2025 Audit Plan Hot Spots

Gartner®

Introduction

Each year, Gartner creates the Audit Plan Hot Spots report by combining input from interviews and surveys from throughout our global network of client organizations, as well as extensive secondary literature reviews and insights from internal experts, to identify the top risks audit should provide assurance over during 2025.

The report highlights current risks and trends in the business environment and helps audit teams more effectively identify risks to the organization and highlight key risks for stakeholders. These risks, or hot spots, are the top-of-mind issues for boards, audit committees and executives in organizations of all sizes across industries and geographic locations.

This abbreviated version of the 2025 Audit Plan Hot Spots report includes:

- Key themes underlying this year's hot spots
- Top 12 risks across IT, operational, financial, and strategic themes
- A deep dive into urgency drivers, recommended actions, and key questions for 3 of the top risks
- Comparison of hot spots across the past 5 years

To access the full research report and related resources, guidance and tools, contact us to learn more about becoming a Gartner client.

Become a Client

Chief Audit Executives can use this research 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 teams' discussions prior to audit engagement planning and scoping.

Assess Key Risks

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

Gartner®

3 Themes Underlying the 2025 Hot Spots

1 Implications of AI Adoption

One theme has dominated both the business world and culture at large in the past year: the burgeoning AI revolution. Yet while organizations are investing heavily in AI, many struggle to quickly achieve high-quality results. A clash between unrealistic expectations and a host of implementation challenges — from lagging data quality to a lack of robust internal controls — could see many organizations falling short of AI's transformative potential, especially in the short term.

2 Optimizing Resilience Investments

The CrowdStrike Windows outage in July 2024 was a resounding wake-up call on the importance of resilience. Scenario planning, while an important preparatory measure, can only scratch the surface of potential sources of disruption across IT systems, cybersecurity perimeters and supply chains. As a result, organizations must invest significant resources in building capabilities to respond quickly to the unexpected. Perhaps the thorniest challenge when it comes to resilience is rightsizing investments, effectively triaging where resources should be allocated.

3 Winning Through Change

Organizations must continue to navigate an environment of larger-scale and more frequent change, creating challenges for both defining and executing strategies. The accelerating pace of technological innovation is inducing organizations to undertake massive digital transformation efforts. Organizations must also actively prepare for longer-term impacts of climate change and demographic shifts that will impact operating models, workforces and consumer markets.

2025 Audit Plan Hot Spots

Hot Spot	Summary	2025 Drivers	2024 Drivers
1. Cybersecurity Vulnerabilities	Identity-related breaches are a pain point in today's evolving threat landscape. Despite the high likelihood of an incident, organizations are not investing as much in cybersecurity resilience (response and recovery) as in threat prevention.	1. Identity Verification and Management Challenges 2. Imbalances Between Defense and Resilience in Cybersecurity Investments	1. Rise in Insider Threat 2. GenAI-Enabled Cyberattacks
2. Data Governance and Quality	Despite consistent data governance efforts, organizations are seeing limited returns on their investments. Meanwhile, insufficiently AI-ready data threatens the viability of AI deployments throughout the business.	1. Limited Return on Data Governance Investments 2. Insufficiently AI-Ready Data	Not a 2024 Hot Spot.
3. IT Governance	Interconnected IT systems present growing challenges for responding to disruptions, while the concentrated cloud environment limits organizations' flexibility.	1. IT-Driven Business Disruption 2. Cloud Concentration	1. IT Infrastructure Complexity 2. Poorly Managed Technical Debt
4. Digital Transformation	Organizations often fail to implement effective project and change management strategies during digital transformation initiatives, limiting ROI. Moreover, organizations struggle to overcome gaps in the IT skills necessary to achieve project objectives.	1. Challenges in Achieving ROI for Digital Transformation Initiatives 2. Gaps in Skills Underpinning Digital Transformation	1. Unclear Project Objectives 2. Unintended Consequences of Digital Initiatives on Employees
5. Regulatory Compliance	Organizations face increased regulatory uncertainty during a year of global elections. At the same time, regulators are increasing expectations and enforcement for reporting in nonfinancial areas.	1. Impact of Electoral Uncertainty on Regulatory Priorities 2. Growing Reporting Needs in Nonfinancial Areas	1. Velocity and Breadth of New Regulations 2. Regulatory Fragmentation
6. Third Parties	As third-party networks continue to expand, organizations increasingly struggle to have visibility into third parties' evolving data usage practices and manage the risks associated with new AI functionalities in vendor products.	1. Limited Visibility Into Third-Party Data Usage and Protection Practices 2. Embedded and Hybrid AI in Third-Party Applications	1. Increased Third-Party Vulnerability 2. Patchwork Third-Party Risk Management

