2019 Audit Plan Hot Spots Report Excerpt

Five Risk Areas to Watch

Gartner®

Objective

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

Benchmark Audit Plan Coverage: Compare, validate and further examine audit plan coverage.

Audit Committee Education: Educate the audit committee on risk trends that impact global organizations.

Audit Team Discussions: Prepare for discussions with the audit team prior to audit engagement planning and scoping.

Risk Assessment: Determine which questions to ask management during risk assessment and audit scoping.

Audit Plan Hot Spots Summary

Audit Plan Risk Areas	Summary	2019 Drivers
Cybersecurity Preparedness	The number of cyberattacks continues to increase significantly as threat actors become more sophisticated and diversify their methods. Damage from these incidents can range from financial loss to loss of intellectual property, resulting in a heightened need to strengthen current cyber risk-mitigation strategies. **This is an evolution of last year's information security behaviors hot spot.**	1. Growing Attack Sophistication 2. Expanding Attack Surface
Data Governance	As organizational data volumes grow, the importance of effective mechanisms to collect, use, store and manage this data expands. Yet most organizations lack adequate governance frameworks, resulting in operational drag, misguided decision making and missed opportunities.	1. Magnification of Poor Data Quality 2. Democratization of Data Analysis
Third Parties	Challenges related to third parties have been a perennial concern for organizations, 66% of which have either experienced a third-party-related disruption in the last two years or lack sufficient visibility into third-party activities to identify a disruption. However, third-party risks are taking on new complexity, as organizations digitize systems and struggle to stay relevant in the digital marketplace, aggravating the effects of failing to manage the risk adequately.	1. Proliferation of Business Ecosystems 2. Nth-Party Risk
Data Privacy	The costs and risks of inadequately managing and protecting data are mounting as companies face more advanced security breaches and a proliferation of regulations like GDPR. However, most organizations still have significant room for improvement when it comes to data protection.	1. GDPR Enforcement Uncertainty 2. Consumer Awareness
Ethics and Integrity	Corporate culture and ethics have made headlines in recent years. These issues become more complex as organizations begin to focus on the social and digital aspects of integrity. Boards and senior management feel increasingly comfortable making public statements reflecting corporate ethics but need to make more progress at actually managing risk. Failure to improve on this front can expose organizations to legal and regulatory risk, reduced productivity and reputational damage. **This is an evolution of last year's culture hot spot.**	1. Gender and Racial Bias in the Workplace 2. Inattention to Digital Ethics

Audit Plan Risk Areas

Gartner®

Cybersecurity Preparedness

Cyber incidents nearly doubled from 2016 to 2017 and most CEOs now believe cyberattacks are inevitable.[2] As attacks become more advanced and threat actors diversify, the cost and frequency of cyber incidents rise significantly. Cybercrime damages are predicted to top $6 trillion by 2021, with business email compromise alone expected to cause global damages exceeding $12.5 billion.[3] By next year, an organization is set to fall victim to a ransomware attack every 14 seconds, with damages totaling 15 times those of two years ago.[4] Damages, however, are not limited to financial loss; loss of intellectual property, reputational damage, as well as compliance issues are also included. As a result, more boards require reporting on cybersecurity and cybersecurity spending increased 22.7% in 2017.[5] Yet less than half of IT professionals believe they can protect their organizations from cyber threats and only 41% of CEOs consider their organization well prepared to address or defend against a cyberattack.[6] As 93% of breaches in 2017 could have been prevented with basic cyber hygiene practices, businesses must strengthen cyber risk-mitigation strategies to keep up with the growing array of cyber threats.[7]

1. Growing Attack Sophistication

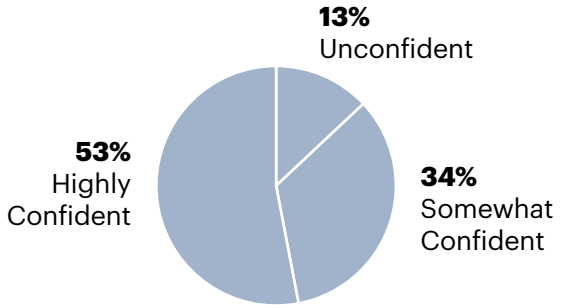
As ransomware and malware attacks continue to rise, organizations are now also contending with new attacks such as cryptojacking, botnets and fileless malware.[8] 2017 saw the advent of network-based ransomware cryptoworms — which remove the human element previously needed for successful attacks — as well as increased use of encryption to conceal command and control activity.[9] Advances in technologies such as artificial intelligence (AI) are proving to be double-edged swords. While cybersecurity professionals leverage AI to better anticipate and identify attacks, cybercriminals are leveraging AI to craft more convincing fake messages for phishing campaigns and can also use it to improve their effectiveness over time. Such technology enables attacks to better mimic human behavior, thereby evading security controls and increasing the likelihood attacks will blend into the IT infrastructure, allowing access and control over sensitive assets. Adoption of new technologies by bad actors makes it harder for security professionals to model attack behaviors and put necessary security measures in place.

