IT Internal Audit – Planning for 2021

Key domains and risks to focus on now
Executive summary

The year 2020 has been a year of significant challenge and transformation. As we noted in our white paper “COVID-19: What the IT auditor can do to help” published in April 2020, COVID-19 has presented IT and Internal Audit (IA) with complex operational and risk management challenges that have disrupted the status quo. While our ways of working have changed, organizations are still advancing complex transformational activities that present new challenges to the IT Internal Auditor to stay relevant and provide value to the organization. Specifically, IT Internal Auditors must:

**Keep up with the transformation activities in the organization** – IT Internal Auditors must stay aware of, and align themselves to, the IT transformation activities across the organization to stay relevant. This can be challenging, as it requires the ability to scale and add relevant technology skills at short notice.

**Cultivate skills into IT Internal Audit teams that can address new technology and emerging risks** – IT Internal Audit departments must keep pace with emerging technology, which can be extremely challenging given the pace of IT change. Being able to call on specific technology subject matter professionals when needed is critical to being effective across the organization.

**Transform how they work** – IT Internal Auditors must continue to evolve to keep pace with the business. The IT Internal Audit department needs to expand its skills and capabilities to remain relevant. This may include expanded use of data in audit activity, refining remote working techniques, or adopting more agile approaches to audit execution.

**Rethink how they report findings and make recommendations** – Risk functions are moving toward a quantifiable view of risk to guide the organization’s risk and control investments in areas of highest return in terms of reducing exposure. IT Internal Audit should follow suit to make their recommendations more impactful.

A challenge IA functions have always had and even more so going into 2021, with a limited budget and resources, is how to best prioritize where your Internal Auditors spend their time. KPMG surveyed IT Internal Audit leaders to help identify areas believed to be highest impact and share ideas on how the IT Internal Audit function can add value and be relevant in 2021.

We surveyed approximately 80 cross-industry engagement leaders, with skills and experience ranging from IT Internal Audit and Sarbanes-Oxley Act (SOX) to emerging technology risk, cyber, as well as governance, risk, and compliance (GRC). Together, they serve hundreds of KPMG clients of diverse sizes, risk profiles, and industries.

**What IT Internal Audit practitioners are seeing**

When asked what disruption will be seen in the next three to six months, the highest-scoring answers were in four areas:

- **70%** of respondents expect IT Internal Audit activity to be deprioritized, potentially leading to increased operational and financial risk exposure
- **67%** expect IT teams to lose focus on control execution as a result of a shift in provision of system availability and support for the remote working environment
- **66%** expect controls will be bypassed or relaxed to accommodate new ways of working
- **63%** expect to see increased cyber risk

**When asked about the most significant IT risks:**

- **66%** of respondents believe service/availability is the most significant
- **36%** of respondents believe confidentiality of data is the most important
- **30%** of respondents believe data integrity is the most important

**When asked about the top C-suite priority:**

- **58%** of respondents believe cost reduction is the top priority
- **42%** believe strategic resilience is the top priority

© 2021 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.
Accelerated plans to adopt emerging technology and automation

IT risks are increasing with accelerated plans to adopt emerging technology and automation as a result of pressure to cut costs.

**Risk:** More adoption of cloud technologies – Cloud deployment has seen a significant upward trajectory over the past few years. Historically, organizations used cloud for virtualization and building private clouds. In today’s environment, many organizations are beginning to build their businesses completely in the public cloud.

**IT Internal Audit activity:**

— **Cloud strategy and framework** – Assess the organization’s cloud strategy, including the physical location of data, as well as broader operational and compliance risks. The IT Internal Audit function should have a good understanding of the organization’s cloud strategy and the cloud roadmap to facilitate the development of a multiyear, risk-based audit plan based on the cloud roadmap. This would allow the IT Internal Audit function to be involved in various cloud projects and provide management with ongoing assessments and feedback throughout the cloud journey.

