2023 Audit Plan Hot Spots

Audit Research Team

Sample Report Excerpt

Gartner®

Table of Contents

Objectives

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.

Educate the Audit Committee

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

Drive Audit Team Discussions

Enable audit teams' discussions during audit engagement planning and scoping.

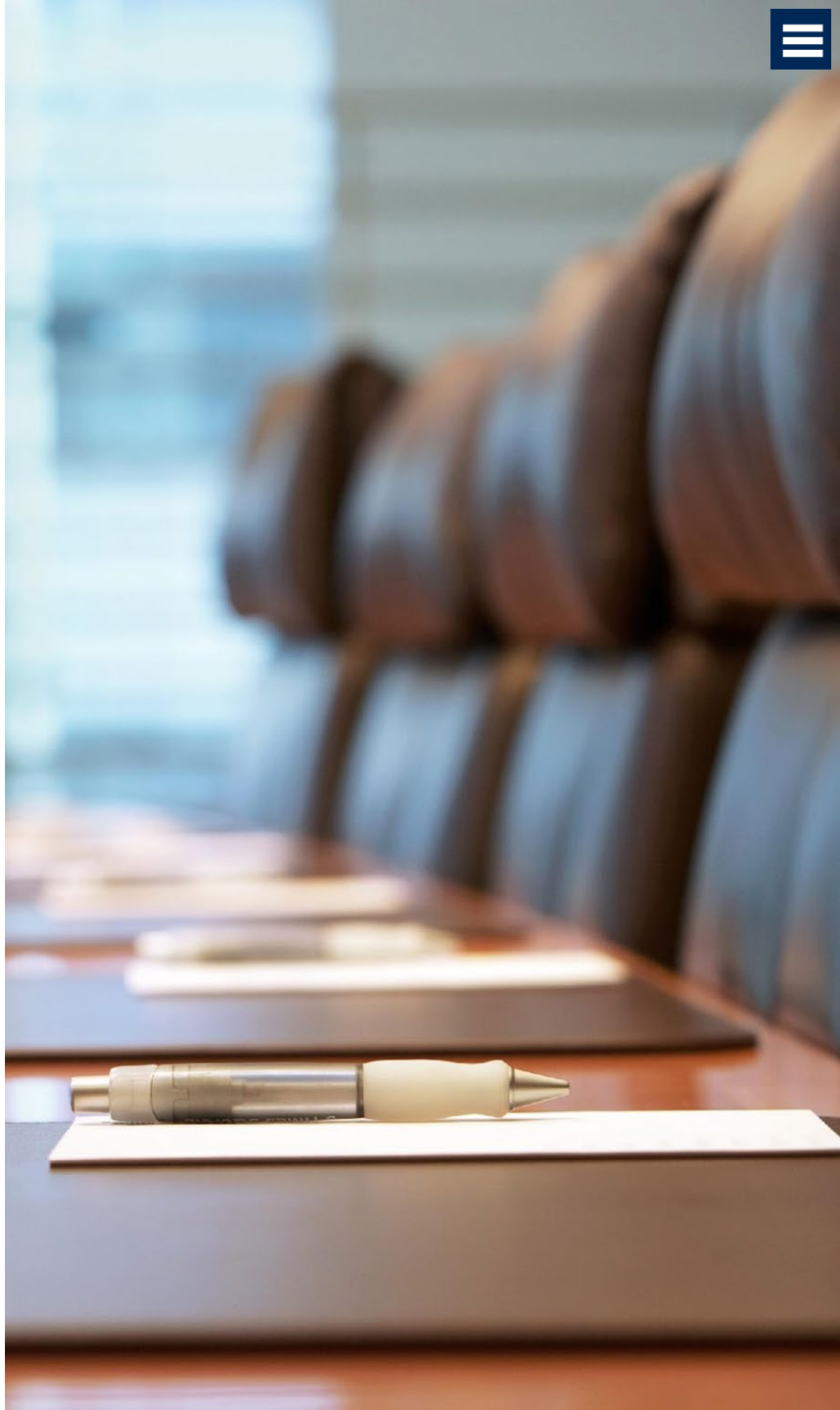
Assess Key Risks

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

Executive Summary

Each year, we create our annual Audit Plan Hot Spots report by combining input from interviews and surveys throughout our global network of client organizations as well as extensive secondary literature reviews. This report highlights current risks and trends in the business environment. It helps audit teams more effectively identify risks to the organization and highlight key risks for stakeholders. This year, three themes underlie the 12 hot spots:

1. The “Triple Squeeze”
2. Renationalization
3. Rethinking Resilience



Executive Summary

The "Triple Squeeze"

Opinions and forecasts are highly divided, but within the next 12 months, a recession is more likely to occur than not. If a recession does happen, then it may be quite different from previous ones. It will include three compounding pressures that most executives have likely never experienced concurrently: persistent high inflation, scarce and expensive talent, and global supply constraints. The potential recession is also positioned to be a highly uneven one, with some regions, industries and companies likely performing stronger than ever while others struggle. These unusual characteristics might manifest in the following risks:

- Going forward, the main squeeze organizations will encounter is the overall upward **cost pressure**. Eighty-two percent of CEOs globally say they are facing upward price pressure for inputs, and more than half expect this to persist at least into mid-2023. Unusually and problematically, the upward pressure is on product inputs, talent costs as well as borrowing costs. In addition, tax codes are changing, looking likely to significantly increase the tax burden.
- The most apparent squeeze during the past 12 months has been in **supply chains**. Driven by pent-up COVID-19 pressure, pandemic-induced lockdowns and misjudged forecasts, further exacerbated by the Russian invasion of Ukraine and energy costs, the delivery of products ranging from semiconductors to construction materials have been curtailed. In response, organizations are questioning their assumptions and looking to make their supply chains more resilient and more geopolitically stable.
- The final factor we observed over the past year, and are likely to see going into 2023, is that of labor scarcity. Due to the "great resignation," we have seen in the U.S. and other large markets an underlying trend of skills shortages in technology areas, as organizations struggle to fill jobs and forecast labor supply. This issue manifests in overall **workforce management** risk, where organizations must weigh competing signals in forecasting talent needs. It also manifests specifically within IT. IT staff's low intent to stay in the organization and the heightened difficulty of recruiting IT talent are a threat to maintaining sufficient **IT governance**.

