Repowering technology audit

Global IT Internal Audit outlook

KPMG International | kpmg.com

Foreword: Transforming the IT Internal Audit function in a new era of opportunity and risk

The technology audit function is enduring various challenges as the pace of change accelerates, and the risk climate soars in today's dynamic global environment.

Revolutionary technology advances in cloud services, artificial intelligence (AI), cybersecurity, data privacy, automation, and the proliferation of hybrid working models are unleashing complex IT risks that have the potential to threaten business operations, competitiveness, regulatory compliance and reputations.

Today's technology audit teams are facing a perfect storm, struggling to manage fast-emerging risks, enhance the scope, speed and frequency of audits, and adopt new digital skills and automation. At the same time, as organizations transform to compete in the digital economy, technology risks are in sharp focus among boards, audit committees and executive leadership teams (ELT) — all now relying on IT Internal Auditors as their primary source to assess and mitigate emerging risks.

By gaining a prominent new voice with leadership and taking a seat at the table to deliver strategic, data-driven insights, Internal Audit will play a new role as a trusted advisor to the business.The future of Internal Audit is here and demands a bold new mindset that takes in not just where a business *is* today but where it is *going* during the transformation journey.

Internal Audit's target operating model should be designed to transcend core operational risks to focus on emerging risks as the digital technology landscape continues to explode. As organizations embrace disruptive new technologies, Internal Audit should become a strategic partner to the transformation team, providing assurance over the transformation process — rather than simply auditing post-implementation.

And there is little time to lose. As KPMG firms' research indicates, only 39 percent of businesses surveyed in the previous edition of KPMG's Global IT Internal Audit report — *Agile, Resilient & Transformative* say the capabilities of their audit team currently exceed or significantly exceed board and leadership expectations. A mere 33 percent of business leaders we surveyed rated their preparedness to audit today's technology-associated risks as good or excellent — leaving a vast majority of businesses unprepared as a new world of risk engulfs them.

This timely, insight-filled KPMG report examines how organizations can propel the IT Internal Audit function toward a new reality that includes being a strategic advisor to the business, performing holistic risk assurance, adopting creative methods to attract talent and embracing innovation in the way we work. The profound disruption of the global COVID pandemic has provided a unique opportunity for audit professionals to evolve beyond their traditional approach. Amid ongoing change, disruption and business transformation, KPMG believes that a new role for audit is inevitable and indispensable.

I want to thank all those who gave their valuable time to participate in this report. We hope you will find it insightful and informative as businesses like yours navigate a new reality of opportunity and risk — one in which IT Internal Audit plays a revolutionary new role.

Anil KV
Global Leader for IT Internal Audit,
KPMG International and Partner,
KPMG in India

Giving technology audit a strategic new role

Creating value through holistic risk assurance

Solving today's critical skills gap

Transforming audit through innovation

Conclusion

Contents

Giving technology audit a strategic new role

In today's digital economy and with the 'need for speed' as the pace of change accelerates, Internal Audit should be seeking a new voice in strategic decision-making and enhance its overall value to the organization. The challenges are significant and complex.

Giving technology audit a strategic new role

Creating value through holistic risk assurance

Solving today's critical skills gap

Transforming audit through innovation

Conclusion

IT Internal Audit leaders should be asking themselves these pivotal questions as the audit playing field shifts:

1. **What is my role in the organization and how can I enhance my brand?**
2. **What value and insights should I be delivering?**
3. **How can I take a leading role in driving assurance to the board?**
4. **How can I sustain leadership confidence and trust in Internal Audit's evolving role?**

KPMG firms are witnessing a big push for Internal Audit to heighten collaboration across the business in response to the risk landscape.

In many organizations, regardless of size, it can be extremely difficult to determine which business functions must provide assurance against technology and data-related risks. Typically, larger organizations are pursuing integrated assurance. Regular forums are in place to discuss and agree on forward-looking planning and other assurance activities, to minimize duplication and gaps and update key stakeholders.

Generally accepted roles and responsibilities across the three lines of defense are as follows:

- First line of defense — operational management, implements controls.
- Second line of defense — assures functions set policies and procedures.
- Third line of defense — enhances and protects organizational value by providing risk-based and objective assurance, advice and insight.

While the three lines of defense model has drawn out some serious debates — offering strong arguments for and against the usefulness and practicality of the model — it's undeniable that organizations should seek to strengthen the relationship between the *second* and *third* lines of defense.

Bringing risk management and Internal Audit teams together can provide a consistent and broad-ranging approach across the entire organization. Collaboration between these two functions aims to cut across silos, leveraging each team's resources, skill sets and experiences to build critical new risk capabilities within the organization.

Clear, integrated assurance is essential

The clear articulation of inherent and residual risks, updated on a near real-time basis using trusted data, plus effective horizon scanning, is vital. And while organizations in other sectors may not be as highly regulated as the others, the ongoing proliferation of data, automated decision-making and scrutiny around sustainability, supply chains and data security all point to a crucial need for alignment around risk assurance.

