

Gartner®

2027 Audit Plan Hot Spots



Introduction

Each year, we create our Audit Plan Hot Spots report using input from interviews and surveys throughout our global network of client organizations, as well as extensive secondary literature reviews.

This report highlights current risks and trends in the business environment. It helps audit teams more effectively identify risks to the organization and highlights key risks for stakeholders.

This year, three themes underlie the 12 hot spots:

1. Pressure to realize AI value
2. Strains on IT governance and oversight
3. Resilience in a fragmented world

Chief audit executives can use this report to:



Benchmark audit plan coverage

Compare, validate and further examine audit plan coverage.



Educate the audit committee

Educate the audit committee on risk trends that affect global organizations.



Drive audit team discussions

Enable audit team discussions prior to audit engagement planning and scoping.



Assess key risks

Determine appropriate questions to ask management during risk assessment and audit scoping.

3 themes underlying the 2027 hot spots

1 Pressure to realize AI value

Organizations are rapidly embedding AI into their core workflows, transferring more decision-making authority to autonomous systems. This swift adoption poses risks, as governance often lags behind AI deployment, creating accountability gaps and incentivizing short-term gains over long-term value. Many organizations are implementing AI without fully integrated strategies, simply adding it to existing processes instead of redesigning workflows for maximum impact.

Additionally, AI is reshaping markets by lowering barriers to entry and disrupting traditional pricing models, while workforce challenges — including skills gaps, layoffs and reduced entry-level hiring — threaten future talent pipelines and institutional knowledge. To realize AI's full potential, organizations must balance speed with robust governance, strategic planning and workforce development.

2 Strains on IT governance and oversight

Rapid AI adoption, increased third-party reliance, and evolving cyberthreats are straining traditional IT governance and oversight. AI systems amplify existing risks by acting at unprecedented speed, exposing weaknesses in data governance and increasing the likelihood of errors and data-quality issues as unreliable outputs are reused.

Cybersecurity vulnerabilities are expanding due to persistent geopolitical tensions and sophisticated AI-enabled attacks, which can overwhelm security teams and are difficult to detect, especially when state-sponsored actors are involved. Additionally, organizations' growing dependence on a few IT vendors deepens lock-in and complicates responses to transparency and security concerns, while accelerating AI adoption exposes weaknesses in digital infrastructure, potentially leading to higher costs and operational disruptions as demand for computing resources outpaces supply. To regain effective oversight, organizations must reassess their governance frameworks to address these emerging risks.

3 Resilience in a fragmented world

The business environment is evolving from uncertainty and chaos to a more fragmented world, characterized by regional alignment and the reversal of global economic integration. Organizations now view supply chain disruptions as a permanent structural feature, prompting the creation of regional ecosystems and redundant sourcing models, which require trade-offs in cost and market access.

Regulatory fragmentation is emerging as nations adopt disparate policies on trade, technology, data privacy and sustainability, increasing complexity and costs for cross-border operations. Building resilience is further complicated by macroeconomic volatility and the outsized influence of a few tech companies, while organizations are shifting more risk management responsibility to business units — often without adequate preparation or a strong challenge culture — making proactive risk management more difficult.

Audit plan hot spots summary

Hot spot	Summary	2027 drivers	2026 drivers
▶ AI governance	Organizations are deploying AI faster than traditional governance can keep pace. Additionally, the proliferation of AI decision making is exposing governance and accountability gaps.	• AI adoption pressure • Proliferation of AI decision making	• Deployment of AI agents • Visibility gaps in AI usage
Cybersecurity vulnerabilities			
Regulatory fragmentation			
Data governance			
AI strategy			
Supply chain disruption			
Workforce strategy			
Risk culture			
IT vendors			
Macroeconomic volatility			
AI-driven market shifts			
Digital infrastructure			

[Become a Gartner client](#) to unlock the complete version of this report, along with related tools, peer best practices and expert insights.

