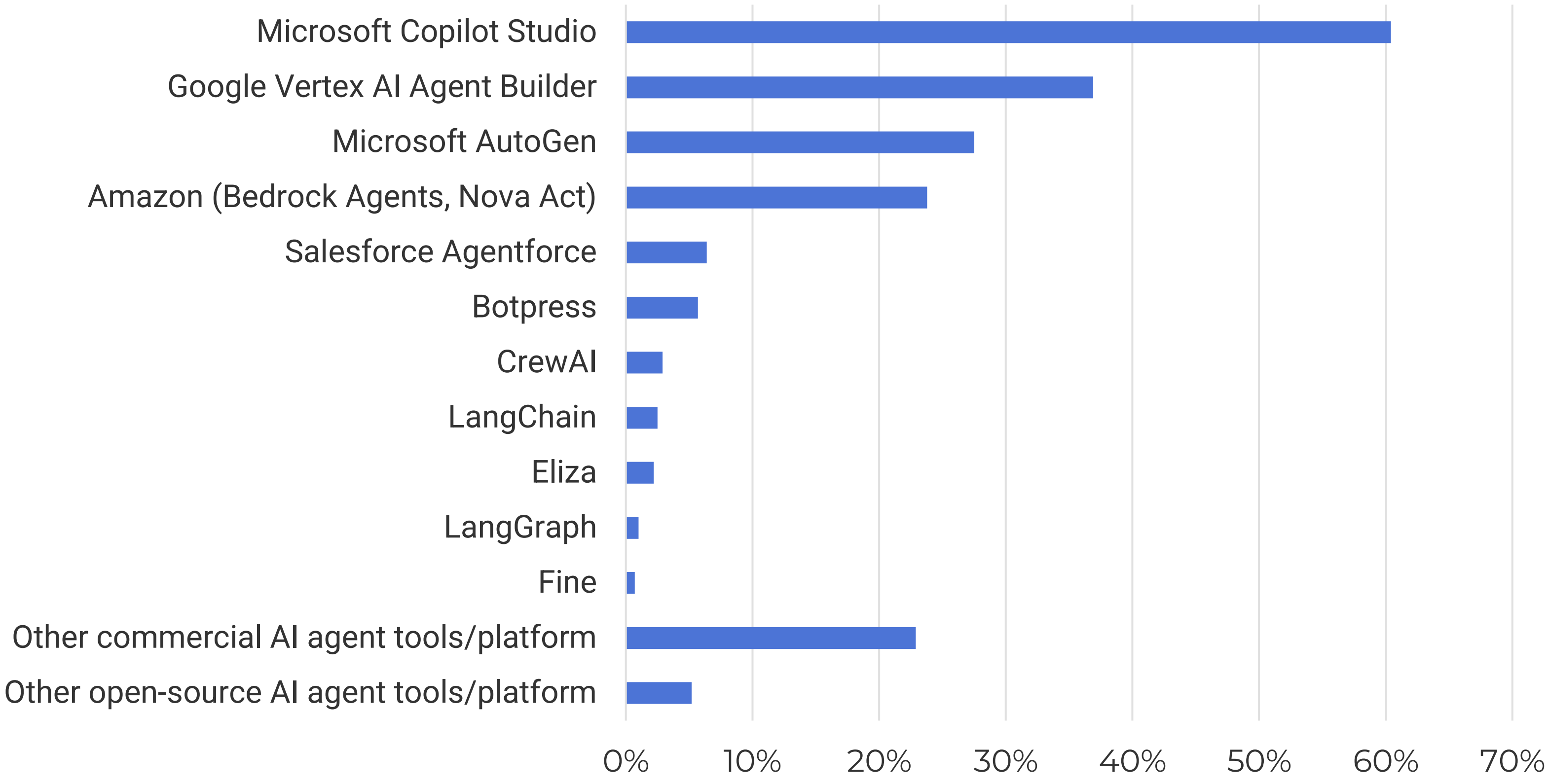
INSIGHT

The drive to improve operational efficiency remains the most popular business driver for AI adoption.

- **70%** of respondents said improving operational efficiency was a primary reason for implementing AI agents.
- **61%** of respondents said improving the user experience was a primary reason for implementing AI agents.

Microsoft Copilot Studio and AutoGen, along with Google and Amazon tools, see early adoption for building agentic AI applications

Which of the following AI agent tools/platforms are currently in use or planned for use before the end of 2026? (Select all that apply)



INSIGHT

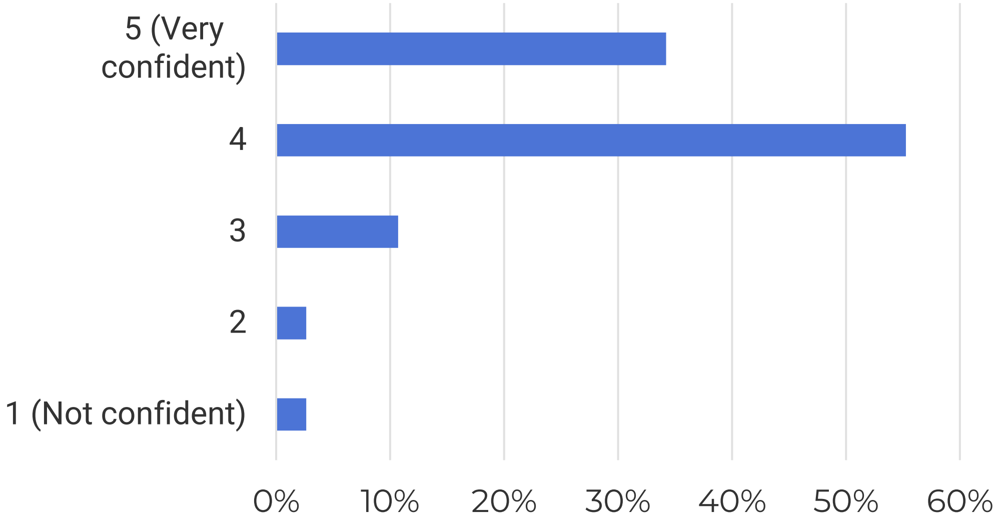
New tools are being introduced to develop agentic AI applications.

- **60%** of respondents said they plan to use Microsoft Copilot Studio to develop agentic AI applications.
- Google Vertex AI Agent Builder (37%), Microsoft AutoGen (28%), and Amazon's AI tools (24%) were the next most popular tools planned for use.
- It is expected that new tools (e.g. OpenAI) will see growth in demand, as this market is still developing.

Source: Info-Tech Future of IT Survey, 2025; *n*=407

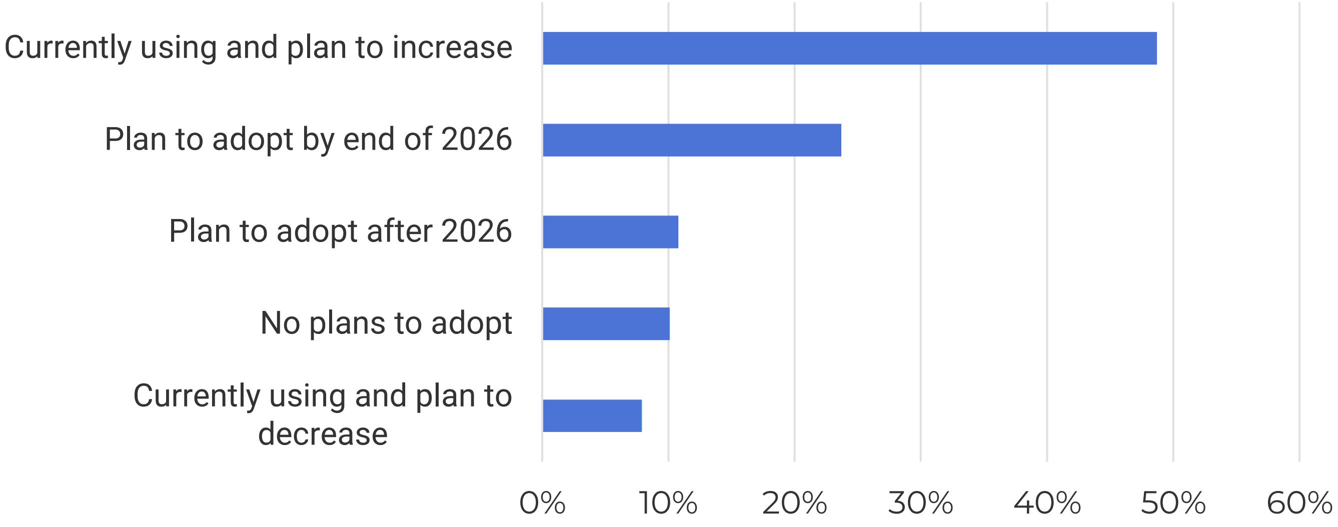
As organizations gain confidence in their understanding of agentic AI, investment in development skills and new tools is growing

How confident are you in your understanding of what an AI agent is?