Unfortunately, many organizations lack a true understanding of precisely how each line of defense functions. While first-line management often fails to see assurance activities as a directly valuable investment — even if they understand its importance — audit's enhanced ability to demonstrate ROI and the need for innovation can drive new investment. As Internal Audit pivots to a more strategic role in the organization, it should take an educational approach and participate in the challenging digital-transformation agenda. Technology audit can play a critical new role in this respect, encouraging the formalization of control frameworks and providing specific and thematic suggestions for control improvements and automation.

> “Make no mistake — the future of audit is here and it is data-driven. Providing pragmatic advice by extracting relevant insights from data is now a key mandate for Internal Audit leaders.”

Phillip J Lageschulte
Global Enterprise Risk Services Leader
KPMG International and Principal
KPMG in the US

Giving technology audit a strategic new role

Creating value through holistic risk assurance

Solving today's critical skills gap

Transforming audit through innovation

Conclusion

KPMG professionals have seen this work most effectively when technology audit uses process mapping, automated scripts, bots and data analytics to identify issues. These serve as a vital 'proof of concept' for new control solutions operated by management and checked by relevant assurance teams. This approach makes it easier for management and assurance teams to monitor process efficiency and free up technology audit for more-strategic input.

Internal Audit should have the profile, credibility and strength of relationships with stakeholders — customers, regulators, suppliers, employees and more — to deliver hard messages and challenges to actively anticipate risks and drive the business forward by effectively redefining its approach to risk and audit work.

A target operating model for the future

Technology audit should not be any transformation program's primary assurance provider. While some organizations rely on Internal Audit to perform detailed assurance on projects and programs, invariably, such assurance is constrained by capacity and generally results in point in time, high-level and limited scope.

Going forward, the ideal role of Internal Audit is to perform thematic reviews across the change portfolio, covering overarching considerations around how, for example, security or data protection has been engineered amid change management or how the organization is ensuring proper budgeting and financial management across all key projects and programs.

The target operating model for a modern technology audit function should be forward-looking, strategic and a true contributor to business value. This includes defining how governance, people, processes and technology will play a strategic role in the organization.

Taking a broader view of the risk landscape

An overarching view of the organization's risk landscape versus its assurance coverage is fundamental to understanding what's required in an Internal Audit function and its technology audit team. Consistent with bringing value to the organization, there is the need to ensure that Internal Audit functions move from predictable areas of risk to less-predictable and more complex themes.

For Internal Audit to make this shift, they should aim to better understand their control landscape and to use, for example, GRC tooling for routine monitoring of key controls managing operational and regulatory risks and objectives. Forward-looking Internal Audit teams increasingly rely on data analytics specialists and agile development practitioners. Evolving technology audit teams are also starting to use automated data analytics and testing routines — including embedding bots in key processes to provide testing and exception reporting.

This evolution is positioning technology audit to take on an important control assurance leadership role in the organization, where routines are piloted by audit before being evaluated and adopted. This positions technology audit to help drive the organization's control-assurance maturity and maintain a strategic role as a pathfinder and innovator. The resilience can only be judged based on its ability to deliver exactly what is required of it, which demands meticulous planning. This includes: understanding the specific assurance needs of the technology audit; identifying what the function already has in place; determining — given the nature, capacity and output of other assurance providers — the required size, capacity and capability of the technology audit function.

> “
> Risk assessment in the Internal Audit space has become more dynamic than ever — moving to an almost real-time basis.”

Tejas Mehta
Head of UK & FS IT
Internal Audit
KPMG in the UK

Audit's enhanced value should enable new investment

Justifying investment that drives the Internal Audit function forward is essential in today's risk-laden environment. Ultimately, this relies on the ability of audit leaders to generate strong relationships with leadership and credibility as trusted partners in safeguarding the organization.

A truly resilient technology audit function features team members who understand the sector and environment in which the organization operates and can deliver timely, insight-driven recommendations in their audit reports that align with the organization's objectives and unique risks. That includes enhancing soft skills to help build organizational networks, improved report writing and better collaboration and business awareness.

The future demands that Internal Audit deliver new value as a strategic business partner that encourages investment and demonstrates ROI to ensure its resilience, relevance and ongoing evolution. Success will demand strong strategic, communication, data and digital transformation skills — ultimately moving from lower-value transactional assurance and working to enhance their brand value and attract investment in their people, processes and technology.

> "The sheer volume of digital and data-led transformation, and the drive for increased efficiencies and automation, mean that we need to be much more digital, data-led and targeted as technology audit professionals."

Charlie Frieze
Associate Director, IT Internal Audit
KPMG in the UK

Creating value through holistic risk assurance

A focus on operational risk remains essential to technology audits to ensure processes and capabilities remain aligned with organizational policies and procedures. But maintaining a traditionally narrow focus in a technology-driven and risk-filled environment fails to add significant safeguards and value to the enterprise.

