



IT internal audit planning for 2025

Key considerations and topics as you prepare
your IT internal audit plan



Introduction



As IT audit teams are actively planning for 2025, it is important for them to understand the organizational IT strategy and align the plan to the strategic direction of the company. With so much change, such as the continued evolution of the cloud landscape, artificial intelligence (AI), increased levels of technical debt, and increased focus from regulators on IT matters, organizations must be able to articulate how their plan is aligned to the risks of the enterprise.

With this understanding, a comprehensive and high-impact technology audit plan should be developed that aligns to company-wide growth strategies and associated risk factors to drive value throughout the entire organization. The use of company-wide strategic objectives, as well as external factors (e.g., new technologies, changes in regulations) and alignment with the enterprise risk team to build the plan can also foster alignment between Internal Audit and business units within the organization (Enterprise Risk Management (ERM), Information Security, Legal, etc.). This can potentially enhance the organization's ability to mitigate risks, and facilitating the creation of value-driven initiatives that drive growth and deliver benefits across the enterprise.

Once key audits have been identified, it is important to be thoughtful about how each is scoped and approached to ensure the plan focuses on the risk objectives previously identified and potential value to the organization. In this publication, we will highlight what we see across the marketplace to help you drive value throughout your plan, as well as “hot” topics to consider as you develop your 2025 audit plan.



What are the big questions to drive value?

IT Internal Audit teams should reflect on the following questions to evaluate whether they fully understand the current risk landscape and align their plan with the overarching business strategy and current risk landscape.

On the CAE Agenda – 2024: There is a spotlight on an overall shift in competencies and skill sets needed for internal audit resources along with the need to upskill resources on IT and enterprise technology topics.



To cope with a barrage of new technology-related risks, IT internal audit teams should be closely aligned to the business and the risk function, to build credibility and relationships and to understand what technologies and processes must be right for the organization to meet its strategic goals and objectives.



Nicole Lauer

Americas IT Internal Audit Leader
KPMG in the US



1

Are we leveraging meaningful data in our risk assessment?

- A data-driven risk assessment plays a pivotal role in developing an effective annual audit plan by providing valuable insights into the organization's risk landscape and identifying emerging risks and trends that may be unknown.
- Data that can be utilized during the risk assessment process can include internal data such as total spend, projects, incidents, as well as external market and industry data.
- Armed with the outputs of the risk assessment, Internal Audit can tailor audit plans to focus on critical areas, ensuring that audits are conducted in a targeted and impactful manner.

2

Are we continuously evaluating the risk landscape and updating the audit plan accordingly?

- Continuously risk assessing your organization's landscape allows Internal Audit to reassess if they are focused on the right topics and provides stakeholders with a higher level of assurance that risks are being actively monitored and managed.
- Continuous risk assessment demonstrates the commitment of the internal audit function to robust and agile risk management practices and strengthens the overall control environment, which can enhance stakeholders' confidence in the organization's operations.
- Continuous risk assessment can also include check-ins with organization leaders to understand their priorities and ensure your plan aligns to their strategic agenda.

3

Do we have the right skill sets to deliver value-add IT internal audit services?

- In a dynamic and changing environment, organizations face evolving risks, technology advancements, and updated compliance and regulatory requirements. The best plan in the world can't be delivered effectively without the right capabilities on the team.
- Having the skills and resources to respond to changing environments enables the Internal Audit team to proactively identify and manage risks, ensure appropriate topics are included on the plan, and for those topics that are included, making sure they are scoped to assess the risks identified.



Topics to integrate for your 2025 planning



01

Application modernization and legacy technology risk

Legacy technology management presents significant risks for organizations, including security vulnerabilities and increased exposure to cybersecurity attacks due to outdated systems and limited support from vendors, leading to potential operational disruption security threats.

02

Cloud strategy

The wide adoption of cloud computing without proper governance measures can lead to security risks, unnecessary costs from underutilization and overpaying for services, as well as challenges to managing multiple cloud providers and optimizing spending.

03

Artificial intelligence (AI)

The emergence of AI technology presents significant disruption and risk due to the need for changes in thinking and behavior, the generation of new operational and strategic risks, as well as potential challenges in quantifying and mitigating risks.

04

Operational technology (OT) / internet of things (IoT)

The increasing sophistication of cyberattacks poses a threat to critical infrastructure and overall organizational stability, requiring alignment between business and IT to achieve operational efficiency and mitigate risks in the complex IT, OT, and IoT systems landscape.

05

Technology resilience

Ensuring operational and technology resiliency is crucial in preventing business interruptions that can impact organizational objectives, necessitating investment in technology solutions and processes for recovering from cyberattacks, system failures, and human errors.

06

IT asset management

Effective IT asset management is essential for establishing strong IT governance, as visibility into the asset lifecycle enables cost optimization, resource allocation, and identification of consolidation or standardization opportunities.

