2021 Audit Plan Hot Spots Report

Gartner Audit Leadership Council

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 Risk 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 risk trends that affect global organizations.

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

Assess Key Risks — Determine which 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 and helps audit teams identify risks to the organization more effectively and highlight key risks for stakeholders. This year three key themes underlie the 12 hot spots, all stemming from a macro theme, the COVID-19 pandemic.

The COVID-19 Pandemic

The global COVID-19 pandemic has significantly altered the risk landscape. From major supply chain disruptions and heightened employee health and safety concerns to an economic recession and shifts in consumer behavior, the pandemic has created new risks and magnified perennial concerns. Organizations have altered their operations to respond, implementing changes that will likely become permanent. Large-scale remote work has amplified existing information security risks, while unplanned or accelerated adoption of cloud and other technologies increases the likelihood of service outages and system breaches. These risks are increasing concurrently, challenging organizations' capacity to respond.

Due to the pandemic, more employees are working outside of traditional office spaces, and the number of nontraditional workers is rising, creating divergent employee experiences. Prolonged remote work, personal responsibilities, isolation due to social distancing and fear of contracting the virus when returning to work are also increasing employee stress. These factors are creating risks of lost productivity and reduced employee engagement. As the line between work and personal lives continues to blur, employers will have to adjust performance management metrics and adopt flexible productivity expectations. Consequently, there is greater emphasis on employers' treatment of their employees and what it means to be a "people-first" organization.

Further, global lockdowns and unanticipated changes in consumption habits have exacerbated the effects of the economic downturn, upending projections and necessitating changes to business strategy. Additionally, volatile economic recovery trajectories, lack of consensus about the ideal time to fully resume on-site activities and the chance of more government-mandated movement restrictions add another layer of complexity to planning and forecasting.

1. Heightened Focus on Organizational Resilience

Organizations are facing extraordinary tests of their abilities to respond, adapt to and recover from disruptions related to people, processes and technology. The combination of widespread changes in workforce arrangements, such as large-scale remote work, and accelerated deployment of new technology significantly heightens operating challenges and the risk of disruption. The speed and scale of these changes increases the risk of control misconfigurations, security gaps and compromised quality. Furthermore, as organizations adjust operations to accommodate a reduced physical presence, they are significantly changing their control environments, increasing the likelihood of governance and control deficiencies.

Organizations are also reprioritizing resilience over efficiency in their operations by redesigning key processes. However, the rapid nature of these changes increases the risk of poor planning and implementation, leading to operational failures and misalignment with long-term strategy. Building in more redundancy to enable flexibility, however, increases costs, and more frequently outsourcing critical operations increases dependence on third parties, as third parties themselves become more vulnerable to disruption. As organizations seek to improve organizational resilience, they will need to consider the risks highlighted in these hot spots:

- Organizations are looking to reduce the likelihood and impact of **supply chain** disruptions by modifying their supply chain strategies and adopting more digital supply chain technology. However, these changes come with increased costs and greater vulnerability to cyberattacks, as the organization's attack surface expands.
- Standard risk events, such as supply chain disruptions and adverse weather events, have been exacerbated by the unprecedented nature of the pandemic, making **business continuity and disaster recovery (BCDR)** a high priority. However, fragmented business continuity management practices and an uncertain and complex planning horizon increase the difficulty of preparing for the range of disruptions organizations face.
- Fluctuating demand and solvency pressures create new challenges for **third-party management**. At the same time, pressure to expedite third-party onboarding often leads to inadequate vetting and due diligence, increasing exposure to regulatory action and financial loss.
- Large-scale shifts to remote work amplified the effects of inadequate cyber hygiene practices. These factors increase organizations' **cyber vulnerabilities**, especially as threat actors escalate attacks to capitalize on the proliferation of endpoints and heightened sense of uncertainty.
- As organizations rapidly scale their remote work capabilities and deploy new technology, IT capacity is increasingly strained. These pressures also magnify access management challenges and increase the likelihood of system outages and data breaches, heightening risks related to **IT governance**.
- Organizations' **data governance** practices have yet to catch up with the speed and volume of data being collected and generated. Data environments are also becoming more complex, increasing the likelihood of duplicated effort and compromised data security.