Technology audit teams must continue to provide assurance over operational risks — but this is no longer enough. Boards, audit committees and ELT are looking for a different kind of assurance. They need the audit function to provide strategic advice related to investments they are making in the future of their business. The percentage of an organization's operating capital that is being invested in technology continues to rise in order to: enable more automation; take out costs; enhance customer experience; deliver new insights; enhance resiliency amid evolving cybersecurity risks; and maintain a consistent level of availability in order to grow the business.

As the risk landscape soars, auditors should aim to step up and translate emerging technology risk into business risk and hold meaningful, insight-filled conversations that can help drive trust and credibility among leadership and boards.

Gone are the days when technology auditors could get by with understanding processes and stable technology. They must understand the business and its strategy and be able to inform the board, audit committee and ELT of risks associated with the investments they're making.

This understanding requires the technology audit team to upskill and establish trust and credibility to be 'invited to the table' and join the strategic discussions. This won't happen overnight, but a plan should be established to begin this journey and move beyond auditing the same IT operational processes.

In this section, we discuss some emerging risks that auditors should understand to demonstrate credibility and provide meaningful insights to the business.

A new audit mindset is crucial as risks soar

Today's audit leaders should make holistic audit plans and broaden their horizons to include a mix of operational and emerging risks. Emerging technology risk areas that Internal Audit functions need to address include:

Cloud governance: Cloud-related risks should always be in focus. Automation from deployment through to monitoring and remediation is key — cutting down on misconfigurations and ensuring compliance with business strategy and needs.

A robust security architecture and knowledge of your cloud provider's technology and security stack are key to strengthening a business's security posture. Knowing security obligations and leveraging options will make deploying, automating and uplifting controls easier.

Cyber defense: The explosive pace of digital transformation, the proliferation of work-from-home business models, and the growing sophistication of today's cybercriminals continue to fuel costly and disruptive cyberattacks worldwide, particularly ransomware events and major supply-chain disruptions.

> "In today's hypercompetitive digital economy, IT Internal Audit is being required to work more efficiently than ever while helping organizations create more value in less time. Rising to this new reality demands modern approaches, skills and capabilities that will foster trust within the organization and enable stakeholders to see the value of the Internal Audit function."

Laurent Gobbi
Global Technology Risk Leader
KPMG International and Partner
KPMG in France

According to KPMG research, audit leaders cite cyber risk as a key challenge today.[1] At the same time, KPMG research also shows that just 43 percent of businesses surveyed reported that their teams perform risk assessments annually, while only 18 percent perform them continuously. In today's reality, technology audit is no longer a point-in-time exercise. Audit's 'need for speed' has never been greater.

Appropriate new controls are now essential to protect high-value assets — the 'crown jewels' of the organization and its clients. Businesses must continually scan for vulnerabilities across their networks and remain ready to respond, recover and re-establish trust as quickly as possible to mitigate damage in the event of a disruption.

Security will only become more challenging as the complexity of supplier ecosystems increases along with regulatory scrutiny. Businesses should seek to transition away from compliance-based strategies to a highly proactive approach that puts continuous monitoring, usage of AI/ML-based solutions, threat intelligence and zero trust at the heart of its ecosystem security model.

Data security, governance and privacy risk: Growing regulation has prompted many businesses to continually enhance data-management capabilities and controls. And as they look to the future, their privacy programs should incorporate privacy-by-design thinking — embedding privacy and security into organizational change, culture, processes, technology and products. Modern data protection now demands a multi-faceted approach featuring close collaboration among cybersecurity, technology and regulatory teams.

The good news is that data security, privacy and governance are gradually becoming core competencies among today's evolving Internal Audit function, and as audit grows in stature, businesses are investing in capabilities to enhance data security and privacy protection.

Zero trust architecture: Zero trust is a modern security mindset that has the potential to revolutionize how audit teams approach cybersecurity. Zero trust shifts the traditional paradigm by assuming a hostile threat actor has compromised the network and thus makes security and access decisions based on identity, device, data and context. By giving users minimal required access to systems, zero trust adds a layer of protection to network resources by verifying that every user request is authentic.

DevSecOps: DevSecOps is gaining momentum amid the need for rigorous security that moves at the speed of cloud and technology adoption. DevSecOps primarily focuses on building, testing and releasing software rapidly, frequently and reliably. A collaborative, multi-disciplinary DevSecOps framework — characterized by a suite of relevant controls, security scanning and automated testing — should be standard operating procedure to facilitate compliant and safe service delivery.

Security automation should be built into every critical intersection point in the software development lifecycle (SDLC), from user stories and secure-code reviews to threat modeling and secure-design reviews — with the help of both static and dynamic application security testing products. By automating as many SDLC aspects as possible, teams can deploy working code continuously. But compliance controls may be siloed from the SDLC, hindering controls, compliance and cross-functional collaboration. Organizations are facing an increasingly complex balancing act in which they must consider developing at speed, protecting against security threats and meeting audit and compliance requirements.