Renationalization

In the past few years, the long trend toward globalized trade that accelerated when China and India joined global markets has reversed due to increased political populism and tension between global players. The supply chain issues caused by the COVID-19 pandemic further increased the need to onshore and "nearshore." The Russian invasion of Ukraine amplified this issue, dividing the world and leading to the need to also "friendshore." Renationalization and the uprooting of long-held assumptions of being able to rely on a global, just-in-time market will have a long-lasting impact and will increase multipolarization and geopolitical assertiveness. This shift may lead to increased regionalization of trade markets and business conducted between organizations of friendlier states. In addition to the pure supply chain risk, we also see the impact in the following risk areas:

- First, renationalization is playing out in the arena of **cyberthreats**. Ninety-two percent of organizations have either recently faced or expect to face a state-sponsored cyberattack, as most state-sponsored attacks target enterprises. This is often for monetary gain, such as North Korean crypto-related attacks, but given the onset of new Russia-NATO and China-U.S. tensions, there is an increased threat of cyberattacks for retaliatory purposes. This heightened threat is also causing regulators to pay increased attention, driving new disclosure rules in the U.S. and the U.K.
- In terms of **ESG (Environment, Social, Governance)**, the world is becoming divided as regulations and scrutiny increase. Western countries, and many Asian countries, are divided on the importance of ESG and the need to regulate it. Further, among Western countries, we have observed increasing divergence on how to standardize reporting requirements and regulations amid debates over where the focus should be. The EU, for example, recently decided to put the S components on hold.
- We also see renationalization being a big issue for the use of data and **data governance**. With the use of artificial intelligence (AI) set to expand and the centrality of data to business models increasing generally, more and more countries are instituting more stringent data requirements (e.g., data localization). Vastly different points of view are emerging on what AI and data risks, like those involving personal data, should be regulated.

Executive Summary

Rethinking Resilience

The third and final theme underlying this year's hot spots is the need for organizations to rethink what resilience means for them, in the sense of increased fragility. Since the onset of the COVID-19 pandemic and its consumer spending and supply chain effects, and then continuing through the Russian invasion of Ukraine and its macroeconomic and geopolitical effects, organizations are increasingly realizing their fragility and the need to implement new types of resilience measures and increase their long-term thinking. Organizations find it increasingly clear that the pace of disruption and the frequency of disruptive events will not slow down, and that we are entering a new "never normal" era. This sense of fragility and the need to focus on resilience is apparent in the following risk areas:

- Environmental sustainability, for the first time, has entered the top 10 of CEO priorities. Increased **climate degradation** requires organizations to go beyond identifying assets that may become an operational risk or formulating a sustainability strategy. Organizations need to prepare for increasingly frequent and extreme weather events and the potential loss of critical infrastructure.
- The external environment of **macroeconomic volatility** is not helping. With interest rates rising rapidly in most main markets, and a reverse currency war starting, organizations need to vastly increase the range of scenarios they plan for to effectively deal with a potential recession, volatile currencies and changes in global demand.
- Another source of fragility that is difficult to discern and mitigate is **third-party risk management**. Organizations' reliance on ecosystems of third and nth parties, which has become the norm in hyperoptimized supply chains and business operations, has not been tested against the current level of volatility. Due to geopolitical tensions and a more financially challenging environment, a potential recession can cause havoc if organizations are overly reliant on small third parties.

Rethinking Resilience

- **Culture** has been a very important source of resilience for many organizations for a long time. That resilience is now under threat, as organizational culture weakens from hybrid and remote work, leading to employee disconnectedness. This challenge is further aggravated by political and social divides that increasingly enter the organizational domain and dominate other cultural norms.
- Finally, what it all comes down to is the need for **organizational resilience**. Defined broadly, this means the ability of the organization to withstand shocks, both to operations and to business models, and persist in the long term in the face of unexpected disruptions. Fast-moving events, like geopolitical reprisals, may provide little warning before manifesting in several, interrelated risks, while the increased pace of change in the last two years strains organizations' ability to respond to them.

Executive Summary

Hot Spot	Summary	2023 Drivers	2022 Drivers
Cyberthreats	Heightened scrutiny on cyber breach disclosures alongside sophisticated state-sponsored attacks makes cyberthreats a growing risk in 2023, increasing organizations' exposure to reputational, litigation and regulatory risk.	1. State-Sponsored Cyberattacks 2. Cyber Breach Disclosure Requirements	1. Lapses in Security Controls 2. Increased Employee Vulnerability to Social Engineering
IT Governance	Higher use of ungoverned SaaS increases organizations' risk exposure, and an ongoing IT talent deficit further hinders enterprise agility and digital capability development. This issue leaves organizations exposed to enterprise growth and governance risks.	1. Ungoverned SaaS 2. IT Talent Shortage	1. Rapid Adoption of New Technologies 2. Access Management Challenges
Data Governance	Organizations increasingly employ AI with little formal oversight and the fragmented regulatory landscape highlights the need for organizations to improve governance over how they use and protect data assets.	1. AI Governance 2. Personal-Data-Related Regulatory Fragmentation	1. Ineffective Data and Analytics Organizational Models 2. Insufficient Data-Sharing Enablement and Controls
Third-Party Risk Management	A combination of new third-party ESG reporting requirements and increasing financial and operational constraints elevate the risk of reputational damage from third parties. Further, the current macroeconomic conditions that raise concerns about third parties' financial viability may result in operational disruptions, high costs of switching vendors, and product quality and reliability issues for the organization.	1. Third-Party Reputational Risk 2. Third-Party Viability	1. Limited Third-Party Risk Monitoring 2. Unsupervised Privileged Access

Executive Summary

Hot Spot	Summary	2023 Drivers	2022 Drivers
Organizational Resilience	Organizations' ability to withstand crises and disruptions is evermore critical, as they are increasingly being tested. Each crisis reveals more areas of organizational fragility.	1. Geopolitical Conflict 2. Diminished Change Capacity	1. Climate Degradation 2. Regulatory Interest in Operational Resilience
Environmental, Social and Governance (ESG)	Expanding and new ESG regulations and increased stakeholder scrutiny mean organizations must build meaningful ESG policies into their strategies to follow all current regulations and avoid accusations of greenwashing.	1. Expanded ESG Reporting Standards 2. Increased Scrutiny of ESG Practices	1. Increasing Capital Tied to ESG Performance 2. Increased Legal and Regulatory Action on ESG
Supply Chain	Increasing geopolitical conflict, resulting in localization measures and logistical challenges across supply chains, has contributed to rising prices and diminishing ability to access critical materials. Organizations face the risk of declines in revenues, profitability, operational effectiveness and the ability to compete.	1. Renationalization of Supply Chains 2. Logistics Challenges Stemming From China's "Zero-COVID" Policy	1. Key Goods and Materials Shortages 2. Logistics and Shipping Challenges
Macroeconomic Volatility	A global economic downturn and a sharp rise in interest rates across the world increase risks to organizational assets and cash flows, threatening long-term financial performance and exacerbating an already highly uncertain operating and risk environment.	1. Rising Interest Rates 2. Currency Volatility	1. Heightened Inflation Uncertainty 2. Variances in the Global Economic Recovery

Executive Summary

Hot Spot	Summary	2023 Drivers	2022 Drivers
Workforce Management	A combination of competitive labor markets with an expected cooling of economic growth fosters further uncertainty for organizations with regards to workforce management. With organizations undecided on their talent needs (in the case of a recession and the future of remote or hybrid work not yet fully determined), those who commit too quickly or too far face talent and business losses that are not easily reversible.	1. Uncertain Talent Needs 2. Uncertain Long-Term Effects of Hybrid Working Models	1. Cultural Disconnects in a Hybrid Workforce 2. COVID-19 Workplace Management Uncertainty
Cost Pressures	Organizations are struggling with persistent cost pressures driven by an unyielding inflationary environment and an increase in regulatory complexity that has heightened the pressure on organizations to reduce costs and revisit their growth strategies.	1. Persistent Inflation 2. Changes to Tax Regimes	Not a 2022 hot spot
Culture	Organizations are increasingly expected to weigh in on social and political issues as societal divisions spill over into the workplace and create potential rifts in organizational culture. At the same time, employees are experiencing high levels of disconnectedness from their organizations and co-workers, increasing exposure to risks from attrition to misconduct.	1. Employee Disconnectedness 2. Increasing Social and Political Expectations	Not a 2022 hot spot
Climate Degradation	As the long-term impacts of climate change begin to take hold, an increased recurrence of extreme weather events threaten business continuity and vulnerable critical infrastructure.	1. Increased Recurrence and Effects of Extreme Weather Events 2. Vulnerable Critical Infrastructure	Not a 2022 hot spot