07

Business modernization and transformation

Implementing business modernization initiatives, whether through new technologies or processes, requires a comprehensive approach to manage risks across operational controls, change management, security, etc., in order to help minimize* disruptions to business operations.

08

Regulatory compliance

Regulatory changes impose new obligations on businesses, and IT organizations must remain informed and assess their impact on systems and processes to ensure compliance, avoiding penalties, legal issues, and reputational harm.

09

Third-party risk

Assessing risks associated with third-party dependencies is crucial for organizations as disruptions or failures from such providers directly impact IT operations, systems, services, and overall organizational goals.

10

Data governance

Data underpins every activity organizations perform, and data governance remains one of the most important areas to be audited.

01 Application modernization and legacy technology risk

Legacy technology management is a major concern as obsolete systems pose security vulnerabilities, operational inefficiencies, increased costs, and regulatory noncompliance. Lack of support and updates for legacy systems make them targets for cyberattacks, jeopardizing sensitive data and critical systems, highlighting the need for comprehensive management, assessment, and mitigation strategies to minimize risks of disruption, financial loss, and security threats.



Key risk context:


- In the ever-evolving digital landscape, legacy technology management has emerged as a significant concern for many organizations. Obsolete and unsupported systems present critical challenges such as security vulnerabilities, operational inefficiencies, inflated costs, and regulatory compliance issues. Additionally, as technology advances, vendors often discontinue or phase out support for legacy systems and do not provide the latest security updates and patches. Cybersecurity attacks frequently target outdated systems and exploit known vulnerabilities, putting sensitive data and critical systems at risk.
- Specifically, without comprehensive management of legacy technologies, inadequate assessments of end-of-life systems and limited interim mitigation strategies, the risk of operational disruption, financial costs, and security threats is increased.


How can IT Internal Audit make an impact?

It's pivotal for organizations to align on their technology lifecycle management practices in a proactive manner to avoid cumbersome technology debt and failure to realize benefits such as stable controls, cost efficiencies, and overall agility. As part of these practices, clear processes must be established to identify, evaluate, and react to risks posed by legacy technology. This cannot be an ad hoc procedure but rather something that is undertaken on a consistently defined cadence. When preparing your 2025 technology audit plan, consider having a discrete audit over technology lifecycle management or IT governance and including specific activities such as:

- Assessing your organization's technology lifecycle management practices to determine if they are proactively addressing the risk that maintaining legacy or outdated technology presents to the business. To do so, functions can establish a clear process to identify, evaluate, and address legacy technology risk. This process should include legacy technology reviews, with results being communicated to all stakeholders to ensure that relevant parties were made aware and held accountable for the actions that came out of the review. Consider what tools your organization may have to provide insights into your technology landscape, such as IT service management (ITSM) tools with incident and configuration management database (CMDB) data.
- Identify how are IT initiatives are prioritized and how those initiatives will modernize current technology. Ensure governance processes included in the initiatives include relevant factors such as cost benefit analysis, understanding of the operational impact(s), including impact on risk (e.g., reduction of cyber risk), and alignment to long term strategic objectives.



 Having Internal Audit involved in assessing and managing these legacy technology risks is crucial to ensure that potential weaknesses are identified and addressed, and overall IT governance is maintained. By leveraging Internal Audit's expertise, organizations can proactively mitigate legacy technology risks, protect valuable assets, and navigate the challenges of modernizing their IT infrastructure.

Michael A. Smith
US Internal Audit Solution Leader
KPMG in the US 

02 Cloud strategy

The rapid adoption of cloud computing without proper governance measures can result in security risks and unnecessary costs for organizations. Issues such as underutilization, overprovisioning, and a lack of visibility and control over resource utilization and costs can arise. Managing multiple cloud providers further complicates cost management and optimization efforts due to limited visibility and control over resource usage across the organization's cloud infrastructure. In the early days of cloud, there was a perception that it could drive cost savings for the organization, but the reality is very different; organizations are beginning to question the costs and value and are calling for tighter governance to ensure their cloud strategy makes sense operationally, financially, and from a risk management perspective.