> “Organizations still have a long way to go to reach a high level of maturity in data and analytics. Artificial intelligence is going to be quickly incorporated into systems and processes — which means that technology audit will have to rapidly develop a strategy for assuring the risk associated with AI.”

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

[1] Agile, resilient & transformative — Global IT Internal Audit Outlook.

Identity and access management: Ongoing data breaches and the growing sophistication of cybercriminals continue to highlight the importance of an effective IAM solution. Current IAM models, built initially to manage digital identities and user access for single organizations, are now being revisited to offer the right level of resilience and critical authentication features.

As digital technologies continue to emerge, many countries and territories have implemented rights-based privacy rules and regulations to give people control of their personal data. With so many diverse regulations, however, the regulatory landscape is increasingly difficult to navigate.

Organizations would be at a distinct disadvantage without automated IAM processes supported by effective metadata management. Internal Audit teams should be at the table to help design and assess automated IAM solutions and ensure risk is appropriately managed.

AI, ML and robotic process automation: The revolutionary capabilities of AI, machine learning (ML) and robotics all hold opportunities for businesses. But this exciting new reality comes with considerable risks — financial, technology, reputational, legal, regulatory and compliance-related.

Boards, audit committees and ELTs are increasingly relying on audit teams to assess the strategic risk of these powerful new technologies. Internal Audit needs to help design and assess appropriate governance and control models as AI, ML and robotics roll out across the organization and as increasingly complex AI/ML models play a growing role in decision-making.

The future demands that technology audits review and help manage automation and robotics oversight, security design, vulnerability assessments, access and change management, and responsibilities. For AI, audit should review methodology, governance, core IT controls, resourcing, intentional/unintentional biases, tolerance limits, training data, change management and access.

Model assurance: KPMG research shows that most businesses the US firm surveyed in their *2022 KPMG US Technology Survey Report* said their organization had a clear definition of AI and predictive analytics models. But they also cited a lack of transparency as a serious risk. Many are using outsourced 'blackbox' models that they lack visibility into, raising questions of whether the software vendor has addressed all potential risks.

There is currently no AI equivalent of Sarbanes-Oxley and no self-certification/third-party certification standard is in sight. Detecting and preventing errors or biases in AI models can be remarkably challenging. A lack of transparency or inadequate governance regarding these models may lead them to deviate from business needs and objectives.

Internal Audit should seek to provide smart solutions via close collaboration with AI experts who can help identify risks associated with AI and predictive models. Using risk and controls expertise, AI professionals can assist the business in identifying key operational risks and help ensure that appropriate controls are in place.

> “The need for clearly aligned risk reporting is paramount today, supported with careful modelling and cyber risk quantification. This can help decision makers understand actual levels of risk exposure and what measures can be taken to manage risk across critical business areas. Great strides have been made in this space in recent years, with the ability to make a real difference when aligned with organizational risk frameworks, and when transparent about the pros and cons of such models.”

Akhilesh Tuteja
Global Cybersecurity Leader
KPMG International and Partner
KPMG in India

Giving technology audit a strategic new role
Creating value through holistic risk assurance
Solving today's critical skills gap
Transforming audit through innovation
Conclusion

Blockchain, smart contracts and NFTs: Blockchain is quickly revolutionizing many industries thanks to its permanent, real-time verification of financial and operational transactions. Blockchain, using non-fungible tokens (NFTs) denoting ownership of digital files and smart digital contracts stored on a blockchain that are automatically executed when predetermined conditions are met, offers the potential for real-time auditing and continuous assurance.

For example, companies can maintain controls around their financial systems by continuously monitoring the blockchain and identifying when a control is circumvented. Blockchain technology designs differ in architecture, and some are more secure than others. For blockchain to proliferate, the technology will need to be taken up widely by businesses — together with a willingness to share a higher level of information.

It remains to be seen how companies will view the required level of transparency and adopt blockchain technology. But some global organizations are leading the pack on blockchain adoption. Blockchain scores highly on the list of key audit areas to be reviewed, making it crucial that audit keeps this emerging technology in focus as its role evolves.

> “As technology continues to advance, and the role of Internal Audit expands, it’s critical for IT audit professionals to remain at the forefront of emerging technology risk to provide timely and broad-ranging risk, controls and assurance advice.”

James Buchanan
Director and Head of IT
Internal Audit in Asia Pacific
KPMG Australia

Solving today's critical skills gap

New skills are critical as audit requirements and expectations grow in scope and complexity. Audit teams need to be technically skilled and knowledgeable about the suite of technologies their business is deploying. They should remain current amid change and work as a trusted partner in managing risk and providing strategic insights that enhance revenue, growth and brand reputation. Businesses are showing greater urgency to close the skills gap, but progress needs to accelerate without delay, as research continues to reveal.