Other hot spots affected by the heightened focus on organizational resilience include:

Executive Summary (Cont.)

- Corporate Financial Management
- Risk Culture and Decision Making
- Talent Resilience
- Corporate Responsibility

2. Elevated Macro Environment Uncertainty

Organizations face a highly uncertain operating and risk environment through at least 2021. Although there were signs of a looming recession before the pandemic, pandemic-induced declines in demand and economic activity, necessitating rapid changes to business models, are amplifying operating challenges. With more employees moving to remote work and more customers favoring online retail, several industries are undergoing substantial, often accelerated, digital disruption. However, organizations' visibility into the permanence of these changes is limited, increasing uncertainty about how to size their technology and real estate investments. Additionally, organizations must account for the possibility of subsequent waves of the virus outbreak and potential lockdowns, which further complicates scenario modeling, forecasting and budgeting. The global, variable nature of the pandemic has also rendered existing crisis response plans inadequate, adding another layer of complexity to business continuity management. As organizations grapple with elevated macro uncertainty, they must pay attention to risks from these hot spots:

- Increased change, stress and uncertainty are creating ideal conditions for fraud and negatively impact **risk culture and decision making**. As organizations prioritize keeping the lights on over implementing controls, they are likely to deemphasize risk-based decision making and control frameworks, increasing the likelihood of compliance violations and financial losses.
- Challenges with maintaining liquidity and the elevated risk of credit default are adversely affecting the ability of organizations and their debtors to meet financial obligations. This increases the likelihood of excess bad debt and reduced profitability, creating new **corporate financial management** risks.
- Consumer behavior has changed significantly in the wake of global lockdowns and the economic downturn, disrupting historical data patterns and heightening the need for accurate **data and analytics** to support rapid decision making. At the same time, data inaccuracies continue to limit successful implementation of advanced analytics tools, resulting in wasted investments and missed opportunities.

Other hot spots affected by the elevated macro environment uncertainty include:

- Business Continuity and Disaster Recovery (BCDR)
- Data Governance
- Supply Chain
- Corporate Responsibility
- Third-Party Management

3. Humanization vs. Dehumanization of the Workforce

Organizations must now manage a larger, varied workforce that encompasses full- and part-time employees, contingent workers and automated bots. The growth of the remote workforce is also challenging how organizations recruit, onboard, incentivize and manage employees. Adapting talent management practices is critical to attracting and retaining talent, especially employees with the technical skills and agility needed to keep pace with accelerated digital initiatives. Further, the pandemic has increased the spotlight on the organization's responsibility to its employees. The adjustment to remote work, financial instability, child care responsibilities and fears of layoffs are increasing employee stress. This threatens their well-being, increasing the risk of burnout and lost productivity. All of these raised expectations for prioritizing well-being and have implications beyond corporate objectives and productivity. While some organizations have responded by enhancing their focus on employee health and well-being, others have prioritized business needs, asking workers to remain on-site without protective gear or additional compensation, even going so far as to mandate workers conceal details of virus spread.

Organizations that fail to consider their employees' treatment on a human level face risks of potential litigation, reputational and brand damage and reduced ability to compete for critical talent. To mitigate these risks organizations must consider these hot spots:

- Workforce arrangements — namely location requirements and terms of employment — are becoming increasingly diverse, complicating traditional HR processes. Consequently, organizations must expand their focus on **total workforce management** or risk lost productivity, increased turnover and difficulties in attracting talent.
- As the level of organizational change continues to increase, **talent resilience** is critical for current and future operations. However, employees are under significant physical and mental stress, and many lack the digital skills needed in a virtual work environment.
- Global racial justice and climate change protests have placed a spotlight on organizations' responsibility for contributing to improved social and environmental outcomes. However, organizations still lag on diversity and inclusion (D&I) initiatives, and are yet to prioritize climate change in decision making, heightening risks to **corporate responsibility**.