— **Cloud adoption, onboarding, and implementation** – Assess the organization’s process for identifying, adopting, and implementing cloud solutions. The IT Internal Audit function should work side by side with the business as it embarks on the transformation. This close collaboration can be achieved in the form of a preimplementation/real-time implementation program audit, in which IT Internal Audit is involved in every step of the transformation, from planning to execution and delivery. The IT Internal Audit function can provide management with critical insights and considerations on a real-time basis, including providing controls and security integration workstream support. These insights could be short and focused reviews lasting a duration of two to three weeks or less, with an abbreviated audit report to provide more timely insights. As the organization progresses through the initial phases of its enterprise resource planning (ERP) in the cloud transformation, IT Internal Audit can participate in more strategic audits such as cloud governance assessments, cloud cyber assessments, cloud roadmap, and cloud architecture reviews. IT Internal Audit can work more closely with management as the controls and security lead on their cloud implementation. Through the latter phases, IT Internal Audit can dive into more resource- and technology-specific assessments such as cloud storage audits and identity access management (IAM) audits. Looking at enabling cloud processes such as continuous integration (CI)/continuous delivery (CD) or DevOps will provide further valuable insight to the organization.

— **Cloud security** – Assess and make available periodic controls validation and testing to provide ongoing monitoring across cloud infrastructure, data, and application layers. At a strategic program level, IT Internal Audit leadership must have a seat at the table as part of the cloud steering or governance committees. While retaining independence is crucial, senior IT Internal Audit leadership can provide valuable advice to help business leaders understand the risk and regulatory considerations stemming from cloud deployments.
Risk: Widespread and accelerated adoption of sophisticated workplace automation (automation/bots/cognitive learning/ AI) – Once an intriguing but far-fetched idea, it has now become almost a given in many organizations. Virtually all business sectors are investing in technologies such as robotic process automation, big data, predictive analytics, cognitive systems, natural language processing, machine learning, and artificial intelligence (AI) to automate knowledge work. In a business environment that is changing at a faster rate than ever before, IT Internal Audit must play an increasingly important role in the adoption of these technologies. With the uncertainties presented by an onslaught of disruptive forces, the IT Internal Audit function must keep pace to help the organization understand and manage the associated risks, achieve expected results from automation, and continue to innovate and add value.

Risk: Third-party risk management – Organizations are increasingly reliant on third-party suppliers to deliver business-critical products and services to their clients and customers. They are unfortunately finding that failures by third parties can rapidly tarnish their reputations and have significant downstream operational and cost implications. As organizations address their concerns about these issues, they need a clear strategy for the selection, approval, and management of third parties. As there are a myriad of stakeholders involved, from the business as well as the procurement and risk-oversight functions, developing and implementing this strategy continues to be highly challenging.

IT Internal Audit activity:

- **Assess governance program/lifecycle** – Assist with GRC considerations throughout the automation program lifecycle as an organization establishes and implements its program. IT Internal Audit can help management implement adequate governance programs to integrate GRC throughout the program lifecycle, from planning to ongoing monitoring following implementation.

- **Automating** – IT Internal Audit can assist management with the identification of opportunities to embed automation-enabled control activities within IT processes and functions that are inefficient or predisposed to failure due to human error. An example can be the use of automating the monitoring and deprovisioning of users’ access once they leave the organization.

- **KPI assessment** – Understand how the business both identifies and measures key performance indicators (KPIs) related to the use of intelligent automation. As there will be several different stakeholders in the business, it is important that there is unified oversight of KPIs, key risk indicators (KRI), risk mitigation, and control activities.

- **Intelligent automation integrity** – Assess the input, logic, and output being used by intelligent automation to facilitate a business process, especially as the use of AI shifts from simplistic screen scraping/data to more complex models with cognitive learning. IT Internal Audit should assist with the development of an approach to think through how assurance over more complex automation could be provided.

- **Third-party risk management** – Assess how the organization can consistently and holistically identify, monitor, and manage the third-party risks of remote contingent workers and third-party services. IT Internal Audit can conduct an independent review of management’s third-party risk management program to assess the organization’s processes and controls over the third-party lifecycle, including third-party selection, contract negotiation, ongoing monitoring of risk and performance, and vendor termination.