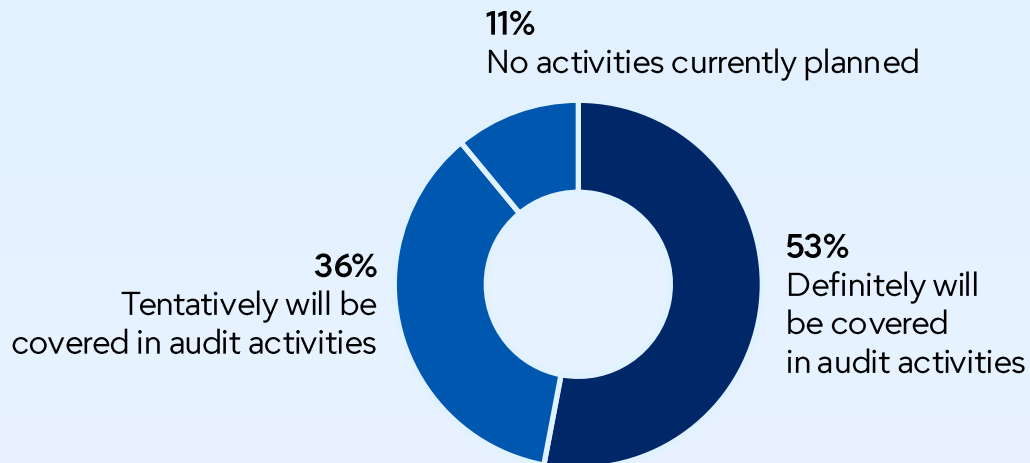
► Hotspot: AI governance

Organizations face a widening governance gap in which AI systems are deployed faster than they can be governed and operate more autonomously than they can be effectively overseen. Median AI spending as a share of organizational revenue is set to more than double between 2024 and 2026.¹ This rapid growth is widespread, with 81% of companies increasing their investment in AI initiatives from 2025.² Governance capabilities have not kept pace, as only 13% of IT and business leaders feel fully equipped to lead AI governance.³ While many organizations have adopted some form of AI governance, 85% lack comprehensive AI governance with policies, decision rights, and defined roles

and responsibilities.⁴ Concurrently, organizations are increasingly willing to grant AI decision authority without first resolving questions about transparency and explainability. Seventy-two percent of data leaders say they would allow AI agents to make critical business decisions without explanation.⁵ If organizations continue expanding AI decision authority without corresponding governance, they risk creating accountability gaps that undermine oversight. These gaps increase the likelihood of compliance violations and operational failures over time, exposing the organization to significant financial and reputational consequences.

Plans to cover AI governance in audit activities in the next 12-18 months

Percentage of respondents

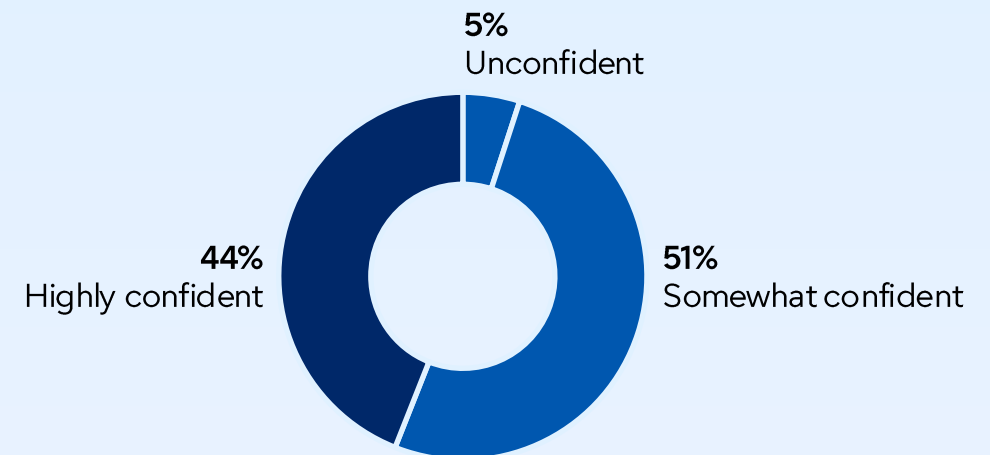


n = 190

Source: Gartner

Confidence in audit's ability to provide assurance over AI governance risk

Percentage of respondents



n = 190

Source: Gartner

► AI governance

Urgency drivers

AI adoption pressure

Intense pressure to adopt AI is leading organizations to implement new technologies faster than governance can be established. Eighty-two percent of CIOs report that AI development exceeds their organization's ability to govern it.⁶ Governance gaps are particularly evident for AI agents, as 63% of organizations cannot effectively restrict what AI agents are allowed to do, 55% struggle to contain agents' access to systems and data, and 60% cannot reliably terminate misbehaving agents.⁷

Pressure can also create misaligned incentives: 74% of CIOs believe their roles are at risk if they fail to achieve quantifiable AI-driven results within two years, encouraging rapid deployment even where governance is incomplete.⁸ This dynamic persists despite known risks, with 67% of business and IT leaders approving AI initiatives even when security concerns are present.⁹

With 64% of organizations lacking formal AI governance bodies, governance struggles to scale at the same pace as AI adoption.¹⁰ The result is a governance gap in which AI systems are introduced and scaled without sufficient oversight. Organizations face increased exposure to security vulnerabilities, compliance failures and unintended operational impacts.

