Gartner

2026 Audit Plan Hot Spots

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 2026.

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 2026 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 report and related resources, guidance and tools, contact us to learn more about becoming a Gartner client.

Become a Client

Chief audit executives (CAEs) 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 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®

4 Themes Underlying the 2026 Hot Spots

1

A Volatile Political Landscape

Early actions by the current U.S. Administration have sent shockwaves through the global economy. Even more than the magnitude of regulatory and policy changes, organizations have struggled to adapt to the volatility and uncertainty around them. Tariff and trade policies alone have been the primary cause of uncertainty, with wave after wave of new announcements and modifications to previous announcements. Globally, there are also widening rifts between competing power blocs in areas such as environmental, social and governance (ESG) policy and the prioritization of bribery and corruption laws.

2

Pressures to Contain and Reduce Costs

Uncertainty is casting a shadow over future economic conditions, raising the difficulty of long-term strategic planning and investment decisions. In this environment, organizations are pursuing cost-cutting and cost optimization strategies to maintain profitability. But such efforts can bring unintended consequences, particularly with respect to workforce planning, employee engagement and the delivery of digital transformation initiatives.

3

Maintaining Security and Resilience Amid Uncertainty

Amid uncertainty and macroeconomic headwinds, organizations must ensure core capabilities in security and resilience remain robust. Cybersecurity vulnerabilities continue to be top-of-mind for executive leaders and boards, and organizations can ill afford to cut corners as threats continue to proliferate. Vulnerabilities in third parties are of particular concern — as vendors also adapt to economic conditions, organizations must ensure security remains a priority. Overall, organizations should grow their capabilities for resilience in the face of powerful disruptive forces.

4

Scaling AI Deployment

While navigating these headwinds, organizations continue to grow their technology investments, particularly with respect to AI. Economic uncertainty increases the urgency for organizations to unlock the productivity promise of AI technologies. However, new developments, such as AI agents, are adding even more complexity to AI risk governance, while the use of AI tools in IT workflows can lead to security and quality issues. Organizations must also adapt data governance to cope with the proliferation of AI-generated material.

Audit Plan Hot Spots Summary

Hot Spot	Summary	2026 Drivers	2025 Drivers
Cybersecurity Vulnerabilities	Cybersecurity teams are overwhelmed by rising vulnerabilities and a crowded information environment. Moreover, organizations must contend with a surge in AI-driven disinformation threats.	1. Strained Capacities for Vulnerability and Threat Management 2. Rise of Disinformation Threats	1. Identity Verification and Management Challenges 2. Imbalances Between Defense and Resilience in Cybersecurity Investments
Data Governance	As organizations continue to increase their use of AI, large volumes of data created by AI outputs pose growing challenges for governance. Meanwhile, a growing number of data sovereignty localization requirements drive up costs and create technical, logistical and compliance challenges for organizations.	1. Governance Challenges Over AI-Generated Outputs 2. Data Sovereignty Restrictions	1. Limited Return on Data Governance Investments 2. Insufficiently AI-Ready Data
Regulatory Compliance	Rapid policy changes and shifting enforcement priorities have created regulatory uncertainty, complicating compliance efforts. Organizations also face a weakening ethical culture and heightened misconduct risk amid macroeconomic headwinds and organizational change.	1. Regulatory and Policy Uncertainty 2. Weakening Ethical Culture	1. Impact of Electoral Uncertainty on Regulatory Priorities 2. Growing Reporting Needs in Nonfinancial Areas
IT Governance	Insider threats are rising as workforces become more disgruntled and geopolitical tensions escalate, driving the need for increased digital and physical asset protection. Meanwhile, growing reliance on AI tools by IT professionals is contributing to skills erosion, reduced code quality and security vulnerabilities.	1. Rising Motivation and Opportunity for Insider Threat 2. IT Skills and Process Degradation	1. IT-Driven Business Disruption 2. Cloud Concentration
AI Governance	Organizations must contend with new difficulties in AI governance, driven by the development of AI technology to include autonomous AI agents as well as gaps in visibility into AI usage throughout the organization.	1. Deployment of AI Agents 2. Visibility Gaps in AI Usage	1. Inflated Expectations for GenAI 2. Excessive Employee Faith in GenAI Outputs
Digital Transformation	Digital transformation leaders are facing greater pressure to deliver cost-effective results, resulting in difficult trade-offs between short-term and long-term objectives. Moreover, in a cost-conscious environment, project teams may deprioritize risk management and controls, an aspect of project execution that is already often underemphasized.	1. Cost and Efficiency Pressures 2. Risk Management and Controls Integration Challenges	1. Challenges in Achieving ROI for Digital Transformation Initiatives 2. Gaps in Skills Underpinning Digital Transformation