Other hot spots affected by the humanization vs. dehumanization of the workforce include:

- Business Continuity and Disaster Recovery (BCDR)

Audit Plan Hot Spots Summary

Audit Plan Risk Areas	Summary	2021 Drivers	2020 Drivers
IT Governance	Rapidly enabling a remote workforce and meeting changing consumer behavior by implementing digital technology is straining IT staff capacity, increasing the risk of service interruptions and security breaches.	1. Rapid Adoption of New Technologies 2. Access Management Challenges	1. Robotic Process Automation (RPA) Governance Challenges 2. Piecemeal Modernization of Legacy Systems
Data Governance	Organizations are still struggling to successfully implement and enforce data governance frameworks. As they accumulate new types of data and rely on fragmented storage systems, they are more exposed to regulatory, ethical and data security risks.	1. Collection of More Sensitive Data 2. Increasingly Complex Data Environments	1. Data Over Retention 2. Insufficient Preparation for Data Migration
Cyber Vulnerabilities	Large-scale remote work has amplified existing security vulnerabilities, magnifying gaps in security controls and leaving employees more susceptible to social engineering attacks. Attackers are exploiting the expanding attack surface as they grow more sophisticated.	1. Lapses in Security Controls 2. Increased Employee Vulnerability to Social Engineering	1. Employee Security Behaviors 2. Cyber-Physical Convergence
Business Continuity and Disaster Recovery (BCDR)	The scale of global and organizational change, compounded by shortcomings in business continuity management practices, is increasing organizations' exposure to risks of operational disruption. **This is an evolution of last year's organizational resilience hot spot.**	1. Fragmented Ownership of Business Continuity Management 2. Outdated Business Continuity Planning Processes	1. Fragmented Risk Management 2. Lack of Board Attention to Resiliency Practices
Talent Resilience	Increased uncertainty, stress and the pressures of working from home are testing employees' ability to adapt and remain productive, increasing the risk of change fatigue.	1. Declining Employee Well-Being 2. Digital Skills Gaps	Not a 2020 Hot Spot
Corporate Responsibility	Renewed emphasis on diversity and inclusion and climate change is highlighting organizations' reputational and financial exposure when they fail to incorporate social and environmental factors into decision making.	1. Slow Progress on Diversity and Inclusion 2. Inadequate Consideration of Climate Change Impact	Not a 2020 Hot Spot

Source: Gartner

Audit Plan Hot Spots Summary (Cont.)