The KPMG 2022 global technology report notes that cybersecurity teams are under immense pressure to keep up with evolving threats as critical talent shortages undermine security efforts. More than half (58 percent) admit they are behind schedule on the need to enhance cybersecurity. The case with technology audit teams is no different. The lack of the right skillsets needed to perform technology effectively is a challenge most audit leaders are grappling with.

With all enterprises leaping to advanced cloud and analytics applications, improving IT auditing practices and providing sufficient assurance over data privacy and cybersecurity are now key concerns for audit leaders.

Leading businesses are responding with innovative strategies

In response to the chronic lack of talent and the need to fill today's alarming skills gap, a growing number of organizations are wisely pursuing or exploring innovative approaches. While technology has the power to revolutionize technology audit, it's not the solution to all challenges facing the function. Audit leaders realize that the real value of technology can only be unlocked when coupled seamlessly with the human element and the ability of people to provide critical thinking, knowledge, good judgment and digital capabilities.

Integrating people and technology: While the global battle for talent is sure to continue, upskilling the existing workforce via a hybrid training program is proving to be a viable response to the technology audit skills gap. Technology audit functions have embarked on a journey to digitize their learning content and make it available on-demand to make it easy and convenient for employees to participate. Mandatory or refresher training programs are ideal for digitization, such as those used by Internal Audit universities that have now set up virtual, self-paced and interactive learning modules. Complex or advanced training, such as cloud security or DevOps, are covered in regional boot camps where classroom or trainer-led sessions are taught in a collaborative and interactive environment. A case study based assessment generally follows this training, where real-life scenarios are presented to the participants to evaluate their understanding and competency of the modules. The top learners of the Internal Audit department are rewarded to encourage a culture of continuous learning and development.

Employee reward and recognition programs: Internal Audit departments now have greater budgets for rewarding and recognizing talent for actions such as: delivering complex audit engagements, identification of automation opportunities, demonstrating an astute risk and controls mindset, working collaboratively with other teams, contributing to the learning agenda of the Internal Audit department and more. Validation and appreciation help to improve employee engagement and contribute to the overall retention strategy. While these strategies have always existed, Internal Audit functions have adopted these practices widely to attract and retain skilled talent.

Smart-sourcing models: Businesses can opt for a balance between in-house, co-sourced or outsourced audit capabilities by using a smart-sourcing approach. Few organizations have all the audit resources, skills, and budget required to maintain, train and develop in-house capabilities. The balance of co-sourced versus fully outsourced varies depending on an organization's size. Many smaller organizations prefer fully outsourced audit capabilities, while larger organizations prefer co-sourcing.

> “Technology audit teams must be technically skilled and knowledgeable in the suite of technologies deployed by the business to translate emerging technology risk into business risk and hold meaningful conversations with leadership and boards.”

Lawrence Amadi
Partner
KPMG in Nigeria

Giving technology audit a strategic new role

Creating value through holistic risk assurance

Solving today's critical skills gap

Transforming audit through innovation

Conclusion

Technology audit hubs can deliver new advantages

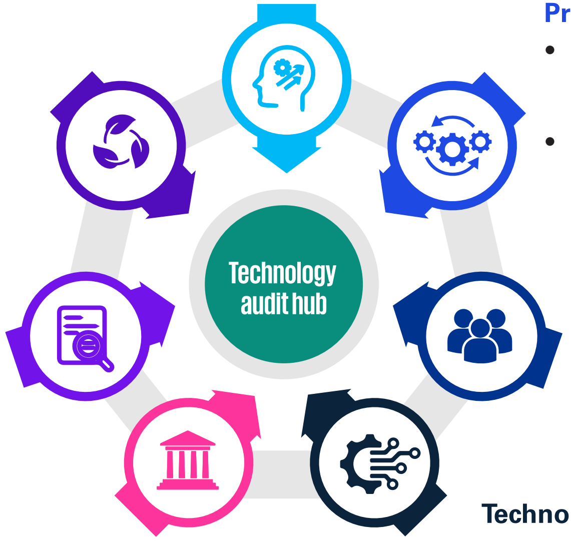
As businesses explore how best to advance audit's technology capabilities, skills and overall value to the business as a strategic partner, many are also discovering the advantages of creating an Internal Audit hub — a specialized center of excellence. This is designed as a physical or virtual function with fungible resources that centrally address the skills gap.

A modern technology audit hub can offer significant benefits by providing access to a skilled global talent pool that can work remotely from strategic locations. Technology audit hubs are operating in Europe, Asia and Africa, with more organizations pursuing the benefits of these innovative centers of excellence. The key characteristics of a technology audit hub include collaboration and contribution as the focus of regional and site resources, as well as strategic alignment and adaptability to changing business conditions and emerging technology.

Technology audit hub architecture

Strategic thinking

- Align vision and mission of the Internal Audit function.
- Refresh technology audit methodologies to align with emerging risks.
- Advise on ongoing enterprise initiatives and design test plans for sufficient Internal Audit coverage.



