2022 Audit Plan Hot Spots

Audit Research Team

Gartner®

Contents

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.

Educate the Audit Committee
Educate the audit committee on the current risk trends.

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 based on input from 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 identify risks to the organization more effectively and highlight key risks for stakeholders. This year, four themes underlie the 12 hot spots:

1. The End of the Global COVID-19 Slowdown

While COVID-19 continues to have devastating effects on humanity, the COVID-19-driven global economic slowdown of 2020 has now been replaced with an uneven economic recovery, marked by supply-and-demand mismatches. Supply chains are reeling from the lingering effects of the COVID-19 shock, and organizations have been repeatedly taken by surprise by increases and declines in customer demand during and after lockdowns. This has led to significant shortages of key goods. Many economies are further facing a significant supply constraint in the form of labor, as many workers left the workforce during the pandemic and have not returned. These supply-and-demand imbalances have led to some of the largest price increases seen in decades — some of which are projected to endure for several quarters, risking permanently higher inflation. These imbalances manifest in the following risks:

- As organizations confront a more constrained labor market, they are facing unusually high employee **retention and recruitment** risks. Employees' and job seekers' expectations have evolved dramatically through the pandemic, especially regarding flexible work arrangements. Given labor scarcity and these new expectations, organizations are now struggling to quickly define and operationalize enhanced employee value propositions.
- Supply-and-demand distortions caused by the pandemic and its aftermath, exacerbated by geopolitical movements and other factors, have created a myriad of **supply chain** risks. Many of the goods and materials shortages are likely transitory, but others are projected to linger, causing procurement and logistical challenges and price inflation.
- General **economic uncertainty** also poses a greater risk than in recent years. This is driven by the unknown future evolution of COVID-19, the vast differences in vaccination rates between countries, and varying levels of government economic support and price controls. Uncertainty around inflation and demand at levels not seen for over a decade. This makes planning and forecasting especially difficult at a time when organizations are rapidly embarking on new strategies.

2. COVID-19-Driven Digital Acceleration

Accelerating digitalization during the COVID-19 era is creating winners and losers among organizations based on their abilities to rapidly transform and harness changes in customer preferences, markets and society. Much of the world is settling into a "new normal" following more than a year of remote working and remote interactions, but given the profound differences in consumer and buyer behavior, organizations find it difficult to tell which changes will become permanent. The need to accelerate digital transformation is acknowledged by almost all organizations, but it remains a challenge given years of underinvestment in the technological, talent and cultural foundations that enable digital strategy execution. This COVID-19-driven digital acceleration and the imbalance between digital ambitions and capabilities manifest in the following risks:

- Organizations are deeply engaged in new digital strategy formulation, making **strategy execution** an especially acute risk. Strategic change management is a key enabler of strategy execution. However, workforces have already endured large-scale changes during COVID-19, impeding organizations' abilities to absorb further changes to the operating and business model.
- Organizations' abilities to execute **digital business transformation** are challenged by growing digital divides. New business strategies and operational plans are reliant on new IT capabilities, but IT departments' goals and cultures are often oriented toward operational excellence rather than supporting business transformation. On the other side, business strategy and planning also remain hampered by an inability to imagine what evolving information technologies like cloud and artificial intelligence (AI) can mean for digital strategy.
- The importance of data and analytics capabilities to power digital business transformation is increasingly recognized by organizations. However, they underestimate the role of **data and analytics governance** in enabling those capabilities. Organizations often lack a systematic organizational model for data and analytics ownership and accountability, leading to a lack of controls, poor data sharing and less benefits from data and analytics investments.

Executive Summary (continued)

- Without focused **IT governance** efforts, the lingering effects of IT departments' sudden shifts enabling remote business during COVID-19 and the resulting changes in IT environments will hamper digital business strategies. IT departments that fail to tackle technical debt and fall behind on modernizing core systems and applications will be unable to support the digital innovation their systems enable.

3. Evolving Societal Expectations

A new set of expectations is rapidly developing for the roles of businesses and other organizations in society. Different stakeholders — including employees, investors, regulators and consumers — have different expectations, but those expectations are converging around organizations' roles in combating climate change and addressing social justice issues. A key conduit for these expectations is ESG (environmental, social and governance): The expectation and, increasingly, the requirement, for organizations to report and assure their efforts on sustainability, DEI (diversity, equity and inclusion) and other areas. COVID-19 also accelerated expectations for several aspects of corporate social responsibility, given the higher levels of employee burnout while working from home and the disproportionate impact of the pandemic on women and people of color. Evolving social expectations for organizations manifest in the following risks:

- The level of **ESG** risk is increasing. ESG disclosures, or the lack thereof, are connected to financing risk because an increasing amount of capital is bound up in meeting ESG standards. Regulatory risk is also increasing. Some regulatory bodies in Europe and elsewhere have already committed to binding action over disclosures.
- Organizations will face complex decisions regarding **workforce management** in 2022, forcing them to weigh employee and societal expectations against other enterprise risks. For instance, hybrid working arrangements, regardless of how they are executed, involve high levels of talent, operational and innovation risk. Many other COVID-19-related decisions, such as enforcing social distancing, requiring vaccination or capacity management, also pit the expectations of many employees and society against organizational interests.

4. New Operational Resilience Frontiers

The pandemic and the ongoing recovery exposed the limitations of business continuity planning as commonly practiced, as risk events became drawn out rather than point-in-time, and the significance of third-party relationships continued to increase. To adapt, plans to respond to sudden disruptions of limited duration must be replaced by plans to respond to long and severe disruptions to supply chains and operations. Similarly, the assessment of third-party risks only at certain points in time such as at the onset of relationships must be replaced by ongoing monitoring. Finally, risk assessment techniques that don't consider the organization's vulnerabilities to cyberattacks, weather disruptions or other operational factors introduced by third and nth parties must be replaced by continuous assessment of such vulnerabilities. New operational resilience frontiers manifest in the following risks:

- The **ransomware** industry is rapidly evolving, as attacks become more common and sophisticated. More organizations are paying the consequences of failing to secure vulnerabilities beyond the network perimeter, with attacks targeting third parties as a conduit to the primary organization or for the organizational data they hold.
- The COVID-19 period demonstrated the limitations of due diligence and other point-in-time techniques for managing **third-party** risks. The events of 2021 left many third parties unable to fulfill guarantees made during vendor onboarding or at the onset of relationships. However, organizations struggled to understand the state of third-party risks because they were not conducting ongoing third-party risk monitoring, most importantly cyber defense and access to privileged systems and data.
- The year 2021 also led to significant changes within **business continuity and organizational resilience**. As organizations encounter long-duration disruptions, such as climate degradation, they find their business continuity planning to be too limited in scope. They must move toward sustained operational and organizational resilience to withstand long and repeated shocks. Operational resilience is also an area of high regulatory interest.

Audit Plan Hot Spots Summary

Audit Plan Risk Areas	Summary	2022 Drivers	2021 Drivers
Ransomware	The increased frequency of ransomware attacks alongside new, highly effective extortion strategies is putting organizations at risk of reputational damage and operational losses from extended downtime and remediation costs. **This is an evolution of last year's cybervulnerabilities hot spot.**	1. Proliferating Ransomware Attacks 2. Evolving Ransomware Extortion Strategies	1. Lapses in Security Controls 2. Increased Employee Vulnerability to Social Engineering
Data and Analytics Governance	The importance of data and analytics capabilities has never been higher, but organizations' immature data and analytics governance is preventing them from reaping the benefit of data investments and is introducing new information risk.	1. Ineffective Data and Analytics Organizational Models 2. Insufficient Data Sharing Enablement and Controls	1. Ineffectiveness of Historical Data for Predictive Models 2. Slow Implementation of Advanced Analytics Due to Poor Data Quality
Digital Business Transformation	Organizations accelerated their digital business transformations by years during the pandemic and plan to continue investing heavily in transformation efforts. As they adopt new advanced analytics and business intelligence initiatives under increasingly fragmented digital strategies, they become exposed to regulatory risk and to pressures from competitors with more comprehensive digital strategies.	1. IT-Business Digital Divide 2. Regulatory Risks to Digital Capability Building	Not a 2021 Hot Spot
IT Governance	IT environments are still reeling from changes introduced quickly during the pandemic, and they need to be modernized to support business strategy.	1. Increased Technical Debt 2. Cloud Modernization Delays	1. Rapid Adoption of New Technologies 2. Access Management Challenges