Audit Plan Hot Spots Summary

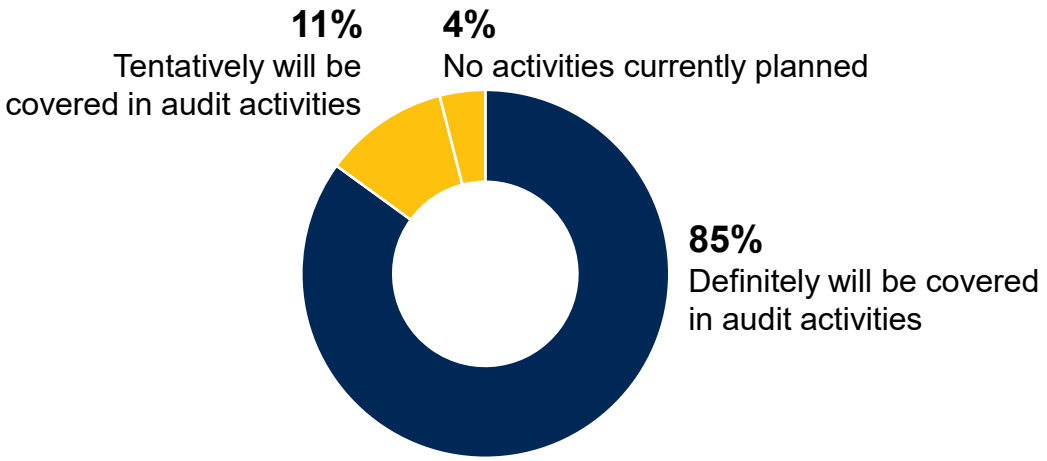
Hot Spot	Summary	2026 Drivers	2025 Drivers
Third Parties	Third-party cybersecurity risks are a major threat to organizational data and assets, compounded by increasing regulatory liability. At the same time, the stability and performance of external partnerships are growing more uncertain in a volatile geopolitical landscape.	1. Expanding Third-Party Cybersecurity Vulnerabilities 2. Geopolitical Disruptions Affecting Third-Party Relationships	1. Limited Visibility Into Third-Party Data Usage and Protection Practices 2. Embedded and Hybrid AI in Third-Party Applications
Organizational Resilience	Business interruptions are growing in volume and frequency, but risks are underemphasized in organizations' strategies, leaving many underprepared. Risks themselves are becoming more interdependent and complex, making it difficult to develop strategies and analyze the risks' potential impacts.	1. Insufficient Attention to Risk in Organizational Strategy 2. Heightened Risk Interdependencies	Not a 2025 Hot Spot
Supply Chain Distortions	An unprecedented volume of tariff and trade policy changes is driving up costs and disrupting operations. Meanwhile, these rapid shifts are also increasing the risk of supply chain noncompliance and regulatory exposure.	1. Tariff Volatility 2. Supply Chain Compliance Challenges	1. Misprioritization of Resiliency Investments 2. Supply Chain Visibility Imperatives
Talent Management	Organizations are struggling to keep their talent strategies aligned with the growing use of AI in daily workflows, hiring and performance management. At the same time, rising employee resentment — driven by change fatigue and cost-cutting measures — is threatening productivity and morale across increasingly strained teams.	1. Uncertain Effects of AI on Talent Strategies 2. Decreasing Productivity Due to Employee Resentment	1. Shifting Workforce Demographics 2. Employee Productivity Pressures
Macroeconomic Uncertainty	Businesses are facing a high risk of reduced consumer demand as tariff-driven price increases and high borrowing costs put pressure on household budgets. Moreover, high levels of economic uncertainty are leading organizations to delay investments, potentially dragging down future growth prospects.	1. Declining Consumer Demand 2. Effect of Policy Uncertainty on Investment and Growth	1. Protracted Interest Rate Elevation 2. Reigniting Trade Tensions
ESG Strategies	Organizations must navigate a challenging set of conflicting requirements, as regulatory and policy regimes around ESG reporting are increasingly diverging across different regions. At the same time, the broader landscape for communicating ESG strategy and commitments is increasingly fraught amid heightened societal controversy.	1. Globally Divergent Regulatory and Policy Mandates on ESG Reporting 2. Fraught ESG Communications Landscape	1. Reporting Regulations Coming Into Force 2. ESG Data Quality and Management Gaps

Cybersecurity Vulnerabilities

Strained capacity of security teams and constant alerts are creating critical blind spots in vulnerability and threat management across increasingly decentralized IT environments. More than half of security professionals report they cannot keep pace with the increasing number of security threats.[1] At the same time, as organizations struggle to keep pace with these core responsibilities, new threats related to disinformation are developing faster than organizations' response capabilities. The spread of manipulated and falsified information — identified by the World Economic Forum's Global Risk Report as the most severe short-term threat — is eroding consumer trust and intensifying global security risks, with GenAI amplifying its scale and impact.[2] In this environment, 50% of senior executives at organizations experiencing mis-, dis- or malinformation report reputational damage as a result.[3] To stay ahead, leaders face an urgent need to rethink cybersecurity processes to more effectively manage vulnerability and threat volume and bolster defenses against AI-driven disinformation.

