2024 Audit Plan Hot Spots

Gartner®

Objectives

The Audit Plan Hot Spots report identifies and analyzes the key risk areas that audit departments anticipate focusing on during the next year. This research enables audit departments to do the following:

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®

Executive Summary

The 2024 Audit Plan Hot Spots report is based on quantitative data from 100+ chief audit executives, interviews and surveys throughout the Gartner global network of client organizations and extensive secondary literature reviews. This year, three themes underlie the 12 hot spots:

1. Cost and Growth Pressures

The run-away inflation that characterized 2022 has slowed, but the world economy continues to face stiff headwinds. Tight credit conditions and subdued demand, combined with continued geopolitical rivalries that threaten supply chains, are exerting upward cost pressures. Organizations are transitioning to new, digital strategies to drive growth, but complex digital transformation projects are costly and a sluggish economy limits resources available for project implementation.

2. Increasing Fragility

Various multidimensional pressures are making organizations more fragile. Organizations must align and adapt their growth strategies, operations and governance frameworks to be flexible and responsive to both short- and long-term vulnerabilities. These efforts must also differentiate between internal threats, where organizations have direct control, and external threats, which they can only mitigate.

3. Heightened Accountability

Organizations are facing higher expectations of accountability from stakeholders such as boards, investors, regulatory bodies and civil society organizations. By a 6-to-1 margin, people expect businesses to be more involved in issues such as climate change, economic inequality and workforce reskilling. Accountability expectations are also elevated internally, as organizations face attrition from middle-management burnout and lack of employee connection.

Gartner®

Audit Plan Hot Spots Summary

Hot Spot	Summary	2024 Drivers	2023 Drivers
Cybersecurity Vulnerabilities	Organizations increasingly struggle to constrain cyberattacks from insider threats. Compounding this problem, the proliferation of Generative AI (GenAI) enables malicious actors access to more sophisticated cyberattack tools.	• Rise in Insider Threat • GenAI-Enabled Cyberattacks	• State-Sponsored Cyberattacks • Cyber Breach Disclosure Requirements
IT Governance	Organizations face challenges to digital initiative success due to complex IT infrastructures and a high willingness to accrue technical debt to attain quicker results. However, these factors slow and reduce effectiveness of digital initiatives in the long term.	• IT Infrastructure Complexity • Poorly Managed Technical Debt	• Ungoverned SaaS • IT Talent Shortage
Regulatory Complexity	Organizations face increased regulatory scrutiny at a faster pace and broader scope than in the past. This problem is compounded by regulatory fragmentation between sovereign and subnational jurisdictions, making compliance more expensive and compliance failures riskier.	• Velocity and Breadth of New Regulations • Regulatory Fragmentation	• Not a 2023 hot spot
Digital Transformation	Organizations' embrace of digital transformation without aligning specific digital goals and strategy results in suboptimal outcomes or transformation failure. Failure to account for negative impacts of transformation on employees risks lower productivity and loss of talent in a tight labor market.	• Unclear Project Objectives • Unintended Consequences of Digital Initiatives on Employees	• Not a 2023 hot spot
Organizational Resilience	Volatility and uncertainty, particularly due to the accelerating impacts of climate change, are putting a premium on organizations' capacities to absorb and withstand disruptions. Nonetheless, organizations are failing to effectively build their resilience, and fragmentation of roles and responsibilities is creating resilience gaps.	• Climate Change-Induced Disruptions • Fragmented Ownership and Oversight of Resilience Efforts	• Geopolitical Conflict • Diminished Change Capacity
Third Parties	As organizations rely on more high-risk third parties to drive growth, disjointed and outdated third-party risk management practices increase the potential for third-party breaches, among other risks.	• Increased Third-Party Vulnerability • Patchwork Third-Party Risk Management	• Third-Party Reputational Risk • Third-Party Viability

