KPMG

Technology enabled internal audit: 2022 and beyond

Aligning to heightened expectations

Executive summary

The changing role of technology enabled internal audit

Technology enabled internal auditors are facing a perfect storm:

— Unprecedented technological advances unfolding at an ever-increasing pace

— Board and audit committee members who have become more knowledgeable about technology and are demanding more insights and expertise from their internal audit functions

— A shortage of professionals with the skills needed to tackle emerging and evolving risks.

With technology more prevalent and more strategic than ever before, boards, audit committees, and senior management are relying on technology enabled internal audit as their primary mechanism to assess the strategic risk of these new technologies. Whether it's increased use of robotic process automation or artificial intelligence to support optimization, further use of evolving cloud technologies, or the evolution of cyber strategy to combat emerging threats, business leaders responsible for governance need technology enabled internal auditors to partner with management to ensure risks are appropriately managed.

Furthermore, independent assurance and opinions are now expected at all stages of the technology lifecycle— from selection through implementation. Key stakeholders want these opinions to be delivered quickly, requiring auditors to think and execute with agility.

In 2022, business leaders will be raising their expectations for technology enabled internal auditors, as management and governance committees pull technology enabled internal audit functions into more strategic initiatives to ensure that the risks around the selection and implementation of emerging technology are being adequately addressed.

However, to be effective, internal audit functions must establish credibility with business leaders by being able to demonstrate their skills, knowledge, and ability to meet these heightened expectations. Without that credibility and stakeholder trust, it will be difficult—if not impossible—for the technology internal audit function to rise to these new challenges required by the business.

In this publication, we will address how technology enabled auditors can overcome some of the barriers they may face in establishing credibility and stakeholder trust to become true strategic advisers to the organization around managing technology and risk.

Global Technology Internal Audit Outlook

Throughout this report, we include select results from the recent KPMG Global Technology Internal Audit Outlook survey. The survey polled 300 participants comprising chief audit executives, audit directors, vice presidents, and senior managers representing audit teams from a wide range of industry sectors across 35 countries and territories.

Click here to learn more.

The three pillars of credibility and trust

Investing in skills of the future
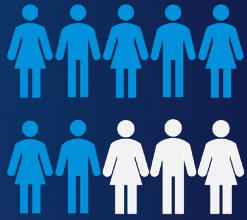
More than six out of ten technology enabled internal audit functions say they are investing in agile coaches and auditors with program management skills.

49%

Forty-nine percent of respondents state that they already have fully implemented agile techniques in their audits or are in the process of piloting them.

39%
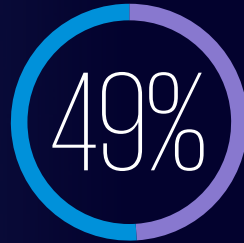
Only thirty-nine percent say their team exceeds or significantly exceeds expectations of the board and senior management.

Technology enabled internal audit teams must build a foundation of credibility and stakeholder trust to meet the heightened expectations from business leaders. That starts by addressing these three pillars:

Skills/Capability

Businesses are investing in emerging technologies that keep evolving at an ever-increasing rate. Technology enabled internal audit teams must be highly technically skilled and knowledgeable in the full suite of technologies deployed by the business.

They must also be able to translate emerging technology risk into business risk in order to hold meaningful conversations with executives and board members.

Agility/Flexibility

As organizations and industries are rapidly changing and increasing their use of agile processes, such as continuous integration/ continuous delivery (CI/CD), mobile technologies, and remote workforces, technology enabled internal audit teams need to think differently about how they deliver their services. That means adopting new methods, including rapid assessments, quick audit memos, and aligning to how the business works.

Insights/Value

Businesses are rapidly increasing the digitization of their operation. As the changes move more quickly, assurance needs to adapt and be able to operate in real time. Leadership needs the technology enabled internal audits' independent perspective on these large, strategic initiatives before it invests significant capital on ineffective programs and potentially introduce new risks. Technology enabled internal audit teams must provide insights above and beyond control issues and use data to address real-time issues.

