GLOBAL PERSPECTIVES & INSIGHTS

Innovation and Technology

PART I: Internal Audit’s Role In Technology Assurance

PART II: Staying On Top Of The Organization’s Technology Adoption

PART III: Internal Audit's Tech Talent Challenge

Wolters Kluwer

The Institute of Internal Auditors

Contents

Part 1: Internal Audit’s Role in Technology Assurance

About the Expert

Jim Pelletier, CIA, CGAP

Jim Pelletier, CIA, CGAP, is a senior product manager with TeamMate Audit Solutions, where he works to continuously improve audit productivity while delivering strategic insights via TeamMate's best-in-class solution. He has more than 20 years of internal auditing experience in both the public and private sectors.

Previously, Jim held a number of leadership roles at The Institute of Internal Auditors, served as City Auditor for the City of Palo Alto, CA, and was Chief of Audits for the County of San Diego, CA. His diverse internal auditing background includes positions with the California State University System, PETCO Animal Supplies, Inc., State Street Corporation, and General Electric.

Introduction

Technology has become the unquestioned driver for change and business innovation. From widespread digital transformation to emerging and evolving artificial intelligence, new technologies are opening opportunities – and risks – as never before. To understand the impacts of new technologies, organizations rely on internal audit for assurance about their adoption and use of technology. This brief will address why technology assurance should be a routine part of any audit. It will cover key areas of vulnerability and discuss opportunities for internal audit to take the lead in bringing consistency and coordination that will deliver more effective technology audits.

A central focus

Because technology pervades every aspect of business, it is natural that technology assurance would already be a central focus for internal auditors. "There is underlying technology risk in essentially all that organizations do," said Jim Pelletier, CIA, CGAP, senior product manager, TeamMate Audit Solutions. There is no longer any separation between operations and technology because technology enables operations and numerous other functions. Evaluating and assuring proper controls thus must include any related technology underlying a process. For example, while internal auditors might have once audited accounts payable — or any other function — and its systems separately, the functions and the systems are now completely intertwined, Pelletier said. "All that you audit involves some degree of technology assurance."

Issues to Consider

Third-party risks and data governance

Recognizing key threat areas

Because of technology's prevalence, there are many issues to examine in providing technology assurance. This section will discuss several high-risk areas.

Third-party relationships

Research has shown that 98% of organizations globally have vendor relationships with at least one third-party that has experienced a breach in the last two years. Companies may also be affected by vendors' downstream connections. A total of 50% of organizations have indirect relationships with at least 200 recently breached fourth-party vendors.[1]

Organizations' extensive dependence on and interrelatedness with third parties is a critical risk, particularly when a problem occurs. Third-party relationships may be especially vulnerable because many organizations incorrectly assume that a vendor is addressing all related risks and that no further review of their efforts is needed or that less rigorous oversight is adequate.

These examples of companies that have suffered third-party data breaches show that any type of organization or industry can be affected: SolarWinds AT&T, Chick-fil-A, LinkedIn, T-Mobile, Uber, Okta, and Dollar Tree.[2]

Technology or related services that third-party vendors provide might include web-hosting platforms and software-as-a-service (SaaS), outsourced data centers, or network security services. While the provider takes on responsibility for the services it offers, the organizations using those services must still ensure that they have the proper controls and risk management processes in place to see that the third party is fulfilling its obligations. "You can't base your organization's safety on the hope that the third party will do its job," said Pelletier.

Internal auditors should consider whether their organization has properly evaluated the third party and its associated risks. Internal audit may not carry out this evaluation, but it should consider how the organization is monitoring and managing its relationship and related risks and verifying that the third party has and is following proper controls. Pelletier recommended including a right-to-audit clause in the contract with the vendor so that internal audit can examine vendor processes and controls as needed, including after a breach.

Data governance

Organizations are collecting rapidly expanding volumes of data and leveraging it for use with emerging technologies such as artificial intelligence. Data can represent a critical risk for organizations because of the importance of maintaining data privacy. In addition, if leadership will be making key business decisions based on the data on hand, the organization must have confidence in data integrity and ensure that it is complete, accurate, and reliable. That includes understanding the reliability of the data source, particularly when working with generative AI.

[1] "SecurityScorecard Research Shows 98% of Organizations Globally Have Relationships With At Least One Breached Third-Party," SecurityScorecard press release based on a study by SecurityScorecard and The Cyentia Institute, February 1, 2022.

