2020 Audit Plan
Hot Spots
Report Excerpt

Risk Areas to Watch
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 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 from across 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 more effectively identify risks to the organization and highlight key risks for stakeholders. This year, four themes underlie the 12 hot spots:

1. Increased Organizational Complexity
As organizations pursue new market opportunities, build greater ecosystems of partners and continue to digitalize, they are becoming increasingly complex. The rapid pace of organizational change, combined with the increasingly volatile risk landscape, leads to higher potential for disruptions and more challenges in strategy execution. New business models are changing the skills profile needed to achieve business objectives, while fragmented risk management practices hinder organizations’ ability to be resilient in the face of inevitable disruption. Further, the use of new technologies is complicating already complex IT infrastructures, requiring more hard-to-find technical talent. Coordination problems continue to plague organizations, leading to risk management lapses as risks become more intertwined and require cross-functional oversight. These factors contribute to the already complex organizational environments and lead to the following hot spot areas:

• Changing employee expectations and expanding business models require organizations to rethink their approaches to strategic workforce planning. The pace of change is resulting in constantly shifting skills needs and organizations are increasingly forced to turn to new work arrangements, such as remote work, to be more attractive in the tight labor market. This leads to questions around employee engagement as well as security vulnerabilities.

• As the list of potential business disruptions continues to expand, the ability for organizations to adapt and respond to disruptive factors is paramount. Organizational resilience will continue to be tested in 2020 by disruptions ranging from extreme weather to disruptive competition, and internal factors such as a lack of crisis preparedness and uncoordinated risk management practices are not helping.

• As recent negative headlines show, it is more important than ever for organizations to ground decision making in a strong risk culture. With regulators increasingly targeting unethical behavior and risk surprises becoming more frequent, organizations need to do more to ensure decisions are made with a risk lens. This becomes even more pressing as the predicted economic downturn will put organizations at higher risk for unethical behaviors.

Other hot spots affected by increased organizational complexity:
• Artificial Intelligence (AI)
• Cyber Vulnerabilities

2. Heightened Stakes for Managing and Protecting Data
Data is a key differentiator for today’s organizations in improving risk management, maintaining competitive advantage and increasing efficiency. However, with the large amounts of data being generated and collected, organizations continue to struggle to manage, protect and capitalize on it. Data management failures have drawn regulator and public scrutiny, leading to increased regulations and pressure for organizations to rethink their use of data. To maximize the ability of data to unlock business value while minimizing the risk of regulatory fines and reputational damage, organizations must address the following hot spot areas:

• Clear governance strategies are essential to harnessing the power of big data, meeting regulatory requirements and making the most of new digital technologies. Despite the strategic importance of data, organizations have been slow to adopt data governance frameworks, putting them at risk for large fines, poor decision making and misallocation of critical resources.

• As the number of data breaches continues to rise, so too do public and regulator scrutiny of data protection practices. As a result, data privacy remains a top concern for organizations across the board. From complying with existing regulations, such as General Data Protection Regulation (GDPR), to preparing for new regulations yet to take effect throughout the world, organizations must establish processes to deal with the growing patchwork of regulatory requirements.

Other hot spots affected by the heightened stakes to manage and protect data:
• Artificial Intelligence (AI)
• Cyber Vulnerabilities
• IT Governance
• Project Management
• Supply Chain
• Third-Party Ecosystems
Executive Summary (Cont.)

3. Digital Business Transformation

Competitive and market pressures are driving organizations to increase their investments in digital transformation. Seeking efficiencies and cost savings, organizations are rapidly undertaking pilots without adequately devising strategies leading to high rates of project failure as well as limited realization of benefits. The expanding deployment of advanced technologies, most notably robotic process automation (RPA) and artificial intelligence (AI), are complicating already complex IT infrastructures and increasing security vulnerabilities. Combined with the need for organizations to move quickly to keep up with competition, this results in a decreased focus on governance and oversight and weakened internal control systems. To mitigate the risks and take advantage of the upside of current and future transformation efforts, organizations must address the following hot spot risk areas:

- As the number of entry points into organizations grows, and cybercrime becomes ever-more profitable, the number of cyberattacks continues to rise. The expanding connection of cyber and physical assets, combined with the exploitability of careless employee security behavior, is escalating cyber vulnerabilities. These factors are making cyberattacks inevitable for nearly all organizations.
- Although widespread implementation has yet to come, investments in artificial intelligence (AI) are rapidly increasing. Underlying the entire business model of new organizations, and improving workflows and creating data insights for established organizations, AI holds significant potential to drive business value. However, without attention to problems with training data and its susceptibility to tampering, organizations risk unintended compliance and ethics violations and significant reputational damage.
- IT serves as the foundation of most organizations’ business strategy, making IT governance a key point of focus. As more organizations increase investments in technologies, such as RPA, and gradually modernize their legacy systems, they must pay attention to governance, security and management of IT assets.
- Projects are essential components to organizations’ strategies to stay relevant and competitive in the current disruptive environment, yet most organizations struggle to establish standardized and effective project management practices. Without these, organizations are wasting resources and indispensable innovation dollars that could be reinvested elsewhere, failing to maximize project outcomes and scale project benefits throughout the organization.

Other hot spots affected by digital business transformation:
- Data Governance
- Organizational Resilience
- Strategic Workforce Planning

4. Heightened Geopolitical and Regulatory Volatility

Similar to 2018, uncertainty and volatility are prevailing features of 2019 with no signs of abating. The number of disruptive forces organizations face continues to grow while important policy questions remain unsolved. Facing challenges to traditional business models, organizations are advancing digital transformation initiatives and redesigning their strategies to remain competitive. From initiating new-in-kind projects to expanding the network of third parties they contract with, organizations are extending their footprints and losing visibility. Escalating global tensions over trade, environment and geopolitical alliances, force organizations to try to plan for and adapt to tremendously unpredictable events. Adding to this, increased regulatory and public scrutiny has led to greater corporate accountability as the costs of compliance and failures continue to rise. These factors lead to the following hot spot risk areas:

- A new wave of regulatory developments – not just on data privacy – is underway in response to escalating cyber breaches and concerns over climate change. Accordingly, organizations must take steps now to comply with existing regulations as well as prepare for potential future regulatory action in these and other areas.
- Expanding geopolitical tensions are creating high levels of uncertainty and volatility in the global trade system, with many organizations already feeling the effects. Combined with the rise in volume and scale of extreme weather events and other natural catastrophes, organizations face significant challenges in terms of supply chain security.
- The number of third parties organizations work with continues to steadily grow along with the diversity and criticality of the tasks they are entrusted to perform. As third parties become more intertwined with critical organization functions, systems and data, negligence and failures at third parties are creating new compliance challenges as well as risk of financial and reputational damage.

Other hot spots affected by heightened geopolitical and regulatory volatility:
- Cyber Vulnerabilities
- Data Governance
- Data Privacy
- Organizational Resilience
- Risk Culture and Decision Making
## Audit Plan Hot Spots Summary

<table>
<thead>
<tr>
<th>Audit Plan Risk Areas</th>
<th>Summary</th>
<th>2020 Drivers</th>
<th>2019 Drivers</th>
</tr>
</thead>
</table>
| Data Governance               | Even as the strategic importance of data grows, few organizations have a formal data governance framework in place, which could enable more effective management and use of data. The absence of data governance is leading organizations to misallocate resources, produce poor quality insights and miss potential business opportunities. | 1. Data Overretention  
2. Insufficient Preparation for Data Migration                                                                 | 1. Magnification of Poor Data Quality  
2. Democratization of Data Analytics                                                                                   |
| Third-Party Ecosystems        | The number and diversity of third parties that organizations are working with continues to rise. However, as organizations entrust these parties with more critical tasks and greater access to organizational data, monitoring practices haven’t kept pace. Failures at third parties are more costly than ever for organizations, as regulators and consumers are raising the stakes in terms of organizational accountability. **This is an evolution of last year’s third parties hot spot.** | 1. Extension of Liability  
2. Deeper Entanglement of Third Parties                                                                                         | 1. Proliferation of Business Ecosystems  
2. Nth-Party Risk                                                                                                           |
| Cyber Vulnerabilities         | Cybercriminals now operating like syndicates with a variety of low-cost hacking tools at their disposal has resulted in a growing number and scale of cyberattacks. Organizations are largely unprepared to detect and respond to most of these attacks as challenges with skills, budget and foundational security measures persist. **This is an evolution of last year’s cybersecurity preparedness hot spot.** | 1. Employee Security Behaviors  
2. Cyber-Physical Convergence                                                                                         | 1. Growing Attack Sophistication  
2. Expanding Attack Surface                                                                                              |
| Data Privacy                  | As organizations collect more data to make strategic decisions, data privacy risk expands. This is underscored by recent high-profile data breach incidents and record-breaking fines. Regulators are reacting with a growing patchwork of data privacy regulations throughout the world with more on the horizon, significantly increasing complexity and the cost of compliance. | 1. Increasing Regulatory Complexity  
2. Underestimation of the Need to Protect Employee Data    | 1. GDPR Enforcement Uncertainty  
2. Consumer Awareness                                                                                                   |
| Risk Culture and Decision Making | Risk culture and its effects on corporate decision making are gaining increased attention from regulators and societal institutions at large. The ability for the business to make risk-informed decisions will only become further challenged as risks grow more connected and the next recession looms. | 1. Complexity and Interconnectedness of Risks  
2. Looming Economic Downturn                                                                                          | Not a 2019 Hot Spot                                                                                       |
| Project Management            | Despite decades of relying on high-impact projects, few organizations report high project management maturity. As organizations increasingly rely on projects to help them remain relevant and competitive, better enterprisewide and strategic coordination is imperative to reduce waste and help support business objectives. | 1. Ill-Defined Project Strategies  
2. Siloed Project Execution                                                                                          | Not a 2019 Hot Spot                                                                                       |
# Audit Plan Hot Spots Summary