Audit Plan Risk Areas	Summary	2021 Drivers	2020 Drivers
Third-Party Management	Organizations' third-party risk management practices have yet to catch up to the pace of risks. Due to recent disruptions, such as the pandemic, many third parties are unable to deliver contracted goods and services, emphasizing the need for consistent monitoring of their continuity and financial health. **This is an evolution of last year's third-party ecosystems hot spot.**	1. Third-Party Continuity and Viability Challenges 2. Insufficient Third-Party Due Diligence	1. Extension of Liability 2. Deeper Entanglement of Third Parties
Risk Culture and Decision Making	Increased macroeconomic volatility and disruptions are causing organizations to deprioritize risk management activities, creating more opportunities for corporate misconduct.	1. Heightened Likelihood of Fraudulent Behavior 2. Internal Controls Degradation	1. Complexity and Interconnectedness of Risks 2. Looming Economic Downturn
Corporate Financial Management	Sharp declines in economic activity combined with an economic downturn are increasing risks to organizations' assets and cash flows and threatening long-term financial performance.	1. Liquidity Crunch 2. Increased Incidences of Credit Default	Not a 2020 Hot Spot
Data and Analytics	Poor data quality continues to impede the implementation of digital initiatives. Simultaneously, significant changes to historical data patterns due to shifts in consumer behavior increase planning complexity and add to the risk of erroneous decision making.	1. Ineffectiveness of Historical Data for Predictive Models 2. Slow Implementation of Advanced Analytics Due to Poor Data Quality	Not a 2020 Hot Spot
Supply Chain	Organizations are facing more supplier disruptions and are adopting new technology and sourcing strategies to build resilience. However, in doing so they are expanding their cyberattack surface and increasing costs.	1. Challenges in Shifting Supply Chain Strategies 2. Cyberattacks Resulting From Supply Chain Digitalization	1. Environmental Disasters 2. Tariffs and Trade Regulations
Total Workforce Management	The workforce is now composed of disparate employment models and working locations, requiring organizations to manage increased complexities and adapt traditional human resource processes. **This is an evolution of last year's strategic workforce planning hot spot.**	1. Complexities of Managing Diversified Work Arrangements 2. Rigid Human Resource Processes	1. Workforce Reskilling Challenges 2. Growth in Nontraditional Work Arrangements

Source: Gartner

Audit Plan Risk Areas (Excerpt)

IT Governance

Mandated mobility restrictions due to lockdowns have accelerated organizations' digital roadmaps, causing organizations to vault five years forward in digital adoption in around eight weeks.[1] As the share of remote workers quadruples and 80% of consumers increase their use of digital services, organizations must quickly adopt new technologies while maintaining productivity, avoiding security risks and supporting consumer preferences.[2] These changes are at least semipermanent as 74% of organizations plan to keep at least part of the workforce remote, and 82% of consumers indicate they will continue using digital services even after restrictions are lifted.[3] Sustaining new digital technologies and accompanying infrastructure updates increases the prevalence of disruptive system outages that cost thousands of dollars per minute, and creates new attack vectors that require protection without years of lead time to prepare for security risks.[4]

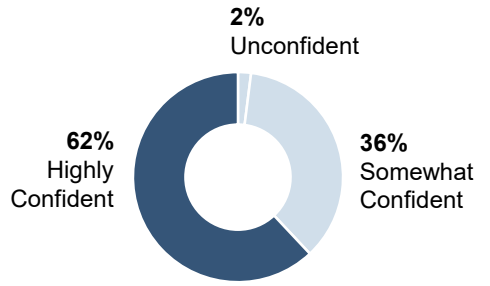
1. Rapid Adoption of New Technologies

The rapid adoption of IT to adapt and maintain operations is raising concerns about lost productivity and disruptions to customer services. Ninety-four percent of business managers report technology glitches reduce employee productivity, and 84% of remote workers lose access to applications at least once a week.[5] More than half of consumers also report an increase in application outages and slow-downs that impact their ability to use business services.[6] IT incident tickets doubled in early 2020, with some industries experiencing up to 11 times more incidents.[7] As a result, 48% of IT departments have shifted resources from upgrades and IT enhancements to maintaining critical business operations.[8] Despite this effort, some support queue waiting times were as high as 2.5 hours, as IT team capacity becomes increasingly strained.[9] Additionally, these shifts mean IT departments are now running behind their 2020 plans, causing delays to service rollouts, system refreshes and infrastructure build-outs meant to reduce security risks and increase operational efficiency.[10]

2. Access Management Challenges

Challenges governing access rights continue to grow due to the influx of access rights requests needed to support remote work, with 57% of IT departments being unable to keep pace.[11] Managing access rights becomes increasingly complex as the use of cloud and personal devices expands. IT teams are hindered by the lack of a unified view of access rights throughout the organization and overreliance on manual processes.[12] Not wanting to slow operations, 62% of IT leaders believe their organization grants privileged access rights that exceed individual roles or responsibilities.[13] Fifty-six percent of IT professionals expect privileged user abuse to increase in the next 12 to 24 months, which is especially troubling as 74% of data breaches stem from privileged access abuse.[14] Failure to properly manage access rights increases the risk of data breaches, financial losses and regulatory fines. Almost three-quarters of data breaches involve privileged accounts and compromised credentials result in the most expensive data breaches — $1 million more than the global average.[15]