Audit Plan Hot Spots Summary

Hot Spot	Summary	2024 Drivers	2023 Drivers
Supply Chain	Geopolitical rivalries and efforts to avoid repeating the breakdowns from earlier in the COVID-19 era are driving organizations to restructure and diversify their supply chains. This trend, together with logistics bottlenecks and the impacts of rising temperatures and extreme weather events, are driving up supply chain costs.	• Supply Chain Restructuring • Ballooning Costs	• Renationalization of Supply Chains • Logistics Challenges Stemming From China's Zero-COVID-19 Policy
Employee Well-Being and Satisfaction	As organizations start to require more time in-office, disconnects between employer and employee perspectives are impacting employee well-being. At the same time, managers are overburdened with additional responsibilities and face low levels of health and satisfaction.	• Employer-Employee Return-to-Office Disconnect • Overburdened Managers	• Uncertain Talent Needs • Uncertain Long-Term Effects of Hybrid Working Models
Environmental, Social and Governance (ESG)	Lack of harmonized regulatory requirements and reporting frameworks leave organizations navigating a maze of different standards and guidance, creating ESG reporting challenges. Slow progress on publicly stated ESG goals exposes organizations to greenwashing or climate-related litigation and reputational risk.	• ESG Reporting Complexity • Slow Progress on ESG Goals	• Expanded ESG Reporting Standards • Increased Scrutiny of ESG Practices
Social and Political Tensions	Heightened geopolitical competition, through trade restrictions and controls, and costly social unrest around the world are affecting where organizations do business and leading to raised expectations regarding their involvement in social issues.	• Geopolitical Competition • Social Unrest	• Not a 2023 hot spot
Generative AI	The hype around GenAI after the release of ChatGPT is making it difficult for organizations to monitor employee use of GenAI applications and creating concerns around the validity and trust in outputs generated with the help of GenAI.	• Governance and Monitoring Challenges • Output Reliability and Trust Gaps	• Not a 2023 hot spot
Macroeconomic Uncertainty	Despite lingering inflation and interest rate hikes, many economies continue to exhibit strong growth and employment, creating a confusing and conflicting short-term picture. Longer-term conditions, however, point to persistent headwinds that will challenge organizations' ability to consistently meet financial performance objectives.	• Conflicting Short-term Signals • Looming Stagnation	• Rising Interest Rates • Currency Volatility

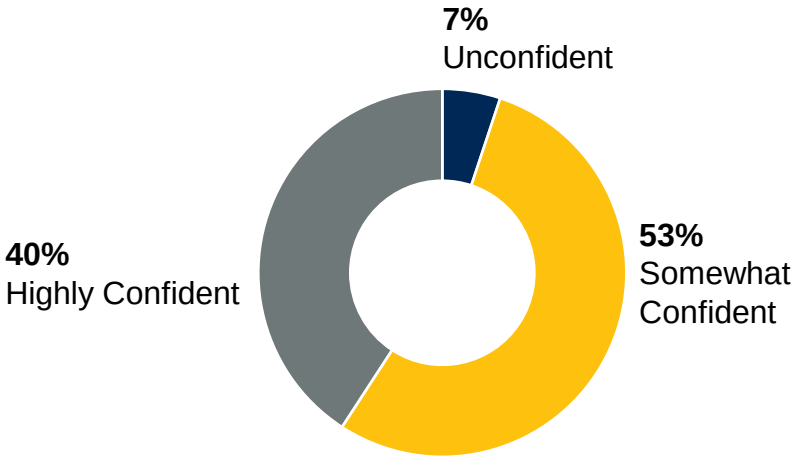
2024 Audit Plan Hot Spots

Organizational Resilience

Few organizations make organizational resilience a strategic priority with executive sponsorship, leaving them vulnerable to more frequent and costly disruptive events. Efforts to develop and operationalize resilience capabilities are often hindered by talent scarcity, lack of organizational awareness and limited funding. Resilience efforts will likely be further strained as organizations cut costs. Continuing to underinvest in resilience capabilities increases the fragility of the organization when inevitable disruptions hit.

Confidence in Audit's Ability to Provide Assurance Over Organizational Resilience Risk

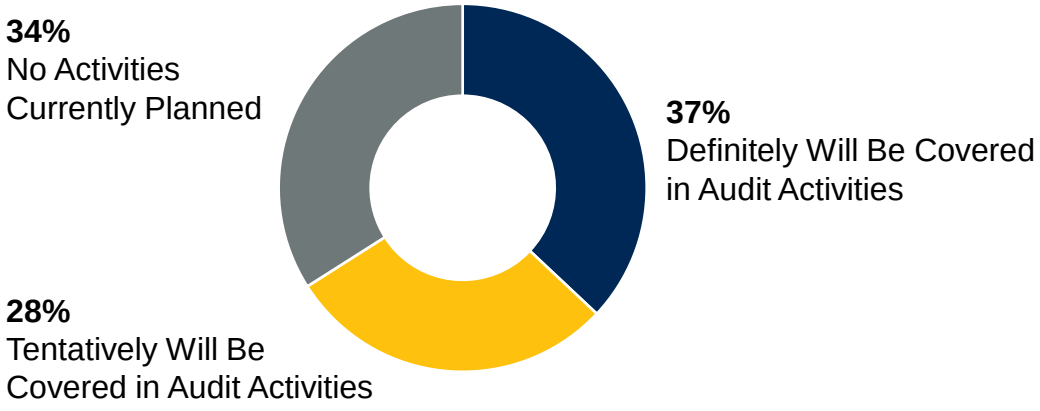
Percentage of Respondents



n = 100
Source: 2024 Gartner Audit Key Priorities and Risks Survey

Plans to Cover Organizational Resilience in Audit Activities in the Next 12-18 Months