Audit Plan Hot Spots Summary (continued)

Audit Plan Risk Areas	Summary	2022 Drivers	2021 Drivers
Third Parties	COVID-19 and its aftermath exposed organizations' reliance on third parties and revealed the need to reexamine how they are reflected in organizations' risk registers and controls. Organizations struggle to achieve adequate oversight of third parties due to limited risk management processes and a lack of knowledge regarding data third parties have access to. **This is an evolution of last year's third-party management hot spot.**	1. Limited Third-Party Risk Monitoring 2. Unsupervised Privileged Access	1. Third-Party Continuity and Viability Challenges 2. Insufficient Third-Party Due Diligence
Business Continuity and Organizational Resilience	Increasing cyberattacks, pandemic disruptions, operational resilience regulations and the accelerating climate crisis are highlighting the need for organizations to move beyond business continuity and focus on organizational resilience. Otherwise, they risk financial exposure, long-lasting operational challenges and potential legal repercussions. **This is an evolution of last year's business continuity and disaster recovery hot spot.**	1. Climate Degradation 2. Regulatory Interest in Operational Resilience	1. Fragmented Ownership of Business Continuity Management 2. Outdated Business Continuity Planning Processes
Environmental, Social and Governance	Rising investor commitment to ESG and increased regulatory action on ESG means organizations must incorporate ESG into their strategies and build sound governance over their ESG programs. **This is an evolution of last year's corporate responsibility hot spot.**	1. Increasing Capital Tied to ESG Performance 2. Increased Legal and Regulatory Action on ESG	1. Slow Progress on Diversity and Inclusion 2. Inadequate Consideration of Climate Change Impact
Supply Chain	The scale of the pandemic and new COVID-19 variants, a global shortage of key goods and materials, and heightened supply chain disruptions are causing logistical challenges that are increasing organizations' costs and extending their recovery.	1. Key Goods and Materials Shortages 2. Logistics and Shipping Challenges	1. Challenges in Shifting Supply Chain Strategies 2. Cyberattacks Resulting From Supply Chain Digitalization

Audit Plan Hot Spots Summary (continued)

Audit Plan Risk Areas	Summary	2022 Drivers	2021 Drivers
Strategy Execution	The pandemic-driven imperative to accelerate digital strategies led organizations to seek to rapidly add strategic capabilities. However, their successful execution is challenged by change fatigue, lack of goal alignment and legacy operating models, increasing the risk of losses in market share and competitive position.	1. Change Fatigue 2. Slow Operating Model Evolution	Not a 2021 Hot Spot
Workforce Management	Organizations are struggling with employee well-being, engagement and retention as they face a new normal with employees in different working models (i.e., in-person, hybrid, remote) and difficulties knowing how to manage COVID-19 in the workplace. **This is an evolution of last year's total workforce management hot spot.**	1. Cultural Disconnects in a Hybrid Workforce 2. COVID-19 Workplace Management Uncertainty	1. Complexities of Managing Diversified Work Arrangements 2. Rigid Human Resource Processes
Retention and Recruitment	Increasing employee demands for work flexibility along with very hot labor markets in some economies are testing organizations' ability to attract and retain the staff they need to deliver on strategic goals. **This is an evolution of last year's talent resilience hot spot.**	1. Hot Talent Market 2. New Employee Expectations	1. Declining Employee Well-Being 2. Digital Skills Gaps
Economic Uncertainty	New inflation expectations, COVID-19 variants and the vast global differences in terms of economic recovery are leading to especially high economic uncertainty. **This is an evolution of last year's corporate financial management hot spot.**	1. Heightened Inflation Uncertainty 2. Variances in the Global Economic Recovery	1. Liquidity Crunch 2. Increased Incidences of Credit Default

Audit Plan
Risk Areas (Excerpt)

Retention and Recruitment

As organizations lift their pandemic-lockdown-induced hiring freezes, they are struggling to attract and retain talent to fulfill current and planned staffing needs.[172] In the U.S., the ratio of job openings to hires reached historically high levels in May and June 2021, and in the EU, unemployment has been dropping rapidly.[173] Currently, 55% of workers neutral on engagement (neither engaged nor disengaged) are actively looking for new employment or watching for openings, and even among engaged employees, that number is 30%.[174]

Morale, a key factor in retention and recruitment, is divergent among leadership and employees: While 61% of leaders say they're thriving right now, only 39% of those in nonmanagerial roles do.[175] Many organizations are in a strategically important time, coming out of COVID-19, and failing to attract and retain employees will mean challenges to deliver on strategy for years to come.

1. Hot Talent Market

Almost two years into the COVID-19 pandemic, employees who were waiting for the pandemic to subside are now switching jobs at record levels, leaving organizations struggling to fill vacancies.[176] In April 2021, the U.S. quit rate reached 2.8% — the highest level ever recorded.[177] Around the same time, the number of available U.K. workers also reached its lowest level since 1997.[178] Workers say they are leaving firms for higher wages and career advancement, but almost as many cite dissatisfactory working conditions such as a lack of flexibility.[179] As such, organizations need to both offer employees opportunities for greater tangible rewards and raise employee satisfaction with initiatives such as increasing recognition or offering more flexible working arrangements.[180] Organizations that fail to adequately adjust their employee value proposition and otherwise be responsive to the evolving labor market may face especially high succession and turnover risk.[181]

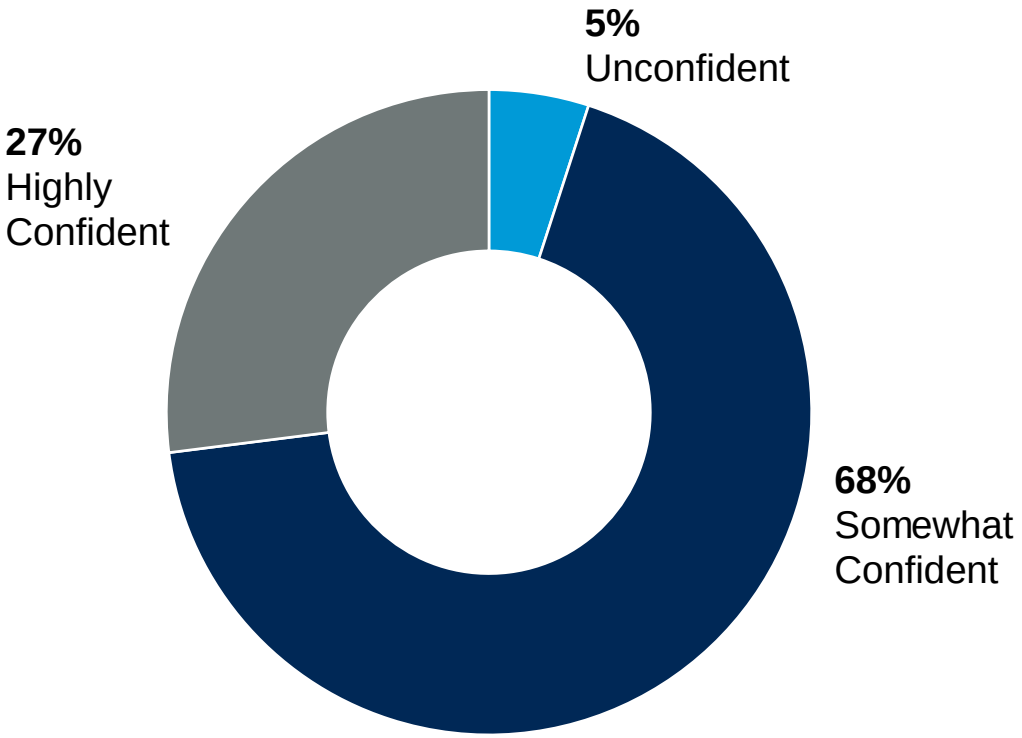
2. New Employee Expectations

Understanding and adapting to new employee expectations provides an especially acute challenge to organizations during a time of increased change and a tight labor market.[182] Employees increasingly prefer to work at organizations that align with their desired work-life balance and working preferences, requiring changes to many workforce plans.[183] This may mean maintaining the more flexible working arrangements brought on by COVID-19.[184] Eighty-four percent of employees believe flexible working arrangements are better suited to support their physical, mental and financial well-being, and 54% would consider changing jobs if they are not afforded the same flexibility in the future.[185] Leaders, however, struggle to understand employees' vision for flexibility.[186] Seventy-five percent of executives think their organization embraces flexible work, but only 57% of individual contributors agree.[187] Organizations that fail to meet employees' vision for a new working model risk failing to attract and retain the best talent.[188]