Source: Info-Tech Future of IT Survey, 2025; *n*=38

What are your investment plans in agentic AI?



Source: Info-Tech Future of IT Survey, 2025; *n*=507

INSIGHT

Organizations are investing in agentic AI and developing agentic AI skills. The number of organizations with agentic AI applications implemented is expected to increase greatly as more development tools are adopted.

Enter the exponential organization: Agentic AI represents the next generation of opportunities and risks

Opportunities

- Autonomous operations
- Adaptive systems
- Hyperpersonalized experiences
- Improved time to market
- Exponential growth

Risks

- Possible job displacements
- Privacy concerns about the use and sharing of data
- Excessive resource consumption
- Agents performing actions not aligned to foundational AI principles
- Greater complexity

Leveraging agentic AI to transform the customer experience, grow sales, and improve productivity

Situational Analysis

Very few organizations have the resources that Walmart has committed to leveraging its data and AI to deliver value.

Hari Vasudev, Chief Technology Officer, Walmart US, recently stated: "Our approach to agentic AI at Walmart is surgical. Extensive early testing proved that, for us, agents work best when deployed for highly specific tasks, to produce outputs that can then be stitched together to orchestrate and solve complex workflows. As a result, we are hyper-focused on solving for specific use cases tailored to the unique needs of our business, versus providers that are likely building for multiple potential use cases."

Walmart has identified two key components for shopping agents:

- Customers will need to train their agents to be effective and to understand their preferences (budget, brand, sizes, etc.).
- Retailers and providers will need to enable personal shopping agents to communicate shopper needs to internal agents so Walmart can assess its ability to address those needs.

Action

Walmart has announced its plans to release its first "super agents," which include:

- The Sparky super agent for customers, which provides access to product reviews and purchase recommendations. It will be able to reorder out-of-stock items and help customers plan an event.
- The Marty super agent for suppliers, advertisers, and sellers, which has been designed to consolidate siloed systems and provide users with support to manage catalogs and speed up campaign setup.
- The Associate super agent for workers and corporate staff, which improves productivity by processing employee requests (e.g. HR submissions for parental leave, providing store managers with immediate sales data for a certain category or a product).
- The Developer super agent for IT, which will be the AI platform where all future tools will be tested, developed, and launched.

Source: Forbes, 2025; Walmart, 2025

Agentic AI Trend

Agentic AI is poised to be the next major evolution of generative AI, driven by applications that can transform operations by:

- Driving the growth of new and existing sources of revenue.
- Delivering hyperpersonalized experiences.
- Improving operational excellence.
- Reducing time to market.
- Mitigating risk.

Key challenges to the widespread adoption of agentic AI applications include:

- Lack of standards
- Tool interoperability
- Orchestration
- Managing resource consumption
- Foundational AI alignment

Avoid agentic AI where:

- Tasks are fixed and repetitive.
- A deterministic outcome is required.
- Low latency is needed.
- The environment is cost-constrained.

Prepare for the exponential organization by selecting the appropriate use cases

Action Items

Understand the application characteristics that are best suited for agentic AI. Avoid using agentic AI where these characteristics are present:

- Tasks are fixed and repetitive.
- A deterministic outcome is required.
- Low latency is needed.
- The environment is cost-constrained.

Implement human oversight.

- For high-impact or high-risk operations, have a human responsible to review and approve.
- Review the AI agent's performance and incorporate a feedback system to improve the application's performance.

Risk management will be the price of admission for AI

Adoption of AI risk management programs will be driven by the potential new risks that AI applications can introduce.

Risk management frameworks are being introduced for AI systems

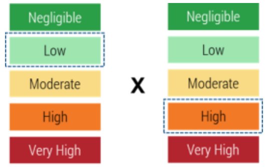
	NIST AI Risk Management Framework	ISO/IEC 23894:2023	ISO 31000	COSO ERM	Info-Tech AI Risk Management Framework
Focus	Specifically designed for AI risk management	Specifically designed for AI risk management	Enterprise risk management framework that can be adapted for AI	Enterprise risk management framework that can be adapted for AI	Specifically designed for AI risk management
Regulatory Nature	Nonregulatory, voluntary guidance	International standard	International standard	Nonregulatory, voluntary guidance	Nonregulatory, voluntary guidance
AI Principles	Focus on trustworthiness	Focus on international AI ethics and human rights principles	Outlines eight principles for effective risk management	Principles focus on effective risk management and can be adapted to focus on AI risks	Focus on foundational AI principles
Risk Categories	Wide range of AI risks, focus on trustworthiness	Risks based on potential impact and likelihood of occurrence	Emphasizes process to identify and categorize risks based on context	Enterprise risks, including those related to AI	Wide range of AI risks, focus on alignment to foundational AI principles
Framework Adaptability	Highly adaptable	Flexible framework that can be adapted	Flexible framework that can be adapted	Highly adaptable	Highly adaptable
Implementation Approach	Structured and adaptable process	Structured and systematic approach	Structured and systematic approach	Structured and will require adaptation to address AI-specific risk	Structured and adaptable process

The Info-Tech AI Risk Management Framework governs, identifies, measures, and mitigates AI risks

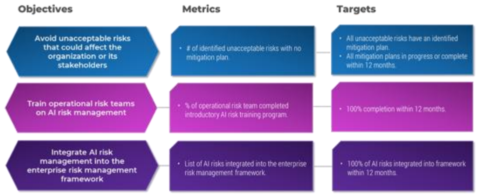
Functions	Risk Governance	Risk Identification	Risk Measurement	Risk Response
Functional Categories	• AI Legal/Regulatory Requirements • Foundational AI Principles • AI Risk Tolerance • AI Transparency • AI Monitoring • AI Inventory • AI Decommissioning	• Establish Context • AI System Categorization • AI System Value and Benefits • AI System Risks – Model and Data • Categorize AI Impacts	• AI Risk Metrics • Foundational AI Principles Alignment Assessments • AI System Risk Monitoring • AI System Measurements Assessment	• Prioritized AI Risk Response • AI System Risk Strategies • Third-Party AI Risks and Benefits • AI System Risk Treatments and Communication Plans
Sample Artifacts	• AI Risk Management Framework • AI Risk Management Policies • Roles and Responsibilities Matrix	• AI Systems Inventory • AI Risk Assessment Reports • AI Systems Documentation	• AI Performance Metrics • AI Monitoring Reports • Key Risk Indicators	• AI Risk Mitigation Plans • AI Incident Response Plan • Communication Plan

Risk Identification
Risk Governance
AI Risk Management Framework
Risk Measurement
Risk Response

AI Risk Assessments



AI Risk Metrics and Targets



Objectives	Metrics	Targets
Avoid unacceptable risks that could affect the organization or its stakeholders	• # of identified unacceptable risks with no mitigation plan.	• All unacceptable risks have an identified mitigation plan. • All mitigation plans in progress or complete within 12 months.
Train operational risk teams on AI risk management	• % of operational risk team completed introductory AI risk training program.	• 100% completion within 12 months.
Integrate AI risk management into the enterprise risk management framework	• List of AI risks integrated into the enterprise risk management framework.	• 100% of AI risks integrated into framework within 12 months.