2025 Audit Plan Hot Spots

Hot Spot	Summary	2025 Drivers	2024 Drivers
7. AI Governance	Unrealistic expectations for GenAI may lead organizations to overspend on underperforming use cases, while user trust in AI could lead to insufficient human scrutiny of outputs used in decision making.	1. Inflated Expectations for GenAI 2. Excessive Employee Faith in GenAI Outputs	1. Governance and Monitoring Challenges 2. Output Reliability and Trust Gaps
8. Environmental, Social and Governance (ESG)	Organizations are running out of time to demonstrate that they comply with finalized ESG and sustainability reporting regulations. Regulations also raise the bar for ESG data quality, which many organizations continue to struggle with.	1. Reporting Regulations Coming Into Force 2. ESG Data Quality and Management Gaps	1. ESG Reporting Complexity 2. Slow Progress on ESG Goals
9. Workforce Management and Engagement	Changing demographics create workforce planning challenges as many employees, especially leaders, approach retirement. At the same time, employee engagement is lagging as organizations increase their expectations for productivity.	1. Shifting Workforce Demographics 2. Employee Productivity Pressures	1. Employer-Employee Return-to-Office Disconnect 2. Overburdened Managers
10. Supply Chain	Organizations are investing in resilience in response to more frequent disruptions, yet many of these investments go unused. Organizations also struggle to achieve sufficient visibility into suppliers, creating challenges for both risk management and regulatory compliance.	1. Misprioritization of Resiliency Investments 2. Supply Chain Visibility Imperatives	1. Supply Chain Restructuring 2. Ballooning Costs
11. Macroeconomic Conditions	While interest rates may start to come down soon, they are likely to remain at relatively high levels overall, putting upward pressure on costs and constraining investment. Trade restrictions, already growing in recent years, may rise further in the aftermath of 2024 global elections.	1. Protracted Interest Rate Elevation 2. Reigniting Trade Tensions	1. Conflicting Short-Term Signals 2. Looming Stagnation
12. Sustainable Growth Strategies	Organizations' ambitions for sustainable growth are under threat due to increasing climate-related business disruptions and rising energy needs of technology investments.	1. Operational Impacts of Climate Change 2. Tensions Between Digital and Sustainability Ambitions	Not a 2024 Hot Spot.

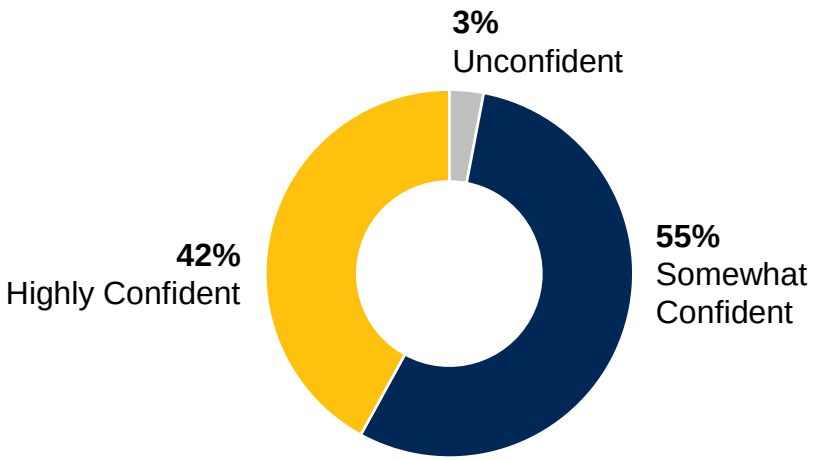
Cybersecurity Vulnerabilities

Deep Dive

Challenges bolstering identity verification techniques, especially to adapt to growing threats like AI, and insufficient investments in cyber breach response and recovery are contributing to what cybersecurity professionals describe as the most challenging threat landscape of the past five years.[1] Cybercriminals are conducting more sophisticated social engineering attacks, and deepfake incidents saw a tenfold increase between 2022 and 2023.[2] Meanwhile, the overall volume of threats continues to grow. Eighty-one percent of organizations experience at least 25 cybersecurity incidents a year, suggesting it is no longer a question of if an attack will occur, but when.[3] Yet investments in response and recovery capabilities are nowhere near the level they need to be. For example, only 25% of CISOs are defining and automating incident response processes across different teams and individuals.[4] Failure to adapt to evolving attack vectors and invest sufficiently in cyber resilience could increase the likelihood of data breaches and business continuity disruptions.

Confidence in Audit's Ability to Provide Assurance Over Cybersecurity Vulnerabilities Risk

Percentage of Respondents

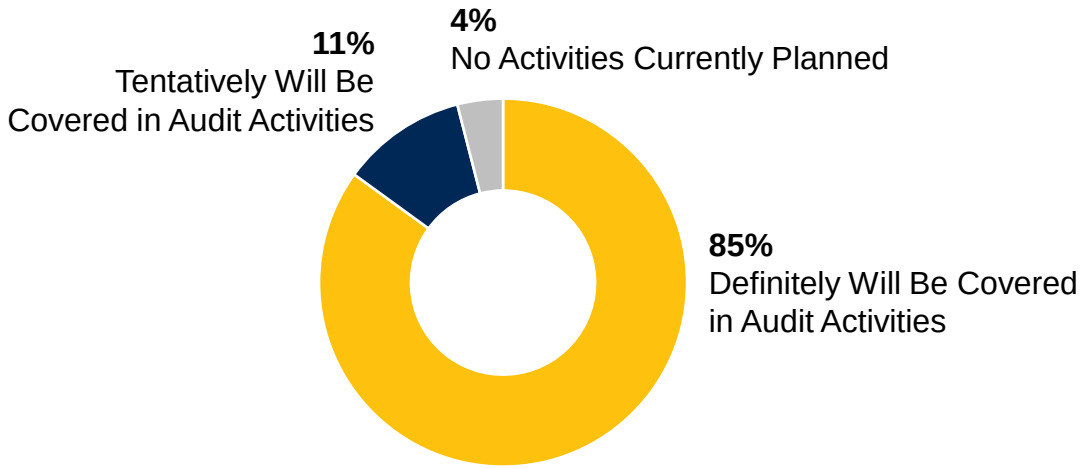


n = 127

Source: Gartner's Annual Survey of CAE Priorities and 2025 Audit Plan Hot Spots

Plans to Cover Cybersecurity Vulnerabilities in Audit Activities in the Next 12-18 Months