2. Expanding Attack Surface

As companies digitalize and further embrace advanced technologies, they are also opening new endpoints and weak links. The use of chatbots and mobile messaging increase the opportunities for threat actors to impersonate legitimate users and take over accounts.[10] One hundred eleven billion lines of new software code are produced each year and by 2020, there will be 20.4 billion connected devices, up from 6.4 billion in 2016.[11] Expanded use of networked devices, like those in the Internet of Things (IoT), increase the access points for botnets, as many devices are unmonitored and difficult to patch. Further, supply chains and vendors are increasingly becoming avenues of exploitation. Fifty-six percent of organizations have experienced a breach caused by a vendor.[12] This is becoming more worrisome, as the average number of third parties with access to sensitive information continues to rise. Now regulators are also holding companies accountable for the actions of their third-party partners.[13] As companies continue to leverage new technologies, they need to ensure they are not outpacing their ability to adequately secure them.

Confidence in Audit's Ability to Provide Assurance Over Cybersecurity Detection and Prevention Risks

Percentage of Respondents

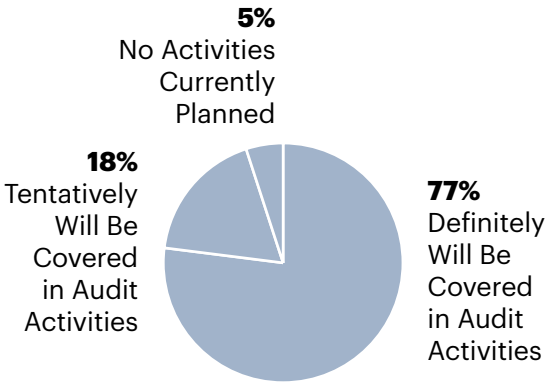


n = 143

Source: Gartner 2019 Audit Key Risks and Priorities Survey

Plans to Cover Cybersecurity Detection and Prevention in Audit Activities in the Next 12-18 Months

Percentage of Respondents



n = 144

Source: Gartner 2019 Audit Key Risks and Priorities Survey

Cybersecurity Preparedness

2019 Recommendations for Audit

- **Review Device Encryption:** Review the extent of encryption on all devices, including mobile phones and laptops. Assess the strength of required passwords and the use of multifactor identification. Evaluate requirements for how often passwords must be changed.
- **Review Access Management Policies and Controls:** Review the policies and procedures for granting systems access and user privileges. Ensure access rights are granted based on defined business needs and job requirements, access rights are terminated in a timely manner as employees leave the organization or change roles and administrator privileges are minimized.
- **Review Patch Management Policies:** Review the process through which the organization is notified of a patch and its installment throughout the system. Evaluate the average time from patch release to implementation and how frequently patches and updates are made. Make sure these patches cover IoT devices.
- **Evaluate Employee Security Training:** Assess the effectiveness of information security awareness and training programs. Review the number of employees that have taken the training, how often training is required and the levels of employees required to complete it. Make sure the training includes education and awareness of common security threats such as phishing.
- **Participate in Working Groups and Committees:** Audit should participate in relevant cyber working groups and committees to provide input on the development of cybersecurity strategy and policies. Audit should contribute to how the organization identifies, assesses and mitigates cyber risk to an acceptable level, as well as how to strengthen current cybersecurity controls.

Key Risk Indicators

- Average or median attack dwell time
- Number of hacking attempts
- Number of public (that is, internet-facing) entry and exit points within the organization's network
- Number of online channels available to third parties, external customers, etc.
- Percentage of crown jewel assets which have been fully hardened
- Percentage of employees who completed cybersecurity awareness trainings
- Percentage of internet-enabled payment services for customer transactions
- Average or median attack response time
- Financial loss per security incident
- Total response cost (for example, legal fees, employee hours, payments for outsourced assistance) per security incident

Questions for Management

- Do you require employees to take security awareness training?
- Do you have an inventory of all devices that can access company networks and systems?
- Do you have a list of third parties with access to sensitive or proprietary information?
- Do you have a reporting process to notify the relevant stakeholders in case of a cyber breach?
- Have you implemented a cyber incident response plan?
- Have you identified potential cyber-related skills gaps?
- How often do you back up critical data? Are your backups encrypted?
- Do you conduct social engineering campaigns to see how many employees click on the emails?
- Have you provided training to employees on methods to identify potential phishing emails?
- Do you ensure that every device has appropriate antivirus protection installed?