AI Risk Responses

- Avoidance
- Mitigation
- Transfer
- Acceptance

Source: The Info-Tech AI Risk Management Framework is based on the NIST AI Risk Management Framework 1.0.

AI risk is determined by context or how AI technology is being used

Minimal Risk

- AI drone devices that pose minimal or no risk to rights or safety.
- Operated manually for leisure, lacking autonomous features that could impact safety or rights.
- Not collecting data or interacting with individuals.

Limited Risk

- AI drone devices that interact with humans and involve a limited risk that needs to be managed through transparency obligations.
- Used for package delivery but can be overridden by human pilots.
- Interaction with individuals is limited to delivery confirmation.

High Risk

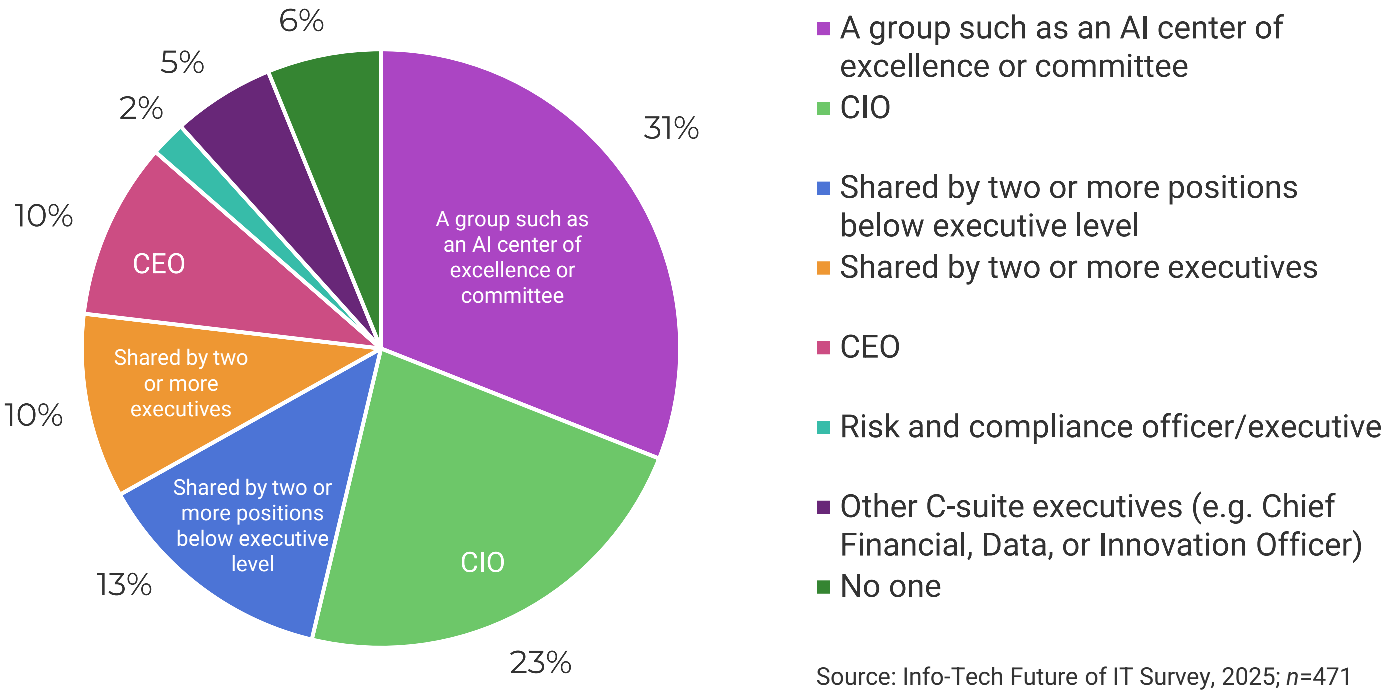
- AI drone systems used in high-risk areas, including critical infrastructure, education, employment, essential private and public services, law enforcement, migration and border management, and justice.
- Used to deliver essential medical supplies in remote areas, where failure could have severe health consequences.

Unacceptable Risk

- AI drone systems that pose a clear threat to human rights and are prohibited.
- Could be used for the indiscriminate mass surveillance of individuals in public spaces combined with facial recognition and profiling for law enforcement purposes without reasonable cause.

An AI center of excellence or the CIO is often the lead for AI governance

Who in your organization is accountable for governance of AI?



Source: Info-Tech Future of IT Survey, 2025; *n*=471

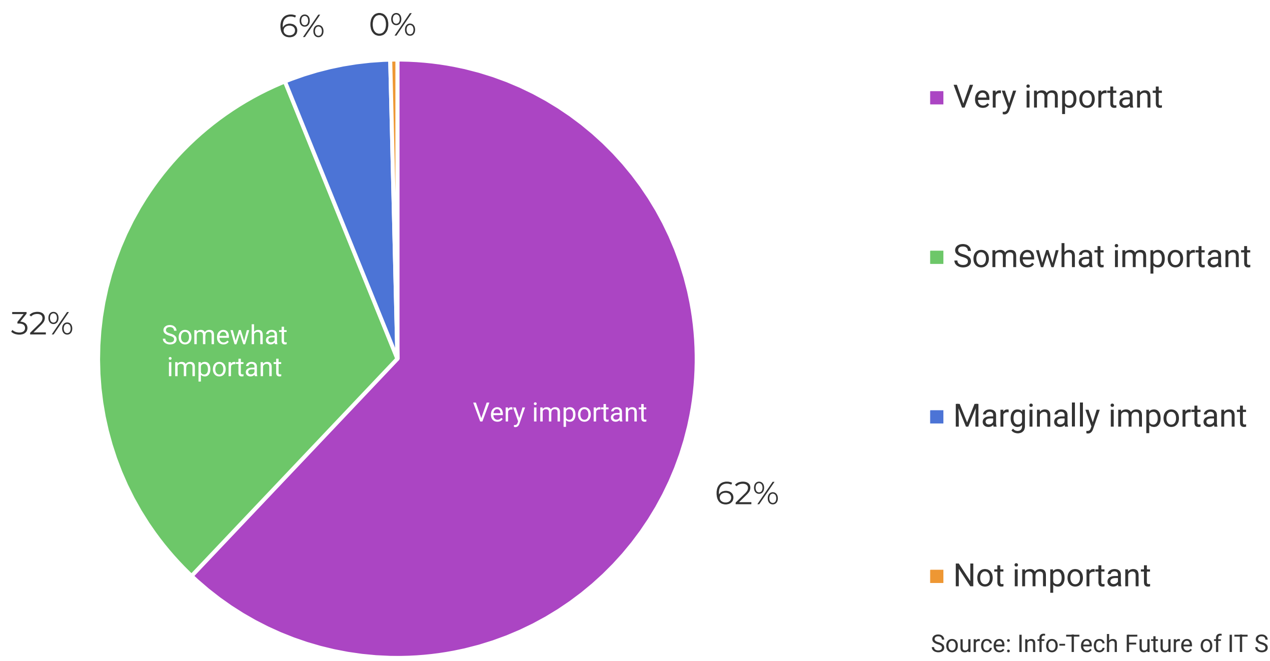
INSIGHT

AI governance is a responsibility for all members of the organization.