Percentage of Respondents



n = 102
Source: 2024 Gartner Audit Key Priorities and Risks Survey
Note: Totals might not sum to 100% due to rounding.

Organizational Resilience

Urgency Drivers

Climate Change-Induced Disruptions

Climate and weather-related events are intensifying challenges for organizations' physical operations and employee well-being. In 2022, global economic losses from extreme weather reached $313 billion, as these events continue to be more frequent and harder to predict.[1] Rising temperatures and natural disasters can not only disrupt operations and raise costs but also create difficult working conditions.[2] Extreme heat and weather events have been linked to worsening employee mental health, increased job tension, higher turnover, workplace hostility and reduced on-the-job safety.[3] 70% of respondents to a global risk survey rate existing measures to prevent or prepare for climate change as "ineffective" or "highly ineffective," and a majority of organizations are failing to conduct climate scenario analysis.[4] These failures to adequately mitigate climate risks come as 50% of CEOs see climate change having a moderate, large or very large impact on their organization's cost profiles.[5] As weather patterns change, resilience strategies must account for not only the ability to withstand climate-related disruptions but also the long-term viability of operations, human capital impact and third-party relationships in specific locations.

Fragmented Ownership and Oversight of Resilience Efforts

Efforts to build organizational resilience are often undermined by unclear or overlapping roles and responsibilities and limited cross-functional coordination. Only 32% of participating organizations have a centralized team dedicated to organizational resilience.[6] More often a variety of C-suite roles have responsibility for specific aspects of resilience; few organizations (20%) say resilience is well-understood or cross-functional in a way that effectively prepares them to withstand disruptions.[7] Yet, critical steps to take in improving resilience are also diffused across the organization. For example, most risk managers believe that to strengthen resilience, organizations need to improve risk culture and risk data aggregation, tasks that require coordination across the organization.[8] Overall, organizations' inability to coordinate and collaborate on resilience makes it difficult for them to strategically prepare for and respond to disruptions.

Key Risk Indicators

- Frequency of extreme weather events in business locations (e.g., supplier locations, warehouses, factories, office locations and ports)
- Percentage of climate change scenario testing completed on a timely basis
- Number of employees affected by climate disruptions
- Percentage of strategic projects that incorporate climate considerations in forecasts
- Forecast revenue loss associated with climate disruptions
- Number of approved business continuity plans (BCPs) as a percentage of the total number of BCPs
- Number of business disruptions within a given time period
- Percentage of senior management not engaged in resilience planning efforts
- Percentage of departments without a business continuity coordinator
- Percentage of past-due mission-critical recovery plan tests

Organizational Resilience

Recommendations for Audit

1

Review Business Continuity Plans for Responding to Extreme Weather Events: Evaluate whether the organization's business continuity plan clearly outlines functional duties and responsibilities following extreme weather events. Confirm the plan is up to date and frequently refreshed with the operational areas most exposed, and it considers a wide range of extreme weather scenarios, including how those scenarios affect the hybrid workforce, key suppliers and major customers.

2

Assess Climate Considerations in Strategic Projects: Review if, and how, climate concerns are integrated in strategic plans and investments to ensure the organization considers the full impact of future initiatives. Consider the physical risks to employees and consumers, efforts to quantify the impact of climate-related business risks, and how to mitigate them.

3

Review Organizational Resilience Risk Culture: Review how the organization evaluates resilience risks and addresses any risk gaps. Recommend the organization maintains a resilience risk gap report and communicates resilience risks to management.

4

Examine Resilience-Related Activities for Completeness and Collaboration: Evaluate the extent to which operational resilience, organizational resilience, business continuity and crisis management plans consider disruptions that may result from events relating to all risks on the enterprise risk register. Assess the degree to which functions responsible for different aspects of resilience (e.g., IT, communications) collaborate on resilience-related initiatives.