Additional Online Gartner Resources

- Structuring IT Audit Engagements and Key Coverage Areas
- Structuring IT Audit Teams and Working with the Business
- Avoid Ransomware - GDPR Cyber-Extortion
- Information Security Controls Mapping Tool
- Five Design Principles for a Better Cybersecurity Program

Data Governance

Big data increases the strategic importance of having effective mechanisms to collect, use, store and manage organizational data.[14] Today, data-driven strategies are a necessity for organizations to increase their efficiency and competitiveness. Ninety-five percent of executives believe data is an integral part of forming business strategy.[15] With these opportunities come raised stakes in terms of data protection and accountability; new data privacy regulations and high-profile breaches are expanding the compliance, financial and reputational risks of data usage and protection. However, only 37% of organizations have a formal data governance framework in place and organizations struggle to establish consistency across the organization and scale their programs to meet the growing volume of data.[16] Left unsolved, these governance challenges can lead to operational drag, delayed decision making and unnecessary duplication of efforts.

1. Magnification of Poor Data Quality

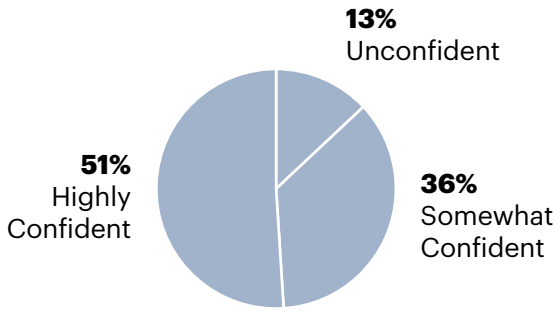
As organizations more broadly leverage data, perennial data concerns such as quality are multiplied, risking missed opportunities, wasted resources and misguided decision making.[17] Even as knowledge workers and data scientists now spend up to 50% of their time on mundane data-quality issues, they have limited confidence in organizational data.[18] An estimated 97% of business decisions are based on data of unacceptable quality and 74% of organizations struggle to use existing data to generate meaningful insight.[19] Thirty-eight percent of organizations undertaking a data migration project view data quality as a top challenge.[20] These challenges are likely to compound as organizations digitalize and automate more processes. However, an estimated 80% of data errors can be eliminated with adequate governance.[21] Poor data-quality standards and processes not only reduce productivity, but also prevent organizations from capitalizing on the opportunities of big data.

2. Democratization of Data Analysis

Analytics projects are starting everywhere throughout organizations. The need for speed and agility is expanding the use of self-service analytics as business units seek to bypass the potential delays caused by reliance on central functions. As a result, the analytics output of business users with self-service tools will soon surpass that of data scientists. However, 43% of organizations report a lack of analytical skills is a challenge.[22] Inexperienced users manipulating data outside of established platforms access both internal systems and external data repositories, creating data redundancies, data integrity issues and security concerns. Inappropriate access controls can also allow self-service users to access sensitive or highly valuable information, increasing the risks of data leakage and breaches. These issues increase the risk of regulatory fines, reputational damage and the loss of proprietary information. Further, data silos may arise when business units create their own metrics and models, sparking questions of data ownership and sharing. Forty-four percent of organizations report being only partially effective at data integration and sharing, with 37% of data inaccuracies being attributed to a lack of communication between departments.[23]