Retention and Recruitment (continued)

Confidence in Audit's Ability to Provide Assurance Over Retention and Recruitment Risk

Percentage of Respondents

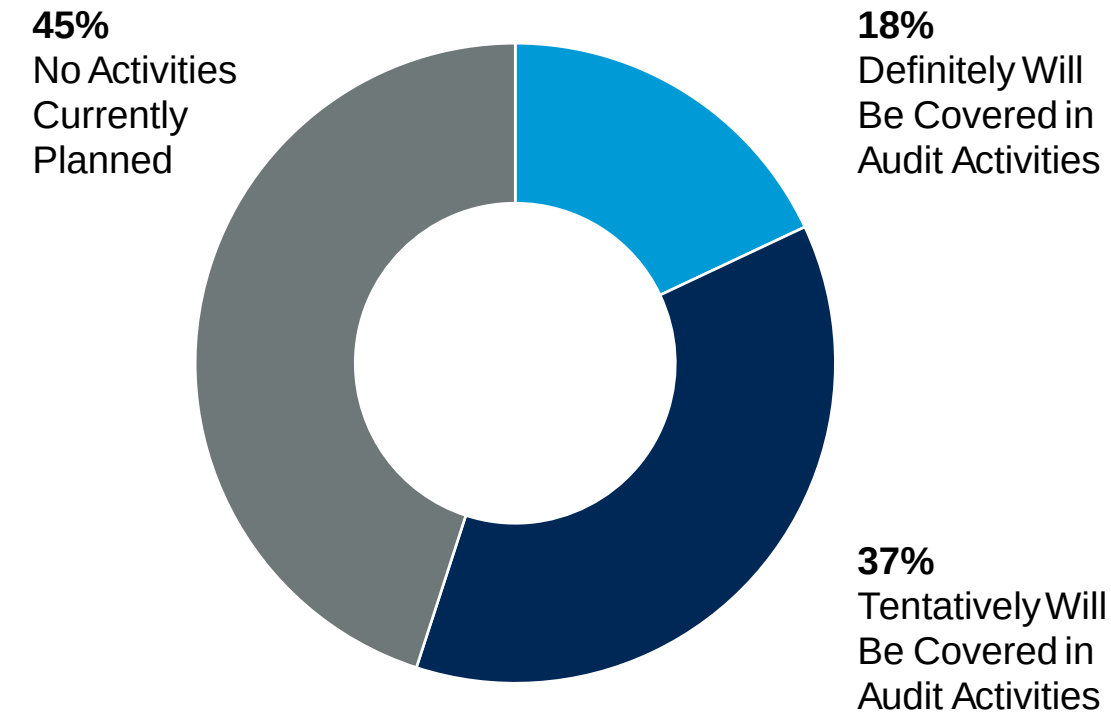


n = 151

Source: 2022 Gartner Audit Key Priorities and Risks Survey

Plans to Cover Retention and Recruitment in Audit Activities in the Next 12-18 Months

Percentage of Respondents



n = 159

Source: 2022 Gartner Audit Key Priorities and Risks Survey

Retention and Recruitment (continued)

2022 Recommendations for Audit

- **Review Employee Engagement Processes.** Examine how the organization measures and responds to varying levels of employee commitment and connection to the organization. Review how management identifies critical and at-risk talent groups and assess the effectiveness of retention strategies on the most critical employees.
- **Review How the Organization Assesses Changing Workforce Expectations.** Determine whether a process exists to assess changing employee expectations and see how often they are reassessed. Review the extent to which managers and leaders listen to employee preferences and see whether managers and leaders can adjust policies as needed based on ongoing feedback from different groups of employees or varying geographies.
- **Assess the Effectiveness of Retention Efforts.** Evaluate whether retention efforts effectively reduce turnover in critical or difficult-to-replace positions. Determine whether the organization monitors industry incentives and turnover trends in comparable roles and see how often the organization completes this review.
- **Assess the Effectiveness of Recruitment Efforts.** Determine where in the recruiting process the organization faces the most challenges or lost candidates. Review peer benchmarking to determine how current recruitment processes align with those of industry peers.
- **Assess Benefits Development Process.** Evaluate processes used to ensure alignment of existing benefits and well-being programs with employee needs. Verify all changes in plan provisions are effectively communicated to employees and consistent metrics or indicators to track utilization are employed to determine necessary adjustments.

Additional Gartner Resources

- Executive Pulse: The 4 Corporate Functions Facing the Most Turnover Risk
- Assess These 4 Threats to Measure "New Normal Era" Retention and Recruitment Risk
- Redesigning Work for the Hybrid World
- 6 Key Gaps Between Leader and Employee Sentiment on the Future Employee Experience
- Benchmarking Employee Turnover Trends and Mitigation Strategies With HR Leaders

Retention and Recruitment (continued)

Questions for Management

- What gaps currently exist between the skills available in the organization and those necessary to successfully execute strategic plans?
- In which part of the business do you see the greatest risk of employee attrition?
- How do you assess employees' attitudes and engagement levels within the organization?
- How do you determine when your remote employees are overworked?
- What common themes have you heard in exit interviews as to why employees are leaving?
- How do current company offerings regarding flexibility align with stated employee desires?
- How do you benchmark your organization's benefits against peers?
- How are you communicating workplace flexibility expectations to the workforce?
- How have encouragement efforts to retain employees changed over the past year?
- How have you adapted training and development plans to cover employee desires and organizational skills needs?

Key Risk Indicators

- Increase in attrition rate
- Increase in incidents of absenteeism
- Trends in remote employee engagement
- Rate at which roles in different parts of the organization are filled
- Turnover rate among key positions
- Offers accepted as a percentage of offers extended
- Average time needed to fill a position
- Number of new-hire terminations
- Well-being offerings utilization levels
- Number of applicants for each external hire

Strategy Execution

Executives believe pandemic-driven shifts in everything from demand patterns and delivery models to working arrangements will change the way their organizations do business over the next five years.[134] As a result, digital transformation efforts have significantly accelerated, and 67% of CEOs are aiming to redesign their businesses.[135] Despite increased uncertainty and large-scale change, nearly three in four executives view the COVID-19-spurred changes as a growth opportunity, and 78% of organizational leaders say the building of strategic capabilities, such as new ways to develop and deliver products and services, is now more important than before the pandemic.[136]

However, less than a quarter of executives believe their organizations have the expertise, resources and commitment to pursue new growth strategies successfully.[137] While senior leaders are increasingly emphasizing the speed of strategy execution, too often the development of operating model capabilities lags, significantly reducing the likelihood of achieving growth objectives.[138] Failing to develop an organized approach to building required capabilities to execute new strategies, or doing so too slowly, risks market share losses, strategic initiative failure and wasted investments.[139]

1. Change Fatigue

Change fatigue can significantly limit organizations' abilities to build new capabilities, and organizations have already made much change in the COVID-19 era.[140] Since COVID-19, employees have adapted to a formidable array of changes to their work (and outside of work), including new workflows for remotely collaborating with peers, new tools to enable digital operations, new business initiatives and more. Employees indicate that such day-to-day changes like remote collaboration and workflows involving new tools create 2.5 times as much burden as general organizational change.[141] As such, employees in 2020 said that they were half as prepared to absorb change before getting fatigued as did employees in 2019.[142] This has lasting implications for strategy execution, as 34% of fatigued employees admit to actively resisting or undermining change, as opposed to only 10% of non-fatigued employees.[143] Given that the success rate of long-term strategic initiatives generally is below 70%, and given the amount of change in which organizations plan to invest, organizations that fail to consider feasibility and employee-oriented change management strategies may risk failed transitions to new strategic initiatives.[144]