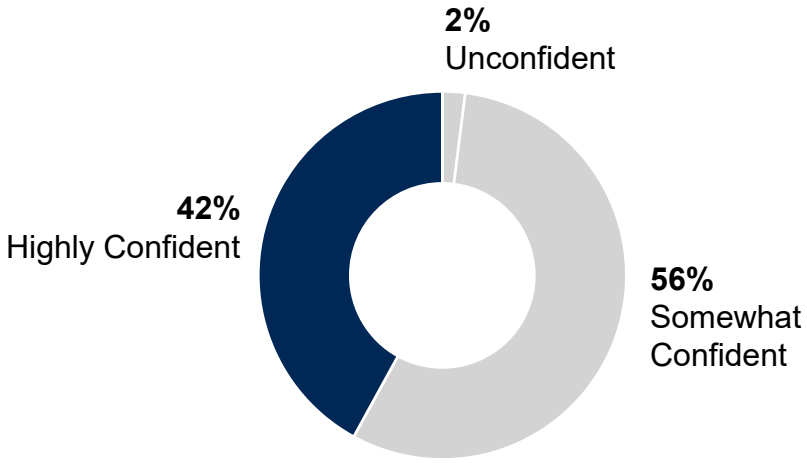
2023 Audit Plan Hot Spots

Cyberthreats

State-sponsored cyberthreats and heightened scrutiny on attack disclosures make cyberthreats a growing risk in 2023. Year-over-year cyberattacks continue to evolve and increase.[1] Sixty-eight percent of organizations experienced at least one ransomware attack in 2021, 65% experienced more than three and 15% experienced 10.[2] Ninety-two percent of organizations say they faced or suspect they might have faced a state-sponsored cyber attack between July 2020 and December 2021, or expect to face one in the future.[3] Russia's invasion of Ukraine and the resulting hostility between Ukraine-aligned states and Russia could expose organizations to increased cyberthreats.[4] Further, increases in personal data breaches have led to new regulatory requirements, which many expect will have significant implications for organizations in cybersecurity reporting, disclosure and governance.[5] On top of the financial cost that a cyberattack can generate, organizations that fail to consider the effects of potential regulation on cyber disclosures may face fines, litigation risk and reputational damage.

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

Percentage of Respondents

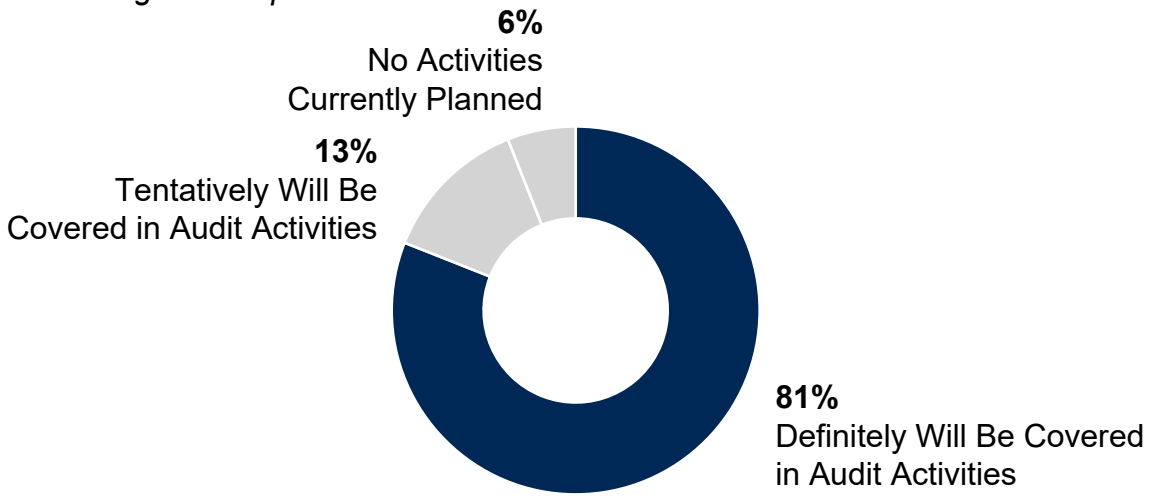


n = 111

Source: 2023 Gartner Audit Key Priorities and Risks Survey

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

Percentage of Respondents



n = 112

Source: 2023 Gartner Audit Key Priorities and Risks Survey

Cyberthreats

Urgency Drivers

State-Sponsored Cyberattacks

State-sponsored cyberattacks against enterprises are already widespread, but attackers' changing motivations could increase and worsen them.[6] Some current attacks steal cryptocurrencies or other assets for revenue generation.[7] North Korea, for instance, allegedly stole nearly $400 million in digital assets in 2021.[8] Others exfiltrate intellectual property to support domestic industries.[9] U.S. authorities opened a China-related investigation every 12 hours in early 2022, many concerning cyber-based intellectual property theft.[10] Even before the Russian invasion of Ukraine, 39% of organizations already believed that Russian state-sponsored actors targeted them.[11] Worse, Ukraine-aligned governments believe Russia could retaliate against critical infrastructure and key economic institutions in an escalation of conflict.[12] State-sponsored attacks against these targets can be hard to prevent or detect due to their sophistication (e.g., lingering in systems and using third parties as vectors). State-sponsored attacks' consequences could rise substantially if the motive behind them becomes retaliation instead of profit.

Cyber Breach Disclosure Requirements

Several new and proposed breach disclosure requirements raise the possibility that organizations may be forced to disclose reputationally damaging information about cyber capabilities and conform to potentially burdensome disclosure standards. A new law in the U.S. requires critical infrastructure companies to report cyber incidents within 24 or 72 hours, depending on the event.[13] The U.S. Securities and Exchange Commission has proposed a further requirement for publicly listed companies to report incidents within 96 hours.[14] In Australia, critical infrastructure operators must report critical and other cyber incidents within 12 or 72 hours, respectively.[15] The U.K. government has also advised legal bodies to consider disclosures of ransomware incidents involving personal data to authorities as a mitigating factor in deciding penalties.[16] Organizations worry these disclosure requirements might harm their reputations as responsible stewards of data or even lead to oversharing intellectual property or cybersecurity practices.[17] Breach disclosure requirements can now turn cyberthreats into substantial regulatory risk for many organizations.