[2] "Top Third-Party Data Breaches in 2023," FortifyData, updated December 4, 2023.

Organizations will need to guarantee that data is not vulnerable to hacking or other improper uses. "Organizations need to evaluate how data is processed and stored," Pelletier said, as well as ensure that specific legal or regulatory requirements have been fulfilled, such as those related to information privacy. If the organization has given customers or business partners assurances about how their data will be used, it will need to ensure it is meeting its commitment. While management is responsible for data governance, internal audit can offer assurance that data governance controls are sufficient.

Data should be stored for the shortest amount of time possible, according to the European Commission. Not only is storage costly but also, in the event of a breach, there is more data for hackers to access. Companies should have appropriate timelines on when data should be reviewed or deleted, keeping in mind any business, regulatory, or legislative requirements that would mandate longer retention periods for some materials. As an example, under the principles of the European Commission's General Data Protection Regulation, the commission points to a situation in which a company maintains CVs from job seekers for 20 years, without taking steps to update them.[3] This data will clearly be obsolete after a short period in many cases, given the rapid turnover in many jobs or industries. The person may miss out on an employment opportunity and the company may miss out on talented people if it relies on this outdated information pool when seeking workers for future openings, or the applicants' personal details may be stolen if the organization is hacked.

Some of the other technology areas where internal audit assurance can identify an organization's failure to implement proper monitoring or protections include:

- **Access controls.** Internal audit can examine whether user access reviews are conducted to ensure that only legitimate users have access to the inner workings of the organization's technology. Among other things, reviews can identify whether a former employee or department member has unauthorized access to applications or infrastructure, according to the ISACA Journal. "This vulnerability can be exploited, resulting in financial and/or reputational loss to the enterprise," it said.[4]
- **Cybersecurity.** "Security patches, strong passwords, asset management, and employee security training go a long way toward staying safe online," according to a Forbes article.[5]
- **Shadow IT.** This term refers to situations in which employees purchase and implement technology without the knowledge or authorization of the IT department. The practice is growing with remote work and the increasing use of personal devices on the job. Risks include failure to fall under the IT team's oversight or to follow the organization's cybersecurity and privacy protocols and other guidelines.
- **Risks related to generative AI and other emerging technologies.** The danger that employees may upload corporate, customer, or personal data to a public generative AI system is one significant concern. (The Institute of Internal Auditors' AI Auditing Framework[6] helps internal auditors understand risks and determine AI best practices and internal controls.)
- **Cultural considerations.** Internal auditors can consider whether a lack of employee engagement or poor communication of technology guidelines or safeguards is a threat.
- **The impact of technology-related legislation or regulation.** Organizations will need to monitor compliance needs related to new laws and standards issued in response to the significant changes that emerging technologies can mean for business and society.

[3] "For how long can data be kept and is it necessary to update it?" European Commission.
[4] "Effective User Access Reviews," Sundaresan Ramaseshan, *ISACA Journal*, August 21, 2019.
[5] "16 Tech-Related Risk Factors Company Executives Often Overlook," *Forbes*, December 21, 2022.
[6] The Institute of Internal Auditors' AI Auditing Framework.

The Value of Coordinated Efforts

Aligning with second-line risk professionals

Internal audit can help coordinate technology risk management

Tech is top of mind for internal auditors

Technology was a central focus in The IIA's 2023 North American Pulse of Internal Audit[7], which collects valuable benchmarking information from internal audit leadership about risk, audit plans, budgets, staff, and other hot topics.

For example, when chief audit executives were asked how they would spend additional budget money if they had it, the second most common choice was technology. (Increased in-house staff came in first.)

While reviews of compliance and operations are traditional priorities, internal auditors are also spending a great deal of time and effort on technology-related topics. In the Pulse survey, respondents said that 10% of their audit plans focused on cybersecurity and 9% on IT overall. The 19% total was higher than the average amount of audit plans devoted to financial reporting (including ICFR), operations, and compliance/regulatory (excluding ICFR). Each one of those was the subject of 15% of audit plans.

Finally, when respondents were asked to choose which issues posed high or very high risks for their organizations, their top three choices were all technology related:

- Cybersecurity, which was chosen by a resounding 78%.
- IT overall, at 57%.
- Third-party relationships, which are often used for IT services, at 51%.

One of the downsides of technology's pervasive presence and impact is the risk that something will be overlooked when attempting to fully understand and provide assurance on this area. "Because there is so much to cover, there will be gaps," Pelletier said. Given the many risks involved, to enhance its efficiency in its role as an assurance provider on technology adoption and usage, internal audit will want to get the best coverage of high-risk areas possible with the available resources.