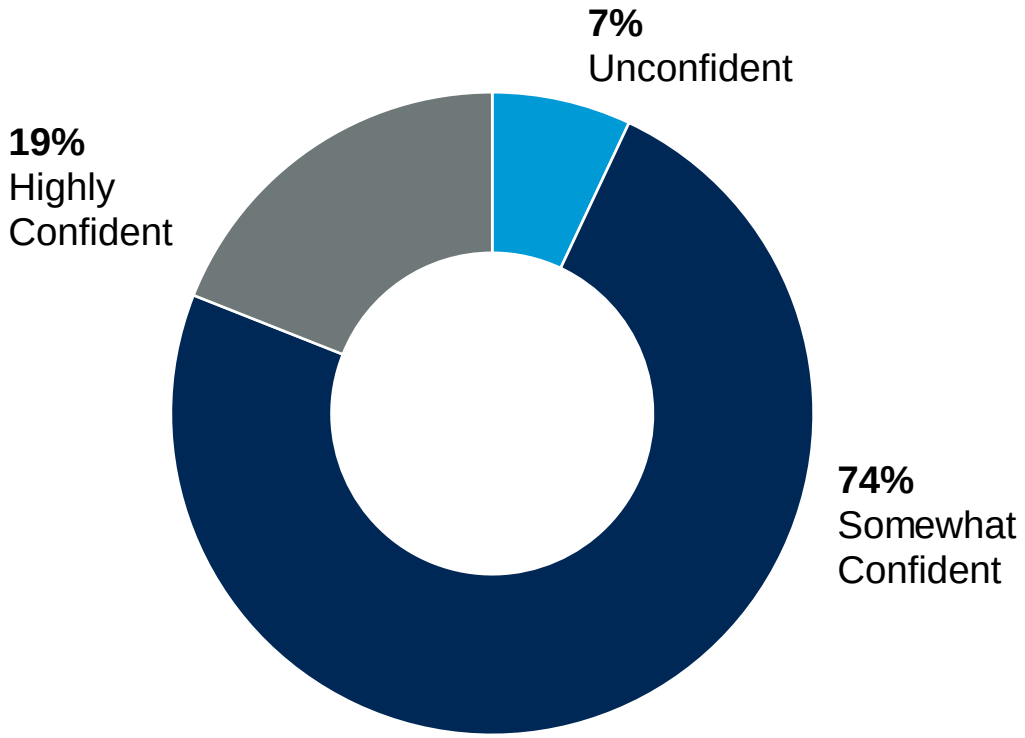
2. Slow Operating Model Evolution

Only 28% of corporate strategy leaders believe their organization develops capabilities fast enough to respond to market changes.[145] Particularly, organizations fault their operating models as a primary culprit.[146] Sixty-two percent of organizations say their inability to evolve their operating models inhibits their ability to develop new strategic capabilities, while 74% of executives report needing to completely rethink their operating models so they are more resilient in the current environment.[147] Ninety-three percent of executives go as far as saying their organization's very existence could be jeopardized by operating models that can't keep pace with strategic initiatives.[148] Particularly, organizations point to the importance of models that can sense strategy execution risks early and adjust more rapidly.[149] Only 6% of organizations say they consistently respond to risks before they have a material impact on execution.[150] Organizations that fail to adapt their operating models to support new goals and capabilities stand to lose out on the profitable growth that organizations with agile operating models can unlock.[151]

Strategy Execution (continued)

Confidence in Audit's Ability to Provide Assurance Over Strategic Change Management Risk

Percentage of Respondents

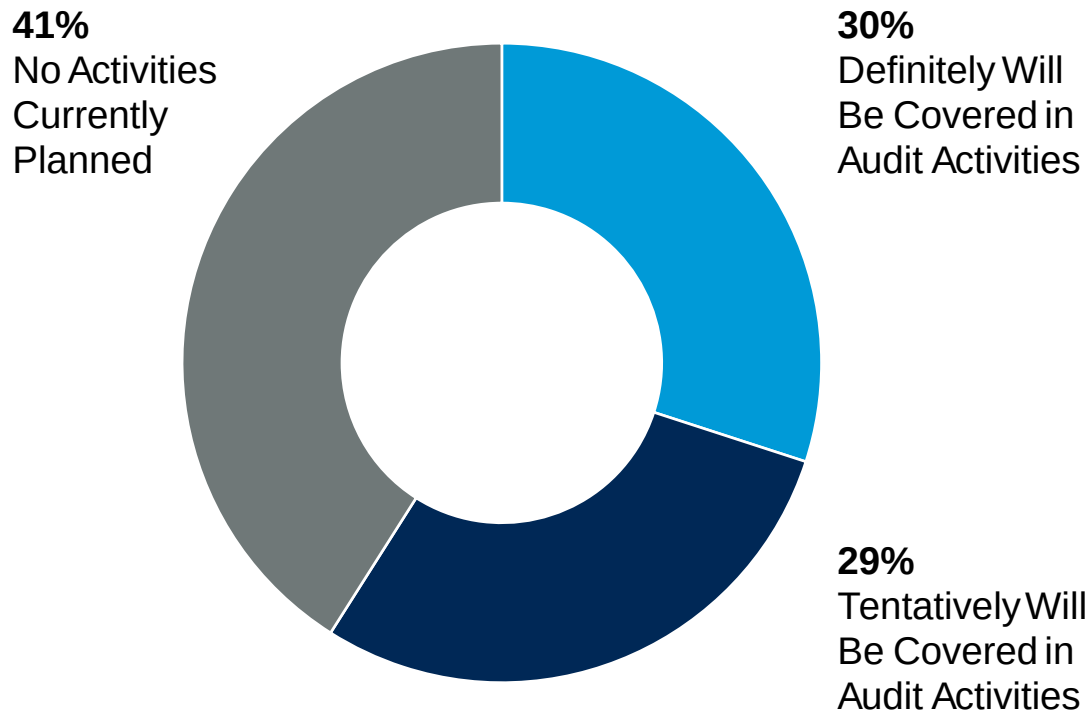


n = 151

Source: 2022 Gartner Audit Key Priorities and Risks Survey

Plans to Cover Strategic Change Management in Audit Activities in the Next 12-18 Months

Percentage of Respondents



n = 159

Source: 2022 Gartner Audit Key Priorities and Risks Survey

Gartner®

Strategy Execution (continued)

2022 Recommendations for Audit

- **Review Change Fatigue Monitoring Efforts.** Assess management's efforts to monitor levels of change fatigue, protocols for communicating change to employees and protocols for proactively involving employees in change management and implementation.
- **Review Employee Engagement Assessments.** Assess practices for identifying and responding to signs of employee disengagement. Evaluate the frequency of engagement surveys and how remote work may necessitate more frequent surveys. Ensure results are documented and action plans exist to address signs of employee disengagement.
- **Assess Operating Model Governance.** Review the governance structure around managing and updating the organization's operating model. Assess how management factors operating model adjustments into strategy formulation and strategy execution.
- **Review Learning and Development Programs Related to Change Management Efforts.** Review the existence of training related to key organizational changes and restructuring. This includes programs related to building skill sets for new business opportunities as well as training related to introducing employees to major changes in the organization.
- **Assess the Quality of Strategy Execution.** Review the status and governance of critical strategic projects, including the number of project delays, where delays most commonly occur and the success of remediation efforts. Evaluate the presence and effectiveness of controls for strategic planning and execution and identify potential control gaps.

Additional Gartner Resources

- Reduce Employees' Change Fatigue for a Successful Recovery
- Tactics to Address Fatigue in Times of Unprecedented Change
- Key Levers to Drive Strategy Execution Alignment
- 3 Imperatives to Capture Growth After the Pandemic
- Why Do Executives Move Forward With Strategic Initiatives Even When They See Pitfalls Ahead?

Strategy Execution (continued)

Questions for Management

- What training does the organization provide to managers and employees related to organizational changes, and how are they held accountable for completing the training?
- How do you monitor, identify and address employee change fatigue, and what preventative measures do you use?
- How do you assess the potential impact of strategic change initiatives on your employee environment?
- How do you assess your employees' motivation and engagement levels, especially for employees responsible for managing risks or controls?
- What role, if any, do employees play in change management and implementation?
- How are operating model considerations factored into strategy formulation and execution?
- What percentage of strategic projects are progressing according to plan, moving faster than planned and moving slower than planned?
- How do you determine if and when a change initiative should be terminated or adjusted?
- Who owns the governance over building new strategic capabilities?
- How are staff working on digital initiatives trained on the risk implications of their projects?