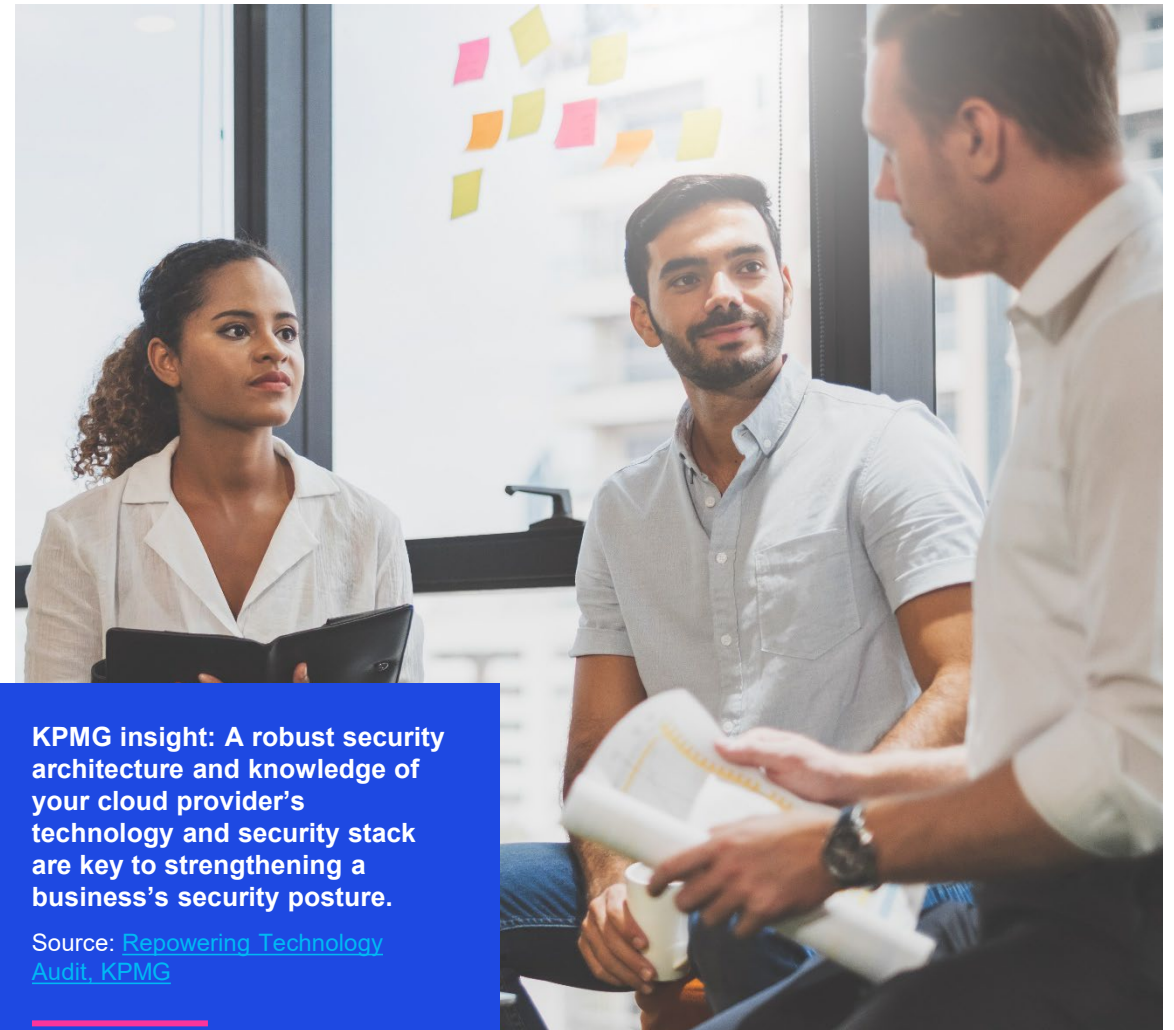
Key risk context:

- In recent years, organizations have embraced cloud computing to capitalize on its scalability, flexibility, and cost-efficiency benefits. However, the rapid adoption of cloud services without adequate governance measures can result in security risks as well as unnecessary costs due to underutilization, a lack of clarity about what cloud services are being utilized (and overpaying for what you truly need), overprovisioning, or failure to decommission unused cloud resources.
- Specifically, we see many clients challenged by cost management related to cloud usage due to the issues highlighted above, complicated by using multiple providers. Managing multiple cloud providers can result in limited visibility and control over resource utilization and associated costs. Tracking usage, identifying unused or underutilized resources, and optimizing spending becomes more challenging due to the distributed nature of the organization's cloud infrastructure.

How can IT Internal Audit make an impact?

Traditional internal audits can focus on the cloud security controls and processes. While this remains relevant and should be considered as part of your plan, with the continual adoption of multiple cloud services and the rising cloud costs that many organizations are experiencing, it is also important to consider how Internal Audit can help management tighten cloud governance, including the management of cloud utilization and cost monitoring. Consider the following activities in your 2025 technology audit plan:

- Assessing your organization's utilization of cloud resources and identifying opportunities for optimization. This involves reviewing the strategy and assessing controls around financial management as well as analyzing query and usage patterns and identifying instances of underutilization.
- Assess and validate any monitoring mechanisms the organization has in place to track the cloud performance, adherence to governance controls, and compliance with policies and regulations. Regular reporting to management and stakeholders helps ensure transparency and accountability.



KPMG insight: A robust security architecture and knowledge of your cloud provider's technology and security stack are key to strengthening a business's security posture.