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

Percentage of Respondents

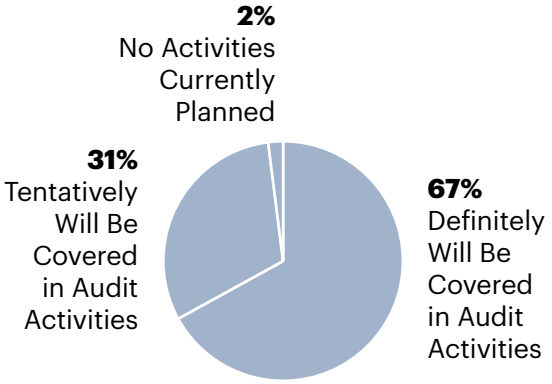


n = 143

Source: Gartner 2019 Audit Key Risks and Priorities Survey

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

Percentage of Respondents



n = 144

Source: Gartner 2019 Audit Key Risks and Priorities Survey

Third Parties

Efforts to digitize systems and work adds new, complex dimensions to the third-party challenges that have been a perennial concern for organizations.[24] Nearly 70% of CAEs reported third-party risk as one of their top concerns in 2017.[25] However, many organizations struggle to manage the risk; roughly 66% have either experienced a third-party-related disruption in the last two years or lack sufficient visibility into third-party activities to identify a disruption.[26] Fines, lost revenues and brand damage have resulted.[27]

1. Proliferation of Business Ecosystems

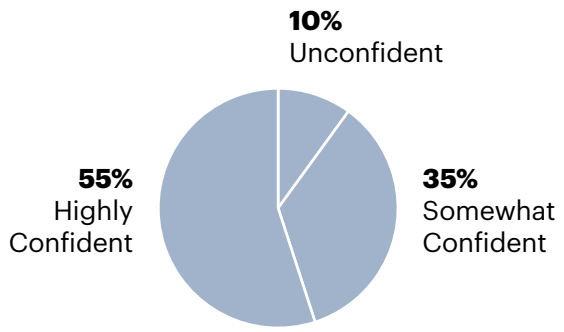
Ecosystems — where businesses sell interconnected and interdependent suites of products, often relying on close third-party relationships — have emerged as a new business model that organizations across industries are using to stay competitive.[28] Seventy-six percent of executives who think that current business models will be unrecognizable in five years identify ecosystem strategies as the main driver of that shift.[29] Firms across industries and geographies — including Microsoft, GE, Ford and major insurance companies and smaller start-ups such as Lyft and Internet of Things (IoT) device companies — are using ecosystem strategies to confirm their economic positions.[30] These strategies, however, come with new challenges, as Google and GE recently learned when they each faced reputational damage related to ecosystem strategies.[31] Despite the promise of ecosystems, their interconnected, diverse nature also increases the complexity of the risk environment.[32] Half of organizations share data with strategic partners to advance their ecosystem strategies and one-third express concerns about cybersecurity and data sharing in this context.[33] Ecosystem relationships present higher stakes than traditional supply relationships, since the failures of ecosystem partners cannot be addressed simply by switching suppliers.[34]

2. Nth-Party Risk

As organizations increasingly rely on external partners — whether ecosystem partners or vendors — to do business, they also rely on their partners' partners (fourth, fifth and nth parties), amplifying operational and regulatory risk exposure.[35] While problems related to vendors deeper in the supply chain rarely make headlines, examples are starting to come to light.[36] Public and government scrutiny resulted from the exposure of location data of hundreds of millions of wireless customers sold to another company by LocationSmart, a firm contracted by the four major U.S. carriers.[37] However, 78% of organizations either lack sufficient knowledge of fourth and nth parties or don't know if they have enough visibility into the operations of these groups.[38] Only 2% of organizations say they regularly identify and monitor fourth and nth parties.[39] Further compounding organizations' need to tackle this issue, regulators in the EU, U.K., U.S. and Hong Kong have instituted requirements for organizations to monitor fourth- and fifth-party vendors.[40]