5

Assess Management's Understanding of Organizational Resilience: Use surveys or interviews to evaluate the extent to which different business leaders and functions have a common understanding and commitment to the organization's resilience goals and how to achieve them.

Gartner®

Organizational Resilience

Questions for Management

What steps are you taking to coordinate with other functions, with the goal of being more resilient in the face of more regular and extreme weather events?

What type of extreme weather event(s), and in what location(s), would have the greatest impact on your business unit?

How are you removing silos between various functions or business units (e.g., IT, human resources, finance, procurement) to align the organization's focus on continuity and resilience?

How are you factoring increased climate-disruption costs into your plans and strategies?

How often, and in what format, are strategies around organizational resilience communicated?

How often do you collaborate with executives in other functions and units who you believe play a key role in organizational resilience?

How often do you reevaluate business continuity and crisis management plans?

How are after-action reports from scenario exercises shared and leveraged?

How are you preparing to clarify roles and coordinate a quick response during a disruptive event?

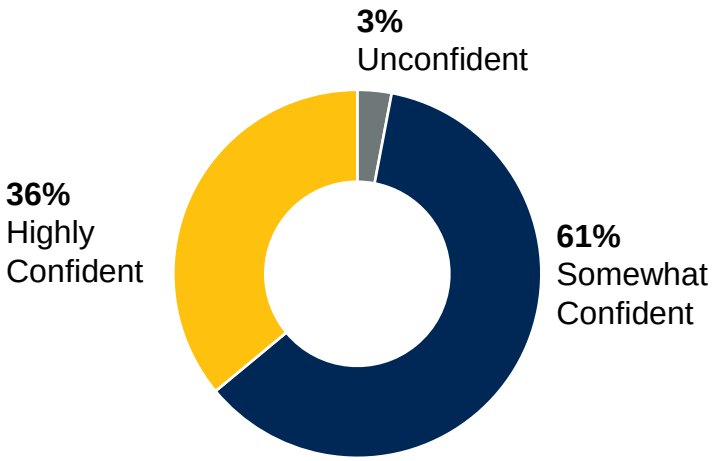
What would you say are the biggest impediments to an agile organizational response to disruptive events?

Third Parties

Organizations increasingly rely on third parties to improve profitability, efficiency and innovation, but greater reliance expands third-party vulnerabilities and exacerbates insufficiencies in third-party risk management (TPRM) strategies. Although organizations are working with more high-risk third parties, they continue to struggle to effectively manage third-party risks. Failure to adapt TPRM strategies to rising threats increases potential for financial, regulatory and reputational risk exposure.

Confidence in Audit's Ability to Provide Assurance Third and "Nth" Parties Risk

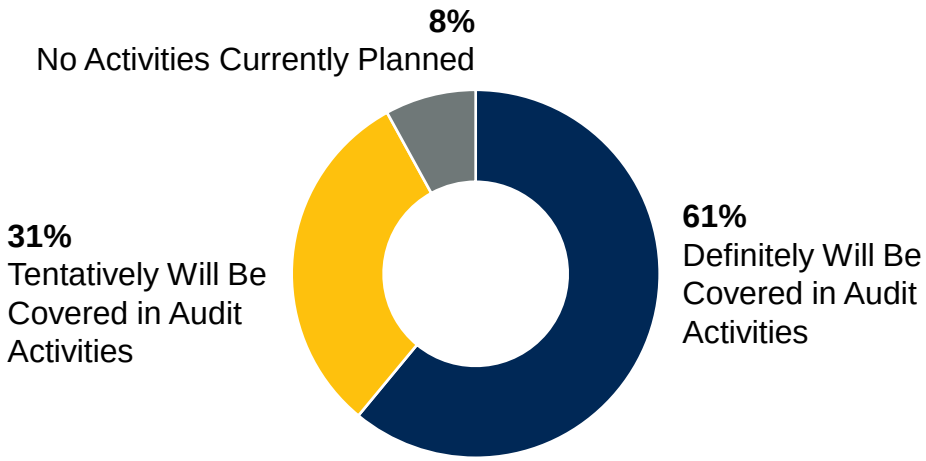
Percentage of Respondents



n = 100
Source: 2024 Gartner Audit Key Priorities and Risks Survey

Plans to Cover Third and "Nth" Parties in Audit Activities in the Next 12-18 Months