Percentage of Respondents



n = 127

Source: Gartner's Annual Survey of CAE Priorities and 2025 Audit Plan Hot Spots

Cybersecurity Vulnerabilities

Urgency Drivers

Identity Verification and Management Challenges

Identities represent one of the biggest threats to organizations: In the last 12 months, 93% of organizations suffered two or more identity-related breaches.[5] Yet organizations struggle to meet evolving needs, as 47% are not adequately staffed for identity and access management (IAM) modernization efforts.[6] One major challenge is securing machine identities, which 49% of security decision makers see as the riskiest identity type.[7] Machine identities are the No. 1 driver of identity growth and are only likely to proliferate with new AI tools, raising the bar for identity verification.[8] Remote work can also create opportunities for identity-based fraud; for example, foreign agents recently posed as U.S. workers to infiltrate over 300 companies.[9] Outside the organization, improvements in deepfake technology have led CISOs to rank voice and image impersonations as the most concerning malicious use case of GenAI.[10] Cheap access only heightens the threat; malicious actors can access deepfake technology online for as low as $20 per minute.[11] Deepfake-related crimes can be costly and disruptive.[12] For example, one company lost $25.6 million following an impersonation of their CFO.[13] Organizations must secure both human and machine identities, as both have access to sensitive data and can be gateways for malicious actors.[14]

Imbalances Between Defense and Resilience in Cybersecurity Investments

Despite 69% of IT leaders saying cybersecurity budgets will increase in 2024, cybercrime is predicted to cost the global economy a record $14.57 trillion in 2024.[15] Malicious actors are likely to succeed at least some of the time, yet organizations spend only 35% of IT security budgets on detection and response combined, with the majority going to breach prevention despite growing limitations.[16] Relatively low investment in detection and response translates to weaker capabilities. Aggregate results from a Gartner maturity assessment tool show that, of the five NIST core cybersecurity functions, organizations are least mature in recovery controls.[17] Underinvestment in cyber resilience and recovery can cause significant financial and operational impacts, as recent high-profile examples across the healthcare, automotive and telecommunications industries illustrate.[18] By contrast, greater investment in resilience pays off: Organizations with high levels of incident response planning and testing saved an average of $1.49 million per incident compared to those with low levels.[19]

Key Risk Indicators

- Number of identity-related cyber breaches
- Number of deepfake incidents in a given period of time
- Percentage of employees who failed phishing tests
- Number of machine identities with access to sensitive data
- Percentage of assets protected by privileged credential access
- Percentage of cybersecurity incidents attributed to human error
- Average or median attack recovery and response time
- Percentage of breach cost covered by cybersecurity insurance
- Percentage of cybersecurity budget spent on recovery
- Percentage of FTE hours spent on cyber incident response and recovery planning

Cybersecurity Vulnerabilities

Recommendations for Audit

1

Assess the organization's social engineering testing and training: Assess how often the organization conducts social engineering test campaigns and training. Evaluate how the organization tracks trends in the number of employees who click on suspicious emails in test campaigns and the effectiveness of phishing-awareness training. Review whether test campaigns incorporate testing developments in social engineering, such as advancements in deepfake technology, as well as whether employees who fail tests are referred to additional training.

2

Conduct GenAI cybersecurity reviews: Conduct advisory reviews of GenAI initiatives and pilots to advise on how cybersecurity is proactively incorporated into development. Evaluate what internal data sources GenAI tools have access to and how access privileges for machine identities are determined and monitored.

3

Review cybersecurity investment decision making: Assess how IT departments and the organization decide on how to allocate cybersecurity budgets on defense and resilience strategies. Assess how ROI is calculated and how often investments are reevaluated.

4

Evaluate cyber incident response plans: Evaluate cybersecurity response plans and whether they account for more sophisticated attacks. Determine whether response plans adequately address potential harm to internal systems, infrastructure and reputation, loss of data and customers, and any regulatory disclosure requirements.

5

Assess the maturity of cyber incident prevention plans: Evaluate the organization's prevention plan by reviewing the strategies, controls and measures in place to proactively mitigate cyber breaches. Assess the adequacy and effectiveness of prevention measures and controls.

Cybersecurity Vulnerabilities

Questions for Management

How have you adapted social engineering testing and training to account for threats from deepfakes?

What triggers do you have in place to detect identity-related breaches?

How are you monitoring what data sources GenAI applications can access?

How often are incident response plans reviewed and, if needed, revised?

How are you enabling employees to report deepfake incidents?

Who in the organization is responsible for responding to cyberattacks and how?

How do you evaluate the effectiveness of investments in cyber breach prevention and response?

How often do you evaluate the effectiveness of identity verification controls in the organization?

How do you assess the maturity of current cybersecurity prevention and recovery controls?

How do you prioritize investments between cyber breach prevention and response?