Confidence in Audit's Ability to Provide Assurance Over Third-Party Risk

Percentage of Respondents

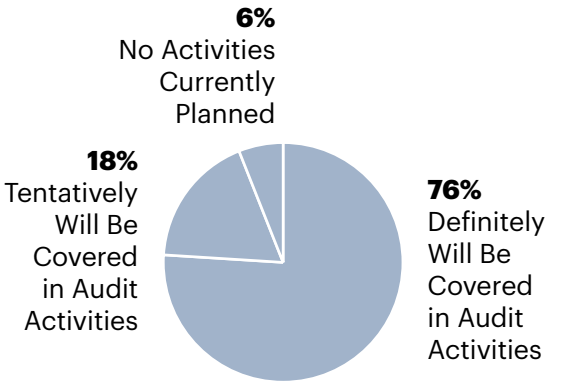


n = 143

Source: Gartner 2019 Audit Key Risks and Priorities Survey

Plans to Cover Third-Party Risk in Audit Activities in the Next 12-18 Months

Percentage of Respondents



n = 144

Source: Gartner 2019 Audit Key Risks and Priorities Survey

Data Privacy

Given the strategic benefits of holding and analyzing customer data, companies are collecting an unprecedented amount of personal information. At the same time, the costs of managing and protecting this data are mounting, as companies face more advanced security breaches and a proliferation of regulations.[41] In 2017, an estimated 1,579 data breaches — a 44.7% increase over 2016 — exposed sensitive information, including millions of names, Social Security numbers and credit card numbers.[42] Recent high-profile breaches, increased public scrutiny over organizations' data protection practices and implementation in the EU of the General Data Protection Regulation (GDPR) in May 2018 have raised the stakes for organizational accountability.[43] In response, 81% of global CEOs report efforts to improve transparency in data usage and storage, but less than half are doing this "to a large extent," signaling there is still significant room for improvement.[44] With the growing array of cyber threats and the increasing importance of consumer trust to competitiveness in the digital economy, data privacy is a critical consideration in 2019.

1. GDPR Enforcement Uncertainty

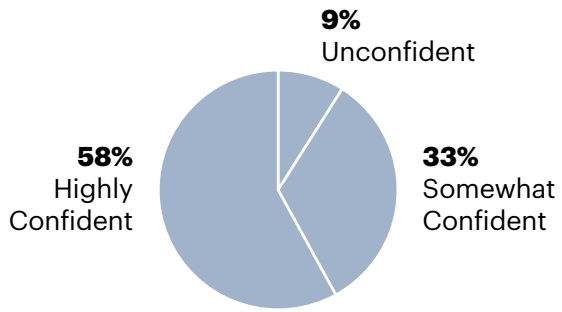
Companies must now shift from GDPR readiness to compliance and expedite the implementation of the regulation's mandates, such as transparency, consent and breach reporting.[45] But only 20% of companies are reportedly compliant and many have not started implementation.[46] As organizations actively work toward GDPR compliance and determine exactly what that entails, there is a high level of uncertainty over how strictly regulators will enforce the regulation and which parts regulators will focus on — for example, data protection officers or data protection impact analysis.[47] A recent survey of 17 EU regulators shows large variation in enforcement criteria, with 60% reporting they will regularly assess "high-risk companies"; fewer say they will inspect a random set of companies.[48] Further uncertainty was sparked by the wave of billion-dollar consumer lawsuits that began surfacing the day of GDPR enactment.[49] Even if many organizations doubt that fines of 4% of global revenues would actually be implemented, a wait-and-see approach is risky, since noncompliance carries reputational risk and GDPR is likely to create a ripple effect of legislation in other jurisdictions.[50]

2. Consumer Awareness

Seventy-three percent of consumers in the EU doubt that websites can keep personal information secure and only 25% of consumers in the U.S. believe that companies handle sensitive data responsibly.[51] Recent high-profile incidents — such as the decline in both consumer trust and market capitalization for Facebook — show the negative impact of potential data privacy failures.[52] Facebook is not alone; data breaches and tracking scandals have marred the reputations and revenues of other large corporations, such as Equifax and Uber.[53] After large breaches like these, customers become more inclined to take their business elsewhere. Consumers' lack of trust and confidence in organizations' ability to safeguard their information also generates broad support for regulatory action on data privacy.[54] Regulators have responded with sweeping legislation, which in addition to GDPR also includes laws in the Philippines and Japan and most recently, California's Consumer Privacy Act of 2018.[55] As a result, organizations not only have to contend with waning consumer trust, but also increased compliance and legal risks.