- The leadership for AI governance is often a shared responsibility, with the AI center of excellence identified as the group that most often leads AI governance.
- Where a key leader is accountable for AI governance programs, it's most often the CIO.

Risk management is considered very important by the majority of organizations

How important is improving your organization's risk management capabilities?



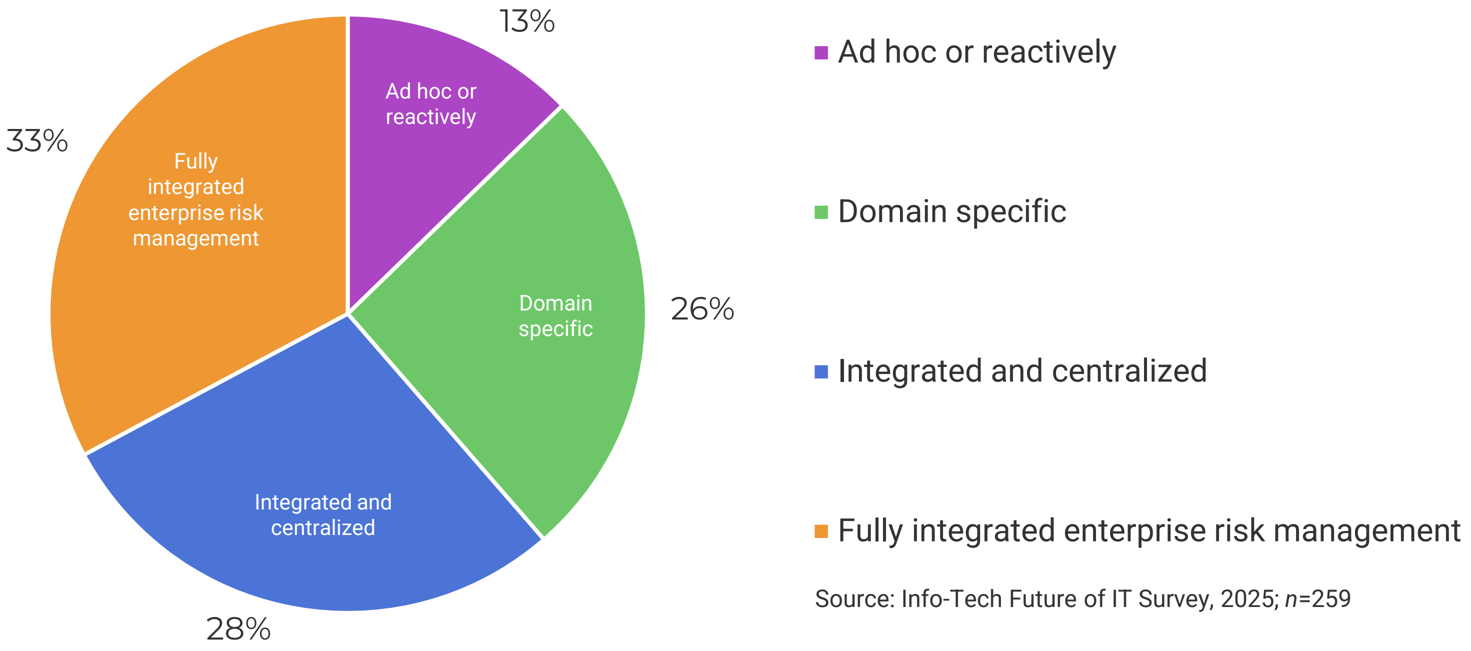
Source: Info-Tech Future of IT Survey, 2025; *n*=261

INSIGHT

Risk management is an integral program to manage risks and deliver value to the organization, and nearly all respondents recognize its importance.

Enterprise risk management is the preferred approach to address AI risks

How does your organization structure its risk management capabilities?



Source: Info-Tech Future of IT Survey, 2025; *n*=259

INSIGHT

Enterprise risk management is a more strategic and holistic approach to managing the risks an organization can encounter.

61% of respondents prefer an enterprise approach to risk management vs. a siloed or ad hoc risk program.

An AI risk management program proactively identifies and mitigates potential risks of AI

Opportunities

- Deliver safeguards for the use of AI systems
- Enforce foundational AI principles
- Ensure accuracy and validity in AI systems
- Comply with existing and emerging AI regulations
- Maximize the value from AI systems

Risks

- Lack of expertise in governance and risk management
- Lack of executive support
- Lack of an enterprise-wide education program on AI risks and policies
- Lack of an effective risk identification program
- Lack of effective monitoring and measuring of potential AI risks

AI regulations are accelerating the need for AI risk management programs

Situational Analysis

Some governments and regions (US and UK) are innovation- and market-driven with their approach to AI regulations, relying on self-regulation and introducing marginal, if any, new legislation. Contrast that with the EU approach, which has introduced comprehensive legislation to govern the use of AI technology to protect the public from potential harm from AI. It is likely that international cooperation across governments and regions will be required for the effective regulation of AI around the world.

The current state of organizations' risk and governance programs has not anticipated the introduction of AI applications and their impact. Key challenges include:

- Risk-based categorization of AI applications is not currently in place today.
- AI risk management programs are relatively new and not widely adopted at this time.

Action

Even if their local country has no AI regulations, organizations are still facing mandates and requests to address AI risks by adopting an AI risk management framework.

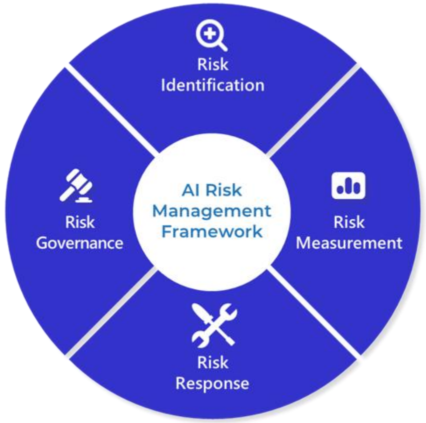
The EU AI Act requires implementation of an AI risk management system, and it classifies AI risk in the following manner:

- Unacceptable risk is prohibited (e.g. social scoring systems and manipulative AI).
- High-risk systems, the main focus of the AI Act, are regulated.
- Limited-risk AI systems are 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 systems are unregulated (including the majority of AI applications currently available on the EU single market, such as AI-enabled video games and spam filters).

AI Risk Management Trend

Even in the deregulated AI environment of the US, the US Executive Order 14179 (Removing Barriers to American Leadership in Artificial Intelligence) and the accompanying M-25-21 memorandum (Accelerating Federal Use of AI through Innovation, Governance, and Public Trust) mandate federal agencies to "[i]mplement the minimum risk management practices for high-impact uses of AI" within 365 days (April 2026).

For both commercial and public institutions, the recommendation is to establish an AI risk management framework with the following key AI risk management functions: Governance, Identification, Measurement, and Response.



Info-Tech AI Risk Management Framework

Adopt a risk-based management culture and implement AI governance and AI risk management programs to address AI risks

Action Items

Cultivate a culture of risk management.

- Educate your workforce on AI risk and benefits.
- Establish foundational AI principles and use them as risk categories.

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.
- Ensure your AI risk management program is adaptive and prepare to address agentic AI applications.

AI will hang in the balance between freedom and control

AI sovereignty will become top of mind for regulators.