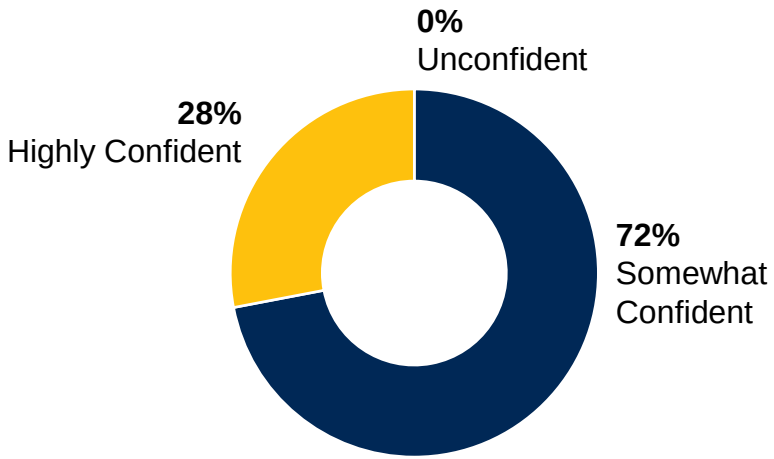
Digital Transformation

Deep Dive

Digital technology is the top strategic business priority for 2024 and 2025, according to nonexecutive boards of directors.[20] In fact, more than half of organizations (59%) underwent at least two significant technology platform changes in 2023, and 52% of organizations are building capabilities to conduct or enhance management decision making with AI.[21] Global spending on digital transformation is forecast to reach nearly $3.9 trillion in 2027 with a 16.1% compound annual growth rate.[22] Yet many organizations struggle to achieve expected ROI from digital transformation projects, as poor project execution adds to costs and ineffective change management limits benefits.[23] Digital transformation projects are also often hindered by talent and skills limitations, both in terms of technical talent shortages and insufficient employee training. For example, 73% of employees are concerned about insufficient training and upskilling opportunities to effectively use AI tools.[24] If organizations hope to realize the full benefits of digital transformation projects, mitigating risks of ineffective change management and insufficient talent and skills will be urgent imperatives to avoid contributing to the 70% of digital transformation projects that fail to deliver successful outcomes.[25]

Confidence in Audit's Ability to Provide Assurance Over Digital Transformation Risk

Percentage of Respondents

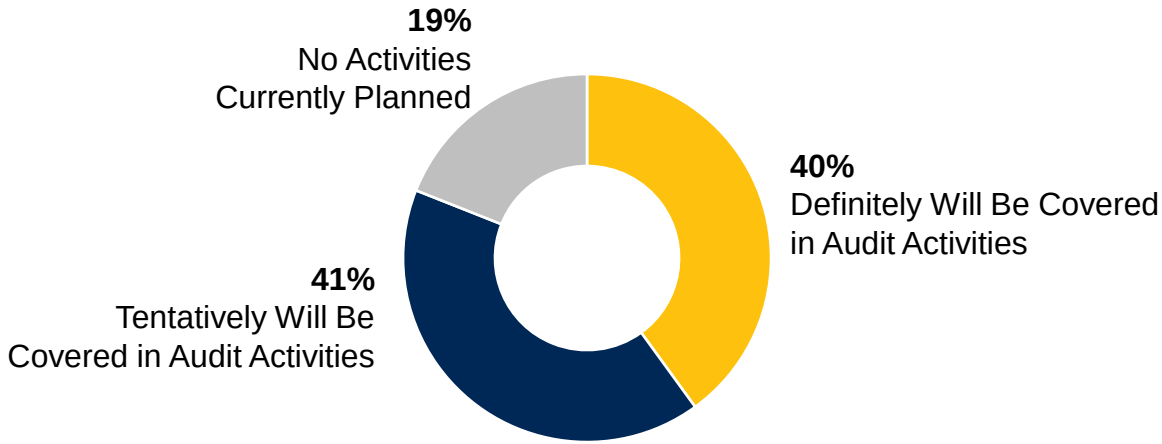


n = 124

Source: Gartner's Annual Survey of CAE Priorities and 2025 Audit Plan Hot Spots

Plans to Cover Digital Transformation in Audit Activities in the Next 12-18 Months

Percentage of Respondents



n = 127

Source: Gartner's Annual Survey of CAE Priorities and 2025 Audit Plan Hot Spots

Digital Transformation

Urgency Drivers

Challenges in Achieving ROI for Digital Transformation Initiatives

Digital transformation initiatives continue to proliferate and become more costly, but organizations often fail to execute and implement projects effectively. Almost half of CIOs and tech executives report their digital technology investments have not met CEO expectations for improving operating margins (47%) or increasing human capital effectiveness (45%).[26] During project execution, organizations often spend more time and money than they plan to. Only about one-third of project leaders report their recent critical transformation projects were completed on time and within budget, and only 54% of projects meet all success metrics.[27] Ineffective change management also often prevents the expected benefits of many digital transformation efforts from materializing during implementation. Only 13% of organizations with poor change management meet or exceed project objectives, whereas 88% of organizations who excel at change management do so.[28] Failure to implement effective project and change management strategies to improve outcomes of digital transformation initiatives could lead to increased costs and poor ROI.