Key Risk Indicators

- Mean time to incident detection
- Mean time to incident resolution
- Mean time to recovery (MTTR) of compromised application
- Average time since last patching of systems and endpoints
- Number of "Shields Up"-type warnings by government agencies
- Percentage of applications with automated disaster recovery
- Frequency of backups and tests
- Volume of traffic originating from unknown IP addresses
- Days since most recent comprehensive network security penetration test
- Percentage of network devices not meeting configuration standards

Cyberthreats

Recommendations for Audit

- **Review Cyber-Risk Management Program and Processes:** Review cybersecurity program definitions, framework, and the quality and thoroughness of assessing risks, mitigations and controls.
- **Review Information Security Threat Intelligence Practices:** Evaluate the thoroughness and completeness of IT and information security's practices around discovering emerging risks and threats.
- **Assess Monitoring Practices:** Examine how the IT department performs monitoring of applications, databases, the network and other assets to detect any unusual activities, especially over assets that are operationally critical or sensitive data or information.
- **Assess the Effectiveness of Escalation and Coordination in Incident Response:** Evaluate current incident response plans to ensure effective and timely escalation, coordination and communication to concerned stakeholders.
- **Review the Incident Response Plan:** Assess how roles and responsibilities are defined to deal with cyber incidents. Test whether the individuals in question are fully aware of their duties.
- **Examine Existing Cybersecurity Reporting Capabilities:** Evaluate the baseline for current cybersecurity reporting capabilities. This should include reporting capabilities for incidents and cyber-defense posture (e.g., the board's cyber expertise, governance and oversight).

Cyberthreats

Questions for Management

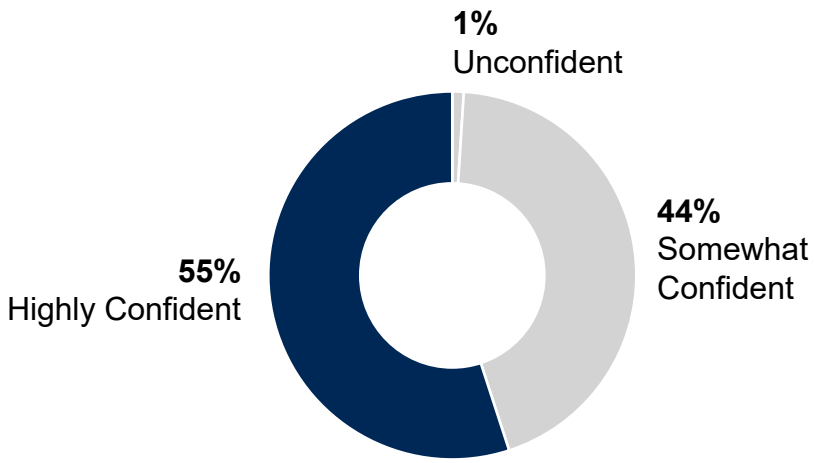
- What indicators do we use to determine whether there is suspicious activity concerning our networks or assets?
- How often do you conduct mock-phishing tests to see how many employees click on suspicious emails, and how do you analyze the results of those tests?
- What procedures are in place for educating the employees who click on the phishing test emails?
- When was the last time the organization carried out a cyber tabletop exercise?
- Who in the organization is responsible for responding to cyberattacks and how?
- What are the highest sensitivity data or digital assets that could be used for extortion?
- What policies are in place to ensure that data is backed up as per risk assessments?
- Who is accountable for including regulatory considerations for new cybersecurity initiatives?
- Who is responsible for drafting cyber disclosures?
- How are cyber disclosures vetted?

IT Governance

Amid increasing pressures around executing digital business models, most organizations plan to increase IT investments.[18] Many organizations plan to improve enterprise agility, business resilience and data and analytics capabilities.[19] However, resourcing and governance challenges, such as the scalability of existing IT governance models, threaten these investments. With more technology spending led by business units themselves, with no or little IT oversight, 69% of IT leaders cite "shadow IT" as a top security concern.[20] Another challenge for IT governance, in the wake of the COVID-19 pandemic, is strained capabilities. An acute scarcity of talent threatens IT's ability to implement new capabilities and maintain existing ones, including controls.[21] Organizations that fail to back digital business acceleration with investments in the IT department that increase its ability to oversee a growing, complex web of digital services may see digital bets pay off slowly, or expose the organization to governance risk as business units find their own solutions to IT's lack of agility.[22]

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

Percentage of Respondents

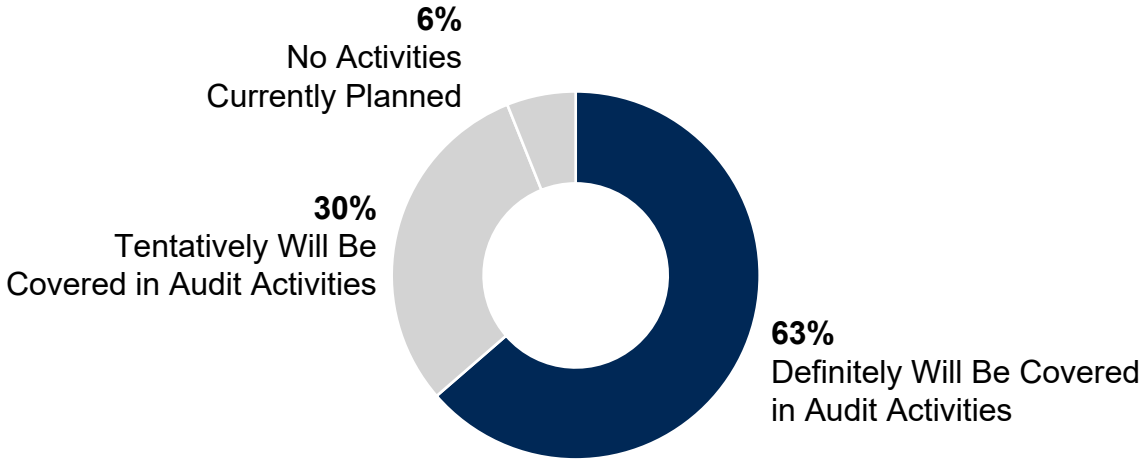


n = 111

Source: 2023 Gartner Audit Key Priorities and Risks Survey

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

Percentage of Respondents



n = 112

Source: 2023 Gartner Audit Key Priorities and Risks Survey
Note: Totals might not sum to 100% due to rounding.

IT Governance

Urgency Drivers

Ungoverned SaaS

As software as a service (SaaS) covers larger segments of business activity and becomes easier to procure, globally, spending on SaaS is expected to increase over 17% though 2023.[23] SaaS providers often market their products directly to business units. The products' ease of use — often operating over internet browsers and offered in "freemium" versions — make them simple for individuals in business units to adopt without IT's involvement. Fifty-nine percent of U.K. organizations believe they have incomplete knowledge of their employees' usage of SaaS.[24] About the same number of U.S. and Canadian organizations acknowledge related management concerns.[25] Deploying these applications and platforms can include unexpected costs, performance issues (e.g., service availability), data recoverability challenges and compliance issues.[26] Furthermore, if a "shadow" SaaS becomes critical to business units, IT departments may find themselves unable to integrate it with other IT services later, potentially harming IT agility. Amid a period of fast business evolution, organizations that fail to provide for both agility and governance in SaaS may find themselves with governance challenges that are difficult to address retroactively.