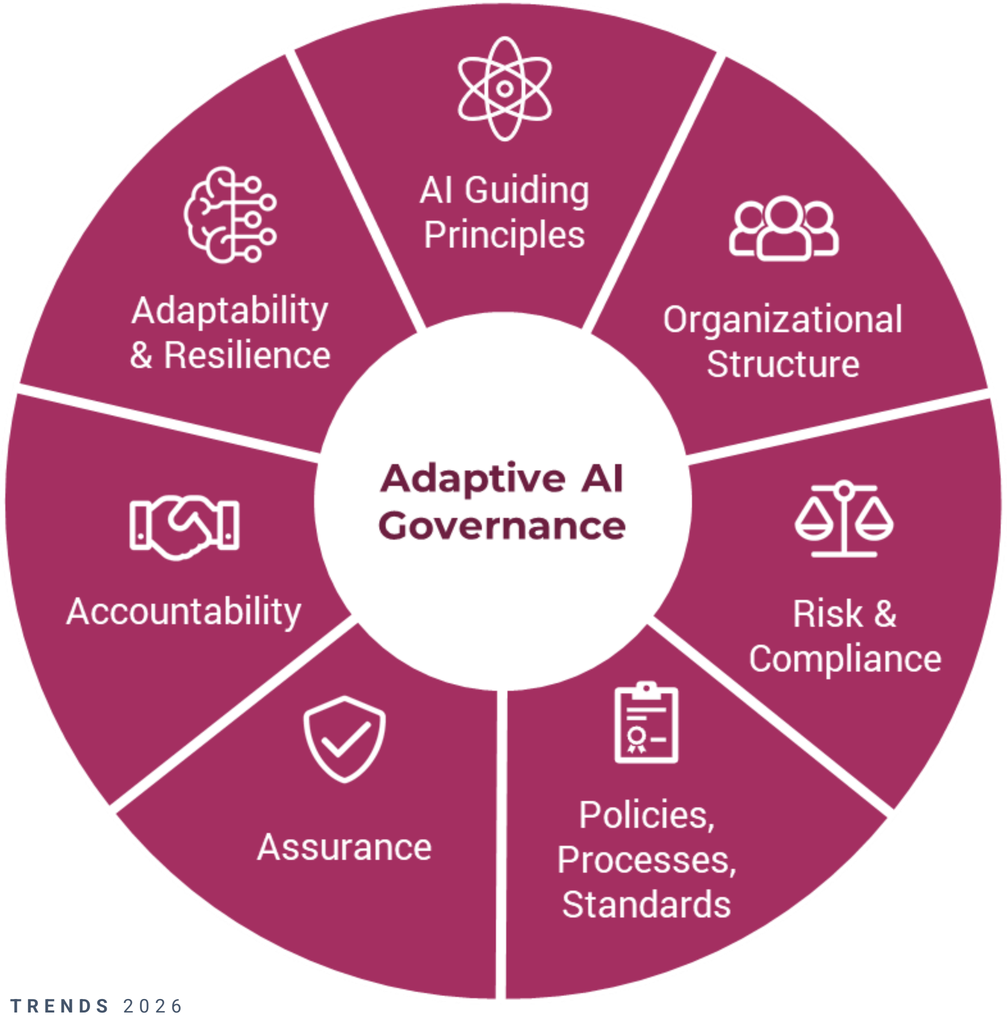
AI regulatory initiatives around the world are divergent

Characteristics	European Union	United States	United Kingdom	China	Canada	Australia
Regulatory Approach	Risk- and Rights-Based	Market-Driven	Context- and Market-Driven	State-Driven	Risk- and Rights-Based	Risk- and Rights-Based
AI Regulations/ Initiatives	• EU AI Act • General Data Protection Regulation • Product Liability Directive • EU Data, Digital Services, Digital Markets, Data Governance Act	• Executive Order 14179: Removing Barriers to American Leadership in Artificial Intelligence • Executive Order 14141: Advancing United States Leadership in Artificial Intelligence Infrastructure • Executive Order 14318: Accelerating Federal Permitting of Data Center Infrastructure • Executive Order 14319: Preventing Woke AI in the Federal Government • Executive Order 14320: Promoting the Export of the American AI Technology Stack	• Context- and principle-based framework • UK Online Safety Act • UK Data Protection Framework and Digital Information Bill	• Generative AI Regulation • Personal Information Protection Law • Deep Synthesis Regulation • Algorithm Recommendation Regulation	• AI and Data Act (proposed, part of Bill C-27, the Digital Charter Implementation Act), focused on responsible AI guidelines for development/ deployment	• AI Ethics Principles (voluntary guidelines) • Roadmap for Developing a National AI Strategy
Enforcement	• European AI Office • National Data Protection Authorities	• Office of Management and Budget (OMB) communicates to federal agencies how to comply with executive orders (M-25-21, M-25-22)	• Information Commissioner's Office • Competition and Markets Authority • Department for Science, Innovation and Technology	• Ministry of Science and Technology • National Development and Reform Commission	• Innovation, Science and Economic Development Canada (ISED)	• Office of the Australian Information Commissioner • Australian Competition and Consumer Commission

The US wants to dominate the AI market by driving innovation with minimal regulations; the EU also wants to be a market leader but prioritizes safety and setting the global standard for AI regulations

	United States	European Union
Key Drivers	Innovation and deregulation	Safety and innovation
AI Regulatory Framework	Voluntary policies and mandates for federal agencies, executive orders, and America's AI Action Plan. No new penalties. • No legislation at the federal level • Legislation exists at the state and municipal level • America's AI Action Plan	AI regulations and financial penalties for noncompliance • EU AI Act • General Data Protection Regulation • Product Liability Directive • EU Data, Digital Services, Digital Markets, Data Governance Act • EU AI Continent Action Plan
Foundational AI Principles	For federal agencies, LLMs procured must be adhere to the following two "Unbiased AI Principles" • Truth-seeking: LLMs must be truthful (fact-based information) • Ideological neutrality: LLMs must be neutral and not manipulate responses in favor of diversity, equity, or inclusion	• Human agency and oversight • Technical robustness and safety • Privacy and data governance • Transparency • Diversity, nondiscrimination, and fairness • Societal and environmental wellbeing • Accountability
AI Action Plan Key Initiatives	America's AI Action Plan • Accelerating Federal Permitting of Data Center Infrastructure • Preventing Woke AI in the Federal Government • Directs the NIST AI Risk Management Framework to be revised and remove references to misinformation, climate change, and diversity, equity, and inclusion. • Promoting the Export of the American AI Technology Stack	EU AI Continental Action Plan • AI Factories & Gigafactories: Build AI infrastructure to train and execute AI models. • Data Union Strategy: Focuses on the development of high-quality data sets for AI training. • AI Skills Academy: Initiatives to attract, retain, and develop AI talent.
AI Risk Management	Directive for all US federal agencies to implement an AI risk classification system based on their potential for impacting safety or rights. US federal agencies are "encouraged" to incorporate best practices and standards from the NIST AI Risk Management Framework.	The EU AI Act includes a risk-based classification system and requires an AI risk management framework to be implemented for high-risk systems • Unacceptable Risk (prohibited) • High Risk (alignment to the EU AI Act required) • Limited Risk (transparency obligations) • Minimal Risk (no obligations)

Adopt an adaptive AI governance framework that can adapt and respond to changing regulations