Percentage of Respondents



n = 102
Source: 2024 Gartner Audit Key Priorities and Risks Survey

Third Parties

Urgency Drivers

Increased Third-Party Vulnerabilities

The continued expansion of third-party networks has created higher third-party risk exposure and more frequent third-party risk events. As organizations increase investment in digital capabilities, third parties increasingly enable more core business operations and are more critical to organizations' profitability than before the pandemic.[9] Despite these benefits, third parties are five times more likely than the organization itself to have poor overall security, and 98% of organizations have experienced a breach resulting from at least one third party in the last two years.[10] The profile of organizations' third-party networks has also shifted toward more risky partners. Forty-three percent use third parties to perform new-in-kind technology services, and 44% of organizations' third-party networks increasingly include startups and innovators (many of whom have high risk appetites and low risk governance).[11] As they use more third parties to drive growth and innovation, organizations must address their low confidence in third-party controls and balance the benefits third parties provide with their greater risk exposure.[12]

Patchwork Third-Party Risk Management

Outdated and disjointed TPRM practices are undermining organizations' ability to effectively monitor and mitigate third-party risks. While 84% of organizations recognize the strategic importance of mitigating these risks, only 13% continuously monitor third-party security risks, and many still heavily rely on manual processes, such as spreadsheets, to manage risks across the third-party life cycle.[13] Further complicating efforts is organizations' continued use of lagging methods such as newsfeeds to learn about third-party breaches.[14] To improve these efforts, organizations are using technology to automate or support TPRM tasks, but they are often unsatisfied with the capabilities and encounter data-related issues.[15] This fragmentation leaves organizations with a disjointed set of TPRM methods further complicated by the various functions involved in TPRM. Almost half of function heads say they inefficiently share TPRM information with other functions, and only 44% incorporate shared information into their risk analysis system.[16] As a result, few organizations maintain an accurate picture of their third-party risk landscape (21%), and even fewer agree they effectively manage third-party risk (18%).[17] A failure to remedy analog TPRM practices and poor internal information sharing threaten to exacerbate rising third-party risk exposure.

Key Risk Indicators

- Number of critical third parties with open critical risk issues or adverse reports from regulators
- Number of reported third-party security breaches
- Number of third-party disruptions, such as lost revenue, operational delays, regulatory fines and loss of critical data
- Year-over-year growth in the number of third-party relationships for critical services or products
- Frequency of updating third-party risk classification
- Percentage of third parties with access or potential access to sensitive organizational data
- Percentage of critical third parties categorized as "high-risk"
- Number of third parties that have provided continuity plans
- Number of third-party contracts established outside designated functions, such as procurement, IT or legal and compliance
- Percentage of third parties identified as startups or innovators

Third Parties

Recommendations for Audit

1

Assess TPRM Roles and Responsibilities: Evaluate which functions are responsible for third-party risk management and whether all relevant functions are aware of their role. Identify any overlap, omission or confusion of responsibilities that should be remediated.

2

Review Third-Party Crisis Communication Protocols: Evaluate whether relevant functions have investigated contractual reporting requirements for when and how a third party will communicate information regarding a breach or failure.

3

Review Ongoing Monitoring of Third-Party Relationships: Assess whether the business monitors third parties and their behaviors and policies throughout the third-party life cycle. Review the frequency of risk profile reassessments and updates and how management addresses material changes.

4

Evaluate the Classification of Third-Party Risk: Evaluate the financial, strategic and behavioral metrics the organization uses to identify and monitor critical third parties, and assess how monitoring differs across different risk profiles. Confirm the business conducts random checks of third parties to evaluate whether their risk categorization accurately reflects their level of risk.

5

Review Decision Making for Implementing Technology in TPRM Practices: Review which stakeholders are involved in decision making for TPRM technology investments and to what extent all parties involved in TPRM are consulted. Evaluate how cross-functional TPRM technology needs are assessed and the extent to which technologies can enable cross-functional collaboration and information sharing.

Gartner®

Third Parties

Questions for Management

What processes are in place to conduct due diligence on third parties before entering strategic relationships with them?

What monitoring and reporting activities are in place to understand changes in third-party risk levels?

How are critical third parties identified and prioritized for risk assessments and monitoring?

What information sources do you use to assess the risks posed by third parties?

How is information from third-party risk assessments shared and leveraged (beyond the function conducting the initial assessment)?

What processes are in place to ensure third-party breaches are communicated promptly?

How is risk tolerance for third parties adjusted when partnering with firms that are critical to growth and transformation projects?

How do you use, or are you planning to use, technology to support third-party risk management activities?

How do you communicate the organization's expectations for risk management and regulatory compliance to third parties?