- **Vendor risk assessment** – Understand the processes the organization executes to assess risk of vendors from the precontracting stage and in an ongoing manner. The IT Internal Audit team can assess management’s evaluation of the risk that arises from working with vendors. A review of the IT vendor risk assessment would include reviewing management’s documentation about the risk of third parties (e.g., geography, services, contracting), concentration risk and initial risk ranking of third parties, review of third-party questionnaires and results, vendor due diligence results, and any IT risk acceptances.

- **IT vendor cyber resiliency** – Assess and understand the cyber resiliency of critical IT vendors. IT Internal Audit can provide assurance to management about their third-party vendors’ capacity to mitigate against large-scale disruptive events, cyber-resiliency preparedness, recovery capability and capacity, oversight of subcontractors, vendor Recovery Point Objective (RPO) and Recovery Time Objective (RTO), data confidentiality agreements, oversight of fourth parties, IT, and cyber insurance.

- **Contract compliance program** – Understand and assess management’s oversight of vendor performance. IT Internal Audit can review the organization’s contract compliance program. This involves a review of management’s analysis of contractual obligations with third parties, IT security considerations, performance metrics, business and infrastructure changes at the vendor, cybersecurity incidents, outages, nonavailability of services, review of penetration test results, SOC reports, and regulatory compliance.
Several factors have propelled an increased focus on cybersecurity and information protection in recent years: rapid shifts in technology, growing volume and sophistication of threats, ongoing migration to cloud-based services, the explosion of and focus on data, and more rigorous regulatory requirements.

**Risk:** Industry-wide deficiency of cybersecurity skills, within IT and broader workforce – There continues to be a lack of adequately trained and appropriately skilled cybersecurity professionals to protect intellectual property and sensitive data. Lack of trained personnel, compounded by decreasing budgets, increases the importance of the implementation of automated tools to focus on cyber risk. In some cases, companies have adequate headcount but are not focused on the highest value-yielding items. Given the changing landscape, this needs to be constantly reevaluated.

**IT Internal Audit activity:**
— **Cybersecurity process/cyber cost optimization** – Identify tasks that are manually intensive and time consuming to challenge ways automation can be leveraged. This allows professionals to focus on strategic tasks and reduce the repetitive aspects of collecting, analyzing, and reporting data related to threat activity. In addition, it may be beneficial to assess the program against a current industry recognized framework.

**Risk:** Data privacy and protection – Both the regulatory environment of the industry and the views of the board of directors set the bar for data privacy and protection throughout the organization. Data has now become an enterprise-wide priority, compounded by industry-agnostic legislation that is sure to impact several organizations. At risk is intellectual property loss, legal expenses, property loss, reputational loss, and time loss, as well as administrative costs.

**IT Internal Audit activity:**
— **Enterprise-wide privacy program** – Assess the organization’s process to plan for both immediate regulatory changes, but also for shifting regulatory climates and consumer expectations, with respect to greater individual control of data. Furthermore, perform a comprehensive review of the enterprise-wide privacy program using a widely adopted framework. Evaluating the scope and effectiveness of the privacy program, including the established governance processes, roles and responsibilities, training, and risk management, can help provide a point of view on how equipped the company is to respond to new regulations like the General Data Protection Regulation (EU GDPR) and the California Consumer Privacy Act (CCPA), and effectively sustain compliance on an ongoing basis.

— **Data management and governance audit** – Privacy must be an integral component of the business model with the goal of creating a sustainable and effective data-protection strategy. Companies should develop a solid framework of best practices to enable quick adaptation to any new regulations. They should also assess data-management/data-governance processes, as well as the adoption of these processes by business units. New accounting standards will require companies to strengthen their data-gathering process and data-governance procedures. IT Internal Audit teams can perform comprehensive data governance and data-management audits to help ensure all data used is consistent, accurate, complete, timely, and secure. As part of the review, IT Internal Audit can review overall data governance, data dictionary and lineage, data quality, metadata, master data management, and data classification. This would also include an assessment of the data domain roles, data change management, data handling and processing, information architecture, data lineage, metadata management, data quality rules, and data classification.
Risk: Understanding of cyber implications with new workforce model – Given the new workforce model, we have seen increased cyber fraud. Attackers continue to target the weakest link (usually an uneducated user behind a computer). Phishing remains one of the toughest threats to defend against. It is not just a limited threat, as hackers now unleash spyware, ransomware, etc. Flexibility is needed, depending on the current trending threat.