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

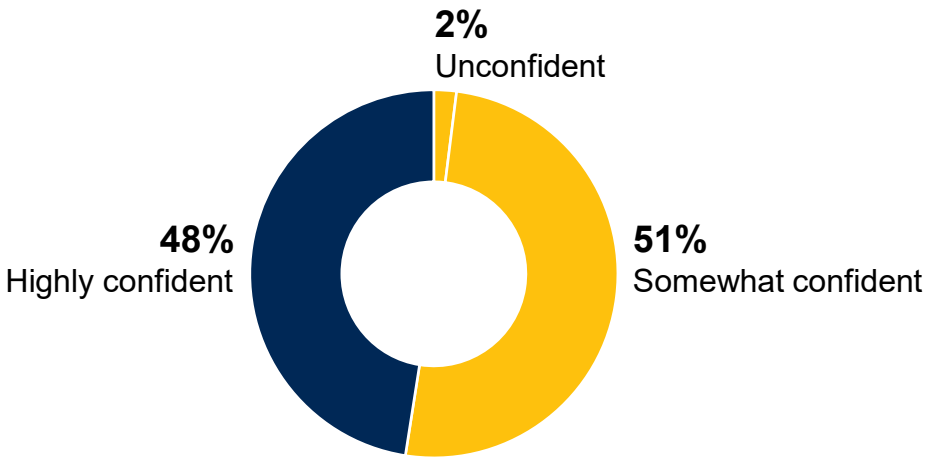
Percentage of respondents



n = 118
Source: Gartner Survey on 2026 Audit Plan Hot Spots

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

Percentage of respondents



n = 160
Source: Gartner Survey on 2026 Audit Plan Hot Spots
Note: Totals may not sum to 100% due to rounding.

Cybersecurity Vulnerabilities

Urgency Drivers

Strained Capacities for Vulnerability and Threat Management

Exploitation of vulnerabilities, such as zero-day attacks on systems, including VPNs and edge devices, now accounts for 20% of all cyberbreaches, compounding challenges for organizations' already strained cybersecurity resources and processes.[4] Amid proliferating vulnerabilities and patching needs, shortages of skilled cybersecurity professionals are contributing to an environment where 41% of IT workers report they are somewhat to very stressed.[5] These high stress levels can increase the likelihood of lapses in security operations: 67% of business leaders are concerned that cybersecurity staff stress, fatigue and burnout will lead to increased errors and compromised systems.[6] Meanwhile, a saturated information environment characterized by multiple tools and alerts, across an increasingly distributed IT environment, is making it harder to identify real threats. Seventy-one percent of security professionals have more than 10 detection and response tools in place, with 45% having more than 20.[7] As a result, 71% worry every week they will miss a real attack buried in a flood of alerts.[8] To ease the burden on overstretched teams, organizations must reassess cyber staff workloads and resourcing, and streamline their security operations by consolidating multiple detection and response tools.

Rise of Disinformation Threats

Growing disinformation is creating a need for organizations to develop disinformation security capabilities, which Gartner defines as measures to discern trust, assess truth and track the spread of misinformation, including techniques to detect deepfakes and protect the organization's reputation.[9] The rise of GenAI has enabled malicious actors to more easily and quickly produce malicious content at scale to conduct fraud schemes and spread false claims about organizations. For example, voice phishing (vishing) attacks have risen by 442% from 1H24 to 2H24.[10] Despite these growing risks, 80% of companies still lack protocols for handling deepfake attacks, revealing a widespread lack of preparedness.[11] At the same time, this technology is now being used to manipulate public opinion and spread false narratives across social media. A striking example involved a falsified memo, allegedly issued by the U.S. Department of Defense, which claimed a semiconductor firm's acquisition target posed security risks, triggering a drop in both companies' stocks.[12] Incidents like this underscore the urgent need for "disinformation security" capabilities to detect, mitigate and respond to these evolving threats.

Key Risk Indicators

- Number of security alerts generated per week
- Ratio of security operations staff to incidents
- Ratio of false positives versus true positives in threat alerts
- Number of applications not directly managed by central IT
- Average time to implement patches in critical systems
- Percentage of overdue patches
- Staff turnover rate in cybersecurity roles
- Trends in employee engagement levels for security staff
- Percentage of disinformation incidents resulting in reputational damage
- Time to detect and respond to disinformation campaigns

Cybersecurity Vulnerabilities

Recommendations for Audit

- **Review cyberthreat monitoring and response procedures:** Examine threat monitoring and incident response workflows, including management's procedures for reviewing and updating them. Assess how current procedures manage alert volume and enable triage in alignment with the evolving threat landscape.
- **Review cyber-response roles and responsibilities:** Assess whether there are defined roles and responsibilities, as well as appropriate communication channels, to foster coordination and accountability for addressing vulnerabilities, especially for decentralized IT systems. Evaluate the effectiveness of collaboration between cybersecurity, IT and other business units in managing threats and vulnerabilities.
- **Assess vulnerability patch management procedures:** Assess the adequacy and effectiveness of procedures for prioritizing vulnerability patches. Review whether patches are applied within the timelines established by the organization's policies. Evaluate how effectively documentation and communication supports the process of patch deployment for decentralized IT systems and applications, where applicable.
- **Assess protocols for disinformation detection:** Assess tools and processes used to monitor social media, news outlets and other forums for disinformation incidents. Validate whether appropriate roles and responsibilities have been established for responding to a disinformation incident.
- **Evaluate cybersecurity awareness training programs:** Assess whether the organization's cybersecurity training includes sufficient coverage of disinformation issues. Evaluate whether employees receive adequate training to recognize AI-powered disinformation threats, such as deepfakes, synthetic media and voice phishing (vishing).