Gaps in Skills Underpinning Digital Transformation

Having the right skills to deploy and use new technologies is critical to transformation efforts' short- and long-term success. Yet organizations are struggling to find and retain the IT talent they need and upskill the broader workforce to maximize transformation efforts. Roughly 44% of organizations need more data analysis skills, and about 36% need more AI and machine learning skills.[29] When skills are lacking, deployment of new technologies suffers. For example, IT purchasing decision makers identified lack of expertise and skilled personnel in AI technology as the second biggest roadblock to AI rollout, while shortages of skills such as IT operations and cloud architecture impact other digital projects.[30] Organizations are struggling to hire their way out of the problem. Demand for AI technical talent is up 323% in the last eight years, and nearly 55% of CIOs find it very difficult to recruit and hire qualified AI and GenAI talent in the current market.[31] Besides specialists needed for development and implementation, employees generally need support to build technical skills to support tool use. Yet 78% of employers say they can't train employees fast enough to keep up with changing technology.[32] Misalignment of digital transformation projects with talent realities risks wasted resources and ineffective implementation, with organizations wasting an average of $18 million on unused applications annually.[33]

Key Risk Indicators

- Number of ongoing digital transformation projects throughout the business
- Percentage of transformation projects meeting ROI goals
- Ratio of failed digital transformation projects to projects undertaken
- Trends in employee productivity in business areas undergoing digital transformation
- Trends in allocation of digital transformation budgets
- Trends in average time elapsed to fill open IT positions
- Percentage of digital transformation projects currently in progress that are delayed
- Retention rates of employees in key IT roles
- Number of trainings and/or reskilling opportunities offered for employees impacted by digital transformation projects
- Time elapsed between IT skills gap assessments

Digital Transformation

Recommendations for Audit

1

Assess change management strategies: Assess the organization's change management strategies and determine whether they align with digital transformation goals. Identify areas of weakness, gaps or potential barriers and discuss with management. Review the frequency and extent of strategy updates as assumptions and organizational priorities change.

2

Review governance of digital project execution: Assess the governance around digital transformation projects. Validate whether appropriate plans are in place to meet cost, timeline and resourcing goals during execution, as well as project management roles and responsibilities.

3

Assess the interaction between IT and business stakeholders: Assess the frequency and types of interaction between IT and business stakeholders involved in transformation initiatives. Examine the degree to which the CIO and senior IT executives engage heads of central business functions and business lines regarding IT investments, including the PMO to determine the strategic change management implications of digital transformation projects.

4

Review IT skills gap assessments: Evaluate how critical IT skills gaps and associated action steps to close gaps are identified. Review execution of training and development to upskill current employees, as well as recruitment and hiring processes to source employees with specialized IT skills externally. Suggest remediating any barriers to executing the proposed strategies to fill identified IT skills gaps and help meet digital transformation objectives.

5

Evaluate workforce reskilling opportunities: Review the organization's processes for implementing and identifying reskilling opportunities for internal employees to stay up to date on in-demand skills so they can help meet digital transformation goals.

Digital Transformation

Questions for Management

How do you ensure that the business and the IT department are aligned on their digital transformation goals?

How are you evaluating whether digital transformation project benefits are aligned with the allocated budget?

What metrics do you use for measuring the performance of digital transformation projects in areas including readiness, adoption and business outcomes?

What are the hiring and recruitment processes for attracting talent with specialized IT skills needed for digital transformation projects?

How are you evaluating the impact of digital transformation projects on employees' capacity for change?

How and how often do you assess IT skills and knowledge gaps among employees?

How do you determine what IT skills are needed to help meet the objectives of digital transformation projects?

How do you ensure you have the necessary change management strategies for digital transformation projects to succeed?

How are you investing in continuous training and development opportunities for employees impacted by digital transformation?

What technical or specialized skills are needed to achieve both short-term and long-term goals?

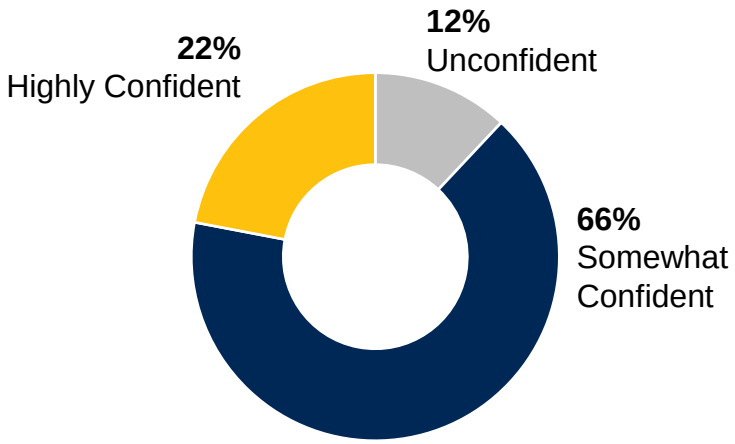
AI Governance

Deep Dive

Organizations are already spending heavily on AI, with more spending ahead: 90% of organizations either have deployed some form of AI or will do so by 2026, and 73% of organizations are increasing their investment in AI or ML.[34] But challenges of achieving meaningful productivity gains and reliable outputs threaten to stymie returns on these investments. GenAI is many organizations' focus, and CIOs see increased productivity as the top business value of adopting GenAI (74%).[35] Yet achieving — and demonstrating — productivity is far from straightforward. Forty-nine percent of technology leaders highly involved in AI cite estimating and demonstrating value as a top barrier to implementation.[36] Meanwhile, increased use of, and familiarity with, AI tools is amplifying risks of decision-making errors due to inaccurate outputs, as employees may put too much faith in the technology. For example, 59% of CIOs cite hallucination and reasoning errors as their top concern about GenAI.[37] With total AI software spending forecast to grow from $124.3 billion in 2022 to $297.9 billion in 2027, organizations must focus spending on the most high-value use cases and ensure effective oversight over AI reliability — or risk lackluster or even negative ROI.[38]