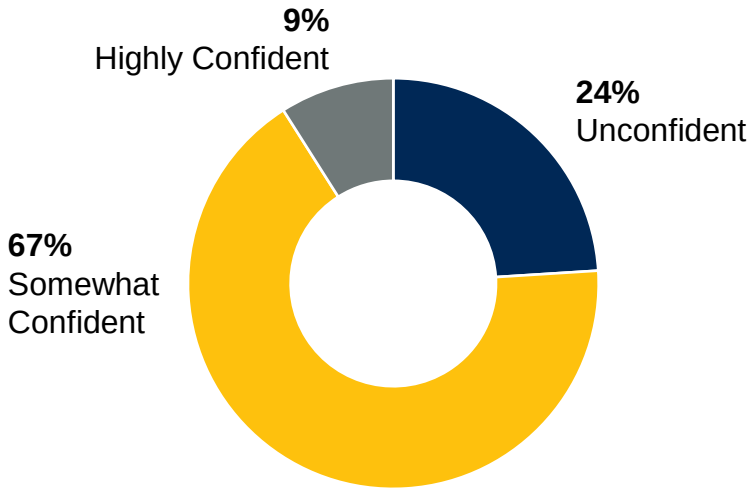
How far down the third-party chain (fourth, fifth, nth) does the organization go to assess third-party risk?

Generative AI

The high-profile release of ChatGPT in November 2022 prompted an explosion of interest in GenAI, defined as AI techniques that learn a representation of artifacts from data, and use it to generate brand-new, unique artifacts that resemble but don't repeat the original data. However, both publicly available GenAI applications and those built in-house create new and heightened risks for data and information security, privacy, IP protection and copyright infringement, as well as trust and reliability of outputs.[18] As organizations rush to adopt these new technologies, they must establish effective guardrails around acceptable uses and validation of outputs to reap the full benefits these tools can offer.

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

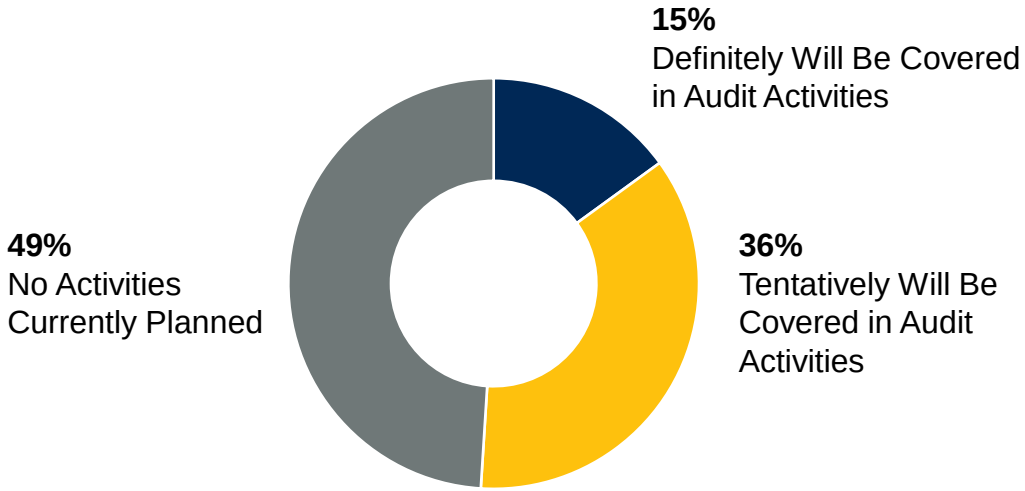
Percentage of Respondents



n = 88
Source: 2024 Gartner Audit Key Priorities and Risks Survey

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

Percentage of Respondents



n = 102
Source: 2024 Gartner Audit Key Priorities and Risks Survey

Generative AI

Urgency Drivers

Governance and Monitoring Challenges

Whether organizations build in-house GenAI applications or access publicly available tools such as ChatGPT and Google Bard, monitoring and governing use is challenging. Nearly half (46%) of professionals use ChatGPT as part of their workday, but 68% of those who do haven't told their bosses.[19] Several incidents of employees inputting confidential, sensitive or proprietary information in a GenAI application have been reported, but organizations don't know how such information is processed in the model or if it is used to train the model.[20] These challenges extend to organizations piloting GenAI. Many applications still require access to third-party services, opening up a host of potential privacy and data protection risks. While establishing organizationwide policies and educating employees around acceptable use of public tools can help, most organizations struggle to keep up with the technology. In Gartner's 2023 IT Leader Poll on Generative AI, 36% of IT leaders said their organization had no guidance yet on GenAI, while another 31% said their organization was halting use while they investigated. As organizations move to reap the benefits of GenAI, they must determine their risk appetite and establish commensurate governance.