IT Talent Shortage

While strategies increasingly rely on IT capabilities, IT departments struggle to retain highly skilled employees and upskill their current workforces.[27] Fifty-three percent of IT leaders say the IT talent shortage is a critical challenge following a record year of attrition in 2021.[28] The skills necessary for IT transformation, such as cloud and agile development, are among the hardest for which to hire in the global talent market.[29] Just retaining IT talent is challenging. Only 32% of IT workers highly intend to stay with their current organizations.[30] Upskilling existing IT employees is a perennial challenge further exacerbated by the COVID-19 era's pace of change. Only 52% of organizations have implemented IT upskilling programs, with around half citing lack of time and budget as barriers.[31] As organizations look to IT to support digital capabilities that enable enterprise agility amid dynamic business plans, shortages of key IT skills may be a primary bottleneck.

Key Risk Indicators

- Number of uses of unauthorized software or services discovered by IT monitoring tools
- Incidents of data sharing between authorized and unauthorized software and services discovered by IT monitoring tools
- Percentage of approved applications monitored by cloud access security broker and other tools
- Growth or decline in number of privileged accounts for SaaS services
- Percentage of new hires in areas identified as IT skills gaps
- Percentage of new certifications in areas identified as IT skills gaps
- Retention rates of employees in key IT roles
- Training hours per IT employee
- Offers for IT roles accepted as a percentage of offers extended
- Trends in average time to fill a vacant IT position over a specific period

IT Governance

Recommendations for Audit

- **Assess How the Organization Monitors for Unauthorized Software Use:** Determine the methodologies, procedures and technologies (especially cloud access security broker tools) in place for monitoring the network for unauthorized software and unauthorized interfacing between authorized and unauthorized software.
- **Review Information Security Policies and Training:** Review information security policies to be sure they explicitly preclude unauthorized software use and that effective training exists to make employees aware of this prohibition. Assess organizational procedures for requesting new software for business purposes and how they are communicated to business units.
- **Review Organizational SaaS Governance Structures:** Review SaaS governance measures in the organization and determine the level of SaaS oversight the IT department has. Ensure the organization has a written directive regarding SaaS ownership to specify governance rules and enforcement.
- **Review IT Talent Assessments:** Determine if IT and business units have targeted assessments of IT and technical talent skills and potential gaps. This review should include how the core competencies and skills needed to meet security and other IT objectives are defined. Review assessments to be sure they consider both short- and long-term business needs.
- **Conduct Ongoing IT Talent Monitoring and Tracking:** Review progress on proposed workforce plans and IT talent risk-mitigation strategies. Assess whether plans are adequately updated as business priorities and organizational needs change. Communicate progress to management to drive urgency and accountability.

IT Governance

Questions for Management

- How does the IT department monitor the use of potentially unauthorized software in the network or unauthorized interfaces between enterprise data and unapproved applications (e.g., CASB, SaaS monitoring tools)?
- How would the IT department respond if it learned that employees were regularly using an unapproved application or service for business purposes?
- How would the IT department respond if it learned that employees had exported data to an unapproved application or service?
- What processes exist for the IT department to vet business-led IT subscriptions and investments?
- How are you ensuring cross-silo collaboration when implementing and scaling IT investments?
- What IT skills do we currently lack that are critical to present operations?
- Which technical skills are needed by the business to reach its long-term goals?
- How do you attract and retain talent with key technical skills?
- How have you adjusted your recruiting efforts to better attract technical talent?
- What metrics are in place to track the quality and efficacy of IT upskilling programs?

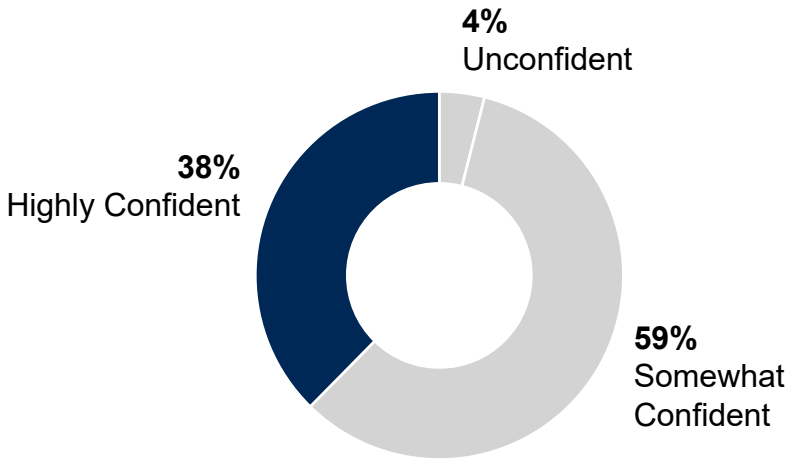
Data Governance

With digital business models increasingly reliant on analyzing customer preferences and behaviors, organizations collect more data subject to legal, regulatory and ethical concerns every year.[32] Artificial intelligence (AI) — long largely an experiment in the business context — is set to become a common means of harnessing such data, with the amount of organizations deploying AI set to approximately triple in the next three years.[33] AI is now learning customer habits, directing data campaigns and changing organizational decision making.[34] However, the way AI algorithms operate, or other key aspects of AI use, may go ungoverned, with organizations often unaware of AI capabilities or even that services in their IT environments incorporate AI.[35] Regulators, too, are in a constant state of catch-up when it comes to data and privacy trends, like AI.

The result is an increasingly fragmented regulatory landscape that produces disparate data requirements, making compliance between jurisdictions expensive and time-consuming. Organizations that fail to govern their emerging data practices risk a wide range of consequences amid an increasingly fragmented regulatory environment.

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

Percentage of Respondents

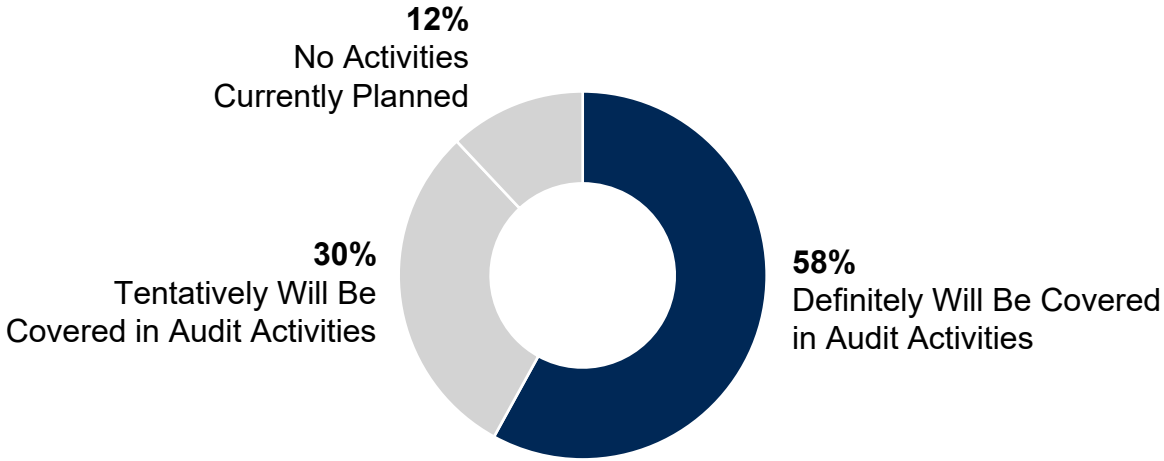


n = 111

Source: 2023 Gartner Audit Key Priorities and Risks Survey
Note: Totals might not sum to 100% due to rounding.