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

Percentage of Respondents

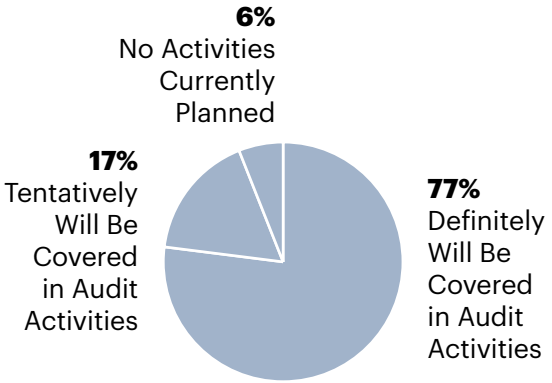


n = 144

Source: Gartner 2019 Audit Key Risks and Priorities Survey

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

Percentage of Respondents



n = 144

Source: Gartner 2019 Audit Key Risks and Priorities Survey

Ethics and Integrity

Corporate culture and ethics have made headlines in recent years, as revelations of fraudulent behavior and attempts to deceive authorities have come to light.[56] Society increasingly expects corporations to demonstrate sound ethical conduct, which has also been shown to lead to better operational performance.[57] Seventy-seven percent of Americans think that CEOs should speak out when their company values are threatened and 89% of employees consider trust an important factor in job satisfaction.[58] Recognizing this, companies have recently taken clear stances on misconduct rather than staying silent, in apparent efforts to head off the controversy that might result from inaction.[59] However, while boards and senior management may feel more comfortable making public statements reflecting corporate ethics, they still have gains to make in actual risk management.[60] Only 26% of organizations recognize culture — which can inform an organization's ethical decision making — as a key risk.[61] Failing to manage these factors can expose organizations to legal and regulatory risk, reduced productivity and reputational damage.[62]

1. Gender and Racial Bias in the Workplace

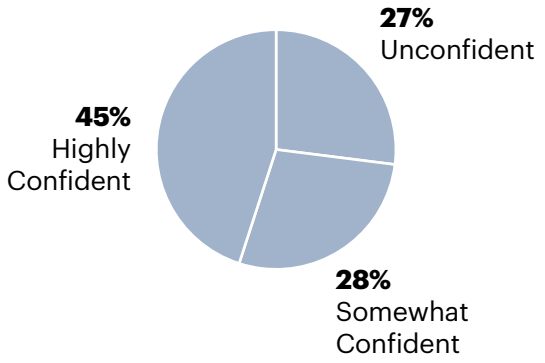
Organizations and their leaders are facing repercussions for failing to adhere to gender- and race-related norms, as awareness of destructive gender dynamics in professional environments has skyrocketed and businesses have been taken to task for racial bias. Globally, large percentages of women — from 20 to 30% in Asia and up to 50% in the EU — report experiencing sexual harassment at work.[63] More than 400 leaders across sectors and geographies have been accused of sexual misconduct in the last 18 months, illustrating the #MeToo movement's global relevance, and numerous executives have been fired for making racist comments.[64] Subtler discrimination, including gender- and race-based disparities in employment, pay and promotion, is also pervasive.[65] These challenges come at a price, in the form of legal costs, diminished brand value and lost revenue, productivity and talent.[66]

2. Inattention to Digital Ethics

Organizations are racing to integrate new technologies into business processes, letting consideration of potential negative impacts take a back seat to rapid development.[67] As valuable analytical capabilities improve, organizations will need to determine whether they should leverage all of these capabilities, given their potentially questionable ethical impacts.[68] Fifty-nine percent of CIOs report facing ethical challenges related to digitalization.[69] The complexity and opacity of algorithmic decisions and algorithms' propensity to "learn" bias from biased data sets create a particular challenge.[70] The effect of biases is expected to increase dramatically, as fields such as medicine and law expand their use of data analytics and artificial intelligence (AI).[71] Inadequately managing ethical implications of digital advances can drive away customers: 87% percent of consumers say they would stop doing business with a company if they didn't trust its use of their personal data.[72] Following GDPR's "right of explanation," which requires organizations to explain automated decisions, and a 2015 U.S. Supreme Court ruling that has paved the way for disparate-impact claims related to unintentional discrimination, inadequate management can also result in legal or regulatory exposure.[73]

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

Percentage of Respondents

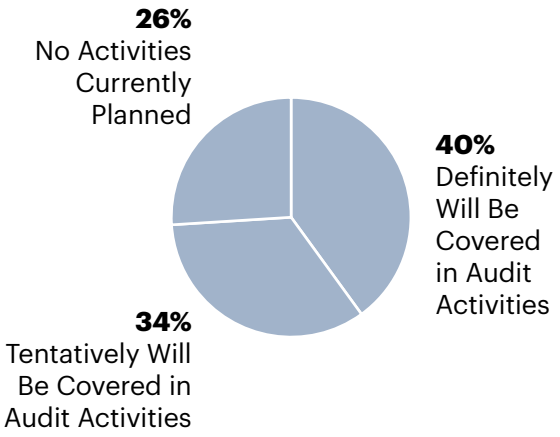


n = 143

Source: Gartner 2019 Audit Key Risks and Priorities Survey

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

Percentage of Respondents



n = 144

Source: Gartner 2019 Audit Key Risks and Priorities Survey

Contact Us to Learn More


+1-866-913-8103


gartner.com/go/audit


audit.support@gartner

Gartner®