Barriers and solutions

With the exponential rise in technology risks and the shift to tech-centric business models, technology enabled internal audit teams will need to be courageous and deliver insightful points of view to the board and audit committee. With the credibility and trust gained by developing the three pillars **of Skills/Capability**, **Agility/Flexibility**, and **Insights/Value**, technology enabled internal auditors can gain access to senior management and a seat at the table during strategic decision-making.

However, technology enabled internal auditors may face some barriers in building up these three foundational pillars. Here are some steps they can take to overcome these obstacles.

Pillar	Barrier	Solution
Skills/Capability	**IT resource constraints** – A challenge that technology enabled internal audit teams have always had and even more so going into 2022, with a limited budget and resources, is how to best prioritize where technology enabled auditors spend their time while maintaining oversight of traditional high-risk functions. Additionally, the changing labor market, including retention challenges and skills shortages, is making it increasingly difficult for audit functions to fill and retain key positions that have the right skill set.	**Investing in resources, adapting delivery model** – With the correct blend of resources, in-depth knowledge of emerging risks and technology, and the investment of audit technologies, the technology enabled internal audit team can position itself to be a problem-solving function that provides guidance on forward-looking risks and trends while continuing to maintain oversight of traditional high-risk functions. Another option to address resource constraints is to augment technology enabled audit teams with a partner either through outsourcing or engaging a service provider that has in-depth knowledge of emerging technologies and IT risks. Indeed, a number of leading technology enabled internal audit functions have recognized that cosourcing is the only way to stay credible and relevant. However, cosourcing must be used strategically, beyond a simple audit execution, to enhance risk assessment, planning, and interactions with management.
Agility/Flexibility	**Adopting agile methods** – Historically, technology enabled internal audit teams have maintained a rigid process and methodology that has not allowed them to quickly adapt to disruption and changing technologies. Many organizations are moving toward agile processes in product development and other areas, delivering multiple phases concurrently. Technology enabled internal audit teams must find ways to apply similar agile techniques to manage the associated risks.	**Agility with emerging risks** – The technology enabled internal audit operating model should leverage a more agile and dynamic approach to respond to the organization's changing risk landscape and deliver on its value promise to protect and enhance organizational value. This includes ongoing, dynamic risk assessment as well as adjusting the reporting cadence based on audit topic. Many internal audit leaders are now looking to invest in agile practitioners to join their teams to help facilitate more efficient and timely audits. This, combined with technology enabled internal audit functions applying agile methods, will help accelerate audit delivery cycles and provide timely and impactful insights.
Insights/Value	**Digitizing the end-to-end audit lifecycle** – Technology enabled internal audit teams need to identify opportunities to leverage digital technologies to enhance their ability to perform their audits with greater efficiencies and to remain credible and trusted with the organization's leadership team. Additionally, technology enabled audit teams need to consistently align their processes with the organization's strategic priorities and projects to add value early and frequently throughout the journey.	**Aligning with the digital transformation of the business** – The overarching goal is to align technology enabled internal 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. This starts with technology enabled internal audit teams getting embedded early to educate the key stakeholders around its missions and objectives, creating and selling a value proposition and getting their buy in on audit focus areas. Technology enabled audit teams then gain their trust by providing objective yet valuable insights through succinct, impactful reporting and collaboration with business stakeholders while leveraging technology throughout the process. Teams keep this trust by adjusting the audit process based on the organization's journey to be nimble and timely (e.g., real-time/rapid assessments; assurance versus preassurance reviews).

More and more internal audit functions choose for a cosourcing partner, not only because they've asked for it, but especially because of Boards and Audit Committees urges CAE's to use these capabilities strategically

Huck Chuah, Partner, Risk and Internal Audit, KPMG Netherlands

In the following pages, we explore each of these focus areas and how technology enabled internal auditors can address them and expand their role as a strategic partner with management and the board.