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

Percentage of Respondents



n = 112

Source: 2023 Gartner Audit Key Priorities and Risks Survey

Data Governance

Urgency Drivers

AI Governance

Most enterprises plan to deploy AI or machine learning (ML) for the first time by 1Q24, and a quarter have already done so.[36] As such, organizations have little time to improve their data governance before AI becomes embedded into business capabilities. Insufficient oversight of data used by AI can pose a wide variety of risks, including in the compliance, reputational and cyber domains.[37] Several high-profile incidents have demonstrated the real effects of "data poisoning," or the malicious introduction of a bias into an AI model.[38] Privacy-related AI risk is another concern, with 41% of organizations having experienced an AI-related privacy breach, and over one in four from a malicious actor.[39] Regulators have taken notice of AI's privacy implications. A draft proposal from the European Commission would empower regulators to order AI models retrained or deleted when systems pose a "high risk" to certain personal data.[40] Despite all of the challenges regarding AI governance, many organizations do not even realize their exposure to these risks, given the increasing amount of AI that is embedded within third-party services.[41]

Personal-Data-Related Regulatory Fragmentation

Though the number of regulations over personal data governance, such as the General Data Protection Regulation (GDPR) in the EU and the California Consumer Privacy Act (CCPA) in the U.S., have been rising steadily for some time, 2023 presents new-in-kind challenges for personal data compliance. The variety of new requirements, some with distinct regulatory intent, may pose a particular challenge. For example, while several data privacy laws will go into effect in the U.S. in 2023, they treat the consent required to process personal data differently.[42] The U.S. laws also differ from the EU's GDPR in that the former require "opt-out" preferences, to sell personal information, and the latter requires "consent."[43] Governments' use of data localization requirements (to host data within a country or region) is also increasing. As of 2022, 75% of countries have implemented data localization rules, but these countries have disparate aims.[44] Some countries plan to protect privacy (e.g., health information), but others plan to protect state security or domestic industries.[45] Personal data regulatory fragmentation along with the prospect of increasing privacy demands may prove a technical challenge to data governance strategies.

Key Risk Indicators

- Number of known AI capabilities embedded in the organization
- Number of product features deployed and in development that rely on AI capabilities
- Frequency of model performance monitoring
- Frequency of AI documentation updates
- Frequency of retention or purging or deletion actions among specified personally identifiable information (PII), compared to requirements
- Frequency of updates to data classification and use policies
- Number of approved exceptions to data and analytics policies
- Number of employees who can access PII
- Frequency of authorized third-party access to PII
- Number of third parties recognized as high-risk with access to PII

Data Governance

Recommendations for Audit

- **Review Documentation for AI Projects:** Review documentation for all AI-related projects to determine how those projects might expose the organization to risks and potential controls and mitigations.
- **Review AI Governance Priorities and Standards:** Review how IT or others identify risks and create standards to allow AI's deployment that controls or mitigates potential risks (including both guidelines and automated controls), and who provides oversight over the mitigations' and controls' implementation. Assess how IT or other risk managers identify the criticality of AI-related applications, data or other assets.
- **Review AI Monitoring Practices:** Evaluate practices for monitoring AI and related data and analytics capabilities for signs of bias or malicious interference.
- **Assess the Organization's Current Level of Data Privacy Regulation Compliance:** Assess the organization's current progress in complying with applicable regulatory mandates and any gaps in current policies. Review how the organization identifies and tracks regulations on personally identifiable information (PII) use.
- **Assess Data Access and Storage Policies:** Review policies that govern data access and storage (i.e., protection, retention and deletion) and determine who is responsible for regular review, evaluation and updates to individual policies.

Data Governance

Questions for Management

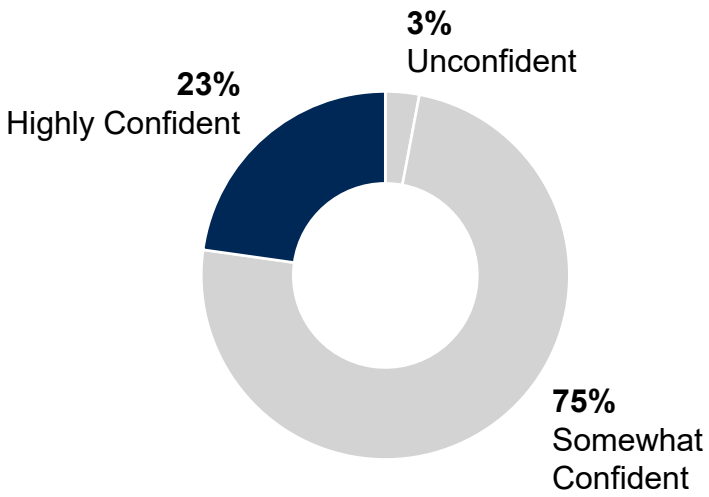
- How do you determine whether an AI capability is ready for deployment?
- How do you understand whether third parties are using AI in the services they provide to the organization, and how is such AI vetted for compliance with organizational policies?
- How do you confirm whether AI capabilities under development or in deployment meet legal and compliance requirements?
- How do you monitor AI for anomalies or drift after deployment?
- How do you ensure that the results of algorithms and AI that use personal data are explainable and transparent?
- What categories of AI-related risk controls does the organization recognize and which categories contain the biggest control gaps presently?
- How does the organization track regulatory developments concerning AI, PII and other data-and-analytics-related issues?
- How is employee training being updated to conform with new regulations concerning PII?
- What guidelines do you follow to identify and classify data retained as necessary for your business unit?
- What are the most important actions you take to monitor third parties' access to sensitive or personal data?

Third-Party Risk Management

Third-party incidents, such as data breaches, compliance issues and supply chain disruptions are increasing annually.[46] Eighty-two percent of organizations say third-party risk incidents disrupted operations at least once in the last 12 months.[47] As a result, 83% of organizations reported increased organizational focus on third-party risk.[48] Yet, many organizations have poor third-party risk visibility. For example, only 11% of organizations monitor supplier risks continuously, and only 48% understand the risk their Tier 1 suppliers face.[49] Forty-five percent of organizations say their third-party risk management (TPRM) programs are primarily focused on IT vendors, leaving a variety of partner relationships either unexamined or examined by siloed functions.[50]
This limited visibility may be especially costly in 2023, when organizations' third parties will likely face a challenging business environment and volatile markets. Organizations that fail to evolve their TPRM practices may expose themselves to a variety of risks that are not always examined in TPRM programs, such as regulatory fines, reputational damage and operational disruptions.