Confidence in Audit's Ability to Provide Assurance Over AI Governance Risk

Percentage of Respondents

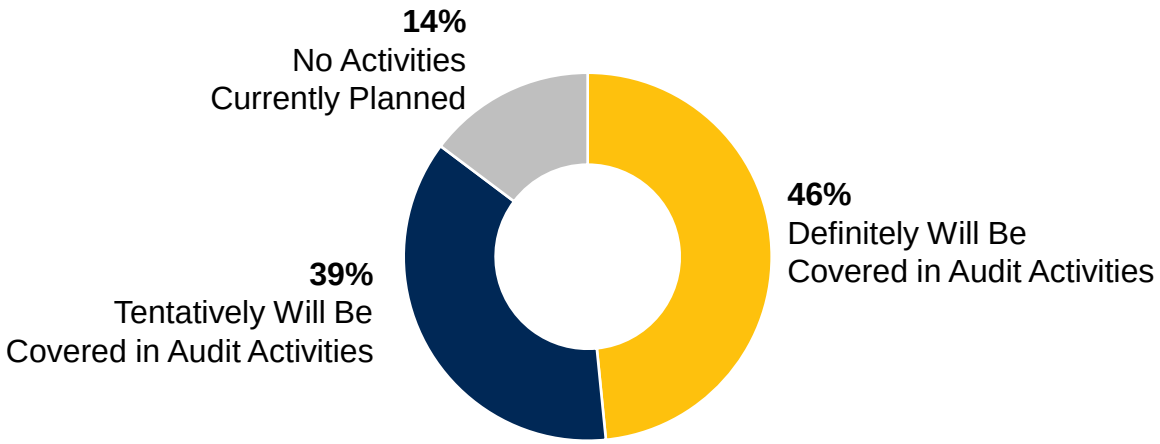


n = 125

Source: Gartner's Annual Survey of CAE Priorities and 2025 Audit Plan Hot Spots

Plans to Cover AI Governance in Audit Activities in the Next 12-18 Months

Percentage of Respondents



n = 127

Source: Gartner's Annual Survey of CAE Priorities and 2025 Audit Plan Hot Spots
Note: Totals may not sum to 100% due to rounding

AI Governance

Urgency Drivers

Inflated Expectations for GenAI

Despite GenAI's impressive capabilities, the hype surrounding it has created unrealistic expectations. McKinsey consultants estimate that GenAI could add the equivalent of $2.6 trillion to $4.4 trillion to global output annually (perhaps more than the entire U.K. economy).[39] But more measured academic analysis suggests only modest impacts: A prominent MIT economist estimates that GenAI's impact on worker productivity will likely contribute a mere 0.9% to global GDP growth over the next decade.[40] Future improvements of the technology may also soon hit a wall due to data scarcity. Experts predict that a hypothetical GPT-5 would need five to 10 times as much data as GPT-4 to show performance improvements comparable to the difference between GPT-3.5 and GPT-4, which already used almost all publicly available data on the internet.[41] Given GenAI's steep price tag and the high failure rate of AI projects — 53% of technology leaders involved in AI report their organizations spent more than $1 million on GenAI in 2023, and some estimates put the failure rate as high as 80% — organizations must be judicious about where and when to use GenAI or risk heavy costs for limited value.[42]

Excessive Employee Faith in GenAI Outputs

As AI usage grows, organizations face the risk that employees may become complacent and overly accepting of potentially flawed or inaccurate outputs. Inaccuracy is a top GenAI risk, cited by 63% of business leaders, and 23% report they have already experienced negative consequences from it.[43] Human review of outputs can help catch accuracy issues, but individuals may struggle to do so effectively. An experiment assessing use of GPT-4 to help solve business problems found that users often took misleading outputs at face value, causing them to perform 23% worse than those who did not use the tool.[44] While humans alone are at least as prone to make some mistakes, the speed and apparent authority with which GenAI tools produce "answers" could encourage user trust when human scrutiny is warranted. In addition, organizations aren't doing enough to prepare employees: Only 36% of organizations surveyed currently have employee training programs for GenAI in place.[45] Failure to maintain appropriate skepticism and critical thinking about AI among employees could heighten organizations' risk of poor work products, legal liability and reputational damage.

Key Risk Indicators

- Number of enterprise deployments of business-facing GenAI tools
- Number of functions using GenAI tools and applications
- Number of AI applications interfacing with customers/users
- Trends in spending on AI tools and applications
- Trends in performance metrics among employees with access to AI tools
- Percentage of AI use cases reviewed by oversight or governance committees
- Number of reported inaccuracies or errors produced by AI applications
- Percentage of AI outputs undergoing human review
- Percentage of employees completing AI training
- Consumption rates (e.g., click-throughs or downloads) for employee AI usage guidelines

AI Governance

Recommendations for Audit

1

Review processes for assessing and approving AI use cases: Determine what bodies and procedures the organization has set up for reviewing AI use-case proposals, such as governance committees and review criteria. Evaluate the adequacy of controls for evaluating and approving use cases. Assess the organization's compliance with written policies and procedures.