IT Internal Audit activity:
- **Cyber awareness/training program** – Understand the effectiveness and success of the cyber awareness program/training. Possibly facilitate the distribution of surveys to gauge awareness of phishing campaigns and assess management’s planned response.
- **Fraud assessment program** – Identify and understand risks to the organization, including weaknesses in controls that present a fraud risk to the organization.
- **Insider threat** – Understand and assess the malicious threat risk coming from inside the organization, such as employees, former employees, contractors, or business associates, who have inside information concerning the organization’s security practices, data, and computer systems.

Risk: Access management – IAM should be an integrated component of design, especially with the increased use of cloud technologies and bots, which increase the complexity of authentication and IAM. Compromised passwords are often the source of identity theft and are frequently how a network is compromised. Companies need to assess at what point it makes sense to employ more advanced authentication methods (touch/face ID/voice) to replace passwords.

IT Internal Audit activity:
- **IAM governance program** – Assess management’s overall IAM governance program, assessing IAM policies and procedures, access lifecycle management, access control, asset management, and procedures in place for monitoring and logging of access/activity.
- **Privileged access** – Assess management’s controls over privileged access, with a focus on management’s definition of privileged access at all layers (application, devices, and supporting infrastructure), classification of accounts, account lifecycle management controls (request, addition, change, deletion), and controls over the scope and use of service accounts.
- **IAM implementation readiness assessment** – Depending on the organization’s maturity level, IT Internal Audit can support management’s discussions about developing a holistic IAM program. This could involve an assessment of the organization’s needs (roles definition, access requirements, etc.) and identification of gaps between those needs and management’s IAM program, including the creation of policies and such things as tools selection.
Business change

In today’s environment, the ongoing effects of COVID-19 as well as the rapidly changing IT landscape are changing the way businesses operate and their outlook for the future.

**Risk:** Return to office – It’s now time for employers to plan a safe return to work for employees and their business partners. As quarantine measures begin to ease, companies know it’s vital to begin reopening their workplaces. During this process, the impact to technology should be assessed and understood as well.

**Risk:** DevOps/Agile – Organizations are challenged to deliver high-quality code fast, often, and securely. The need to innovate and deliver at scale is becoming an expectation of agility, not an exception.

**IT Internal Audit activity:**

---

**Assess the scalability and capacity of remote IT service management** – In the event that a remote working environment continues to be in place longer term or for the indefinite future, the process followed by IT service management and the capacity of IT service management to assist with end-user issues related to an “at home” IT environment should be reviewed. We are seeing IT service management functions overwhelmed with new requests from end users to support issues related to home printers, home Wi-Fi connectivity, etc.

**Assess technology implications of return-to-office framework/strategies** – Assess how the IT environment has been impacted, both short term and long term. The IT Internal Audit function needs to understand what IT risk assessments would be beneficial to execute once a number of employees return physically to the office or continue to work remotely. Some areas to consider:

- Does threat assessment/risk remain the same or should it be adjusted?
- What updates are needed to the Business Continuity Planning/Disaster Recovery Planning plan?
- Does the target operating model (TOM) change if a portion of IT professionals are remote and some are physically in the office?
- What is the level of IT involvement in the return-to-office steering committee?

---

**Evaluate DevOps strategy, governance, and training** – Evaluate the DevOps strategy by focusing on governance adoption of DevOps practices, production management, DevOps capabilities, and training/development. IT Internal Audit should conduct an assessment of the overall governance and strategy around DevOps. A review can be completed over the product team’s adoption of DevOps practices and production management, DevOps capabilities, and training/development.