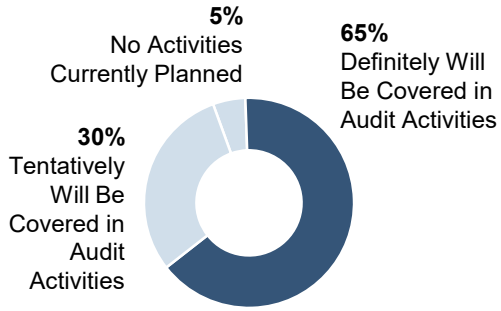
Confidence in Audit's Ability to Provide Assurance Over IT Governance Risk
Percentage of Respondents



n = 94

Source: 2021 Gartner Audit Key Risks and Priorities Survey

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



n = 94

Source: 2021 Gartner Audit Key Risks and Priorities Survey

IT Governance

2021 Recommendations for Audit

- **Review Access Management Policies and Controls:** Assess the policies and procedures for granting system access and user privileges. Assess whether access rights are granted based on defined business needs and job requirements, and are terminated in a timely manner as employees leave the organization or change roles, and administrator privileges are minimized.
- **Conduct IT Governance Advisory Reviews:** Conduct advisory work on IT governance for all IT projects, system and application implementations and assess where new controls are needed. Work with IT to determine the existence of shadow IT that employees or business units may have turned to to operate in the new virtual environment, and assess whether IT is aware of all assets in the environment and that they are accounted for in the fixed asset register.
- **Review IT Organizational Agility**: Determine whether the IT department has plans to rapidly adjust in times of crisis by reallocating IT staff and funds to support priorities that keep the most critical IT systems operating. Evaluate overall IT spend to assess whether enough is being allocated toward IT resilience and enabling continuity in times of crisis.
- **Review IT Monitoring and Reporting**: Determine whether IT monitoring and reporting enables proactive response and preparation in advance of spikes in IT incidents. Evaluate whether IT has plans to adequately increase capacity to address a spike in IT incidents and limit response time.
- **Review IT Asset Management Policies**: Evaluate how the organization provisions and tracks IT assets throughout their life from purchase to disposal. Assess whether a comprehensive inventory of IT assets exists and any gaps created by the need to quickly equip a remote workforce.

Additional Gartner Resources (Available November 6th)

- Adapting IT Operations Processes for the Digital Era: A 2020 Benchmark Report
- Addressing IT Concerns in the Remote Work Transition
- Ignition Guide to Creating a Strategic IT Workforce Plan
- Technology Investments Aren’t Meeting Productivity Expectations? Here’s Why.
- Enable Digital Business Growth While Ensuring Security at Midsize Enterprises

Questions for Management

- What procedures exist to respond to a prolonged increase in IT incidents?
- How have IT resources changed as a result of additional remote work?
- How do you assess appropriate IT staffing and resourcing?
- How long does it take to terminate access rights after an employee, contingent worker or contractor is terminated?
- What kind of governance and reporting is in place for event management and business disruption?
- What processes are in place for the request, approval, change and removal of access for applications and systems?
- How long are requests for creation, change and deletion of user access rights retained?
- How do you confirm user and administrator access rights are commensurate with current job description and responsibilities?
- What procedure exists to ensure only appropriate users have access to documents or applications to minimize risk of sensitive information disclosure?
- What kind of monitoring activities are in place to identify inappropriate access?