Key Risk Indicators

- Percentage of managers and employees completing change management training
- Number of active change initiatives
- Percentage of employees reporting change fatigue
- Trends in the results of employee engagement surveys
- Percentage of projects meeting ROI goals
- Average time needed to develop a product or service
- Percentage of strategic projects currently in progress that are delayed
- Number of actual versus targeted days to execute capability-building projects
- Frequency of reviews of organizational capabilities to execute strategic change initiatives as assessed by executives involved in strategy formulation
- Frequency of updates to plans to overhaul enterprise capabilities that are material to new strategy execution

Environmental, Social and Governance

Stakeholder pressure on ESG management has continued driving organizational urgency to demonstrate and document meaningful progress.[102] Stakeholders increasingly demand organizations provide evidence of ESG progress in the form of tangible data and other verifiable proof, creating risks for organizations both in selecting and reporting ESG metrics.[103] Investors are increasingly incorporating ESG data into their investment analyses and decision-making processes.[104] Global regulators are also responding to calls for stronger ESG regulation from consumer groups and others that want clear, consistent ESG rules or standards.[105]

Consumers and employees have also indicated they will end relationships with organizations that have poor ESG records.[106] Organizations with lagging ESG management and disclosure will face increasing regulatory, operational and financial repercussions.

1. Increasing Capital Tied to ESG Performance

Increasing investor pressure on organizations to demonstrate ESG progress has led to increased capital being tied to ESG performance.[107] Over the past two years, the number of institutional investors committed to investing responsibly more than doubled.[108] In the first half of 2021, creditors issued approximately $350 billion worth of sustainability-linked loans (which adjust interest rates according to ESG performance), up from $197 billion in all of 2020.[109] Many organizations, however, struggle to demonstrate their ESG credibility to investors, creditors and others, both because of uncertainty over what to disclose due to the lack of universal standards as well as uncertainty over how to measure and prove ESG metrics.[110] Many investors, weary of "greenwashing" or other superficial efforts, and skeptical of the validity of organizations' ESG progress, are calling for external assurance over ESG data.[111] An inability to improve and validate metrics that demonstrate ESG progress may make firms less attractive — for investors and creditors, potentially limiting access to capital and inclusion in ESG funds, portfolios and exchanges — or otherwise pose reputational risks.

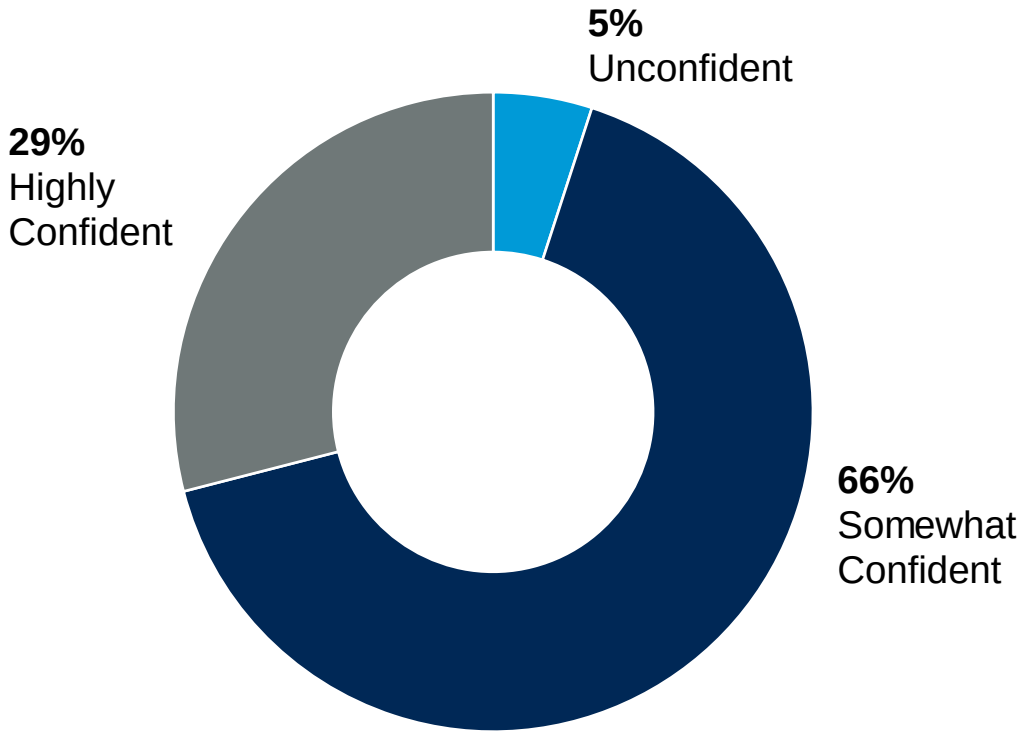
2. Increased Legal and Regulatory Action on ESG

Global legal and regulatory action on ESG is increasing, pushing organizations to set emissions reduction targets and report standardized ESG data.[112] This has taken the form of legal action in some cases. In May 2021, a Dutch court ruled that Shell must reduce global carbon emissions by 45% by 2030 compared with 2019 out of a duty of care to the citizens of the Netherlands.[113] Further, recent rulings from U.S. federal judges have halted fossil fuel extraction projects based upon climate impacts, and U.S. President Biden announced plans to enhance regulation of key industries to achieve emissions reduction targets.[114] Regulators are also accelerating the creation, monitoring and enforcement of ESG reporting standards.[115] The EU has proposed a new Corporate Sustainability Reporting Directive (CSRD) that will require most public and large companies to disclose on strategy, governance, resilience, material information and processes for selecting material topics, forward-looking information, and more beginning in 2023.[116] In the U.S., regulators convened a task force to monitor ESG reporting and identify material gaps or misstatements in the disclosure of climate risks, initially under existing rules.[117] Organizations that fail to reduce emissions and comply with increasing ESG reporting requirements could face increased operational shutdowns, costly projects to meet enhanced regulator standards, regulatory fines and legal actions.[118]

Environmental, Social and Governance (continued)

Confidence in Audit's Ability to Provide Assurance Over ESG Commitment and Reporting Risk

Percentage of Respondents

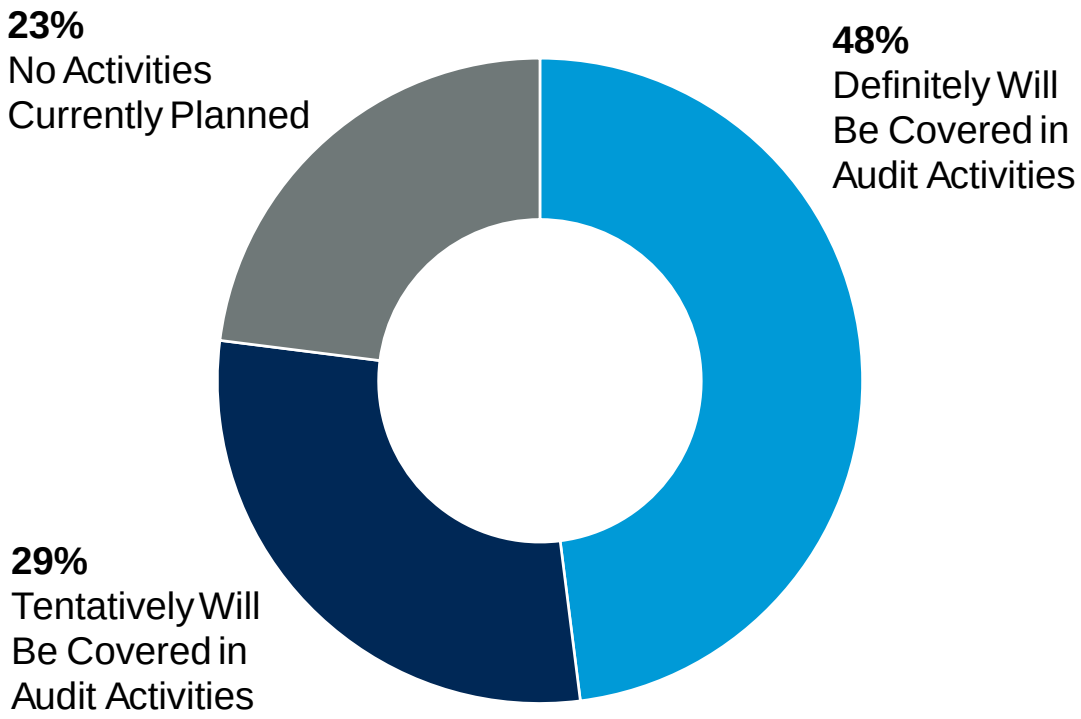


n = 151

Source: 2022 Gartner Audit Key Priorities and Risks Survey

Plans to Cover ESG Commitment and Reporting in Audit Activities in the Next 12-18 Months