Cybersecurity Vulnerabilities

Questions for Management

How do you prioritize which vulnerabilities to patch first?

How do you monitor for unpatched vulnerabilities across decentralized IT environments?

How do you triage the volume of information and alerts generated by security tools?

How do you distinguish between false positives and real threats in your alerting systems?

How do you evaluate your portfolio of security tools when considering acquiring new tools or consolidating existing tools?

What processes are in place to ensure timely involvement of security teams when developing new solutions, particularly in cases of decentralized initiatives not owned by central IT?

How, and how often, do you assess engagement and fatigue levels of cybersecurity staff?

How do you monitor for manipulated or falsified information about the organization?

What procedures are in place to identify and respond to incidents of disinformation affecting the organization?

What processes are in place to monitor and track the costs associated with complying with data localization and sovereignty rules?

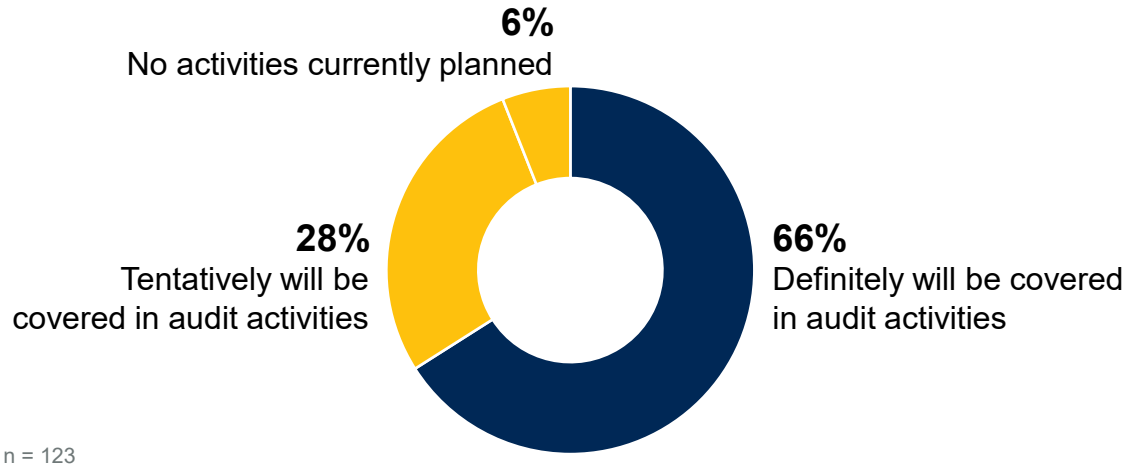
Data Governance

Organizations' data governance efforts face new challenges for managing the volume and classification of AI-generated outputs, as well as heightened risks related to data localization and sovereignty as regulations proliferate. In relation to AI, 77% of organizations are currently working on AI governance, which includes oversight of data quality and data pipelines, as the organization's data is leveraged for AI implementation.[13] But organizations focus on enabling data as an input for AI — most data leaders cite data quality as the most important aspect of data governance — leaving potential blind spots with respect to AI outputs.[14]

Meanwhile, organizations face an increasingly complex patchwork of data sovereignty and localization requirements, as 155 countries now have some form of privacy and data protection laws.[15] Organizations must grapple with diverse requirements across jurisdictions as well as uncertainty over the legal status of transnational agreements governing cross-border transfers, such as the U.S.-EU Data Privacy Framework.[16] Failure to enact governance over AI-generated outputs and address data localization requirements means facing a heightened risk of data leakage and higher operational costs.

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

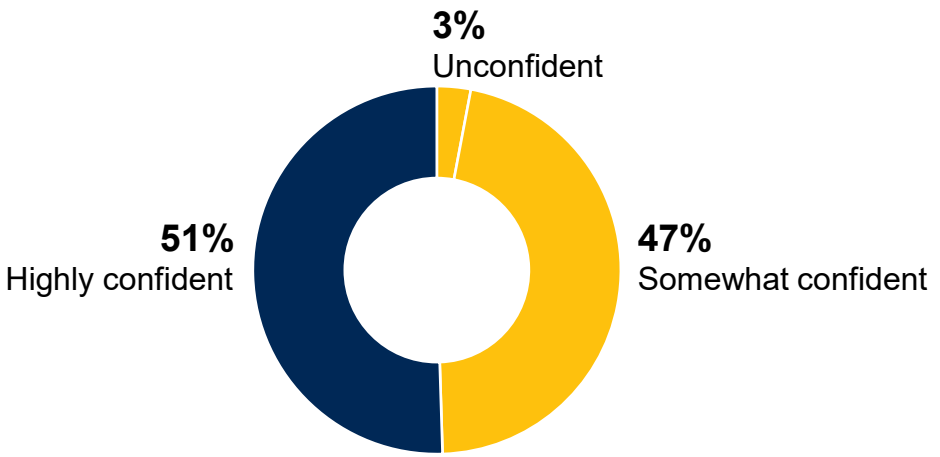
Percentage of respondents



n = 123
Source: Gartner Survey on 2026 Audit Plan Hot Spots

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

Percentage of respondents



n = 159
Source: Gartner Survey on 2026 Audit Plan Hot Spots
Note: Totals may not sum to 100% due to rounding.