Key Risk Indicators

- Percentage change in the number of IT events month over month
- Average IT incident response time
- Average time of network/system downtime
- Trends in frequency of upgrades, diminished support levels or significant staff changes
- User satisfaction with available IT
- Frequency of privileged access reviews
- Number of incidents leveraging vulnerabilities for which patches exist
- Number of concurrent system logins using the same ID
- Number of past due manager access reviews
- Trends in help desk tickets opened

Talent Resilience

Employee change fatigue was a top concern pre-pandemic, as the average employee experienced 12 organizational changes a year, and the COVID-19 pandemic only amplified this risk.[52] Rapid digitalization and unplanned workplace changes, combined with concerns about social unrest, health and financial security, child care and workplace safety, are focusing greater attention on employee physical and mental health.[53] Postpandemic, 67% of employees report higher stress, 53% are emotionally exhausted and 62% lose at least one hour of productivity a day due to stress.[54] Adding to this, the rapid shift to remote work magnifies limited employee digital dexterity, leaving many ill-equipped to connect and operate from their new home offices. Change-stressed employees perform worse, costing $32.5 million per $1 billion in revenue.[55] This raises the bar for supporting employee resilience, which is the extent to which employees can experience change without succumbing to change fatigue. Failing to build a resilient workforce can result in significantly lower engagement and reduced productivity.

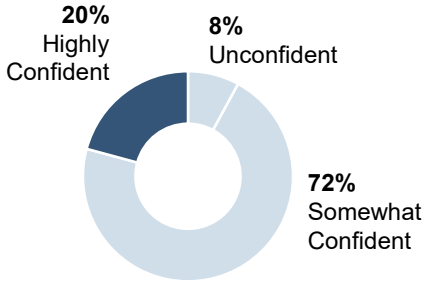
1. Declining Employee Well-Being

The current environment is challenging all aspects of employee well-being — financial, physical, mental and social.[56] In July, 69% of employees reported feeling burned out, a nearly 20% jump from just two months earlier, as employees continue to adjust to new ways of working while frequently working more hours and taking less time off.[57] However, utilization rates for existing employee-assistance programs remain low due to lackluster communication or fear of retribution.[58] Employees need and increasingly expect employers to help them cope, yet less than half of organizations are enhancing healthcare benefits and well-being programs, and only 33% plan to enhance leave or vacation programs.[59] Organizations under financial strain are also considering cutting expenditures such as wellness benefits and 401(k) contributions.[60] As a result, 41% of employees believe their employers do not support their well-being, and nearly half don't feel supported by their bosses in the remote environment.[61] Failing to invest in employees erodes employee loyalty, reduces current and future productivity and increases the likelihood of errors.[62]

2. Digital Skills Gaps

Organizations invested nearly $1.3 trillion in digital transformation initiatives in 2019, and 97% of executives say prolonged remote work has further accelerated their digitalization plans.[63] However, nearly one-third of U.S. workers and 37% of European workers lack even basic digital skills, leaving only 45% of the workforce adaptable to the new world of work.[64] Fifty-eight percent of organizations report the need for a digital skills transformation due to rapid advances in cloud computing and automation; however, 50% of learning and development plans have been canceled or postponed in the U.S., and almost 100% have been canceled in Asia and Europe due to COVID-19.[65] Without appropriate skills to navigate digital change, day-to-day activities can be disrupted, causing apathy, frustration and fatigue. This can hinder the success and resilience of digital initiatives and workflows.