Agility with emerging technology risks

KPMG insight

Most technology enabled internal audit functions feel unprepared to deal with the evolving IT risk landscape. For example, the prevalence—and cost—of increasingly sophisticated ransomware attacks continue to grow unabated. New cloud approaches require an overall governance approach that can help control their increased complexity. Artificial intelligence holds unprecedented opportunities for business but with it comes huge risks—financial, reputational, legal, and regulatory and compliance—that are difficult to quantify.

In response, internal audit must become more agile to effectively deal with emerging technology risks. Technology enabled internal audit should become partners with the business, working with the three lines model to identify new technology risks and conduct unplanned, quick-hit audits over the design and implementation of new technologies as needed.

The use of agile methods can help technology enabled internal audit build trust and credibility by enabling it to deliver real-time reporting, accelerate escalations, improve stakeholder relationships, and increase alignment to organizational objectives and visibility to risk and issues—all while ensuring project objectives are achieved.

Areas of emerging focus

Ransomware/Technology resilience

The "2020 Ransomware Resiliency Report" found 66 percent of companies estimate it would take five or more days to fully recover from a ransomware attack if they did not pay the ransom.* Increasing ransomware attacks also lead to unplanned outages. Technology enabled internal audit should ensure there are sufficient controls around ransomware and other cybercrimes to prevent account ID theft, bot attacks, synthetic ID frauds, etc.

Robotics process automation (RPA)/Artificial Intelligence (AI)

Technology enabled internal audit should review bot oversight, security design, vulnerability assessments, algo-logic review, access and change management, and roles and responsibilities. For AI, technology enabled internal audit should review the methodology, governance, resourcing, intentional/unintentional biases, tolerance limits, training data, change management, and access.

DevSecOps

Organizations are trying to deliver new functionality and code frequently and fast to their technology solutions. This presents new risks related the security of the development and the tools supporting the DevOps processes.

*Source: "The 2020 Ransomware Resiliency Report," Veritas Technology LLC, 2020

33%
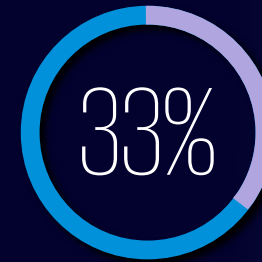
Of respondents rate their preparedness for auditing technology associated risks as "good" or "excellent"

Adapting to an evolving risk landscape

Cyber risk and operational resilience are the key focus areas of technology enabled internal audit teams today.

With the enhanced risk landscape, the priority is to build resiliency through the use of technologies and agile auditing techniques, in response to new and emerging threats.

Aligning with the digital transformation of the business

KPMG insight

Digitization is increasingly becoming vital for a business's success, and companies are continuing and, in many cases, accelerating their digital journey. Historically, technology enabled internal audit has been called upon after the fact to identify when issues occurred.

Today, technology enabled internal audit is now being called upon to go hand in hand with the business on its journeys around major project implementations and activities. Technology enabled internal audit can now be expected to consult and provide insight as it relates to designing controls and processes as these projects unfold.

Put simply, if internal audit is perceived as being credible, it will be seen as a stakeholder and key project player that is expected to get in front of problems—that is, identifying risk factors before investments are made or issues arise.

Areas of emerging focus

Preassurance reviews

Preassurance reviews should be implemented for new technology processes (adopting DevOps, outsourcing IT functions) and process/control automation. As new processes, technologies, and third-party support are introduced to existing processes, they bring with them new and emerging risks. As new processes are adopted, involving technology enabled internal audit early and often provides the opportunity for technology enabled internal audit functions to provide meaningful insights into risks to consider in addition to scalable best practices.

Technology selection and implementation reviews

Technology implementation reviews should be conducted for new systems and tools. As organizations push to quickly acquire, develop, and implement new technologies, governance and security controls may often fall to the wayside. Additionally, internal audit functions should be involved in the selection of technology—where they can provide real value—before the business makes a very expensive mistake. In-flight implementation reviews give technology enabled internal audit teams the opportunity to weigh in on risks and key themes for teams to consider while implementation projects are ongoing. As a result, collaboration between development, business teams, and technology enabled internal audit teams increases, and system go-live activities are streamlined.