2

Evaluate methods for measuring the value and ROI of AI tools: Determine what metrics management has identified for assessing the value and ROI of AI tools. Assess the extent to which costs and benefits are appropriately weighed for AI use cases and how assessments are being used in decision making.

3

Review processes for controlling AI costs: Evaluate the organization's procedures for monitoring spending on AI tools and applications. Assess whether use-case approval processes estimate the cost impact of predicted usage and appropriately weigh costs against benefits. Determine and assess the adequacy of controls in the contract negotiation process for limiting costs.

4

ReviReview policies and guidelines on employee AI use: Examine the organization's policies and guidelines governing employee use of AI tools and applications. Evaluate the extent to which appropriate and sufficient guidance on inaccuracies, errors and quality issues is incorporated into policies. Assess the organization's processes for ensuring compliance.

5

Assess procedures for monitoring AI model performance and accuracy: Review the procedures and methodologies used to spot accuracy and performance issues by teams responsible for AI tools and applications used in the organization. Independently review a sample of outputs to assess the effectiveness of these controls.

AI Governance

Questions for Management

What process do you use to review, assess and approve AI use cases?

How do you track deployment and usage of AI tools and applications within the organization?

What is your methodology for measuring the value and impact of AI tools and applications?

How are problems with AI outputs reported?

What steps have you taken to control costs associated with AI tools and applications?

What guidance and/or training is provided to employees regarding how to assess AI outputs for accuracy and quality?

Who is accountable for errors and inaccuracies produced by AI models?

How are you assessing changes in productivity for employees using GenAI tools?

What processes exist within your function to ensure human review of AI outputs?

How are you monitoring performance and accuracy of AI models?

Audit Plan Hot Spots: 5-Year Comparison

2021	2022	2023	2024	2025
IT Governance	Ransomware	Cyberthreats	Cybersecurity Vulnerabilities	Cybersecurity Vulnerabilities
Data Governance	Data and Analytics Governance	IT Governance	IT Governance	Data Governance and Quality
Cyber Vulnerabilities	Digital Business Transformation	Data Governance	Regulatory Complexity	IT Governance
Business Continuity and Disaster Recovery (BCDR)	IT Governance	Third-Party Risk Management	Digital Transformation	Digital Transformation
Talent Resilience	Third Parties	Organizational Resilience	Organizational Resilience	Regulatory Compliance
Corporate Responsibility	Business Continuity and Organizational Resilience	Environmental, Social and Governance (ESG)	Third Parties	Third Parties
Third-Party Management	Environmental, Social and Governance (ESG)	Supply Chain	Supply Chain	AI Governance
Risk Culture and Decision Making	Supply Chain	Macroeconomic Volatility	Employee Well-Being and Satisfaction	Environmental, Social and Governance (ESG)
Corporate Financial Management	Strategy Execution	Workforce Management	Environmental, Social and Governance (ESG)	Workforce Management and Engagement
Data and Analytics	Workforce Management	Cost Pressures	Social and Political Tensions	Supply Chain
Supply Chain	Retention and Recruitment	Culture	Generative AI	Macroeconomic Conditions
Total Workforce Management	Economic Uncertainty	Climate Degradation	Macroeconomic Uncertainty	Sustainable Growth Strategies

Endnotes

Cybersecurity Vulnerabilities

[1] 2023 ISC2 Cybersecurity Workforce Study, ISC2.
[2] Technology and Cyber Crime: How to Keep Out the Bad Guys, The Financial Times (subscription required).
[3] 2023 Cybersecurity Skills Gap: Global Research Report, Fortinet.
[4] The CISO Report, Splunk (download required).
[5] Identity Security Threat Landscape 2024 Report, CyberArk.
[6] 2023 Gartner IAM Modernization Preventing Identity-First Security Survey.
[7] Identity Security Threat Landscape 2024 Report, CyberArk.
[8] Ibid.
[9] Charges and Seizures Brought in Fraud Scheme, Aimed at Denying Revenue for Workers Associated With North Korea, U.S. Department of Justice.
[10] The CISO Report, Splunk (download required).
[11] Allianz Risk Barometer 2024, Allianz Commercial.
[12] Global Cybersecurity Outlook 2024, World Economic Forum.
[13] Identity Security Threat Landscape 2024 Report, CyberArk.
[14] Ibid.
[15] Businesses Increase Cybersecurity as Budgets Surge in 2024, InfoSecurity Magazine; 2023 Was a Big Year for Cybercrime — Here's How We Can Make Our Systems Safer, World Economic Forum.
[16] Allianz Risk Barometer 2024, Allianz Commercial.
[17] Gartner Cybersecurity Controls Assessment Benchmark.
[18] Change Healthcare Confirms Ransomware Hackers Stole Medical Records on a 'Substantial Proportion' of Americans, TechCrunch; Hacked Change Healthcare Makes Progress in Recovery, but Concerns for Small Clinics Remain, CNN Business; How Did the Auto Dealer Outage End? CDK Almost Certainly Paid a $25 Million Ransom, CNN Business; Cyber Attack Takes Frontier Communications Systems Offline, Affecting Millions of Broadband Customers, ITPro.
[19] IBM Report: Half of Breached Organizations Unwilling to Increase Security Spend Despite Soaring Breach Costs, IBM.