Source: [Repowering Technology Audit, KPMG](#)

03

AI/Emerging technology

AI has the potential to disrupt the internal audit profession like no other technology before it, bringing new operational and strategic risks across the organization. While AI and other emerging technologies offer unprecedented opportunities, they also introduce risks such as bias, accountability, and privacy concerns that can be challenging to quantify. The increasing adoption of AI across all business units raises the velocity of risk, particularly when third-party models are utilized without adequate consideration for data governance, increasing the risk of data loss and low data quality impacting results. Organizations must weigh the strategic importance of AI against the protection of their data and make informed decisions on the associated costs and risks.



Key risk context:

- AI may be the single most disruptive technology ever. We are yet to fully understand the extent of its impact, but it is expected to disrupt the internal audit profession like no technology before it. AI will change how internal auditors need to think and behave, generative and generate new operational and strategic-level risks across the organization. AI and other emerging technologies hold unprecedented opportunities for the business but bring with them new risks (e.g., bias, accountability) that can be hard to quantify, while possibility extrapolating other risks and exploiting existing vulnerabilities in areas such as privacy, legal, and data governance.
- Specifically, we are seeing the entire enterprise adopt AI across all business units, increasing the velocity of risk to new levels. As new large language models are utilized and are being fed organization data to train them, without adequate consideration for the governance of that data, the risk of data loss and/or the use of poor-quality data to drive results increases. The organization must balance the strategic importance of AI with the protection of its data.



Artificial intelligence is going to be quickly incorporated into systems and processes—which means that not only will technology audit have to rapidly develop a strategy for assuring the risk associated with AI, but also all internal auditors will have to change their mindset to approach operational audits. New risks will need to be considered during planning and execution and internal auditors will need new skills and techniques to audit AI models. The professional must be prepared to evolve.



Richard Knight
US Technology Internal
Audit Solutions Leader
KPMG in the US



How can IT Internal Audit make an impact?

Whether your organization is just beginning to utilize public generative AI models or starting to deploy your own models, AI should be on your 2025 technology audit plan.

Consider including specific activities, as follows:

- Conduct a review of select governance processes over the adoption and implementation of AI solutions (or other emerging technologies) within the organization’s environment. This can include a review of frameworks and policies encompassing how emerging technologies are governed, a review of roles and responsibilities across stakeholder groups, and a review of training programs developed.
- Use Advisory IA products to help design and assess appropriate governance and control models that the organization can adopt to manage the risks associated with AI. Perform assessments against industry frameworks (e.g., NIST AI RMF) to assess current adoption and ensure that all risks are being appropriately managed.
- Consider challenging the business on the processes that are the foundation of a successful AI program, such as data governance, access management, change management, etc., to ensure process-level weaknesses are addressed before they are exploited by the use of AI.



04 OT/IoT

Recent cyberattacks targeting internet of things (IoT) devices have exposed organizations to significant cybersecurity risks, posing threats to critical infrastructure and overall stability. The complexity and interconnectedness of IT, operational technology (OT), and IoT systems present unique challenges, requiring alignment between business and IT to achieve operational efficiency and reduce downtime. Segmentation of OT and IT environments and appropriate controls are essential for effectively identifying and responding to cyber incidents in the OT environment.



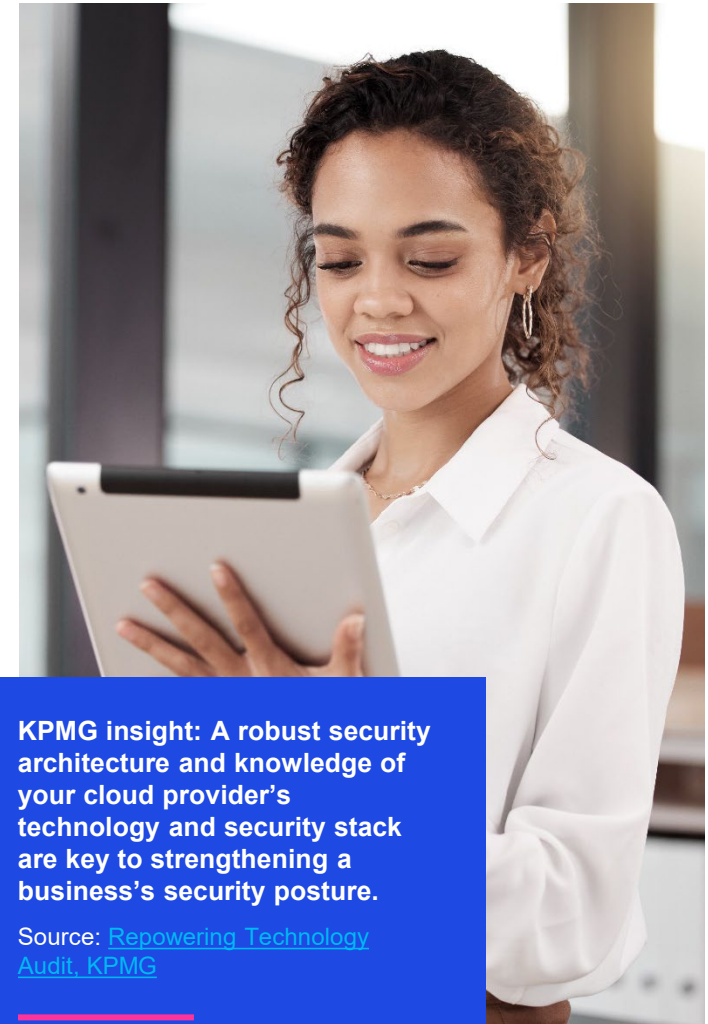
Key risk context:

- Recent cyberattacks targeting internet connected, or IoT devices have exposed organizations to significant cybersecurity risks and potential business disruptions. The increasing prevalence and sophistication of these attacks pose a significant threat to critical infrastructure, industrial processes, and the overall stability of organizations.
- The complexity and interconnected nature of IT, OT, and IoT systems pose unique challenges to organizations. With the increasing integration of IT and OT systems, there needs to be alignment between the business and IT to achieve operational efficiency, improve productivity, and reduce downtime.
- Specifically, we have seen clients have challenges with segmenting their OT and IT environments and ensuring adequate controls are in place to identify and respond to a cyber incident in their OT environment.

How can IT Internal Audit make an impact?

First things first: Does your organization know where all OT and IoT devices are used across your facilities. Even if you are not a manufacturing company, IoT devices have a growing presence throughout your office space. Instead of only relying on reports and data, you can visit a variety of your organization's facilities and experience the real-world application of OT and IoT solutions. Concurrently, risk assessments provide key insights into the existing challenges and potential control gaps within your OT and IoT landscape. Consider including the following activities in your 2025 technology audit plan:

- Utilize relevant organizational data and analytics, such as the number of connected devices by site, to select a representative sample of facilities at the organization to visit and assess the processes and technologies used related to OT and IoT.
- Perform evaluations over the risk landscape of the organization's OT and IoT environment to understand current risks and control gaps.
- Across both activities, relevant focus areas could include asset management, remote and physical access, segmentation, incident response and recovery, and security monitoring.
- Consider assessing the supply chain of OT devices; significant reliance on third parties to manage the OT environment may be exposing the organization to potential vulnerabilities.



KPMG insight: A robust security architecture and knowledge of your cloud provider's technology and security stack are key to strengthening a business's security posture.

Source: [Repowering Technology Audit, KPMG](#)

05 Technology resilience

Investing in technology solutions and processes is crucial for operational and technology resiliency to prevent significant business interruptions. Recovering from cyberattacks, system failures, and human errors is essential to maintain your reputation and trust from customers, investors, and stakeholders. Organizations must identify and document the technology critical to their operations, ensuring business-critical data availability, and considering resilience strategies for both cloud and on-premise systems.



Key risk context:

- OT resiliency is critical to prevent significant business interruptions that have a direct impact on the organization's objectives. A key consideration for enabling resilience is investing in technology solutions and processes that provide the ability to recover from cyberattacks, system failures, and human errors. Technology disruptions can have a significant impact on an organization's reputation and brand image. Customers, investors, and stakeholders may lose trust if an organization fails to recover quickly or adequately respond to technology-related incidents.
- Specifically, organizations may still lack appropriate processes to identify and document the technology critical to their business operations, which can result in business-critical data not being available in the event of an incident. Additionally, the interplay between cloud and on-premise systems and ensuring the resilience strategies should consider all your technologies, regardless of where they are hosted.

How can IT Internal Audit make an impact?

The most effective approach to conducting a Technology Resilience audit begins with performing a thorough examination of your organization's process to identify critical systems. By gaining a comprehensive understanding of these critical systems, auditors can subsequently develop and implement more substantive approaches for validation. Consider including the following activities in your 2025 technology audit plan:

- Review crisis management procedures, tabletop exercises, or other planning scenarios to determine if the plans adequately address potential threats and if they can be successfully executed during a simulated event.
- Evaluate the organization's capability to recover from technology disruptions. This includes reviewing recovery time objectives (RTOs) and recovery point objectives (RPOs) to assess if they align with business requirements, ensuring there are appropriate action plans in the event of a disruption, and results are communicated to appropriate stakeholders throughout the organization.
- Review select business-critical systems to confirm backup and recovery processes are being followed in accordance with organizational policies.



KPMG Insight: During a cyber incident, organizations need a response that is measured in minutes and hours, not days and weeks. Cyber resilience is vital for maintaining business operational capabilities, safeguarding customer trust, and reducing the impact of future attacks.