Data Governance

Urgency Drivers

Governance Challenges Over AI-Generated Outputs

In 2024, the volume of data created, captured, copied and consumed worldwide reached 147 zettabytes — nearly three times as much as in 2020 — which was driven in large part by AI usage.[17] Moreover, AI is forecast to drive a 24% compound annual growth rate for data generation.[18] As a result, organizations face the daunting task of managing their AI-related data volume: 63% of organizations report that they generate text and 36% report generating images from GenAI models alone.[19] This growth in data volume compounds already low maturity in tracking data assets — 51% of data management leaders say metadata practices are based on manual inventories — and extends visibility challenges over extensive AI-related data.[20] Meeting recordings and transcripts generated by AI meeting assistants, a common feature on applications like Zoom Communications' Zoom, heighten governance concerns as transcripts may become discoverable records, and retention and deletion policies are often overlooked.[21] Lack of effective governance over AI-generated outputs, like meeting summaries, can expose the organization to potential leaks of company secrets and intellectual property, as well as legal liability.[22]

Data Sovereignty Restrictions

The growing body of data sovereignty and localization laws creates technical and logistical challenges for organizations: An OECD analysis of regulations found that over two-thirds combine both data storage and cross-border data flow restrictions.[23] To ensure compliance with a complex patchwork of rules, organizations must adapt processes and infrastructure, including costly duplications and redundancies, to appropriately handle both data at rest and data in motion.[24] While 90% of security and privacy professionals report that their data would be inherently safer if it could be stored within their country or region, 88% report that data localization adds a significant cost to operations.[25] But failure to comply with localization and transfer rules can also be costly, as organizations face significant fines and penalties. In the U.S., civil penalties for transfers of personal data can reach up to $377,700 per transaction, and in Europe, Ireland's Data Protection Commission fined TikTok $600 million for violating data transfer regulations.[26]

Key Risk Indicators

- Trends in amount of new data generated per quarter
- Number of applications with automated transcription and/or summarization features
- Percentage of AI projects having undergone privacy impact assessments
- Frequency of updates to data storage and deletion policies
- Percentage of data records retained longer than permitted under deletion policies
- Percentage of employees completing data classification and protection training
- Percentage of data records stored in compliance with applicable localization and sovereignty requirements
- Number of data localization and sovereignty rules applicable to the organization
- Year-over-year costs associated with complying with data localization and sovereignty requirements
- Number of data localization enforcement actions in the organization's industry or in jurisdictions where the organization operates

Data Governance and Quality

Recommendations for Audit

- **Assess monitoring and oversight for AI-generated outputs:** Review the organization's AI policies and data governance policies and determine whether policy language sufficiently addresses the risks associated with governing AI-generated outputs. Advise policy owners on potential amendments that may be needed to improve governance.
- **Review controls for retention and deletion of AI-generated outputs:** Assess the adequacy and effectiveness of controls governing data retention and deletion. Verify whether newly introduced AI-based applications or systems are integrated into the organization's retention and deletion governance. Assess whether appropriate roles and responsibilities are established for managing AI-generated records.
- **Assess data classification for AI-generated outputs:** Evaluate any frameworks used to manage and classify AI-generated outputs that include sensitive data. Assess the effectiveness of procedures and/or monitoring tools used to detect misclassification or inappropriate access.
- **Evaluate data localization and sovereignty compliance programs:** Review the processes in place to identify data localization and sovereignty rules that apply to the organization and monitor new developments. Evaluate the adequacy and effectiveness of compliance policies and procedures for data localization.
- **Assess monitoring of data flows:** Review how the organization tracks cross-border data flows, including systems for determining which legal and regulatory frameworks apply. Assess the adequacy and effectiveness of controls in place to maintain compliance with localization and sovereignty requirements.

Data Governance and Quality

Questions for Management

How is the organization managing the retention and deletion of AI-generated outputs?

How has the organization accounted for AI-generated outputs in AI governance and data governance policies?

What processes are in place to provide notice and opt-out opportunities for users interacting with AI-based applications?

How is the organization communicating policies governing AI-generated outputs to employees?

What controls are in place to validate the accuracy of data classification for AI-generated outputs?

How is the organization accounting for AI-generated outputs in records management processes?

What processes are in place to monitor new and evolving data localization and sovereignty regulations?

What controls are in place to validate that data assets are stored in compliance with relevant data localization regulations?

How is the organization monitoring cross-border data flows?

How do you train employees to recognize and report disinformation, deepfakes and vishing attacks?