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

Percentage of Respondents

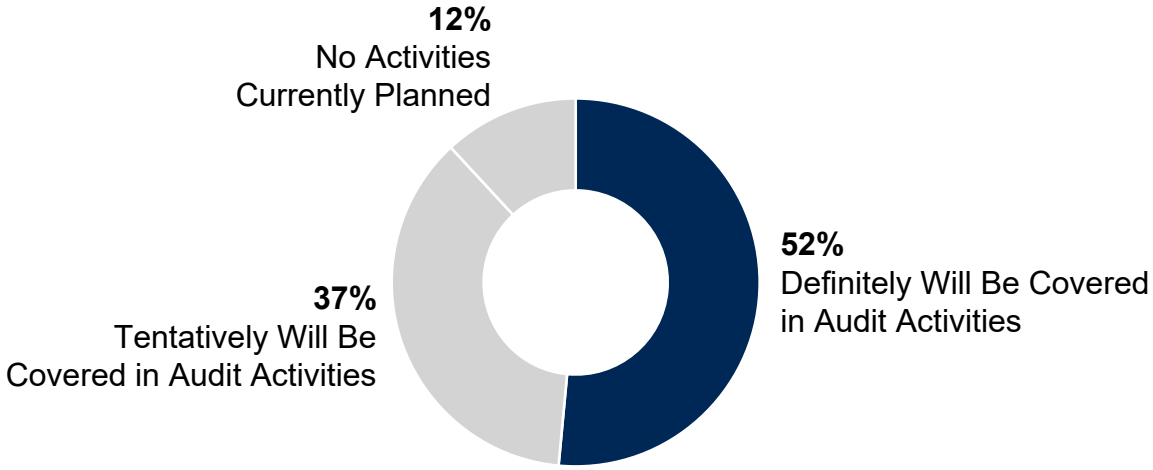


n = 110

Source: 2023 Gartner Audit Key Priorities and Risks Survey
Note: Totals might not sum to 100% due to rounding.

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

Percentage of Respondents



n = 112

Source: 2023 Gartner Audit Key Priorities and Risks Survey
Note: Totals might not sum to 100% due to rounding.

Third-Party Risk Management

Urgency Drivers

Third-Party Reputational Risk

The combination of new third-party reporting requirements and increasing financial or operational constraints could increase the risk of reputational damage from third parties in 2023. Due to inputs, staffing and other economic challenges, suppliers and others may reorient focus from supply chain ethics and ESG toward more acute problems.[51] This shift may increase incidents in an area over which organizations already have limited visibility.[52] Additionally, new reporting requirements will raise third-party reputational risk exposure from supply chains. In 2022, Germany and Norway joined other countries in requiring reporting on ethical supply chain due diligence, while EU and Canadian officials have proposed similar measures.[53] Meanwhile, the U.S. proposed joining other countries in requiring reporting of Scope 3 emissions (from "upstream or downstream" activity), while the U.K. and EU will enhance existing Scope 3 requirements.[54] Because consumers tend to hold the organization liable for third-party ethical lapses rather than the organization's suppliers or partners, more stringent reporting requirements and third parties' potential shifting priorities increase reputational risk exposure.

Third-Party Viability

Current macroeconomic conditions raise concerns about third parties' business continuity, including their financial viability. As a long period of low interest rates and low inflation gives way to ballooning costs and volatility, investors are derisking portfolios, and banks are restricting credit.[55] Analysts forecast this movement, combined with dwindling government support, will raise business insolvencies by 14% in 2023.[56] Particular suppliers or partners may be especially vulnerable. In the U.S., 43% percent of small businesses (often critical providers to larger ones) say their own supply chain issues have worsened since the beginning of 2022, while 56% percent report deteriorating economic circumstances generally.[57] Some sectors, like retail in the U.S., may see bankruptcy waves from pandemic-related realignment of spending habits.[58] Organizations in some regions may also be at greater risk, such as in those with less government support, like the U.K., or high business debt-to-GDP ratios, like Japan and the eurozone.[59] Yet, 36% of organizations do not regularly assess third-party business or financial risks, potentially exposing organizations to disruptions, high costs of switching vendors, and product or operational issues.[60]

Key Risk Indicators

- Number of critical third parties
- Frequency of updates to third-party risk profiles
- Number of disruptions and failures involving or triggered by third parties
- Number of third-party disruptions, such as operational delays, regulatory fines and loss of critical data
- "Downstream" Scope 3 emissions (e.g., use of products, end-of-life processing of sold products)
- "Upstream" Scope 3 emissions (e.g., preproduction supply chain emissions)
- Critical supplier days payable outstanding
- Critical supplier percentage of invoices paid on time
- Third-party current ratio; working capital ratio; acid test ratio
- Number and size of regulatory fines (e.g., GDPR fines) per period

Third-Party Risk Management

Recommendations for Audit

- **Review How (and Whether) Scope 3 Emissions are Assessed:** Review materiality assessments or other ESG assessments to determine whether and how the organization assesses Scope 3 emissions.
- **Review Ethical Supply Chain Compliance Tracking:** Assess the organization's process for identifying and interpreting relevant ethical supply chain regulations in all applicable jurisdictions, and determine whether the organization's ethical supply chain practices currently address their requirements.
- **Assess the Extent of Continuous Monitoring of Key Third-Party Relationships:** As initial due diligence does not ensure continuing third-party compliance with requirements, assess whether relevant functions monitor third-party behaviors and policies on an ongoing basis. Review the frequency of which risk profiles are reassessed and updated.
- **Assess Third Parties' Effects in Business Continuity Management:** Assess whether third-party risk management is integrated into business continuity management approaches and plans. Review the third-party portfolio to ensure that when the organization relies on a single partner for services, it has a strategy in place for managing business interruptions should the third party be unable to deliver services.
- **Assess Third-Party Contracts:** Evaluate the process for writing and approving contracts with third-party vendors and contractors, ensuring they adequately stipulate information security, data privacy and other requirements. Assess activities aimed at ensuring third-party adherence to contracts, particularly for critical or high-risk third parties.
- **Assess Third-Party Access to Personally Identifiable Information:** Assess the extent of third-party access to customers' and employees' personally identifiable information.

Third-Party Risk Management

Questions for Management

- How does the organization evaluate the criticality of its third parties?
- What monitoring and reporting activities are in place to understand changes in third-party risk exposure levels?
- Which functions most commonly lead third-party assessments?
- How is information from third-party risk assessments shared and leveraged (beyond the function conducting the initial assessment)?
- How far down the third-party chain (e.g., fourth, fifth) does the organization assess third-party risk?
- How often do you review third-party relationships to ensure compliance with policies and procedures?
- How does the organization track new compliance risks facing or caused by third parties?
- How do you use third parties' internal audit findings, compliance reviews and misconduct records in your third-party risk assessments?
- Which third-party risks (e.g., business, finance) does the organization track in its third-party risk monitoring program?
- What are the top third-party-related issues identified by the ESG materiality assessment?