Source: [The Cybersecurity Considerations for 2024 Outlook](#), KPMG

06 IT asset management

Effective IT asset management is fundamental to IT governance, enabling organizations to optimize costs by eliminating unnecessary or underutilized assets, allocating resources properly, and identifying opportunities for consolidation or standardization. It also plays a critical role in cybersecurity and risk management, allowing CIO/CISOs to track and monitor assets, identify vulnerabilities, manage access, apply security patches, and protect sensitive data. However, many organizations still lack a comprehensive inventory of assets and the ability to fully understand the connections and service mappings among them.



Key risk context:

- Effective IT asset management sets the foundations for effective IT governance, so it follows that you can't govern something if you don't realize it exists in your environment. By gaining visibility into the asset lifecycle, costs can be optimized by eliminating unnecessary or underutilized assets, ensuring proper allocation of resources, and identifying opportunities for consolidation or standardization.
- Appropriate IT asset management practices are critical to cybersecurity and risk management efforts. CIO/CISOs can track and monitor assets to identify vulnerabilities, ensure timely security patches and updates, enable efficient access management by accurately identifying unauthorized users, and ensure privacy safeguards are in place to protect sensitive data.
- Specifically, we continue to see clients without a comprehensive inventory of their assets and the ability to correlate the connections and service mappings across assets.

How can IT Internal Audit make an impact?

Effective internal audit IT asset management reviews require a review of every stage of an asset's lifecycle—from initial acquisition to eventual retirement. It calls for scrutinizing processes for procurement, deployment, utilization, maintenance, and disposal, offering insights into how effectively assets are managed. This is a foundational topic that impacts many other IT processes; therefore, consider including the following activities in your 2025 technology audit plan:

- Evaluate the organization's processes for managing assets throughout their lifecycle, from acquisition to retirement. This includes reviewing processes for asset procurement, deployment, utilization, maintenance, and disposal.
- Perform an assessment of the organization's asset management tooling capabilities. For example, assess the current usage of standard tools such as a CMDB to track and store asset relationships and dependencies.
- In conjunction with the tools utilized, review the organization's asset inventory to ensure its accuracy and completeness. If tools are not utilized, review offline inventories.



KPMG Insight: During a cyber incident, organizations need a response that is measured in minutes and hours, not days and weeks. Cyber resilience is vital for maintaining business operational capabilities, safeguarding customer trust, and reducing the impact of future attacks.

Source: [The Cybersecurity Considerations for 2024 Outlook](#), KPMG

07 Business modernization and transformation

Implementing business modernization initiatives, whether through new technologies or processes, requires considering risks across multiple areas to ensure smooth transitions and limited disruption to business operations. It is crucial to adopt a risk-managed approach when deploying new systems and applications, with a clearly defined methodology for software development and project management. Without proper risk management, there is a risk of unrealized benefits, cost overruns, weak internal controls, cybersecurity issues, noncompliance, and expensive remediation efforts.



Key risk context:

- Implementing business modernization initiatives, whether those are new technologies (increased use of AI, cloud migrations, new ERPS, etc.) or new processes, often requires changes in ways of working. It is important to consider the risks across a multitude of areas (operational controls, change management, security, etc.) to ensure the risks of changes are managed and there is limited disruption to business operations.
- Specifically, too often we see the lack of a risk-managed approach to deploying new systems and applications. Without a clearly defined software development and project management methodology, there is a significant risk that benefits will not be realized, costs will spiral out of control, and systems will be implemented with weak internal controls structures. In turn, this can lead to cybersecurity issues, noncompliance with significant regulations, and many other challenges that lead to expensive and time-consuming remediation activity.

How can IT Internal Audit make an impact?

Internal Audit should have a seat at the table for the most critical business modernization and transformation initiatives. This helps ensure collaboration with the Project Team, allowing for real-time response as project timelines shift and critical milestones are achieved. Through this integrated approach, Internal Audit can dynamically adapt, responding aptly to change and help the business course correct. In addition, by aligning audit procedures with key project activities, internal audit can deliver post-action reports that offer insights on your organization's initiatives. The result is a more involved and adaptable audit process that affords your organization comprehensive and timely insights. The exact scope will be dependent on your organization's modernization and transformation initiative; however, consider the following approaches:

- Embed internal audit procedures into high-risk/critical projects by attending weekly project status meetings and adding identified risk areas to the project risk log. This approach allows Internal Audit to collaborate directly with the Project Team as the project timeline changes and key milestones are met, and to provide assurance to not only the Project Team but to executive and board-level stakeholders.
- Internal Audit can align their procedures with key project activities and report out after these activities take place. For example, Internal Audit can perform detailed procedures to support vendor management during a vendor's implementation or by validating that data has been migrated completely and accurately prior to go-live, and they may use this information to input at stage gates for the Project Team to support their go/no-go decision.



KPMG insight: Most successful organizations have leveraged ERP transformation by embedding internal audit and internal control streams. Our survey responses indicate that just 26 percent of internal audit teams are involved in all stages of organizational change journeys.