Proliferation of AI decision making

Organizations increasingly deploy AI systems to make independent operational decisions despite unresolved concerns about reliability, explainability and documentation. AI is now embedded in core workflows, with 53% of organizations using AI agents, most commonly to automate operations and technology.¹¹ Yet, only 21% report mature governance for autonomous agents, highlighting a widening control gap.¹² Four out of five organizations report risky AI behaviors and 91% lack real-time visibility into agent actions.¹³

These governance and visibility gaps become more consequential with the speed of AI. While typical applications perform around 50 actions per minute, AI agents execute approximately 5,000.¹⁴ As AI systems assume greater decision authority, accountability becomes more difficult to define, creating gaps where decisions with material financial or operational consequences may be executed without clear attribution of responsibility or escalation pathways.¹⁵

In some cases, abandoned or unmonitored AI agents can remain active and operate with effectively zero oversight.¹⁶ Failure to address these accountability gaps limits organizations' ability to explain, challenge or remediate outcomes, making it harder to investigate failures, assign responsibility and maintain confidence in AI-driven decisions.

Key risk indicators

- Number of AI agents in development or in deployment
- Number of AI high-risk use cases identified after they were already deployed
- Percentage of AI use cases found noncompliant with AI policy requirements
- Percentage of employees using AI tools that are not approved or monitored by the organization
- Number of incidents attributable to AI systems or agents, resulting in material financial, operational, compliance, cybersecurity, legal or reputational exposure
- Percentage of applications with embedded AI capabilities
- Percentage of identified AI use cases registered in the enterprise AI inventory
- Percentage of business processes with AI-driven decision-making authority
- Time to analyze or validate AI-driven decisions postexecution
- Time to halt or override AI systems or agents (e.g., "kill switch" effectiveness)

► AI governance

Recommendations for audit

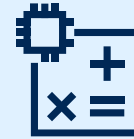
- **Review governance over AI agents:** Assess whether the organization's AI governance framework, policies, roles and responsibilities, and oversight processes appropriately address the unique risks of AI agents, including autonomy, tool use, data access, decision-making authority, monitoring, human oversight and accountability. Evaluate whether controls are designed and operating effectively to govern AI agents throughout their life cycle.
- **Assess AI inventory and monitoring capabilities:** Evaluate whether the organization has effective processes and tools to identify, inventory and continuously monitor AI systems, models and agents throughout the enterprise. Assess the completeness and accuracy of the AI inventory, including AI agents developed internally or acquired from third parties. Review approaches for detecting shadow AI, unregistered AI use cases and unauthorized AI agents, and determine whether management has sufficient visibility to govern AI-related risks effectively.
- **Evaluate controls over AI decision making and autonomy:** Assess the adequacy and effectiveness of controls governing AI-driven decision making, including delegation of decision authority to AI systems or agents. Evaluate whether appropriate guardrails, approval mechanisms and human oversight are in place for high-risk or business-critical processes.
- **Assess processes for managing AI risk tolerance:** Evaluate how the organization identifies, documents and manages exceptions to AI governance policies, including cases in which AI systems are deployed despite known risks. Assess whether appropriate escalation, approval and monitoring mechanisms are in place to address governance gaps and limit exposure.
- **Assess AI incident response and recovery capabilities:** Assess whether the organization has effective mechanisms to halt, override, restrict or disable AI systems and agents when they behave unexpectedly or produce undesirable outcomes. Evaluate the design and effectiveness of emergency shutdown procedures, human override controls, escalation processes and recovery plans. Review whether these capabilities are periodically tested and whether management can rapidly contain AI-related incidents and recover from disruptions caused by autonomous actions.

► AI governance

Questions for management



How do you maintain and update an inventory of all AI systems, models and agents used throughout the organization?



What controls are in place to govern AI decision making and reduce the likelihood of unintended, noncompliant or high-risk outcomes?



What processes are in place to ensure AI use cases are reviewed and approved before deployment?



How do you ensure AI-generated decisions or outputs can be explained, validated or audited when needed?



How do you detect and respond to employee use of unsanctioned or unauthorized AI tools?