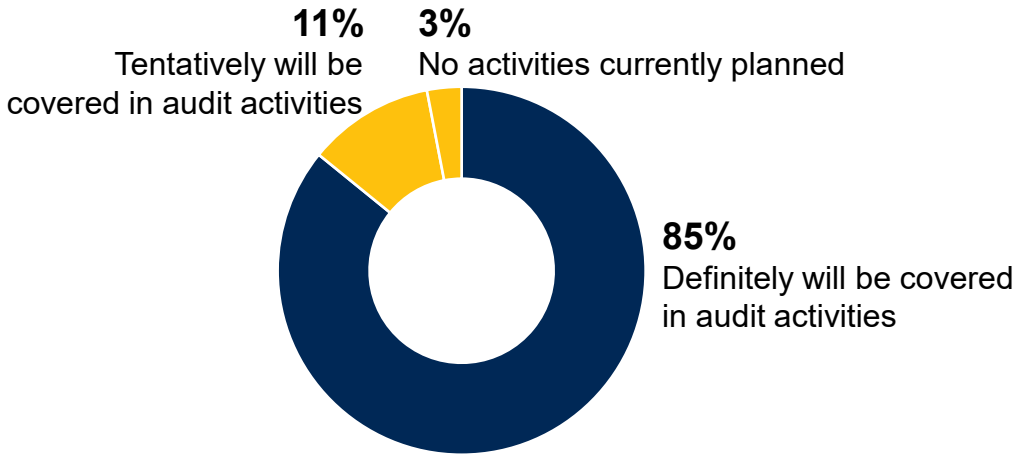
Gartner®

Regulatory Compliance

Amid a deregulatory push from the current U.S. administration, organizations must confront significant policy uncertainty, as well as increased pressures on ethical behaviors. In the first 100 days of the current U.S. administration, 142 executive orders were signed, creating challenges for organizations to keep up with the flood of rapidly shifting policy directives.[27] The changing regulatory environment creates uncertainty and complicates compliance strategy; meanwhile, organizations must also contend with internal and external pressures on ethical culture. Misconduct by employees, agents and third parties is more likely amid a weakening macroeconomic environment and organizational change, together with confusion stemming from shifting priorities and enforcement stances related to the U.S.'s Foreign Corrupt Practices Act (FCPA).[28] As enforcement expectations appear to shift, the resulting ambiguity increases the risk of unethical behavior. Organizations are navigating a clouded and uncertain information environment, forcing them to scramble to adapt and maintain an adequate compliance posture.

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

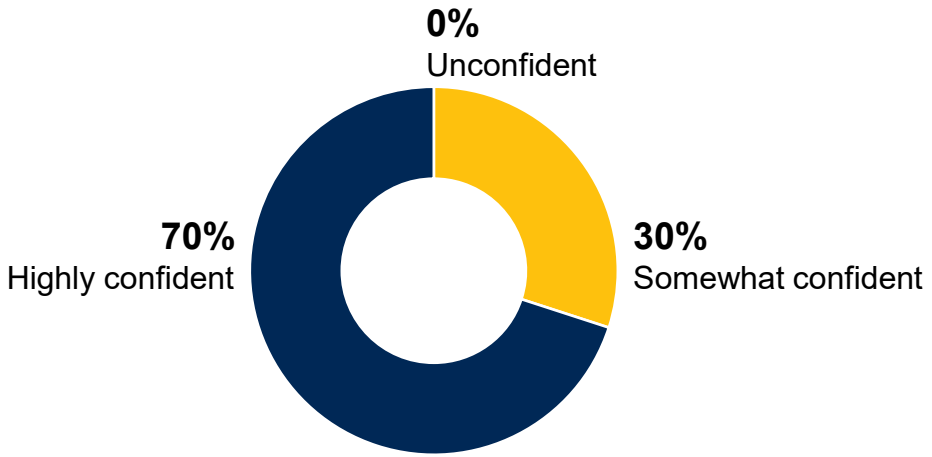
Percentage of respondents



n = 115
Source: Gartner Survey on 2026 Audit Plan Hot Spots
Note: Totals may not sum to 100% due to rounding.

Confidence in Audit's Ability to Provide Assurance Over Compliance Risk

Percentage of respondents



n = 160
Source: Gartner Survey on 2026 Audit Plan Hot Spots

Regulatory Compliance

Urgency Drivers

Regulatory and Policy Uncertainty

Eighty percent of legal leaders perceive heightened legal risk due to regulatory uncertainty.[29] While deregulation is a stated priority for the U.S. administration, rapid changes and reversals from previous administrations, as well as ongoing legal challenges concerning these policy shifts, have raised the difficulty of assessing policy impacts. Some shifts, such as in trade policy, have been short-lived or reversed, with similar patterns seen in federal funding and layoffs.[30] Moreover, from January to June 2025, there were 315 legal challenges contesting the administration's policies, further clouding organizations' planning horizons.[31] Uncertainty is driving heightened time investment for organizations to sort through information overload. For example, a March 2025 Gartner survey of general counsel found that 42% spent most of the previous month evaluating government policy effects.[32] U.S. volatility is also causing ripple effects in other jurisdictions; for example, the European Commission has proposed reducing some requirements of the Corporate Sustainability Reporting Directive and is considering potential modifications to the AI Act in an effort to remain globally competitive.[33] Organizations face increased costs related to adapting to this shifting environment, as well as an increased risk of noncompliance if they are too slow to respond.