Sustainability

- Agile operations to accommodate changes to Internal Audit strategy.
- Defined success criteria to measure effectiveness and course correct.
- Continuous feedback and improvement.

Process

- Standard operating procedures with templates and approaches to auditing.
- Usage of technologies to accelerate audit execution.

Data

- Aggregation of data sources to ensure consistency in reporting.
- Generate insights to streamline Internal Audit processes and facilitate decision-making.
- Visualization and dashboard creation of key performance indicators.

People

- Skilled technology auditors.
- Ability to operate with overlaps across multiple timezones.

.

Governance

- Representation from all required stakeholders to ensure open communication.
- Periodic reporting to demonstrate success and efficiency.

Technology

- Consistent usage of relevant platforms/tools/technologies/ infrastructure enabling interface with each other for regular and on-demand reporting needs.
- Strong focus on automation to enable greater efficiency in repeatable activities or tasks.

Businesses should focus on these key success factors during a technology hub initiative:

- Ensure the continuous participation of senior leadership
- Bring key stakeholders together to assess collaboration potential and identify roadblocks
- Agree on priorities and standard operating procedures to avoid conflicts by design
- Conduct workshops and training as needed for the internal team
- Utilize existing technology wherever feasible
- Test efficacy of design by pilot engagements and allow for continuous improvement
- Engage with providers capable of deploying an experienced and fungible workforce

> “Internal Audit leaders now have an ambitious vision and plan for technology audits, given the evolution of the IT landscape. But employers are struggling to identify the right people to execute these plans. A dedicated technology audit centre of excellence, which houses auditors with specialized technical subject matter abilities, helps streamline some of these challenges.”

Mallika Chandra
Associate Director
KPMG in India

Transforming audit through innovation

In today's fast-evolving, hypercompetitive environment, management and governance committees are engaging technology audit teams in more strategic initiatives to ensure risks related to the implementation of emerging technologies are adequately addressed. These changes in organizational dynamics have caused stakeholder interests to shift — from viewing Internal Audit as an assurance function to how it can help meet organizational objectives.

Technology audit leaders now need to do more with less and modify their resourcing models to incorporate technology and automation. This has led to innovation becoming a strategic priority for the function, with several initiatives being launched to improve audit effectiveness, quality, and coverage.

Many Internal Audit functions are now looking to incorporate audit professionals from diverse backgrounds — technology, analytics, statistics and project management, to enable the free flow of thoughts and ideas that could transform the function. Another key enabler of audit innovation is the adoption of an agile approach to audit.

Agility in a technology audit context also requires agile resourcing within the audit team, directly impacting the audit function's resilience. It can be impractical, inefficient, and costly for technology audit to encompass an array of highly specialized experts. Many organizations are choosing partnerships with external parties that offer relevant expertise. Bringing agility to technology audits demands the ability to deliver assurance in a timely and flexible manner. Some audit assignments might not require full terms of reference or a long, detailed report, but a short, sharp investigation and concise reporting to help mitigate areas of high risk. Agility means being faster and better at everything you do and leaving behind traditional, outdated approaches that add little value.

For most Internal Audit functions, adopting agile techniques is a gradual evolution of existing methodologies to ensure effective change management and organizational buy-in. The service of an agile coach is usually undertaken to help set up and train the scrum team for a seamless transition into the new operating model. Relevant agile or scrum-related certifications are also provided to team members to enhance their understanding of key agile concepts. Continuous feedback across various stakeholders is sought so that these principles are applied in future audits, along with any best practices.

Agile audits can help enhance value and build trust

Adopting agile auditing techniques that promote a fluid, risk-based audit approach is critical. That means adopting new methods, including rapid assessments and quick audit memos. Many technology auditors recognize the need to reduce audits and report cycle times as risks and leadership expectations rise.

Agile methods can help technology audit build trust and credibility by delivering real-time reporting, accelerating escalations, improving stakeholder relationships, and increasing alignment with organizational objectives — all while ensuring project objectives are achieved.

Agile auditing best practices

Focused on **business value.**

Increased **audit quality** and **reduced cost.**

Accelerated audit cycles and **efficient** and **effective** delivery.

Outcome and **value driven**, focused on **risk**. Continuous **prioritization** of focus areas.

Increased collaboration between **audit team** and **auditee**, improving expectation management and increasing productivity.

Increased and **continuous communications.**

Improved **project visibility** and status **transparency.**

Timely insights delivered by **brief and just-in-time reporting.**

Reduced waste and **reduced documentation** requirements.