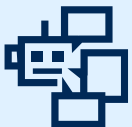
What processes are in place to identify, investigate and resolve incidents caused by AI systems or agents?



What processes ensure each AI system has a clearly defined owner responsible for its oversight and risk management?



What mechanisms are in place to halt, override, contain or restrict AI systems when they behave unexpectedly or produce undesirable outcomes?



How do you determine which business processes can be automated or supported by AI systems?



How do you measure whether employees understand and follow AI governance policies?

Audit plan hot spots dashboard

This dashboard compares hot spots over the last five years:

2023	2024	2025	2026	2027
Cyberthreats	Cybersecurity vulnerabilities	Cybersecurity vulnerabilities	Cybersecurity vulnerabilities	AI governance
IT governance	IT governance	Data governance and quality	Data governance	Cybersecurity vulnerabilities
Data governance	Regulatory complexity	IT governance	Regulatory compliance	Regulatory fragmentation
Third-party risk management	Digital transformation	Digital transformation	IT governance	Data governance
Organizational resilience	Organizational resilience	Regulatory compliance	AI governance	AI strategy
Environmental, social and governance (ESG)	Third parties	Third parties	Digital transformation	Supply chain disruption
Supply chain	Supply chain	AI governance	Third parties	Workforce strategy
Macroeconomic volatility	Employee well-being and satisfaction	ESG	Organizational resilience	Risk culture
Workforce management	ESG	Workforce management and engagement	Supply chain distortions	IT vendors
Cost pressures	Social and political tensions	Supply chain	Talent management	Macroeconomic volatility
Culture	Generative AI	Macroeconomic conditions	Macroeconomic uncertainty	AI-driven market shifts
Climate degradation	Macroeconomic uncertainty	Sustainable growth strategies	ESG strategies	Digital infrastructure

Endnotes

¹ 2025 Gartner Modern Data Value Realization Survey; [Invest 2x More in Foundations Than AI Tools](#)

² 2026 Gartner CIO and Technology Executive Survey

³ 2025 Gartner Evolution of D&A Governance for AI Survey

⁴ 2025 Gartner Cybersecurity Innovations in AI Risk Management and Use Survey; [3 Ways GC Must Drive Improved AI Governance Maturity](#)

⁵ [Global AI Confessions Report: Data Leaders Edition](#), Dataiku.

⁶ [Building a Firewall Against Cybersecurity Burnout](#), Hack The Box.

⁷ [What Happens When You Give AI Agents Real Power](#), Kiteworks.

⁸ [7 Career-Making AI Decisions for CIOs in 2026](#), Dataiku.

⁹ [Organizations Overlook AI Risk as Governance Fails to Keep Up](#), Trend Micro.

¹⁰ 2025 Gartner Cybersecurity Innovations in AI Risk Management and Use Survey

¹¹ [Investment and AI Agent Deployment Surge as Execution Becomes the Differentiator](#), KPMG.

¹² [From Ambition to Activation: Organizations Stand at the Untapped Edge of AI's Potential, Reveals Deloitte Survey](#), Deloitte.

¹³ [2026 AI Risk and Readiness Report](#), Netskope; [Deploying Agentic AI With Safety and Security: A Playbook for Technology Leaders](#), McKinsey & Company.

¹⁴ [AI Security: IAM Delivered at Agent Velocity](#), Cloud Security Alliance.

¹⁵ [Answering the Top Trending AI Agent Questions, Part 2: Current State](#)

¹⁶ [Tech FutureSight: Stop Zombie Agent Threats to Systems, Data With Preemptive Security](#)

Actionable, objective insights

Position your audit function for success. Explore these additional complimentary resources and tools:

Webinars



Join a Virtual Event

Hear the latest insights from Gartner analysts at an upcoming or recorded event.

Watch Now

Tool



Score your Audit Function

Measure your function’s performance across six objectives and 25 discrete activities.

Learn More

Insights



Strategic Planning for Your Function

Turn your strategy into action with these tools and templates.

Download Now

How We Help



Gartner for Chief Audit Executives

Discover how we can help you tackle your mission-critical priorities.

Learn More

Already a client? Get access to even more resources in your client portal. [Log In](#) ↗

Connect with us

Get actionable, objective business and technology insights that drive smarter decisions and stronger performance on your mission-critical priorities.

U.S.: 1 855 322 5484
International: +44 (0) 3300 296 946

Become a Client

Learn more about Gartner for Chief Audit Executives
gartner.com/en/audit-risk

Stay connected to the latest insights