**Assess integration of security in the DevOps process** – IT Internal Audit can assist management in identifying opportunities to increase security through an evaluation of controls, behaviors, or capabilities across the software development life cycle (SDLC) for risk reduction. This can be achieved through “light-touch” security testing across the organization’s most critical applications, which could then translate to more detailed security requirements to provide to developers at project initiation.

**Assess possible segregation of duties (SOD) concerns and mitigation** – Perform a deep dive on change management covering related access controls and SOD to identify gaps brought about by the developed access to production.

**Review key tools supporting the CI/CD process** – Conduct a review to understand critical process and tools supporting the CI/CD and DevOps processes. For identified critical processes/tools, IT Internal Audit can perform a process review to identify gaps and key controls unique to CI/CD automation and tools.
The achievement of operational resiliency is a necessity to meet expectations of business partners, customers, and regulators. With the recent impact of COVID-19, a real-life disrupting event has occurred, which will put these frameworks to the test.

**Risk:** Resilience and recovery or service/availability – Whether on premises or in the cloud, IT resiliency is the ability to adapt to planned or unplanned events while keeping services and operations running continuously. When the highest IT resiliency is implemented, data remains available, IT infrastructure stays operational, disruptions are minimized, and service levels are restored quickly. This is accelerated through the widespread adoption of cloud technologies.

**IT Internal Audit activity:**

- **Assess investment process for updating legacy systems and infrastructure** – Assess how the organization prioritizes investment decisions for modernizing legacy systems and strengthening technology infrastructure.

- **Assess dependencies between internal and third parties** – Assess how dependencies and interconnectedness between internal and third-party technology are mapped, analyzed, and tested to validate the feasibility of stated recovery time objectives and achieve resumption of the end-to-end business services. This would also include a review of penalties for third parties that fail to deliver services and ensure there are exit strategies for each vendor. With the new workforce model, the availability of collaboration tools has become increasingly critical. In the event of a disruption with these critical collaboration tools, remote working may be at a standstill.

- **Review communication plans** – Review communication and crisis management plans to ensure they provide timely information to, and manage the expectations of, customers, other market participants, and regulators following a disruptive event.

- **Disaster recovery system architecture design assessment** – Consider the current state of disaster recovery architecture for the IT network, systems, and applications to identify any gaps in the ability of IT disaster recovery to meet stated business requirements (e.g., identification of technical single points of failure and assessment of recovery times versus business needs).

- **Ransomware resilience** – Assess both the proactive and reactive capabilities and respective processes to recover from a ransomware attack. This should include a review of the process to identify, contain, and recover impacted systems compromised by the attack. IT Internal Audit should assess management’s identification of systems that are most vulnerable to ransomware attack, including third-party managed systems and risk mitigation/controls, to help prevent and/or limit the impact of a ransomware attack.

- **Business impact assessment regarding loss of site and loss of key technology scenario** – Consider and report on the ability of IT disaster recovery capabilities to meet business requirements given a range of agreed-to disruption scenarios including but not limited to:
  - Loss of key site(s) housing technology equipment/services
  - Loss of key third-party IT service providers
  - Loss of key IT service personnel

---

© 2021 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization. NDP126573-1A
For more insights, please visit read.kpmg.us/TRM

Contact us

Cynthia Izzo
Service Network Leader
Technology Risk Management
KPMG LLP
T: 617-988-5613
E: cizzo@kpmg.com

Nicole Lauer
Solutions Leader
Technology Risk Management
KPMG LLP
T: 410-949-8949
E: nlauer@kpmg.com

Richard Knight
Service Champion, IT Internal Audit
Technology Risk Management
KPMG LLP
T: 703-286-8393
E: raknight@kpmg.com

Matt Tobey
Managing Director, IT Internal Audit
Technology Risk Management
KPMG LLP
T: 480-459-3601
E: mtobey@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.

© 2021 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization. NDP126573-1A