Output Reliability and Trust Gaps

Inaccuracy of outputs is among the most-cited risks of GenAI applications, leading organizations to be concerned about what comes out of the models as much as what goes into them.[21] In Gartner's 2023 CIO Generative AI survey, CIOs rank the propensity to hallucinate facts (i.e., present false or inaccurate claims) and make reasoning errors as their second highest concern around GenAI use. Examples such as ChatGPT fabricating legal citations and prompting defamation lawsuits reflect the unreliability of GenAI outputs.[22] In addition to inaccurate individual outputs, GenAI may also produce materially different outputs at different times in response to similar queries. An analysis of GPT-4 found that while it exhibited 97.6% accuracy in identifying prime numbers in March 2023, its accuracy in the same task plummeted to 2.4% in June.[23] Overall, only 43% of employees using GenAI say they trust ChatGPT will provide accurate results, further raising concerns as organizations use GenAI in areas such as data analysis and prediction, marketing and advertising, and customer service.[24] As organizations leverage GenAI, erroneous model outputs threaten reliable decision making and organizational reputation.

Key Risk Indicators

- Number of LLM use cases in the organization
- Amount of spending on GenAI initiatives aimed at people-oriented analysis and decision making
- Number of employees with needed GenAI skill sets
- Number of third parties involved in GenAI design or operation
- Number of data breaches related to employee use of GenAI
- Percentage of new hires with GenAI skills
- Number of operational failures related to GenAI outputs
- Percentage of GenAI outputs thoroughly reviewed by human reviewers and subject matter experts
- Frequency of communications to employees around the use of GenAI
- Percentage of employees using GenAI in their daily work

Generative AI

Recommendations for Audit

1

Review GenAI Monitoring Practices: Evaluate practices for monitoring GenAI use by employees and potential leaks of data, intellectual property or other sensitive information.

2

Assess Organizational Communication and Training on GenAI: Evaluate the frequency and thoroughness of organizational communication and employee training on GenAI use. Assess the level of visibility of these policies to employees and review metrics such as unique page views and training completion rates to assess penetration.

3

Advise Organizational GenAI Working Groups: Advise committees and working groups on GenAI to highlight the risks of large language models (LLMs) and their impact on strategic priorities.

4

Assess Organizational GenAI Policy Decision Making: Review how the organization creates its GenAI use policy and assess the rationale behind the breadth and limits of the policy. Evaluate plans for updating the policy and if rules are differentiated for specific groups or business units.

5

Review Processes for Approving GenAI Use: Assess the processes and systems for approving GenAI use cases in the organization, as well as the roles and responsibilities behind approving the decisions and changing the policy. Review the extent to which active usage has complied with approval procedures.

Gartner®

Generative AI

Questions for Management

What procedures are in place in the organization and IT department to conduct an inventory of LLM use and associated risks and controls?

How often does the organization update its guardrails for GenAI use?

How are GenAI use cases in the organization meeting the goals set for its use by leadership?

How does the organization ensure employees do not input sensitive data into GenAI applications?

How does the organization determine if a GenAI use case is appropriate?

How do you understand whether third parties are using GenAI in the services they provide the organization, and how is such use vetted for compliance with organizational policies?

What processes exist for vetting outputs from GenAI?

How does the organization equip employees to responsibly use GenAI?

How do you gather data on GenAI use in the organization?

What categories of GenAI-related controls does the organization recognize, and which categories contain the biggest control gaps presently?

Gartner

Audit Plan Hot Spots Dashboard

2020	2021	2022	2023	2024
Data Governance	IT Governance	Ransomware	Cyberthreats	Cybersecurity Vulnerabilities
Third-Party Ecosystems	Data Governance	Data and Analytics Governance	IT Governance	IT Governance
Cyber Vulnerabilities	Cyber Vulnerabilities	Digital Business Transformation	Data Governance	Regulatory Complexity
Data Privacy	Business Continuity and Disaster Recovery (BCDR)	IT Governance	Third-Party Risk Management	Digital Transformation
Risk Culture and Decision Making	Talent Resilience	Third Parties	Organizational Resilience	Organizational Resilience
Project Management	Corporate Responsibility	Business Continuity and Organizational Resilience	Environmental, Social and Governance	Third Parties
IT Governance	Third-Party Management	Environmental, Social and Governance	Supply Chain	Supply Chain
Regulatory Developments	Risk Culture and Decision Making	Supply Chain	Macroeconomic Volatility	Employee Well-Being and Satisfaction
Organizational Resilience	Corporate Financial Management	Strategy Execution	Workforce Management	Environmental, Social and Governance
Supply Chain	Data and Analytics	Workforce Management	Cost Pressures	Social and Political Tensions
Strategic Workforce Planning	Supply Chain	Retention and Recruitment	Culture	Generative AI
Artificial Intelligence (AI)	Total Workforce Management	Economic Uncertainty	Climate Degradation	Macroeconomic Uncertainty