Percentage of Respondents



n = 159

Source: 2022 Gartner Audit Key Priorities and Risks Survey

Environmental, Social and Governance (continued)

2022 Recommendations for Audit

- **Review and Benchmark the Sustainability Plan.** Review management efforts to define sustainability goals, actions and timetables. Assess the sustainability plan's balance between reasonableness and ambition, taking into account industry sector, relevant international agreements (e.g., the Paris Agreement), third-party contributions, organizational strategy, regulator requirements, investor demands and employee input. Compare sustainability commitments against the plans and progress of industry peers, including their ESG ratings, project initiatives and sustainability targets.
- **Review Sustainability Progress.** Evaluate the plans established to achieve the defined goals, the involvement of appropriate subject matter experts in reviewing the specific goals and actions and executive leadership's responsibility to deliver. Review the governance over the projects and activities to achieve the goals together with the process to update goals and targets. Evaluate the information provided on the organization's current progress toward defined and published sustainability targets.
- **Review ESG Reporting Progress.** Assess the organization's adherence to established frameworks and standards for reporting on sustainability, DEI and other ESG metrics to regulators, investors and the public. Ensure the relevant departments follow regulatory developments and that the business keeps pace with regulatory and compliance risk.
- **Review ESG Data Governance, Collection and Reporting.** Evaluate the governance of management's selection and tracking of ESG metrics. Assess decisions on the necessity and reliability of data, efficiency of collection, aggregation, consistency across the organization, and access to third-party data. Assess whether audit can conduct the audits needed or if the organization needs to use a third party for an ESG audit based on peer benchmarking, regulatory standards and investor guidance.
- **Assess ESG-Related Operational Risk.** Assess management's access to information and advice on ESG-related operational risks to current and planned products, projects, processes and facilities based on global and local regulatory developments, government action, investor demands, media commentary and changing compliance requirements.

Additional Gartner Resources

- The State of ESG Disclosures
- Audit's Role in Supporting and Assuring ESG
- Standardizing Climate Risk Reporting in ESG Disclosures
- A Guide to Understanding ESG Ratings and Setting Long-Term ESG Strategy Plans
- Craft Your ESG Reporting Using These 4 Frameworks

Environmental, Social and Governance (continued)

Questions for Management

- What methods do you use to measure the organization's carbon footprint?
- What internal controls, policies and personnel does the organization have in place to accurately track and disclose climate, sustainability and other ESG information?
- What are your plans for adjusting operations, product and service offerings to reach your carbon emission reduction goals by specified dates, and what is the governance structure for these plans?
- What are investors' and stakeholders' expectations around the tracking and disclosure of climate risk data, and is the information needed by investors disclosed?
- What steps are you taking to prepare for heightening ESG regulations and reporting requirements?
- What is the governance structure used for tracking ESG data (e.g., carbon emissions)?
- Who is responsible for verifying ESG data and metrics?
- What process do you use to verify ESG metrics, and has there been a change in the difficulty of verifying metrics?
- What technology investments are you planning to improve sustainability metrics?
- How is ESG incorporated into strategic project planning and product design and development?

Key Risk Indicators

- Change in ESG rating score from external ESG rating agencies
- Percentage of carbon-free energy use
- Number of relevant environmental disclosure laws and regulations
- Level of environmental and social disclosures compared with industry peers
- Percentage change in water usage per unit
- Number of investor inquiries about ESG
- Number of requests for ESG data verification
- Percentage of completion of ESG goals
- Percentage of ESG metrics verified
- Change in number of ESG reporting requirements

Ransomware

Ransomware attacks have become increasingly prevalent and sophisticated, and have become a top concern to boards and management.[1] Most board directors now say cybersecurity is almost always on the board agenda, with ransomware becoming a growing concern.[2] Over a third of organizations experienced ransomware attacks already last year, and this year, the number of global ransomware attacks has risen by 57%.[3] Increasingly effective extortion tactics are leading to higher costs, extending beyond the ransoms paid.[4] Considering downtime, technology-related costs, opportunity costs and the ransoms themselves, the average ransomware attack recovery costs doubled in 2021.[5]

Worse, only 8% of organizations received all their data back even after paying the ransom.[6] Despite the threat, only 50% of information security professionals believe their organization can repel a ransomware attack, and only 39% of organizations successfully stopped attacks before hackers encrypted their data.[7] Failing to prevent, detect, mitigate and respond to ransomware increasingly poses not only downtime and financial risks, but also information and reputational ones.[8]

1. Proliferating Ransomware Attacks

The ransomware industry's evolution is increasing the scale of the ransomware problem as the delivery model changes.[9] Ransomware attacks are easier than ever to carry out, and cybercriminals now specialize in different aspects of ransomware attacks.[10] The "Ransomware as a Service" model provides ransomware kits to cybercriminals that only specialize in attacks (including support forums, user reviews and feature updates).[11] This model now accounts for 64% of all ransomware attacks.[12] This increases the breadth of the ransomware threat, while the decentralized nature of attacks also makes them harder to track.[13] Regardless of their size or revenue, organizations should assume they will be targeted with ransomware, and they should examine their prevention, detection, mitigation and response measures.

2. Evolving Ransomware Extortion Strategies

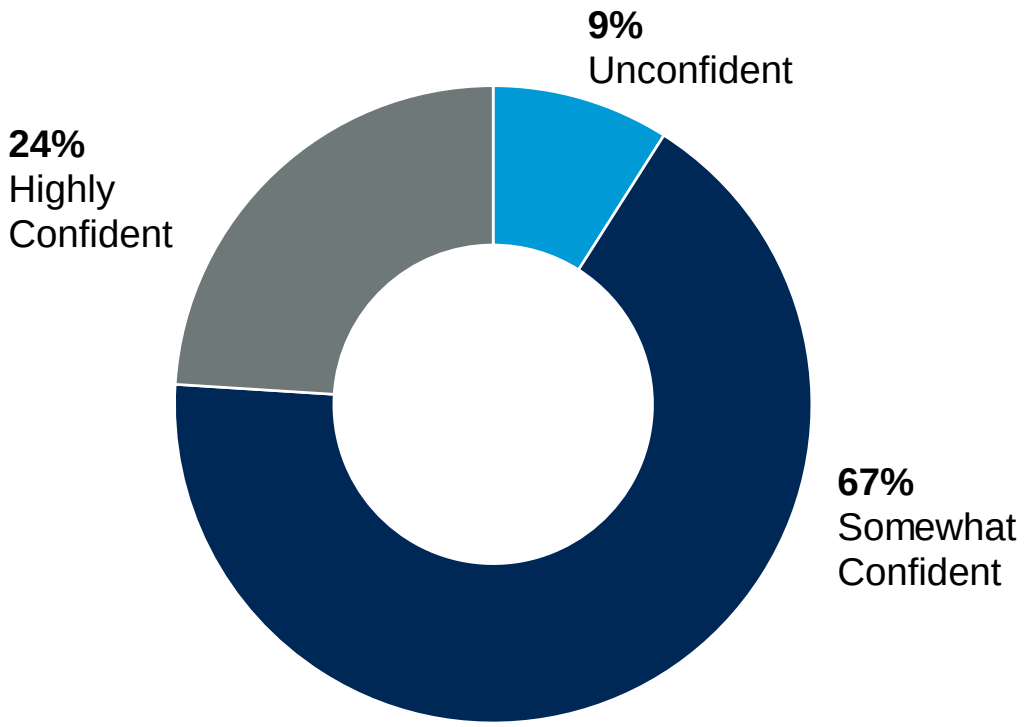
Cybercriminals are going to great lengths to ensure payments from their ransomware attacks by raising the level of consequences among ransomware victims. As many governments are warning against and even considering prohibiting paying ransoms, potentially causing some organizations to be more reluctant to pay, cybercriminals are adding new tactics to their portfolio of extortion strategies.[14] This includes increasingly sophisticated ransomware extortion strategies, such as attacks that use third parties as vectors, "fileless" attacks and others that are harder to detect, demands for separate ransoms for data and unlocking systems, or demands of ransoms from multiple parties such as a hacked organization and its customers.[15] Attacks that target and infect a trusted partner, like a software vendor or service provider, allow for further consequences as seen with the Kaseya attack that resulted in encrypted data at up to 1,500 additional businesses.[16] Additionally, cybercriminals have realized that by threatening to release stolen personal data, customers will put pressure on organizations to pay ransoms.[17] As an extra measure, some cybercriminals are also employing distributed-denial-of-service attacks, which overwhelm and disrupt company operations, and locking and threatening to leak or destroy data.[18] Failure to act on ransomware is resulting in data loss, reputational damage among customers and other increasingly difficult-to-predict consequences.