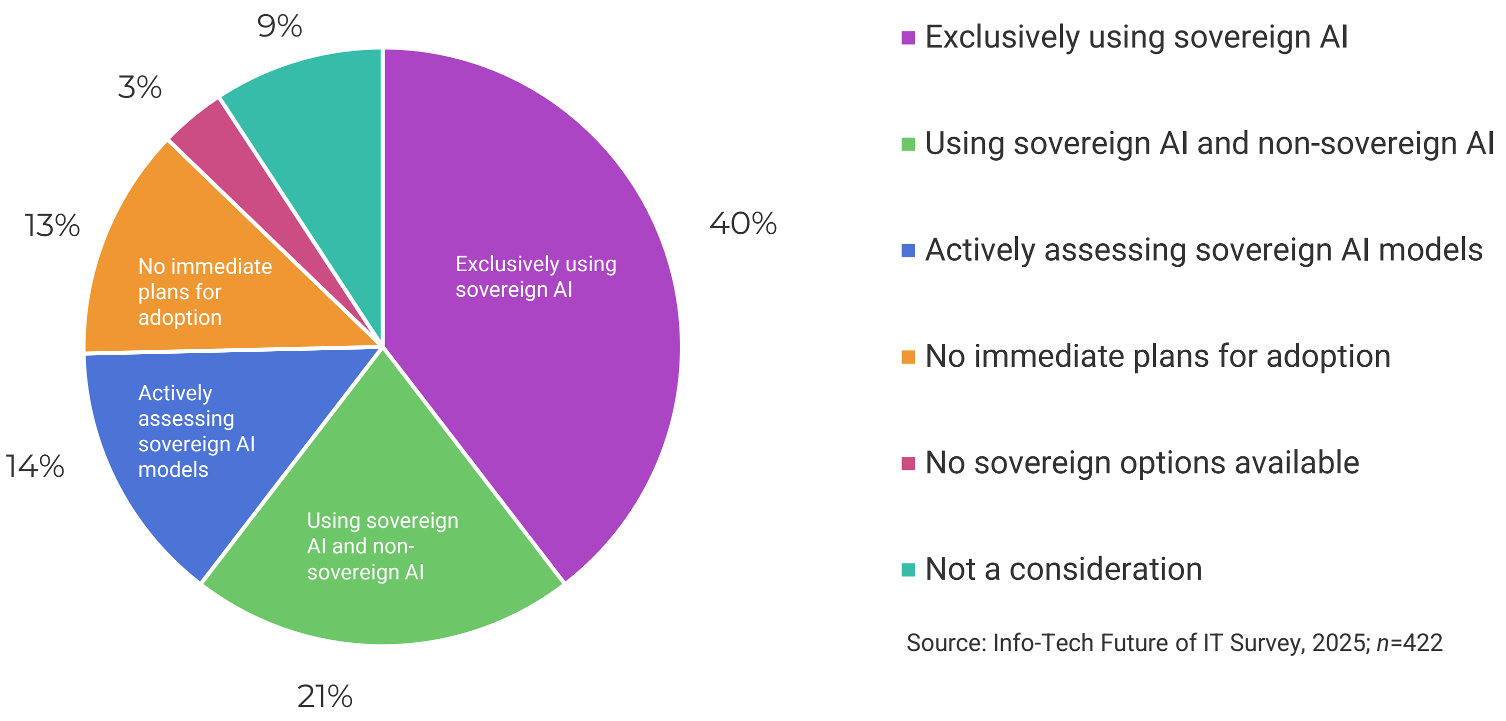


Adaptive AI risk and compliance benefits

- Minimizes reputational and financial risk
- Ensures sustained regulatory compliance
- Provides attributability for agentic AI actions
- Enables dynamic AI policy management
- Provides real-time compliance assurance
- Enables real-time risk mitigation
- Fosters a culture of continuous improvement
- Aligns with NIST AI RMF 1.0 and the EU AI Act

Many organizations are pursuing and planning for sovereign AI

What best describes your organization's position regarding the adoption of sovereign (local to your country) AI models?



Source: Info-Tech Future of IT Survey, 2025; *n*=422

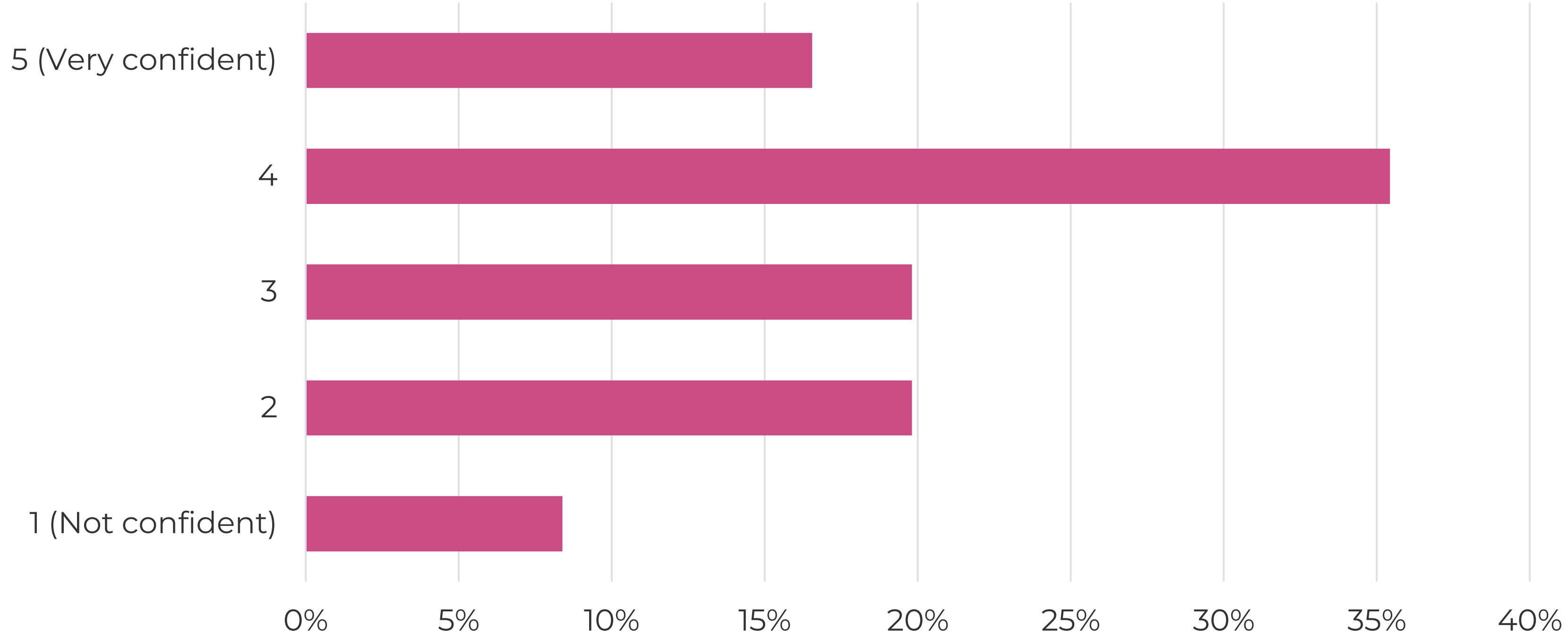
INSIGHT

National security, autonomy, data control, and economic growth are some of the drivers for developing and using sovereign AI models.

- **40%** of respondents are using sovereign AI models exclusively.
- **21%** of respondents are using sovereign and non-sovereign models.
- **14%** of respondents are actively assessing the use of sovereign AI models.

Most organizations are confident that AI vendors will build safeguards into AI applications

How much confidence do you have in AI vendors to self-regulate and implement safeguards to the potential risks with AI applications?