Source: [Trailblazing Digital Frontiers: The KPMG Global IT Internal Audit Outlook, KPMG](#)

08

Regulatory compliance

Regulatory changes require IT organizations to stay updated and assess their impact on systems and processes to ensure compliance. Regulators are focusing more on technology, introducing regulations related to AI, privacy, cybersecurity, and operational resilience. This increased regulatory focus on IT imposes greater complexity on internal risk and compliance functions, leading to a rise in control and remediation projects in the market.



Key risk context:

- Regulatory changes often introduce new requirements and obligations for businesses. The IT organization needs to stay informed about these changes and assess their impact on IT systems and processes. By understanding regulatory updates, CIOs can ensure that their organization's IT infrastructure and operations comply with the changing rules and regulations, avoiding noncompliance penalties, legal issues, and reputational damage.
- Regulators continue to focus on technology in their regulatory remit. Whether it is emerging regulations around the use of AI, increased focused on privacy, expecting organizations to tighten cybersecurity governance to protect consumers or focusing on resiliency and continuity of operations, regulators are expecting more from businesses. A recently implemented regulation affecting public filers is the cyber incident reporting for SEC registrants. This includes disclosure rules and cyber incident reporting laws as well as a focus on incident response processes.
- Specifically, we continue see more regulatory focus on IT and increased complexity for internal risk and compliance functions in staying on top of this focus, evident in an increase in the volume and complexity of control and programmatic remediation projects in the market.

How can IT Internal Audit make an impact?

Internal Audit can critique your organization's regulatory compliance programs and the associated operating models to help stay abreast of existing and emerging regulations. Internal Audit can also advise the business on how to respond to regulatory requirements through the design and implementation, continuous monitoring, and remediation (if necessary) of controls. Consider including the following activities in your 2025 technology audit plan:

- Review processes established for continuous monitoring and updating of IT regulatory changes. This involves staying informed of ongoing regulatory developments, assessing their impact to the organization, and ensuring that compliance efforts remain up to date.
- Work with IT and the business (e.g., ERM, Legal & Compliance, Operations) to identify high priority regulations. Prior to your organization presenting its compliance to regulators, review and validate any self-assessments or internal remediation used to assess current maturity against the regulatory requirements.
- For publicly traded companies, within your next security incident response review or audit, include a specific scope area around the SEC cyber disclosure requirements, specifically testing the organization's ability to respond to cybersecurity incidents according to the SEC requirements.



KPMG insight: 42percent of CROs believe regulatory changes are the biggest challenge to their organization over the next 2–5 years.

Source: [The 2024 Chief Risk Officer Survey, KPMG](#)

09

Third-party risk

Organizations rely heavily on third-party providers for various technology services, making it essential for CIOs to assess the associated risks. Any disruption or failure from a third-party provider can directly impact IT operations and services, as well as the organization's goals. CIOs should evaluate the security practices and protocols of third-party vendors to protect against data breaches and unauthorized access to sensitive data. Understanding and mitigating the risks associated with third-party dependencies have become increasingly important in recent events and client examples.



Key risk context:

- Almost all organizations rely on third-party providers for various technology services and solutions, including cloud services, managed IT services, software development, or hardware maintenance. CIOs need to assess the risks associated with these dependencies, as any disruption or failure from a third-party provider can directly impact the organization's IT operations, systems, and services and ultimately the goals of the organization.
- Third-party vendors often have access to sensitive data or critical IT infrastructure. If a third-party vendor experiences a data breach, a loss of operations, or has inadequate security measures in place, it can result in loss, theft, or unauthorized access to the organization's data. CIOs need to evaluate the security practices and protocols of third-party vendors to ensure they meet the organization's security standards and protect against potential data breaches.
- Specifically, in both public recent events as well as specific client examples, the importance of understanding the exposure to your organization's use of third parties and how to mitigate and monitor that risk has become even more important.

How can IT Internal Audit make an impact?

While third-party risk is not new, issues and incidents with third parties continue to be more common. The risk is increasing, and the velocity of issues/events is becoming more rapid. It is important for Internal Audit to review and assess third-party services holistically, which could include the example activities stated below.

- Evaluate the vendor risk management program and the adequacy of risk mitigation measures implemented for high-risk vendors, such as contract clauses, vendor performance monitoring, and incident response plans.
- Ensure the organization has a process to systematically review key metrics such as service level agreements (SLAs), key risk indicators (KRIs), and key performance indicators (KPIs) to ensure these partners meet expected standards and outcomes are achieved.
- Understand any fourth-party risk and review the initial setup of the vendor to ensure right to audit, and embed risk management in the contract to review to ensure controls covers subservice organizations.
- Assist management committees or other key stakeholders in being prepared for potential vendor incidents, such as data breaches or a loss of operations, by assessing whether adequate cybersecurity controls and risk management practices are in place for vendors.