Gartner®

Ransomware (continued)

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

Percentage of Respondents

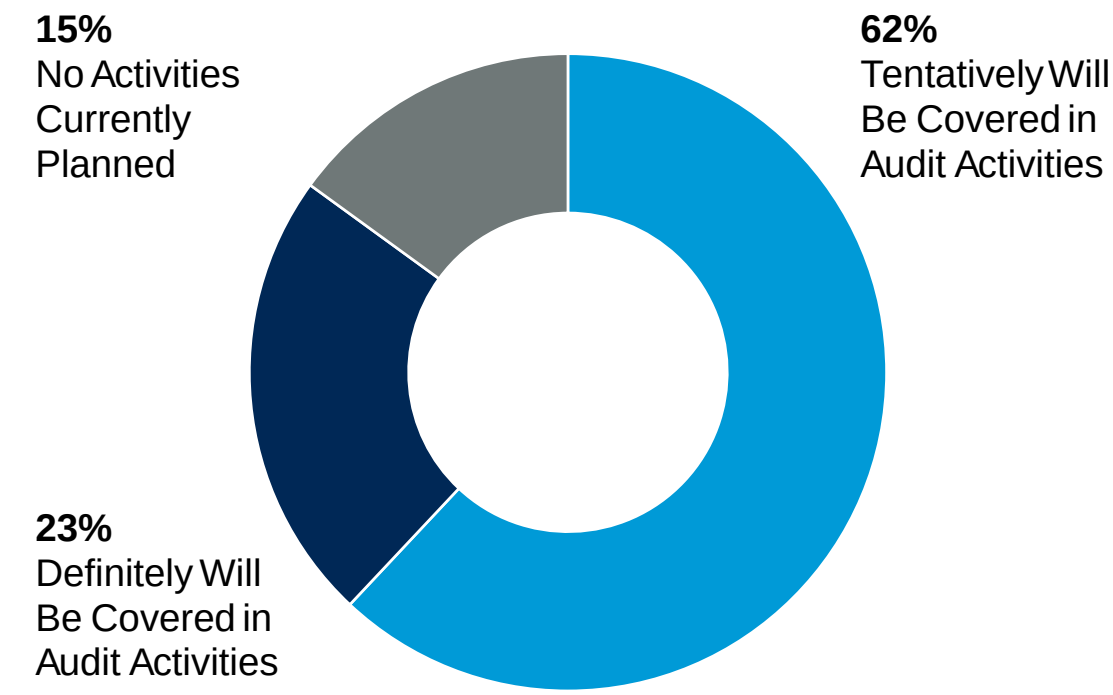


n = 151

Source: 2022 Gartner Audit Key Priorities and Risks Survey

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

Percentage of Respondents



n = 159

Source: 2022 Gartner Audit Key Priorities and Risks Survey

Ransomware (continued)

2022 Recommendations for Audit

- **Evaluate Employee Security Training.** Assess the effectiveness of security awareness and training programs, specifically social engineering and phishing tests. Review the number of employees who have taken and passed training and how often it is required. Make sure the training includes education and awareness of the most up-to-date ransomware threats and adequate guidance on securing devices in both in-office and remote environments.
- **Assess External Relationships for Ransomware Support Services.** Determine whether the organization has an appropriate level of external support services (such as incident response retainers). Review the expertise these support services provide and see whether the expertise properly compliments the services the organization can provide in-house. Ensure the organization has a plan detailing when to contact each service provider in the event of a ransomware attack.
- **Review Ransomware Attack Response Plans.** Assess whether the organization's ransomware response plan includes mitigation, communication, recovery and resolution strategies. These strategies should align with organizational priorities and establish clear processes to respond to an attack. Assess whether plans include defined roles and responsibilities throughout the organization, particularly beyond IT.
- **Assess Data Storage Policies.** Review policies that govern data storage, including the protection, retention and deletion of organizational data. Review the process by which management decides which data and assets are most important to protect and who is responsible for protecting them. Make sure business units have sufficient security controls in place for data that could be used in a double- or triple-extortion attack.
- **Review Service Provider Ransomware Attack Communication Protocols.** Evaluate whether relevant functions have investigated contractual reporting requirements for when and how a service provider will communicate information regarding an attack. Determine whether the service provider's response plan is in line with the organization's internal response plan.

Additional Gartner Resources

- Respond to Ransomware With More Than IT
- The SolarWinds Orion Breach and Enterprise Risk Management: A Pragmatist's Guide
- Board Briefing: Protection Against Cyber Extortion and Ransomware
- Ransomware Payments: How to Assess Emerging U.S. Legal Risks
- When Employees and Third Parties Work Remotely: Privacy and Security Risks

Ransomware (continued)

Questions for Management

- What protocols are in place for responding to ransomware attacks?
- Who in the organization is responsible for responding to ransomware attacks?
- How often does the organization perform ransomware tabletop exercises?
- What organizational data could be used for extortion?
- What are the profiles of employees who fail phishing tests?
- How is cybersecurity training differentiated for employees who work remotely?
- Have you mapped out how clients or customers could be impacted by a ransomware attack?
- What insight does the organization have on how critical third parties address cybersecurity and ransomware threats?
- What type of nonpublic data (e.g., customers, employees) can third parties access, and how much reputational or financial damage would this data create if released?
- What controls are in place to protect backup systems from malware infection?

Key Risk Indicators

- Average attack dwell time
- Trends in failure rates for employee information security training
- Frequency of review of organizationwide information security training
- Year-over-year growth in the number of third-party software or service providers
- Average days between patch release and patching
- Frequency of backups and testing
- Percentage of cybersecurity incidents attributed to human error
- Percentage of unmanaged devices detected on the network
- Number of ransomware-related incidents reported by industry peers in last 12 months
- Volume of traffic originating from unknown IP addresses

Appendix

Endnotes

Retention and Recruitment

[172] Millions of Jobs and a Shortage of Applicants. Welcome to the New Economy, CNN Business; The Labor Market May Be Tighter Than the Level of Employment Suggests, Federal Reserve Bank of Dallas; Eurozone Unemployment Is Rapidly Declining as Economies Reopen, ING.

[173] U.S. Job Openings Surge to New Record High, Hiring Increases, Reuters; Unemployment Statistics, Eurostat.

[174] U.S. Employee Engagement Holds Steady in First Half of 2021, Gallup.

[175] The Next Great Disruption Is Hybrid Work — Are We Ready? Microsoft.

[176] Shelter in Job? For 74% of the U.S., That Cautious Path Feels Right in 2021, LinkedIn; 'I Quit': Workers Change Jobs at a Record Pace Amid Burnout, New Openings with Higher Pay, USA Today.

[177] States Where Americans Are Quitting at the Highest Rates, U.S. News & World Report.

[178] UK Employers Struggle With Worst Labour Shortage Since 1997, The Guardian.

[179] UK Employers Struggle With Worst Labour Shortage Since 1997, The Guardian.

[180] How Recognition and Rewards Can Increase Retention and Engagement, PayScale.

[181] Despite High Unemployment, Companies Still Struggling With Employee Turnover, Express Employment Professionals.

[182] The Next Great Disruption Is Hybrid Work – Are We Ready? Microsoft; Talent Accelerator: The Forces That Are Shaping the New Working World, Citrix; Managing Talent Risks in a Tightening Labor Market, Risk Management.

[183] The Next Great Disruption Is Hybrid Work – Are We Ready? Microsoft; Robert Half Research Points to Strong Job Optimism Among U.S. Workers, Robert Half.

[184] Talent Accelerator: The Forces That Are Shaping the New Working World, Citrix.

[185] Talent Accelerator: The Forces That Are Shaping the New Working World, Citrix; More Than Half of Employees Globally Would Quit Their Jobs If Not Provided Post-Pandemic Flexibility, EY Survey Finds, EY.

[186] 2021 Gartner Hybrid Work Employee Survey

[187] 2021 Gartner Hybrid Work Employee Survey

[188] Managing Talent Risks in a Tightening Labor Market, Risk Management.