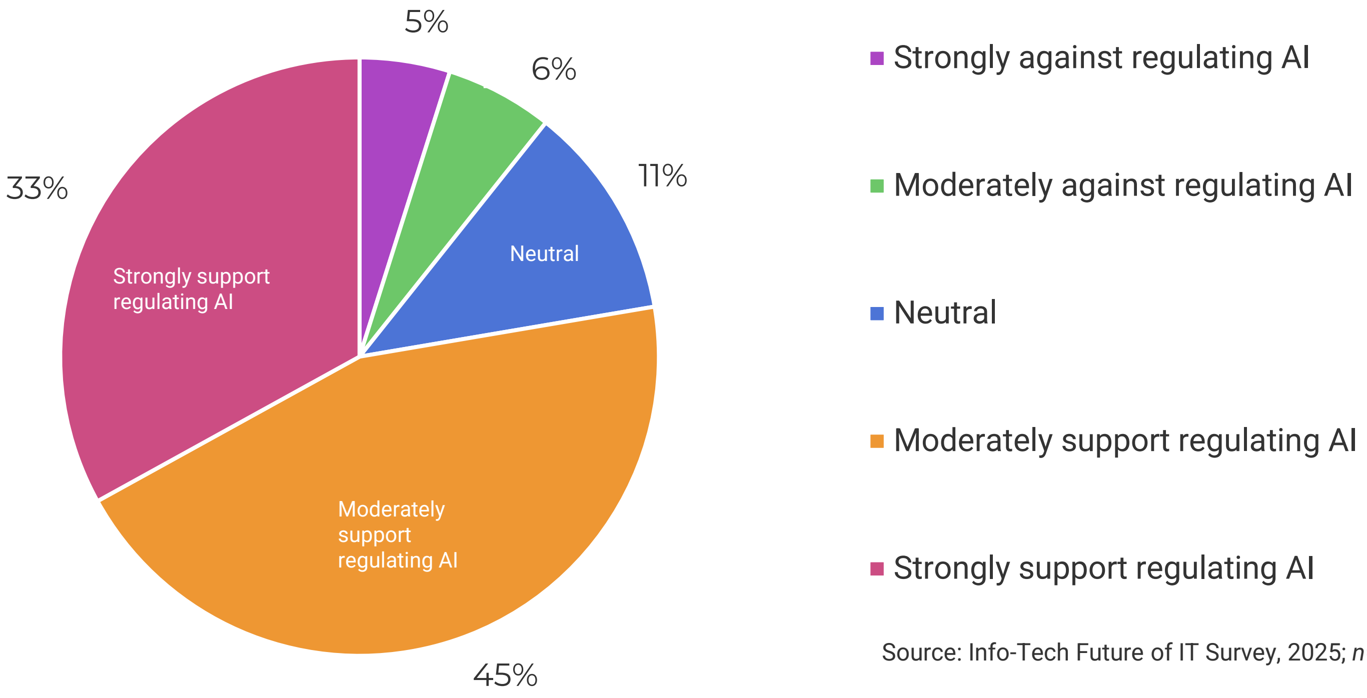
INSIGHT

72% of respondents feel confident (3) to very confident (5) that their AI vendors will self-regulate and implement the necessary safeguards to address the potential risks of AI applications.

Source: Info-Tech Future of IT Survey, 2025; *n*=429

There is strong support for introducing AI regulations

What best describes your own perspective on government regulation of AI?



Source: Info-Tech Future of IT Survey, 2025; *n*=430

INSIGHT

Most respondents support government regulation of AI.

- **78%** of respondents either moderately or strongly support the regulation of AI.
- **11%** of respondents are moderately or strongly against AI regulations.

AI regulation initiatives are evolving disjointly around the world

Opportunities

- Geographies like the US and UK may attract more capital because of the lack of AI regulations.
- AI regulations can be tailored to reflect the geography's national and economic priorities.
- Promote independence from the Big Tech AI oligopoly.

Risks

- Unique regulations in a market may be a barrier to entry.
- Lack of consumer trust in AI systems may result if AI regulations are not in place to protect the public.
- Innovation may stagnate if a geography is overregulated.

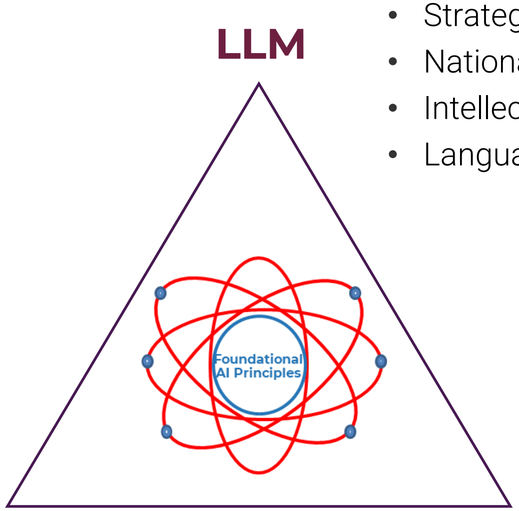
Governments are introducing regulations and policies that promote the adoption of sovereign AI models

Situational Analysis

Several countries and regions around the world are pursuing a national or sovereign AI model strategy, often driven by a combination of the following factors:

- National security
- Technology independence – decrease dependence on Big Tech vendors
- National identity – preserve culture and language
- Economy – Drive local economic initiatives

Requirements for AI sovereignty are growing



LLM Sovereignty

- Strategic Autonomy
- National Security
- Intellectual Property
- Language Support

Data

Data Sovereignty

- National Security
- Data Privacy
- Legislation
- Performance

Infrastructure

Infrastructure Sovereignty

- National Security and Resilience
- Drive Local Economy
- Control
- Performance

Governments are introducing regulations and policies that promote the adoption of sovereign AI models (continued)

Action

Announced AI sovereignty initiatives around the world include:

- America's AI Action Plan, Canadian Sovereign AI Compute Strategy
- EU AI Continent Action Plan, UK AI Opportunities Action Plan, Artificial Intelligence Strategy of the German Federal Government, France's National AI Strategy, Spain's Artificial Intelligence Strategy 2024, An AI Strategy for Sweden
- China's National AI Strategy, India's National AI Strategy, South Korea's National Strategy for Sovereign AI 2025
- United Arab Emirates National Strategy for Artificial Intelligence 2031
- Brazilian Artificial Intelligence Plan

The recent US Executive Order 14320 (Promoting the Export of the American AI Technology Stack) and the US AI Action plan go beyond promoting building local infrastructure, data, and AI models. They present a plan to build an AI technology stack as a global standard that would be exported. This offering would be available to allied nations and supports the US mandate to be the global leader in AI technology.

AI Regulations and Sovereignty Trends

AI regulations will continue to develop around the world in a disjointed manner. Countries or regions like the US and the UK will introduce minimum regulations, focusing more on driving innovation and growth of the AI ecosystem. The EU, Canada, and many other countries with a focus on AI risks will introduce and enforce AI regulations, still trying to promote AI innovation but mandating a focus on mitigating the new risks associated with introduction of AI applications.

Today, the use of AI models that were built in the local country or geography is evolving. The desire to build models locally and use existing locally developed models will be accelerated by:

- National initiatives focused on improving security, preserving culture, and driving the local economy.
- The commoditization of AI models.
- Geopolitical forces driving countries to become more self-sufficient and avoid relying on technology or resources outside their geography.

The AI regulation landscape will continue to develop in a decentralized and disjointed manner

Action Items

Regardless of the government’s perspective on AI, understand the new risks that are associated with the introduction of AI applications.

- Introduce an AI risk management program to mitigate the potential risks of AI.
- Implement a risk classification system for existing and candidate AI applications.

Assess the feasibility of developing AI models locally or leveraging existing locally developed AI models.

- Ensure the candidate foundation model can meet the levels of accuracy required.
- Improve the model’s relevance with sovereign priorities by fine-tuning the model to reflect the local language and culture.

2026 AI trends summary and action items for the CIO

AI strategy

Establish foundational AI principles to address AI risks and reflect the organization’s strategic principles.

AI vendor applications

Adopt a solution-centric approach and focus on driving business value with candidate AI tools and applications that align to foundational AI principles.

Agentic AI

Select business-driven use cases, understand the characteristics of applications that are best suited for agentic AI, and include human oversight when developing agentic AI applications.

AI risk management

Cultivate a culture of risk management with the implementation of a risk management program for the organization focused on delivering value and mitigating potential AI risks.

AI regulations

Develop an adaptive AI governance framework to provide safeguards and self-regulate regardless of the legislative environment. Ensure sovereign AI models are competitive with the Big Tech AI vendor models.