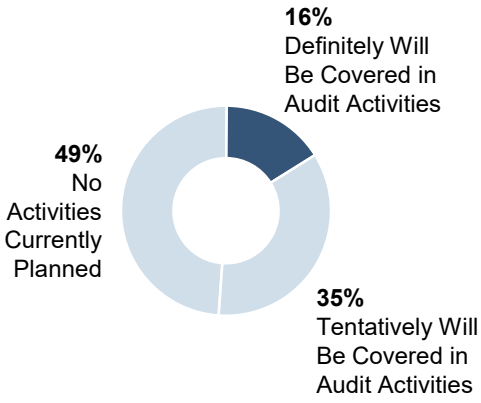
Confidence in Audit's Ability to Provide Assurance Over Talent Resilience Risk
Percentage of Respondents



n = 92

Source: 2021 Gartner Audit Key Risks and Priorities Survey

Plans to Cover Talent Resilience in Audit Activities in the Next 12-18 Months
Percentage of Respondents



n = 94

Source: 2021 Gartner Audit Key Risks and Priorities Survey

Talent Resilience

2021 Recommendations for Audit

- **Review Assessments of Employee Engagement**: 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, and ensure results are documented and action plans exist to address signs of employee disengagement.
- **Assess Progress on Learning and Development Plans**: Review progress on proposed learning and development plans and talent risk-mitigation strategies. Assess whether plans are adequately updated as business priorities and organizational needs change and critical training isn't delayed or cancelled.
- **Review Digital Skills Assessments**: Evaluate how critical digital skills gaps are identified. Assess HR and senior management awareness of gaps in skills necessary to execute the digital strategy and sustain remote work and the plans in place to close them.
- **Assess Benefits and Benefits Communication 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.
- **Review Change Communication Processes**: Verify an established cadence for sharing and discussing important change-related information with employees is in place. Assess guidance given to managers to encourage transparency and empathy while communicating organizational changes.

Additional Gartner Resources (Available November 6th)

- Tailor Well-Being Benefits to Support Resilience During Change
- How to Support Employee Well-Being: Peer Examples and Guidance
- How to Reduce Employees' Risk of Change Fatigue
- Building a Digital Skills Organization
- The Risks of Remote Work: The Employee Experience

Questions for Management

- What lessons have you learned so far in regards to managing and motivating a largely remote workforce?
- How do you assess employee engagement levels?
- How do you respond to low levels of engagement?
- What mechanisms do you have in place to measure, track and respond to change fatigue in employees?
- How do you determine when your employees are overworked?
- What steps are you taking to evaluate employee satisfaction with current benefit offerings?
- How do you communicate existing or new benefits and well-being programs to employees?
- What gaps currently exist between the skills available in the organization and those necessary to successfully execute digital strategy?
- What actions have you taken to ensure continued progress against learning and development objectives?
- How have you adapted training and development plans to cover immediate skills requirements?

Key Risk Indicators

- Amount spent on different health and welfare plans compared to benchmarks
- Percentage of employees who haven't taken PTO in the last six months
- Average number of unused vacation days
- Utilization levels of well-being offerings, such as mental health services
- Average benefits expense per employee
- Frequency of digital skills gap assessments
- Level of digital skills gaps identified in talent assessments
- Percentage of remote workforce below performance standards
- Increased incidents of absenteeism
- Number of requests processed by the employee assistance program

Thematic Overview of the 2021 Hot Spots

Hot Spot	Heightened Focus on Organizational Resilience	Elevated Macro Environment Uncertainty	Humanization vs. Dehumanization of the Workforce
IT Governance	✓		
Data Governance	✓	✓	
Cyber Vulnerabilities	✓		
Business Continuity and Disaster Recovery (BCDR)	✓	✓	✓
Talent Resilience	✓		✓
Corporate Responsibility	✓	✓	✓
Third-Party Management	✓	✓	
Risk Culture and Decision Making	✓	✓	
Corporate Financial Management	✓	✓	
Data and Analytics		✓	
Supply Chain	✓	✓	
Total Workforce Management			✓

Source: Gartner

Want to learn more?

Gartner Audit Leadership Council provides research insights, advice, tools and data to equip chief audit executives to make the right decisions and stay ahead of change. Learn more about how Gartner can support your success.

Phone: 1 855 658 7387
Email: gartnerbusinessleaders@gartner.com
Web: gartner.com/en/audit-risk
Follow: Connect on LinkedIn

End Notes

IT Governance

[1] The COVID-19 Recovery Will Be Digital: A Plan for the First 90 Days, McKinsey & Company.