Digital Transformation

[20] 2024 Gartner Board of Directors Survey on Driving Business Success in an Uncertain World.
[21] 2023 Gartner Change Management Landscape Survey; 2024 Gartner Growth Agenda Survey.
[22] Spending on Digital Transformation Technologies and Services Worldwide from 2017 to 2027, Statista.
[23] 2023 KPMG U.S. Technology Survey Report, KPMG (download required).
[24] How Businesses Can Stop Skyrocketing AI Use From Fueling Anxiety, EY.
[25] $2.3 Trillion Wasted Globally in Failed Digital Transformation Programs — Costly and Complex Business Strategies Are 'Not Necessary', Taylor & Francis.
[26] 2024 Gartner CIO and Technology Executive Survey.
[27] 2023 Gartner Audit AER Survey.
[28] What Is Change Management and How Does It Work?, Prosci.
[29] Workforce Skills Gap Trends 2024: Survey Report, Springboard (download required).
[30] The Era of Hybrid Cloud Storage, Nasuni (download required); Within Two Years, 90% of Organizations Will Suffer a Critical Tech Skills Shortage, Computerworld.
[31] AI At Work Is Here, Now Comes the Hard Part, Microsoft and LinkedIn; Gartner CIO Talent Planning for 2024 Survey.
[32] Agile Talent in the Age of AI, World Employment Confederation.
[33] 2024 SaaS Management Index Reveals an Average of $18M in Annual License Waste, With Significant Security Risks From Employee-Expensed Apps, Zylo.

AI Governance

[34] 2024 Gartner CIO and Technology Executive Survey.
[35] 2024 Gartner CIO Generative AI Survey.
[36] 2023 Gartner AI in the Enterprise Survey.
[37] 2024 Gartner CIO Generative AI Survey.
[38] Gartner (2023).
[39] The Economic Potential of Generative AI: The Next Productivity Frontier, McKinsey & Company.
[40] The Simple Macroeconomics of AI, Daron Acemoglu.
[41] For Data-Guzzling AI Companies, the Internet Is Too Small, The Wall Street Journal (subscription required).
[42] 2023 Gartner AI in the Enterprise Survey; Keep Your AI Projects on Track, Harvard Business Review (subscription required).
[43] The State of AI in Early 2024: GenAI Adoption Spikes and Starts to Generate Value, McKinsey & Company.
[44] How People Can Create — and Destroy — Value with Generative AI, BCG.
[45] Gartner Generative AI 2024 Planning Survey.

Actionable, objective insight

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

Research

Develop an Audit Strategic Plan You Can Use

Put your audit strategic plan on one page with this template.

Download Now

Research

The Digital Audit Function: Embed Audit Technology to Transform Assurance

Harness audit technology to optimize processes and transform assurance.

Download Now

Webinar

How Audit Can Drive Success in Critical Transformation Projects

See how leading internal audit teams support transformation success.

Watch Now

How We Help

Gartner for Audit

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

Gartner®

Everything you need in a single solution to:

Accelerate technology investments • Increase functional productivity • Modernize risk management approaches

Expert Insights and Interactions

- Tap into latest insights on functional improvement and personal effectiveness, as well as emerging topics like generative AI.
- Get direct access to our global team of research and advisory experts.

Service Delivery Support

- Available in the self-directed delivery model with the support of a service associate.

Peer Experiences

- Quickly solve urgent challenges. Connect with a community of business and tech peers.
- Engage in forums, 1:1 chats, polls and product ratings and reviews from verified peers.

Must-Attend Events

- In-person and virtual events arm you with actionable plans.
- Be inspired by world-class speakers, thought leaders, experts, demos and peers.

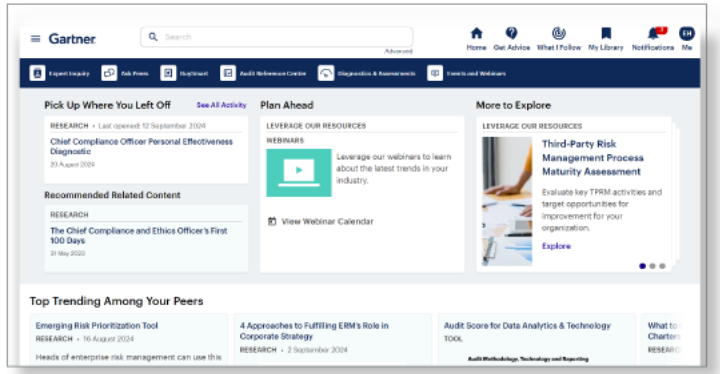
Workflow and Benchmark Tools

Practical tools and benchmarks to turn strategy into action by helping accelerate key initiatives and drive better business outcomes, including:

- Functional maturity assessments
- Risk assessments
- Budget and efficiency benchmarking

Gartner.com Experience

A customized gartner.com experience that gives you access to the most relevant insights and tools for your role.



Connect With Us

Get actionable, objective insight to deliver on your mission-critical priorities. Our expert guidance and tools enable faster, smarter decisions and stronger performance. Contact us to become a client:

U.S.: 1 855 811 7593

International: +44 (0) 3330 607 044

Become a Client

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

Stay connected to the latest insights

Gartner®