Appendix

Endnotes

Cyberthreats

1. Check Point Research: Cyber Attacks Increased 50% Year Over Year, Check Point Software Technologies.
2. 2022 State of the Phish: An In-Depth Exploration of User Awareness, Vulnerability and Resilience, Proofpoint.
3. Trellix Global Threat Research: In the Crosshairs: Organizations and Nation-State Cyber Threats, Trellix.
4. Russia Cyber Threat Overview and Advisories, U.S. Cybersecurity & Infrastructure Security Agency; Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure, U.S. Cybersecurity & Infrastructure Security Agency.
5. Cybersecurity Legislation: Preparing for Increased Reporting and Transparency, McKinsey & Company.
6. Microsoft Digital Defense Report, Microsoft.
7. North Korean Hackers Have Prolific Year as Their Unlaundered Cryptocurrency Holdings Reach All-time High, Chainalysis.
8. Russia Cyber Threat Overview and Advisories, U.S. Cybersecurity & Infrastructure Security Agency; Trellix Global Threat Research: In the Crosshairs: Organizations and Nation-State Cyber Threats, Trellix.
9. Russia Cyber Threat Overview and Advisories, U.S. Cybersecurity & Infrastructure Security Agency; The Threat Report: Summer 2022, Trellix.
10. FBI Director Wray Says Scale of Chinese Spying in the U.S. "Blew me away", NBC News.
11. Trellix Global Threat Research: In the Crosshairs: Organizations and Nation-State Cyber Threats, Trellix.
12. Russia Cyber Threat Overview and Advisories, U.S. Cybersecurity & Infrastructure Security Agency; Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure, U.S. Cybersecurity & Infrastructure Security Agency.
13. Cybersecurity Legislation: Preparing for Increased Reporting and Transparency, McKinsey & Company; Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), U.S. Cybersecurity & Infrastructure Security Agency.
14. New SEC Cybersecurity Reporting Requirements: Three Things Companies Need To Do Now, Forbes; Fact Sheet: Public Company Cybersecurity: Proposed Rules, U.S. Securities and Exchange Commission.
15. Critical Infrastructure Cyber Notification Obligations: When Do You Need to Comply?, Lexology; Report a Cyber Security Incident, Australian Cyber Security Center.
16. Letter From the U.K. Information Commissioner's Office, U.K. Information Commissioner's Office.
17. Cybersecurity Legislation: Preparing for Increased Reporting and Transparency, McKinsey & Company.

Endnotes

IT Governance

18. 2022 Gartner CIO and Technology Executive Survey.
19. Gartner (2021).
20. 2022 SaaS Visibility and Impact Report, Torii.
21. 1Q22 Gartner Global Labor Market Survey.
22. Gartner (2022).
23. Gartner (2022).
24. Perception vs. Reality: The State of SaaS Management, Cledara.
25. The State of SaaS Management, Productiv.
26. Gartner (2022).
27. 2Q22 Gartner Global Labor Market Survey; Gartner (2022).
28. White Paper: Multicloud Annual Research Report 2022, Rackspace Technology.
29. Gartner TalentNeuron.
30. 2Q22 Gartner Global Labor Market Survey.
31. The Upskilling IT 2022 Report: Empowering Professionals for the Jobs of Today and Tomorrow, DevOps Institute.

Data Governance

32. Tech Trends 2022, Deloitte.
33. 2022 Gartner CIO and Technology Executive Survey.
34. Gartner (2022).
35. Gartner (2022).
36. 2022 Gartner CIO and Technology Executive Survey.
37. Gartner (2021).
38. IBM's DeepLocker: The Artificial Intelligence Powered Sneaky New Breed of Malware, Packt; Malicious AI Isn't A Distant Reality Anymore, Forbes; How Data Poisoning Attacks Corrupt Machine Learning Models, CSO; Poisoned Robots: Data Poisoning Threatens AI-Powered Mechanisms, JDSUPRA.
39. 2021 Gartner AI in Organizations Survey.
40. Europe's AI Act Contains Powers to Order AI Models Destroyed or Retrained, Says Legal Expert, TechCrunch; The European Union AI Act: Next Steps and Issues for Building International Cooperation in AI, Brookings.
41. Gartner (2022).
42. The State of U.S. State Privacy Laws: A Comparison, The National Law Review.
43. From CCPA to CPRA: What to Know About the California Privacy Law, Cimatri.
44. Localization of Data Privacy Regulations Creates Competitive Opportunities, McKinsey & Company; Gartner (2022); The State of U.S. State Privacy Laws: A Comparison, The National Law Review; From CCPA to CPRA: What to Know About the California Privacy Law, Cimatri.
45. Localization of Data Privacy Regulations Creates Competitive Opportunities, McKinsey & Company; Gartner (2022); The State of U.S. State Privacy Laws: A Comparison, The National Law Review; From CCPA to CPRA: What to Know About the California Privacy Law, Cimatri.

Endnotes

Third-Party Risk Management

46. The 2022 Prevalent Third-Party Risk Management Industry Study: TPRM Programs Are at a Crossroads, Prevalent.
47. 2022 Gartner ERM Client Survey on Third-Party Risk.
48. The 2021 Prevalent Third-Party Risk Management Study: Looking Beneath the Cyber Risk Surface, Prevalent.
49. Resilience 2022: Interos Annual Global Supply Chain Report, Interos.
50. The 2022 Prevalent Third-Party Risk Management Industry Study: TPRM Programs Are at a Crossroads, Prevalent.
51. PwC Digital Trends in Supply Chain Survey 2022, PwC.
52. Resilience 2022: The Interos Global Supply Chain Report — Focus: Financial Services Sector, Interos.
53. EU Mandatory Human Rights and Environmental Due Diligence, Article One; European Union Releases Draft Mandatory Human Rights and Environmental Due Diligence Directive, Center for Strategic & International Studies; Bill S-211: Impact on M&A Transactions, Norton Rose Fulbright; ESG Reporting Mandates to Know for Third-Party Risk Management, ProcessUnity; Germany: New Law Obligates Companies to Establish Due Diligence Procedures in Global Supply Chains to Safeguard Human Rights and the Environment, U.S. Library of Congress; Norway's Transparency Act: What You Need to Know, Sedex.
54. EU and U.K. Climate Disclosure Programmes: An Overview, Watershed; EU Nears Adoption of Expansive Corporate Sustainability Reporting Requirements, Sullivan & Cromwell.
55. The Coming Credit Crunch, Bloomberg. (Paid subscription required.); Brutal Stock Selloff Is a Multitude of Bear Cases Coming True, Bloomberg. (Paid subscription required.)
56. Global Insolvency Report: Growing Risks and Uneven State Report, Allianz Research.
57. Survey: From Bad to Worse, Goldman Sachs.
58. Survey: From Bad to Worse, Goldman Sachs.
59. The Retail Industry Is Facing a Potential Wave of Bankruptcies — Here's Why, CNBC.
60. Global Insolvency Report: Growing Risks and Uneven State Report, Allianz Research; The 2021 Prevalent Third-Party Risk Management Study: Looking Beneath the Cyber Risk Surface, Prevalent; Guarding Against Supplier Insolvency, GrowthBusiness.

Actionable, objective insight

Explore these additional complimentary resources and tools for audit & risk leaders:

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

Research

Develop an Audit Strategic Plan

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

Download Research

Webinar

Join a virtual event

Hear the latest insights from Gartner Audit and Risk experts at an upcoming or on-demand event.

Watch Webinar

Connect With Us.

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

U.S.: 1 855 811 7593

International: +44 (0) 3330 607 044

Become a Client

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

Stay connected to the latest insights

Gartner