Endnotes

Environmental, Social and Governance

[102] The High Stakes (and Critical Stakeholders) of ESG, Workiva; Gartner (2021)

[103] The High Stakes (and Critical Stakeholders) of ESG, Workiva; Gartner (2021)

[104] MSCI Investment Insights 2021, MSCI.

[105] Investors, Companies, Organizations Call on U.S. Securities and Exchange Commission to Mandate Corporate Climate Disclosure, Ceres; Tech Companies Join Calls for Disclosure Mandate to Meet U.S. Emissions Goals, CQ Roll Call; Investors Call for Urgent Action by Steelmakers on Carbon Emissions, Reuters.

[106] Beyond Compliance: Consumers and Employees Want Business to Do More on ESG, PwC; 2021 Gartner EVP Employee Survey; 2020 Gartner Civic and Social Engagement in the Workplace Survey

[107] Investors Call for Urgent Action by Steelmakers on Carbon Emissions, Reuters; Global Investors Driving Business Transition, Climate Action 100+.

[108] Investors Call for Urgent Action by Steelmakers on Carbon Emissions, Reuters; Global Investors Driving Business Transition, Climate Action 100+.

[109] How ESG Scores Can Affect the Cost of Credit, GreenBiz Group; Sustainability-Linked Loan Supply Outpaces Green Bonds and Loans Amid US Surge, S&P Global; Junk Firms Are Posing as Green Warriors to Reduce Debt Costs, Bloomberg. (Paid subscription required.)

[110] ESG Impact Is Hard to Measure — But It's Not Impossible, Harvard Business Review. (Paid subscription required.); What's Really Behind Corporate Promises on Climate Change? The New York Times (Paid subscription required.); Can the Market Save the Planet? FedEx is the Latest Brand-Name Firm to Say It's Trying, The Washington Post. (Paid subscription required.)

[111] Junk Firms Are Posing as Green Warriors to Reduce Debt Costs, Bloomberg. (Paid subscription required.)

[112] #DeloitteESGnow — The ESG Regulatory Whirlwind: Accountability on the Horizon, Deloitte.

[113] Shell Says a Court Ruling on Greenhouse Gases Will Speed Up Its Plans to Cut Emissions, The New York Times. (Paid subscription required.)

[114] #DeloitteESGnow — The ESG Regulatory Whirlwind: Accountability on the Horizon, Deloitte; As Biden Urges Global Warming Action, Courts Shape Climate Policy at Home, The Washington Post. (Paid subscription required.); FACT SHEET: President Biden Sets 2030 Greenhouse Gas Pollution Reduction Target Aimed at Creating Good-Paying Union Jobs and Securing U.S. Leadership on Clean Energy Technologies, The White House.

[115] Companies Turn to Auditors to Verify Sustainability Data, The Wall Street Journal. (Paid subscription required.)

[116] Proposed EU Directive on ESG Reporting Would Impact US Companies, Harvard Law School Forum on Corporate Governance.

[117] SEC Announces Enforcement Task Force Focused on Climate and ESG Issues, U.S. Securities and Exchange Commission.

[118] As Biden Urges Global Warming Action, Courts Shape Climate Policy at Home, The Washington Post. (Paid subscription required.); Kentucky Regulators: West Virginia Coal Plant Should Close in 2028, The Ohio Valley ReSource.

Endnotes

Strategy Execution

[134] The Consumer Demand Recovery and Lasting Effects of COVID-19, McKinsey & Company; The New Digital Edge: Rethinking Strategy for the Postpandemic Era, McKinsey & Company; Innovation in a Crisis: Why It Is More Critical Than Ever, McKinsey & Company.

[135] COVID-19 and the Future of Business, IBM; 2021 Gartner CEO and Senior Business Executive Survey

[136] Innovation in a Crisis: Why It Is More Critical Than Ever, McKinsey & Company; Rethink Capabilities to Emerge Stronger From COVID-19, McKinsey & Company.

[137] Innovation in a Crisis: Why It Is More Critical Than Ever, McKinsey & Company.

[138] 2021 Gartner Strategy Capability Development Survey

[139] The New Digital Edge: Rethinking Strategy for the Postpandemic Era, McKinsey & Company.

[140] Gartner (2021)

[141] 2019 Gartner Change Fatigue Survey; Gartner ReimagineHR Employee Survey (July 2020)

[142] 2019 Gartner Change Fatigue Survey; Gartner ReimagineHR Employee Survey (July 2020)

[143] 2019 Gartner Change Fatigue Survey

[144] 2020 Gartner Long-Term Initiative Resourcing Benchmark Survey

[145] 2021 Gartner Strategy Capability Development Survey

[146] 2021 Gartner Strategy Capability Development Survey

[147] 2021 Gartner Strategy Capability Development Survey; The Resilient Operating Model: Overcoming Corporate Bureaucracy Through People, Partners and Insight, Accenture.

[148] The Resilient Operating Model: Overcoming Corporate Bureaucracy Through People, Partners and Insight, Accenture.

[149] Gartner (2020); The Impact of Agility: How to Shape Your Organization to Compete, McKinsey & Company.

[150] 2020 Gartner Enabling Strategic Success Survey

[151] The Resilient Operating Model: Overcoming Corporate Bureaucracy Through People, Partners and Insight, Accenture.

Ransomware

[1] Gartner (2020); The State of Ransomware 2021, Sophos.

[2] Ransomware: What Board Members Should Know and What They Should Be Asking Their Technical Experts, U.K. National Cyber Security Centre; Boards and Cybersecurity, McKinsey & Company; 2022 Gartner View From the Board of Directors' Survey

[3] The State of Ransomware 2021,Sophos; Breaking Down the Ransomware Trends in 2021, Cyware.

[4] The State of Ransomware 2021, Sophos; Breaking Down the Ransomware Trends in 2021, Cyware; Ransomware Uncovered 2020/2021, Group-IB.

[5] The State of Ransomware 2021,Sophos; Global Ransomware Damage Costs Predicted to Reach $20 Billion (USD) by 2021, Cybersecurity Ventures.

[6] The State of Ransomware 2021, Sophos.

[7] The State of Ransomware 2021, Sophos.

[8] ISACA Survey: IT Security and Risk Experts Share Ransomware Insights in the Aftermath of the Colonial Pipeline Attack, ISACA; The Hidden Costs of Ransomware, Carbonite and Webroot.

[9] Ransomware as a Service (RaaS) Explained, CrowdStrike; Ransomware Uncovered 2020/2021, Group-IB; Ransomware: What Board Members Should Know and What They Should Be Asking Their Technical Experts, U.K. National Cyber Security Centre.

[10] Ransomware as a Service (RaaS) Explained, CrowdStrike; Ransomware Uncovered 2020/2021, Group-IB; The State of Ransomware 2021, Sophos.

[11] Ransomware as a Service (RaaS) Explained, CrowdStrike; Ransomware Uncovered 2020/2021, Group-IB.

[12] Ransomware Uncovered 2020/2021, Group-IB.

[13] Ransomware as a Service (RaaS) Explained, CrowdStrike; Ransomware Uncovered 2020/2021, Group-IB.

[14] States Consider Legislation to Ban Ransomware Payments, Government Technology.

[15] Q2 Ransom Payment Amounts Decline as Ransomware Becomes a National Security Priority, Coveware; The Hidden Costs of Ransomware, Carbonite and Webroot; How Fileless Ransomware Works, CrowdStrike.

[16] Important Notice August 4th, 2021, Kaseya.

[17] Acronis Cyberthreats Report: 2021 Will Be the "Year of Extortion," Acronis; Mental Health Patients From Finland Being Blackmailed After Suspected Databreach, GovHealth IT.

[18] Welcome to the New World of Triple Extortion Ransomware, Security; Triple-Extortion Tactics on the Rise for Ransomware Gangs, Netscout.

Actionable, objective insight

Explore these additional complimentary resources and tools for audit leaders:

Research

Scale Audit Coverage at the Speed of Business

Scale audit coverage by enabling internal audit foresight in a high-change environment.

Download Research

Research

Five Steps for Developing Audit Key Risk Indicators

Identify, measure and report on audit key risk indicators with this step-by-step guide.

Download Research

Webinar

Join a virtual event

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

Reserve Your Place

How We Help

Gartner for Audit

Discover how we can help you to achieve your most critical priorities.

Learn More

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

Gartner®

Get More.

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:

gartner.com/en/audit-risk

Stay connected to the latest insights

Gartner®