Giving technology audit a strategic new role

Creating value through holistic risk assurance

Solving today's critical skills gap

Transforming audit through innovation

Conclusion

Audit transformation is a journey, not a destination

For Internal Audit to deliver value as a strategic partner to the business, it should continually innovate and transform. Audit transformation for a new era needs to be approached not as a destination, but as an ongoing, iterative, and incremental journey. Innovation focus groups represent a relatively new concept, and they follow an iterative cycle that involves:

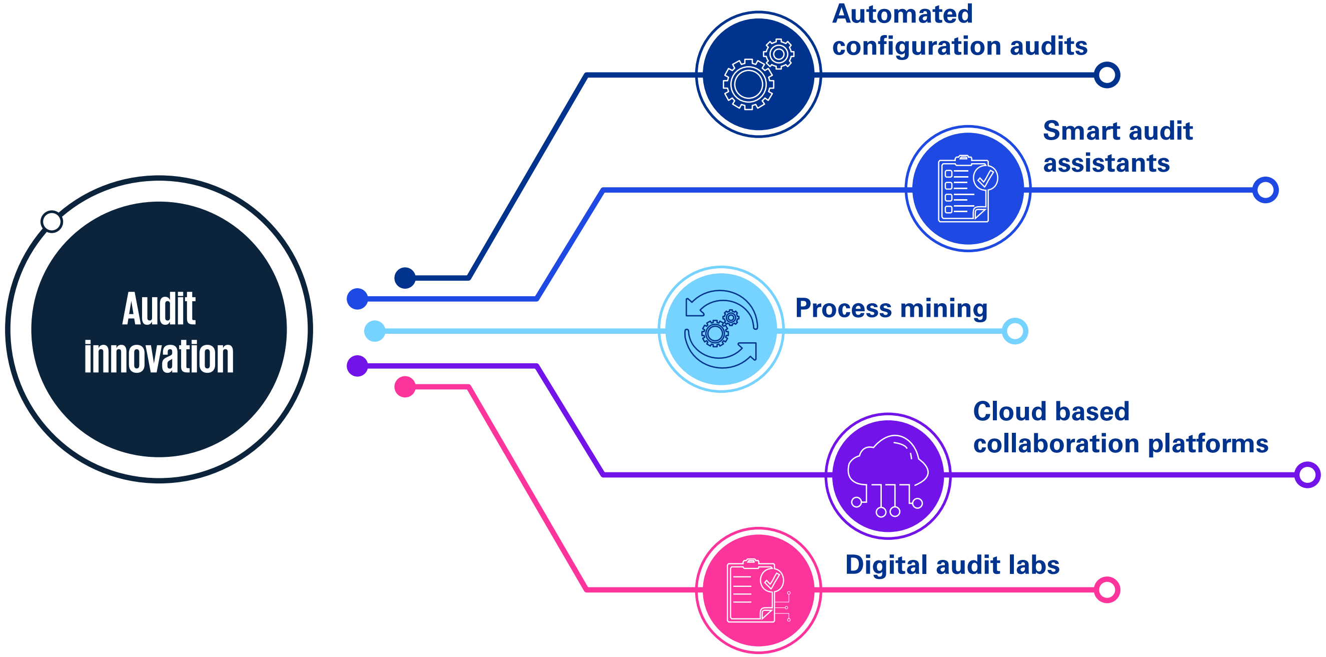
- Generating insights by framing problem statements and doing continuous research.
- Refining insights by bringing together and examining all insights and their implications.
- Generating and defining ideas and concepts by articulating value propositions and creating value models and roadmaps.

Amid the increasing volume and complexity of structured and unstructured data generated by organizations, a new set of auditors is fast evolving: data scientists and engineers. They are commonly referred to as "Embedded Data and Analytics Auditors."

As the name suggests, they are integrated within each Internal Audit division or unit and are required to work closely with the core technology audit teams to build reusable analytical tools that will help make audit testing more efficient and insightful. These professionals typically tend to have a mix of advanced data query skills, programming languages such as Python and Java, data analytics workflows such as Alteryx and visual dashboarding using Power BI/Tableau.

Audit innovation — The game changer!

The innovation agenda of the technology audit function needs to be sufficiently backed by investments and senior management sponsorship of key initiatives. Clear and transparent communication on the objectives of these programs is a must to ensure the active participation of all team members. Adopting a forward-thinking mindset focused on collaboration and fostering an environment that encourages creativity can help create a culture of innovation in the Internal Audit function.



Automated configuration audits: Because of digital transformation, several new trends are emerging, for example: transitioning from legacy applications to smaller micro-services based architecture or to a cloud-based platform, leading to the generation of more data. This would require automated testing solutions that can potentially identify security misconfigurations and generate alerts when activity levels go beyond a certain threshold. These solutions may be designed to give an on-demand or real-time view of security risks in these applications. They can be equipped with dashboarding or visualization capabilities for reporting to audit committees and other governance bodies.

Smart audit assistants: Mature Internal Audit functions are creating smart audit assistants by adopting advanced deep learning, natural language programming (NLP) and AI technologies, which can help scan through audit documentation and identify or detect anomalies, grammatical inconsistencies, or errors. These ML models can automatically correct identified errors without manual intervention making them a popular choice for audit leaders.