Weakening Ethical Culture

A flagging global economy, high levels of organizational change and shifting regulatory enforcement priorities are heightening the risk of unethical behavior. Economic downturns can intensify all elements of the fraud triangle — motivation, opportunity and rationalization. In fact, 80% of certified fraud examiners believe fraud rises during times of economic distress.[34] Organizational instability compounds these risks. Gartner shows a link between leadership and organizational change and higher rates of employee misconduct; from 2024 to 2025, 71% of employees have experienced one or more senior leadership transitions, while 67% have experienced significant organizational restructuring.[35] Meanwhile, whiplashing U.S. Department of Justice enforcement and messaging on priorities for the FCPA — including a temporary pause, resumption and ongoing ambiguity — is likely to lead to confusion and a greater chance of misconduct.[36] Employees, agents and third parties may respond more to the "tone at the top" of U.S. administration messages than internal policy communications, or misinterpret expectations altogether. Organizations that do not effectively mitigate pressures on ethical behavior stemming from macroeconomic conditions, organizational change and mixed signals risk significant legal and financial penalties, as well as potential reputational damage.[37]

Key Risk Indicators

- Number of changing laws and regulatory requirements by risk category per quarter
- Frequency of scheduled reviews or updates to the employee code of conduct
- Number of whistleblower events within a reporting period
- Number of regulatory changes identified but not assessed within required timeframes
- Frequency of ethics and misconduct training throughout the organization
- Year-over-year trends in scores on employee-facing culture or ethics surveys
- Number of confirmed misconduct or ethics violations per reporting period
- Trend in the volume of hotline calls or reporting
- Percentage of employees completing ethics training
- Number of enforcement actions relating to bribery and corruption in the organization's industry or region

Regulatory Compliance

Recommendations for Audit

- **Review regulatory intelligence processes:** Evaluate the effectiveness and timeliness of management's processes for identifying, monitoring and responding to regulatory changes. Review procedures for communicating regulatory updates to the affected business units.
- **Evaluate policy impact assessment processes:** Review the frequency and quality of management's assessments of how emerging regulations and executive actions affect business operations and compliance. Evaluate how the assessments are translated into timely updates to organization policies, procedures and training programs.
- **Evaluate organizational ethics programs:** Validate the existence of appropriate ethics and conduct policies and the expectations for employees, contractors, third parties and agents, including the specification of roles and responsibilities to address incidents of misconduct. Assess the adequacy of training, communication and monitoring activities.
- **Review communications on employee code of conduct:** Assess the effectiveness and clarity of management's communications to employees and third parties regarding ethical expectations and the code of conduct, especially in light of recent shifts in U.S. Enforcement priorities. Identify opportunities to improve messaging and awareness in response to evolving policies and enforcement trends.
- **Audit whistleblower reporting mechanisms:** Assess the effectiveness of the organization's whistleblower program, including the accessibility, confidentiality and responsiveness of reporting channels. Evaluate management's process for investigating reports.

Regulatory Compliance

Questions for Management

How do you track and assess the impact of new executive orders and regulatory directives on the organization?

How has the organization accounted for recent changes in regulatory enforcement priorities in its compliance program strategy?

What processes support timely identification, evaluation and response to regulatory changes within all applicable jurisdictions?

How does the organization evaluate and address regulatory uncertainty?

How do you incorporate insights from recent enforcement actions or legal rulings into ongoing compliance risk assessment?

How is the organization monitoring and assessing financial transactions for potential fraud?

What factors and indicators do you look for to determine whether the risk of fraud or misconduct is elevated in a particular region or business unit?

What controls are in place to detect and prevent potential bribery, corruption or other unethical conduct?

How is information about ethical expectations and the code of conduct communicated across different levels of the organization?

How are whistleblower reports and other internal feedback used to identify and address gaps in compliance or ethical conduct?

Audit Plan Hot Spots: 5-Year Comparison

2022	2023	2024	2025	2026
Ransomware	Cyberthreats	Cybersecurity Vulnerabilities	Cybersecurity Vulnerabilities	Cybersecurity Vulnerabilities
Data and Analytics Governance	IT Governance	IT Governance	Data Governance and Quality	Data Governance
Digital Business Transformation	Data Governance	Regulatory Complexity	IT Governance	Regulatory Compliance
IT Governance	Third-Party Risk Management	Digital Transformation	Digital Transformation	IT Governance
Third Parties	Organizational Resilience	Organizational Resilience	Regulatory Compliance	AI Governance
Business Continuity and Organizational Resilience	Environmental, Social and Governance	Third Parties	Third Parties	Digital Transformation
Environmental, Social and Governance	Supply Chain	Supply Chain	AI Governance	Third Parties
Supply Chain	Macroeconomic Volatility	Employee Well-Being and Satisfaction	Environmental, Social and Governance	Organizational Resilience
Strategy Execution	Workforce Management	Environmental, Social and Governance	Workforce Management and Engagement	Supply Chain Distortions
Workforce Management	Cost Pressures	Social and Political Tensions	Supply Chain	Talent Management
Retention and Recruitment	Culture	Generative AI	Macroeconomic Conditions	Macroeconomic Uncertainty
Economic Uncertainty	Climate Degradation	Macroeconomic Uncertainty	Sustainable Growth Strategies	ESG Strategies

Endnotes

Cybersecurity Vulnerabilities

[1] 2024 State of Threat Detection and Response: The Defenders' Dilemma, Vectra AI.
[2] The Global Risks Report 2025: 20th Edition — Insight Report, World Economic Forum.
[3] 2025 Gartner Readiness for World Without Truth Survey.
[4] 2025 Data Breach Investigations Report, Verizon.
[5] 2024 CDW Cybersecurity Report, CDW (download required).
[6] Building a Firewall Against Cybersecurity Burnout, Hack The Box.
[7] 2024 State of Threat Detection and Response: The Defenders' Dilemma, Vectra AI.
[8] Ibid.
[9] Gartner (2024).
[10] 2025 Global Threat Report, CrowdStrike.
[11] 1 in 10 Executives Say Their Companies Have Already Faced Deepfake Threats, Business.com.
[12] Disinformation's New Role in Corporate Sabotage, ManageEngine Insights.