60%
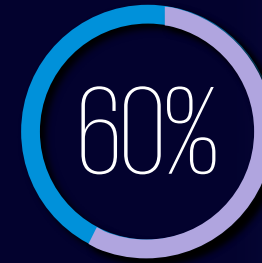
Of survey respondents cited they have a high degree of maturity in their technology capabilities.

Embracing digital technologies

Data and technology are improving the performance of the internal audit teams, with increased funding made available for new technology investments.

Technologies such as RPA, AI, and ML continue to be aspirational for internal audit teams and are yet to see extensive usage.

Maintaining oversight of traditional high-risk functions

KPMG insight

It is easy to become overly focused on new market trends and emerging technologies. While it's clearly vital to keep up with the pace of change, it's also important to remain focused on the basics to ensure a baseline secure environment is maturing and is another area where technology enabled internal audit can build credibility and trust. This is even more important given the evolving remote workplace where basic controls can be tossed aside, and security principles ignored or forgotten. Technology enabled internal audit teams need to leverage data analytics, process mining, and RPA as well as existing organizational tools to balance resource constraints while still providing coverage over traditional high-risk areas.

Based on survey and conversations in the marketplace, the following remain areas of heightened risk and subject to attention from technology enabled internal audit:

While certain domains within cyber are emerging, many domains remain foundational areas for review.

Traditional cyber security audit activities include:

— Threat and vulnerability management assessments

— Identity and access management strategy and design

— IT asset management audit

— Network configuration and system hardening review

— Remote, mobile, and wireless security assessment

— Operational technology risk assessment.

General IT controls and automated process controls remain a core competency of technology enabled internal audit teams.

Traditional audit activities include:

— Backup and recovery effectiveness

— Segregation of duties assessment

— IT change management effectiveness

— Controls integration and continuous controls monitoring.

Data privacy continues to rank high as a priority given the evolving regulatory landscape, as does cloud governance given the continued shift by organizations.

Traditional audit activities include:

— Data governance assessment

— Privacy regulation compliance

— Cloud strategy and governance

— Cloud migration assessments.

Final thoughts

In 2022, technology enabled internal audit teams will have the opportunity to enhance their role as a strategy partner with business leadership, as organizations continue to adopt emerging technologies and move forward with digitization. However, to be successful, technology enabled internal audit will need to take steps to evaluate and develop their own organization to help ensure that they are perceived as credible and trusted by leadership and stakeholders.

Boards and audit committees have become much more knowledgeable about technology issues. So, technology enabled internal audit will need to ensure their teams possess the required skills, which can be achieved through hiring and training as well as the use of cosourcing. However, cosourcing must be used strategically. Using a vendor to simply deliver an audit won't help technology enabled internal audit prove its credibility with leadership nor win its trust. They will need to leverage cosourcing to enhance risk assessment and planning and to support interactions with management outside of the audit execution.

Likewise, emerging technologies present new risks, and technology enabled internal audit teams will need to embrace agile methodologies to work with the business as it implements new technology projects. Moreover, as it becomes more of a partner with the business, technology enabled internal audit will also be expected to become more a proactive problem solver, not just a problem spotter.

Finally, even as it expands its role, technology enabled internal audit will need to keep up its vigilance on traditional high-risk areas, such as IT change management, cyber security, data privacy, and cloud governance, especially in light of the rapidly evolving workplace.

Learn more by visiting home.kpmg/nl/internalaudit.

Contacts

Huck Chuah

Internal Audit
Partner, KPMG

T +31 20 656 4501
M +31 64 636 6013
E chuah.huck@kpmg.nl

Pascal Raven

Internal Audit
Senior Manager, KPMG

T +31 20 656 7546
M +31 65 149 4568
E raven.pascal@kpmg.nl

KPMG **home.kpmg/nl/internalaudit**

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