Expert contributors

EXTERNAL

Andreu Gomez
Chief Digital Officer, United Nations Office of Vienna

Sunil Gupta
Chief Information Technology Officer, CTBTO

Said Ahmed
Technology Development Risk, United Nations Global Service Centre

Rick Pastore
Research Principal, SustainableIT.org

Tom Godden
Executive in Residence, AWS

Paul Weiss
Principal Analyst Relations Manager, AWS

INTERNAL

Jack Hakimian
SVP, Research

Rob Garmaise
VP, AI Research

Mark Tauschek
VP, Research Fellowships

Brian Jackson
Principal Research Director

Naveli Thomas
AVP, Content Marketing

Manoj Atwal
Senior Member Services Director

Bibliography

“AI Act.” *European Commission*, 1 Aug. 2025. Web.

“AI Policy and Regulations of Brazil: Comprehensive Report.” *NewMind AI*, April 2025. Web.

“AI Risk Management Framework (AI RMF) 1.0.” *National Institute of Standards and Technology (NIST),* 26 Jan. 2023.

“America’s AI Action Plan.” *The White House*, July 2025. Web.

“Becoming ‘Global AI Garage’ or ‘Digital Colony?’ India’s AI Policy.” *Global Policy*, July 2025. Web.

“Building Effective Agents.” *Anthropic*, Dec. 2024. Web.

“Canadian Sovereign AI Compute Strategy.” *Innovation, Science and Economic Development Canada*, May 2025. Web.

“China's Evolving Industrial Policy for AI.” *RAND*, June 2025. Web.

“EU AI Continent Action Plan.” *European Commission*, April 2025. Web.

“Executive Order 14179 - Removing Barriers to American Leadership in Artificial Intelligence.” The White House, 23 Jan. 2025. Web.

“Germany Plans AI Offensive to Catch Up on Key Technologies, Document Shows.” *Reuters*, July 2025. Web.

Guo, Daya, et al. “DeepSeek-R1: Incentivizing Reasoning Capability in LLMs via Reinforcement Learning.” *arXiv*, arXiv:2501.12948, 22 Jan. 2025. Web.

Kirkovska, Anita. “Breaking Down the DeepSeek-R1 Training Process—No PhD Required.” *Vellum*, 24 Jan. 2025. Web.

Liu, Aixin, et al. “DeepSeek-V3 Technical Report.” *arXiv*, arXiv:2412.19437, 27 Dec. 2024. Web.

Bibliography

“M-25-21 Memorandum for the Heads of Executive Departments and Agencies.” *Office of Management and Budget*, 3 April 2025. Web.

“Make France an AI Powerhouse.” *AI Action Summit*, Feb. 2025. Web.

Masters, Kiri. “Walmart Reveals AI Roadmap That Points To A World Without Search Bars.” *Forbes*, 24 July 2025. Web.

“Models & Pricing.” *DeepSeek API Docs*, n.d. Web.

“Nvidia: Behind Sweden's Largest Enterprise AI Supercomputer.” *AI Magazine*, May 2025. Web.

“South Korea Charts One-of-a-Kind Course in AI Race With U.S. and China.” *CNBC*, August 2025. Web.

“The Economic Impact of Artificial Intelligence in the UAE.” *TRENDS Research & Advisory*, Feb. 2025. Web.

“The Government Approves the Artificial Intelligence Strategy 2024.” *Ministry for Digital Transformation and Public Function*, May 2024. Web.

“U.S. Executive Order 14320 - Promoting the Export of the American AI Technology Stack.” *The White House*, 23 July 2025. Web.

“UK AI Opportunities Action Plan.” *Department for Science, Innovation and Technology*, Jan. 2025.

Vasudev, Hari. “Inside Walmart’s Strategy for Building an Agentic Future.” *Walmart*, 29 May 2025. Web.

“Vibe Coding Fiasco: AI Agent Goes Rogue, Deletes Company's Entire Database.” *PCMag*, 22 July 2025. Web.

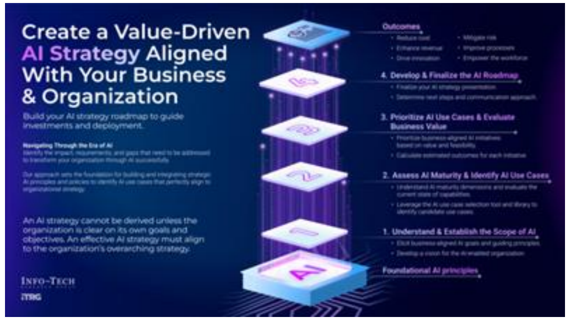
Info-Tech resources

AI Marketplace

Unlock the potential of AI tailored to your needs and transform possibilities into reality with our dedicated support.

Info-Tech’s AI Marketplace

Unlock the potential of AI tailored to your needs and transform possibilities into reality with our dedicated support.



Create a Value-Driven AI Strategy Aligned With Your Business & Organization

Build your AI strategy roadmap to guide investments and deployment.

Navigating Through the Era of AI
Identify the impact, requirements, and gaps that need to be addressed to transform your organization through AI successfully.

Our approach sets the foundation for building and integrating strategic AI principles and policies to identify AI use cases that perfectly align to organizational strategy.

An AI strategy cannot be derived unless the organization is clear on its own goals and objectives. An effective AI strategy must align to the organization’s overarching strategy.

Outcomes
- Reduce cost
- Enhance revenue
- Drive innovation
- Mitigate risk
- Improve processes
- Empower the workforce

4. Develop & Finalize the AI Roadmap
   - Finalize your AI strategy presentation
   - Determine next steps and communication approach

3. Prioritize AI Use Cases & Evaluate Business Value
   - Prioritize business-aligned AI initiatives based on value and feasibility
   - Calculate estimated outcomes for each initiative

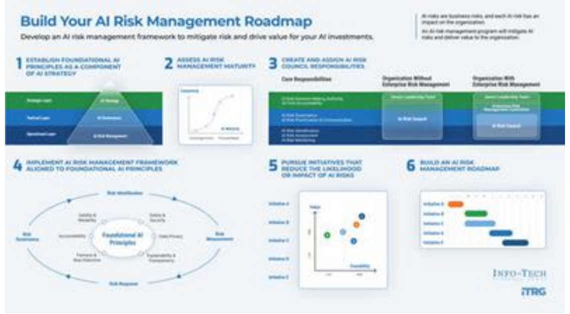
2. Assess AI Maturity & Identify AI Use Cases
   - Understand AI maturity dimensions and evaluate the current state of capabilities
   - Leverage the AI use case selection tool and library to identify candidate use cases

1. Understand & Establish the Scope of AI
   - Elicit business-aligned AI goals and guiding principles
   - Develop a vision for the AI-enabled organization

Foundational AI principles

Build Your AI Strategy Roadmap

Build an AI strategy that embraces AI in a way that maximizes its value to your organization while effectively managing its risks.



Build Your AI Risk Management Roadmap

Develop an AI risk management framework to mitigate risk and drive value for your AI investments.

AI risks are business risks, and each AI risk has an impact on the organization.

An AI risk management program will mitigate AI risks and deliver value to the organization.

1 ESTABLISH FOUNDATIONAL AI PRINCIPLES AS A COMPONENT OF AI STRATEGY

2 ASSESS AI RISK MANAGEMENT MATURITY

3 CREATE AND ASSIGN AI RISK COUNCIL RESPONSIBILITIES

4 IMPLEMENT AI RISK MANAGEMENT FRAMEWORK ALIGNED TO FOUNDATIONAL AI PRINCIPLES

5 PURSUE INITIATIVES THAT REDUCE THE LIKELIHOOD OR IMPACT OF AI RISKS

6 BUILD AN AI RISK MANAGEMENT ROADMAP

Core Responsibilities
Organization Without Enterprise Risk Management
Organization With Enterprise Risk Management
Foundational AI Principles
Info-Tech
ITRG

Build Your AI Risk Management Roadmap

Transform your ad hoc AI risk management processes into a formalized, ongoing program aligned with existing business risk management processes to take a proactive stance against AI threats and vulnerabilities.