KPMG insight: Creating an ongoing and enterprise-wide risk management strategy that ensures third-party vendors are worth the investment is critical to the organization.

Source: [The 2024 Chief Risk Officer Survey, KPMG](#)

10 Data governance

Data governance is an essential area to be audited as data drives organizational operations. With the rise of emerging technologies like AI, effective data governance becomes even more crucial, instilling confidence in employees to leverage automation and innovation. It enables faster operations, the development of new products and services, and the generation of reliable financial and nonfinancial reports, particularly valuable in highly regulated industries.



Key risk context:

- In today's dynamic business landscape, data plays a pivotal role in driving organizational operations, making data governance a crucial area to be audited. The significance of data cannot be overstated, as it underpins every activity within an organization.
- With the continuous growth of emerging technologies like AI, effective data governance becomes even more critical. It provides employees with the confidence to utilize AI and advanced automation, facilitating faster operations, innovation with new products and services, and the generation of robust financial and nonfinancial reports that can withstand intense scrutiny, particularly in highly regulated industries.

How can IT Internal Audit make an impact?

Internal audit functions can act as a catalyst for improving data governance practices over organizations, helping to enhance data quality, data privacy, and overall data management capabilities. Consider the following topics in your 2025 technology audit plan:

- Leverage IA's core expertise to support the organization in mapping out data flows, enabling the business to identify key data risks and subsequently establish effective controls.
- Evaluate the effectiveness of data governance mechanisms the organization has in place, such as data quality controls, data classification, data access controls, and data privacy measures.
- Review processes established for continuous monitoring and updating of regulatory changes. Example regulatory changes could be the California Consumer Privacy Act (CCPA) and/or GDPR (General Data Protection Regulation). Both of these review processes have put pressure on organizations to manage personal data with care and attention.



Data quality underpins everything, and with increased use of AI models, issues with data governance will be exposed more frequently and the impact will be more meaningful. Data governance is a critical discipline for the business to get right and for IT Internal Audit to support. A robust approach to data governance is important to allow organizations to make better business decisions, reduce cybersecurity risks, and to promotion external stakeholder confidence. Internal Audit can help organizations get it right.



James Buchanan
ASPAC Head of IT
Internal Audit
KPMG Australia



Final thoughts:

By building a robust and thoughtful 2025 technology audit plan, you can enhance Internal Audit's role as a strategic partner with business leaders as the organization continues to evolve and adapt. Fostering alignment between Internal Audit and the senior leadership teams enhances the organization's ability to mitigate risks and facilitates the creation of value-driven initiatives that drive growth and deliver benefits across the board. To build this plan, key considerations to keep in mind include:

- Reviewing and adjusting top risks to your company on a periodic basis.
- Aligning audit objectives with company-wide growth strategies while considering external risk factors to drive value throughout the entire organization.
- Ensuring your Internal Audit team has the right training and skill sets to identify and deliver the identified audits, adding value to the business.

Finally, aligning the audit plan to the risk agenda for your organization is crucial. It requires a deep understanding of your organizational IT strategy and a careful assessment of the core activities that are essential for your success. By identifying these key areas, you can develop a technology audit plan that is tailored to your organization's specific needs and risk profile. This targeted approach helps ensure that the audit plan aligns with your company-wide growth strategies and addresses the most pressing risks and challenges you may face. By selecting the right topics, you can drive value throughout your entire organization and lay the foundation for a successful future in the rapidly evolving technological landscape.

How KPMG can help:

Given how closely KPMG works with many of the world's leading organizations, we have deep insights based on extensive industry experience that help us understand what a business must get right to deliver on its objectives. An audit plan should never be constrained by the resources you have available. The breadth of services that we provide allows us to bring subject matter knowledge and experience to many audit topics, which can bring not just credibility to your internal audit function but can also bring value to the organization. Based on the risk within your organization and the demand for audits, we can help you to scale your resource model to be able to effectively develop and deliver your plan.



Read our companion article

Trailblazing digital frontiers: Global IT internal audit outlook

Discover how technological advancements are reshaping the audit landscape and what organizations should focus on to keep pace with these changes.

[Read it here.](#)

For more information about how KPMG can assist and improve your internal audit team, please visit our [website](#) or contact one of the following:

Connect with us



Richard Knight

Principal, Internal Audit and Controls
T: 703-286-8393

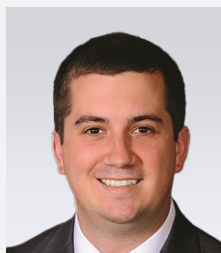
E: raknight@kpmg.com



Matt Tobey

Principal, Cyber Security and Technology Risk
T: 480-459-3601

E: mtobey@kpmg.com



Brian W. Krebs

Director, Internal Audit and Controls
T: 410-949-2794

E: bkrebs@kpmg.com



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

Learn about us:



kpmg.com

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.

© 2024 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. USCS022440-1A

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.