[2] Stanford Research Provides a Snapshot of a New Working-From-Home Economy, Stanford; When Everyone Can Work From Home, What's the Office For? PwC; Survey: More Than Half of Consumers Have Experienced Increased Digital Service Problems During Work from Home Period Despite IT Confidence in Current Tools and Processes, XMatters.

[3] Gartner (2020); Survey: More Than Half of Consumers Have Experienced Increased Digital Service Problems During Work From Home Period Despite IT Confidence in Current Tools and Processes, XMatters.

[4] The Hidden Costs of Downtime, Forbes; The Cyber-Risk Paradox: Benefits of New Technologies Bring Hidden Security Risks, Security Boulevard; Managing the Fallout From Technology Transformations, McKinsey & Company.

[5] Remote Work Is the New Normal. But the Tech Problems Won't Go Away, ZDNet; IDC: COVID-19 Hits SD-WAN, Data Center Gear; Enterprise Impact Varies, NetworkWorld.

[6] Survey: More Than Half of Consumers Have Experienced Increased Digital Service Problems During Work from Home Period Despite IT Confidence in Current Tools and Processes, XMatters.

[7] IT Service Desks Rush to Support Remote Work Amid Pandemic, Stemcell.

[8] Gartner (2020).

[9] Ibid.

[10] Ibid; Digital Pulse: Coronavirus Flash Survey March 2020, S&P Global.

[11] Most Expect the Risk of Privileged User Abuse to Increase, Help Net Security; KuppingerCole Analysts Name CyberArk "the One to Beat" in Privileged Access Management, Security Boulevard; Does Privileged Access Equal Trusted Access? Vectra; 74% of Data Breaches Start With Privileged Credential Abuse, Forbes.

[12] Most Expect the Risk of Privileged User Abuse to Increase, Help Net Security.

[13] Ibid.

[14] New Research on Privileged Access Management Reveals the Status Quo Is Not Secure, Ponemon Institute; 5 Reasons Why Privileged User Abuse Is a Top Security Concern in the Cloud, FairWarning; 74% of Data Breaches Start With Privileged Credential Abuse, Forbes.

[15] Privileged Access Management in the Modern Threat Landscape, Centrify; Compromised Employee Accounts Led to Most Expensive Data Breaches Over Past Year, Security Magazine (subscription required).

Talent Resilience

[52] 2019 Gartner Change Fatigue Survey.

[53] Engaging and Enabling Your People Through Change, Korn Ferry.

[54] How CEOs Can Support Employee Mental Health in a Crisis, Harvard Business Review (subscription required); HRE's Number of the Day: Coronavirus Stress, Human Resource Executive.

[55] Gartner (2020).

[56] 5 Things to Know About Well-Being and COVID-19, Human Resource Executive.

[57] Employee Burnout Amid Coronavirus is On the Rise: Poll, Fox Business; HRE's Number of the Day: Fitness Benefits, Human Resource Executive.

[58] Is COVID-19 a Turning Point for Workplace Mental Health?, Human Resource Executive.

[59] Here's How Employers are Changing Benefits Due to COVID-19, Human Resource Executive.

[60] Ibid.

[61] Ibid.

[62] COVID-19: What Employees Need From Leadership Right Now, Gallup.

[63] Digital Transformation: How Technology Is Changing Business, Apty; Digital Transformation: Affected and Accelerated by COVID-19, Help Net Security.

[64] As COVID-19 Increases Need for Digital Skills, Don't Neglect Soft Skills, American Enterprise Institute; The Digital Skills and Jobs Coalition, European Commission; Win With Empathy: Global Talent Trends 2020, Mercer.

[65] Gartner (2020); Gartner (2020); 3 Ways COVID-19 is Transforming Learning and Development, HRD Connect.