Data Governance

[13] AI Governance Profession Report, IAPP.
[14] 2025 State Of Enterprise Data Governance, Enterprise Data Strategy Board.
[15] Data Protection and Privacy Legislation Worldwide, UN Trade & Development.
[16] The Legal Uncertainty Facing EU-U.S. Data Transfers — Storm Over the Atlantic, Clifford Chance.
[17] Data Volume Is Soaring. Here's How the ICT Sector Can Sustainably Handle the Surge, World Economic Forum.
[18] The AI Data Cycle, Western Digital (PDF).
[19] The State of AI: How Organizations Are Rewiring to Capture Value, McKinsey & Company.
[20] 2024 Gartner Evolution of Data Management as a Dedicated Function Survey.
[21] Permission to Record: Considerations for AI Meeting Assistants, Faegre Drinker.
[22] AI Assistants Are Babbling Our Embarrassing Work Secrets, The Washington Post.
[23] Cross-Border Data Flows, OECD.
[24] Global Data Sovereignty: A Comparative Overview, Cloud Security Alliance.
[25] The Privacy Advantage: Building Trust in a Digital World — 25 Data Privacy Benchmark Survey, Cisco.
[26] DOJ Issues Final Rule Prohibiting and Restricting Transfers of Bulk Sensitive Personal Data, White & Case; TikTok Fined $600 Million for China Data Transfers That Broke EU Privacy Rules, AP.

Regulatory Compliance

[27] Trump Sets Executive Order Record in His First 100 Days, CBS News.
[28] Guidelines for Investigations and Enforcement of the Foreign Corrupt Practices Act (FCPA), U.S. Department of Justice.
[29] Mobilizing for Uncertainty: How In-House Legal Leaders Are Responding to 2025's Policy, Economic and Business Shockwaves, Axiom.
[30] Full Speed, Then Reverse: Trump's Biggest U-Turns in His First 100 Days, U.S. News & World Report.
[31] Litigation Tracker: Legal Challenges to Trump Administration Actions, Just Security.
[32] 2025 Gartner General Counsel Voice: Corporate Governance and Emerging Legal Risk Trends Webinar Poll.
[33] Commission Simplifies Rules on Sustainability and EU Investments, Delivering Over €6 Billion in Administrative Relief, European Commission; EU Commission Opens Door to 'Targeted Changes' to AI Act, POLITICO.
[34] Impact of Recession on Fraud: A Study of the Impact of an Economic Recession, Association of Certified Fraud Examiners.
[35] Gartner (2020); 2025 Gartner Organizational Culture Employee Survey.
[36] FCPA Enforcement Resumes: DOJ Outlines New Investigative Priorities, The National Law Review.
[37] Misconduct may be prosecuted in other jurisdictions even if U.S. enforcement of the FCPA is reduced. The U.K. Bribery Act, for example, can result in unlimited fines on commercial organizations.

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.

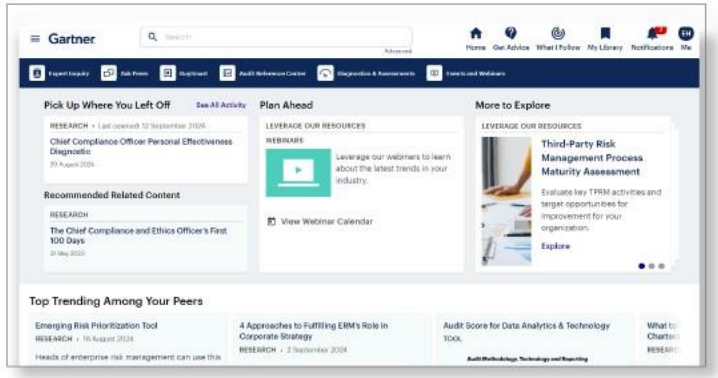
Workflow and Benchmark Tools

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.



Actionable, objective insights

Explore these additional complimentary resources and tools for customer service and support leaders:

Webinars

Join a Virtual Event

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

Watch Now

Template

Develop an Audit Strategic Plan You Can Use

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

Download Now

Research

Benchmarking Generative AI in Internal Audit

Benchmark the prevalence of GenAI in internal audit, the types of audit tools used and the most common use cases.

Download Now

How We Help

Gartner for Legal, Risk & Compliance Leaders

Discover how we can help you tackle your most critical priorities.

Learn More

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

Gartner®

Connect with us

Get actionable, objective business and technology insights that drive smarter decisions and stronger performance on your mission-critical priorities. Contact us to become a client:

U.S.: 1 855 322 5484

International: +44 (0) 3330 296 946

Become a Client

Learn more about Gartner for Legal, Risk & Compliance
gartner.com/en/audit-risk

Stay connected to the latest insights