Endnotes

Organizational Resilience

[1] 2023 Weather, Climate, and Catastrophe Insight, Aon.

[2] Extreme Heat Is Hitting Companies Where It Hurts, Time.

[3] Climate Change Effects on Mental Health: Are There Workplace Implications?, Oxford Academic; How Extreme Heat Affects Workers and the Economy, The New York Times (subscription required).

[4] WEF Global Risks Report 2023, World Economic Forum; When Will Climate Disclosures Start to Impact Decarbonization?, EY.

[5] PwC's 26th Annual Global CEO Survey, Winning Today's Race While Running Tomorrow's, PwC.

[6] 2021 Gartner Organizational Resilience Survey.

[7] Gartner (June 2023); Toward True Organizational Resilience: Deloitte's Global Resilience Report, Deloitte.

[8] From Risk Management to Strategic Resilience, McKinsey & Company.

Third Parties

[9] 2022 Gartner Cross-Functional Third-Party Risk Management Survey.

[10] Close Encounters of the Third (and Fourth) Party Kind, Security Scorecard & Cyentia Institute.

[11] 2022 Gartner Cross-Functional Third-Party Risk Management Survey.

[12] 2022 Gartner Cross-Functional Third-Party Risk Management Survey; 2022 Gartner ERM Survey on Third-Party Risk.

[13] Navigating Third-Party Security Risks in 2023: Mid-Year Insights and Trends, Panorays; The 2023 Third-Party Risk Management Study, Prevalent.

[14] The 2023 Third-Party Risk Management Study, Prevalent.

[15] Third-Party Risk Management Outlook 2022, KPMG.

[16] 2022 Gartner Cross-Functional Third-Party Risk Management Survey.

[17] 2022 Gartner Risk Committee Survey.

Generative AI

[18] Managing the Risks of Generative AI, PwC.

[19] Nearly 70% of People Using ChatGPT at Work Haven't Told Their Bosses About It, Survey Finds, Business Insider.

[20] CheatGPT: The Hidden Wave of Employees Using AI on the Sly, Business Insider; Samsung Bans Staff's AI Use After Spotting ChatGPT Data Leak, Bloomberg (subscription required); Amazon Warns Employees Not to Share Confidential Information With ChatGPT After Seeing Cases Where Its Answer 'Closely Matches Existing Material' From Inside the Company, Business Insider (subscription required).

[21] The state of AI in 2023: Generative AI's Breakout Year, McKinsey & Company.

[22] Lawyer Apologizes for Fake Court Citations From ChatGPT, CNN Business; First ChatGPT Defamation Lawsuit to Test AI's Legal Liability, Bloomberg (subscription required).

[23] How Is ChatGPT's Behavior Changing over Time?, Chen, Lingjiao, Zou, J. (Stanford University) and Zaharia, M. (UC Berkeley) arXiv.org; Gartner (August 2023).

[24] ChatGPT in the Workplace: Korn Ferry Survey Shows Majority of Professionals Would Use the Tool, Though Less Than Half Trust its Accuracy, Korn Ferry; The State of AI in 2023: Generative AI's Breakout Year, McKinsey & Company.

Gartner®

Actionable, objective insight

Position your organization for success. Explore these additional complimentary resources and tools for corporate controllers:

Template

Develop an Audit Strategic Plan You Can Use

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

Download Now

Webinar

The Top 2024 Audit Plan Hot Spots

Anticipate emerging risks that organizations will face in 2024.

Watch Now

Webinar

Internal Audit's Support of Critical Transformation Project Success

See how leading internal audit teams support critical transformation project success.

Watch Now

Already a client?
Get access to even more resources in your client portal. Log In

Gartner®

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 Legal, Risk & Compliance
gartner.com/en/legal-compliance

Stay connected to the latest insights

Gartner®