<table>
<thead>
<tr>
<th>Audit Plan Risk Areas</th>
<th>Summary</th>
<th>2020 Drivers</th>
<th>2019 Drivers</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT Governance</td>
<td>Organizations are undertaking technology initiatives critical to their growth or even their survival. As organizations continue to look to IT to advance business strategy and initiatives, IT governance is even more important. Poor IT governance can lead to project failure, security vulnerabilities in mismanaged IT assets and operational delays.</td>
<td>1. RPA Governance Challenges</td>
<td>Not a 2019 Hot Spot</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Piecemeal Modernization of Legacy Systems</td>
<td></td>
</tr>
<tr>
<td>Regulatory Developments</td>
<td>Regulatory risk continues to be a top concern for companies. Divergent regulations spanning various geographies and levels of government present a challenge as companies grapple with new compliance requirements. At the same time, companies report compliance activities have become more onerous in the past few years and expect this trend to continue. <strong>This is an evolution of last year’s regulatory uncertainty hot spot.</strong></td>
<td>1. Regulatory Focus on Cybersecurity</td>
<td>1. Rapid Evolution of the Digital Economy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Waste Reduction and Climate Resiliency</td>
<td>2. Heightened Expectations of Regulators</td>
</tr>
<tr>
<td>Organizational Resilience</td>
<td>Organizations that nimbly adapt and respond to business incidents can lower their impact and decrease recovery time. However, siloed risk management and poor cross-functional collaboration hamper effective responses to business interruptions. Additionally, insufficient focus from board leadership may result in inadequately funded business continuity functions and contribute to disjointed responses in a crisis. <strong>This is an evolution of last year’s operational resilience hot spot.</strong></td>
<td>1. Fragmented Risk Management</td>
<td>1. Complacency About Macroeconomic Conditions</td>
</tr>
<tr>
<td>Supply Chain</td>
<td>Many organizations have combined globally distributed supply chains with lean processes heavily dependent on a small number of suppliers. The fragility of these supply chains means supplier risk events can hinder organizations’ access to vital materials, and increases in extreme weather and trade restrictions make such supplier risk events more likely.</td>
<td>1. Environmental Disasters</td>
<td>Not a 2019 Hot Spot</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Tariffs and Trade Policy</td>
<td></td>
</tr>
<tr>
<td>Strategic Workforce Planning</td>
<td>Organizations’ pursuit of digital initiatives, combined with changing employee expectations, are requiring employers to reevaluate workforce strategies. To remain competitive in a tight labor market and evolving business environment, organizations are increasingly adopting remote work arrangements, employing more contingent workers and trying to reskill employees to meet changing skill demands.</td>
<td>1. Workforce Reskilling Challenges</td>
<td>1. Unclear Impacts of Automation</td>
</tr>
<tr>
<td>Artificial Intelligence (AI)</td>
<td>Investments in AI are on the rise as organizational leaders are keen to tap into the ability of AI to fundamentally change how they do business. While some benefits, such as workflow improvements and enhanced data insights, are being achieved, AI algorithms can lead to a range of regulatory, ethical and security challenges.</td>
<td>1. Unintended Consequences of AI</td>
<td>Not a 2019 Hot Spot</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Vulnerabilities of AI Algorithms</td>
<td></td>
</tr>
</tbody>
</table>
Contact Us to Learn More

+1-866-913-8103
gartner.com/go/audit
gartnerbusinessleaders@gartner.com