Process mining: Process mining is a powerful tool that simplifies the detection of anomalies by providing valuable insights on trends, patterns, and outliers in the risk management landscape, which can aid in planning and scoping of future audits. As an extension of process mining, large Internal Audit functions are piloting process mining for monitoring and tracking efficiency of their own audit lifecycle to generate insights on lead times to predict future audit timelines and necessary corrective actions.

Cloud-based collaboration platforms: In a heavily digitized and global environment and with the inclusion of more tech-savvy auditors in the Internal Audit function, having a collaborative mindset is essential and can be a huge differentiator in the way a technology audit team operates. Several cloud-based collaboration platforms are now available in the marketplace, specifically for Internal Audit, which makes hybrid or remote working arrangements seamless, ensuring real-time knowledge and information sharing, greater responsiveness to audit related queries and smoother communication. These tools are popular in audit teams with a global footprint to ensure 24/7 communication, despite the collaborators working across different time zones.

Digital audit labs: Large Internal Audit functions have invested in creating a digital audit lab that operates like an accelerator or incubator, where new ideas, technologies, solutions, or products are implemented before large scale adoption. Detailed feasibility studies, integration tests and cost-benefit analyses are carried out to assess the potential of each initiative and project plans are prepared prior to implementation. New and upcoming areas, such as distributed ledger technology, are evaluated in a 'sand-box' environment to explore its functionalities and potential alignment with their Internal Audit priorities. Such labs help cultivate a creative and entrepreneurial spirit and have often led to pioneering innovative solutions to benefit the broader Internal Audit function.

> “The overarching goal is to align technology audit with the corporate digital journey, and to become a strategic stakeholder for the organization, providing valuable insights as it navigates new technologies and risks.”

Abhisek Bhattacharyya
Partner
KPMG in the Lower Gulf

Conclusion

Adapting to a modern technology audit function

As modern technology unleashes a complex and challenging new reality of risk, future-focused businesses are wisely embracing a strategic new role for the IT Internal Audit function. The future of audit is clear and inevitable — it demands:

- A modern holistic approach to risk assurance that's built on three key pillars: data-driven insights and value, new digital skills, and enhanced agility.
- A new mindset that delivers new capabilities in cyber defense, data protection, cloud governance, IAM, AI, ML, automation and more.
- The advantages of an Internal Audit hub that can provide access to a global talent pool of new audit skills.
- The adoption of automation tools and emerging new technologies that enhance audit capabilities while addressing ever-evolving risk and regulatory landscapes.

It's an opportune time for IT Internal Audit to power through the era of digital transformation and position themselves as agents of change, in the boardroom and beyond.

> “
>
> Strengthening the technology risk ecosystem is now of paramount organizational importance, and IT Internal Audit can become a key enabler in this mission. Ultimately, it's all about coverage, speed and effectiveness.“

Nicole Lauer
Americas IT Internal Audit Leader and Principal
KPMG in the US

Contacts

Phillip Lageschulte
Global Enterprise Risk Services Leader, KPMG International and Principal
KPMG in the US
pjlageschulte@kpmg.com

Laurent Gobbi
Global Technology Risk Leader, KPMG International and Partner
KPMG in France
lgobbi@kpmg.fr

Anil KV
Global Leader for IT Internal Audit, KPMG International and Partner
KPMG in India
anilkv@kpmg.com

Nicole Lauer
Americas IT Internal Audit Leader and Principal
KPMG in the US
nlauer@kpmg.com

James Buchanan
Director and Head of IT Internal Audit in Asia Pacific
KPMG Australia
jbuchanan01@kpmg.com.au

Abhisek Bhattacharyya
Partner
KPMG in the Lower Gulf
abhattacharyya1@kpmg.com

Charles Frieze
Associate Director
IT Internal Audit
KPMG in the UK
cb.frieze@kpmg.co.uk

Lawrence Amadi
Partner
KPMG in Nigeria
lawrence.amadi@ng.kpmg.com

Mahendrakumar Khiani
Director
KPMG in the Lower Gulf
mkhiani@kpmg.com

Mallika Chandra
Associate Director
KPMG in India
mallikachandra@kpmg.com

Richard Knight
Principal
KPMG in the US
raknight@kpmg.com

Tejas Mehta
Director
KPMG in the UK
tejas.mehta@kpmg.co.uk

Kareem Sadek
Partner, Emerging Tech Risk Leader
KPMG in Canada
ksadek@kpmg.ca

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 endeavour 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 on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG refers to the global organization or to one or more of the member firms of KPMG International Limited ("KPMG International"), each of which is a separate legal entity. KPMG International Limited is a private English company limited by guarantee and does not provide services to clients. For more detail about our structure please visit kpmg.com/governance.

Throughout this [document/film/release/website], "we", "KPMG", "us" and "our" refers to the global organization or to one or more of the member firms of KPMG International Limited ("KPMG International"), each of which is a separate legal entity.

Publication name: Repowering technology audit

Publication number: 138593-G

Publication date: April 2023