To enhance those resources, the internal audit function has an opportunity to align with second-line assurance functions such as information security, internal controls, risk management, and compliance, according to Pelletier. To provide senior management and the board with a higher degree of comfort that risks are being identified, internal audit can coordinate its activities with these functions to obtain a holistic picture of how technology assurance — and key technology risks — are being handled throughout the organization.

While internal audit must remain independent of these second-line functions, coordination with them can help internal audit determine which risks are already being covered and to what degree. "Internal audit should not operate in a silo," Pelletier said. In minimizing duplication of effort, alignment allows internal audit to focus its own resources on the most important risks. As part of the effort, internal audit can evaluate the work that second line functions are doing related to technology assurance.

This alignment can also help to minimize "assurance fatigue," which occurs when numerous functions ask department managers for reports on the same data or perform similar reviews. This can be avoided if internal audit and second-line functions work together to gather the core information they need.

Internal audit can take on a leadership role in coordinating this alignment around assurance activities throughout the organization and making the best use of existing activities, Pelletier said. As a beginning, internal auditors can drive greater consistency in technology

[7] 2023 North American Pulse of Internal Audit, The Institute of Internal Auditors, March 2023.

assurance efforts by determining if the risk management, compliance, internal audit, and other functions each have their own systems of evaluating and rating risk. In discussions with the board and management, these inconsistencies among the functions may present a confusing or perhaps seemingly incomplete picture. Internal audit can recommend and lead a coordinated effort using a common risk taxonomy. Communications about risk to the board and senior management will be more understandable if internal audit and second line functions are speaking the same language. All of these functions' results or assessments don't necessarily have to agree, but the terms and approaches they use should be consistent.

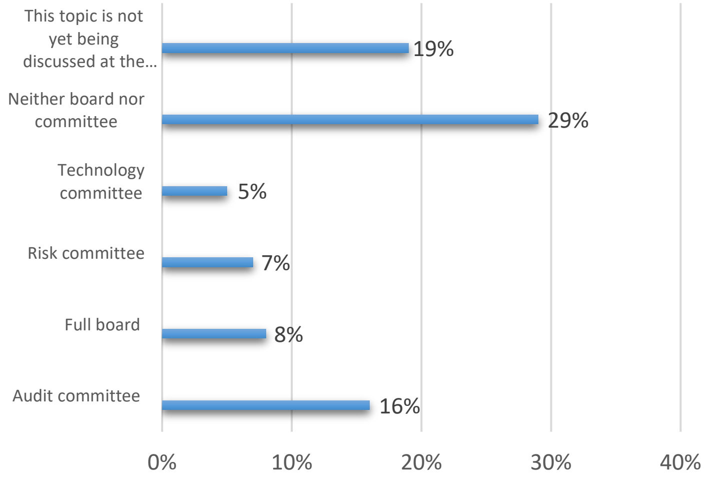
Keeping an eye on AI

With many companies still grappling with their use of AI and generative AI, internal auditors have an opportunity to drive better oversight of emerging technologies and their organizations' use of them.

In a survey[8] by Deloitte and the Society for Corporate Governance of large and mid-cap companies done in 2023, only 13% had a formalized AI oversight framework. Just 9% had revised corporate policies related to cybersecurity, risk management, records retention, and others to address AI use. However, the National Association of Corporate Directors noted that a year earlier, 94% of corporate respondents said that AI was critical to their company's short-term success.[9]

Despite the importance of AI, boards seem to have not yet gotten their arms around related concerns. The survey found that a total of 48% of respondent's boards either weren't considering AI yet or had not assigned responsibility for it (see chart). Among those that had assigned responsibility for AI, it was most likely to be under the oversight of the audit committee, which is often the group that they chief audit executive reports to. Internal audit can add considerable value by helping organizations to recognize and address the disconnect between the importance of AI and their own response to it.

Who has primary oversight for AI on the company's board?



Source: *Deloitte and Society for Corporate Governance Board Practices Quarterly: Future of tech: Artificial intelligence (AI)*, August 2023.
Note: Other/don't know responses not included in chart.

[8] *"Deloitte and Society for Corporate Governance Board Practices Quarterly: Future of tech: Artificial intelligence (AI),"* August 2023.
[9] "Artificial Intelligence: An Emerging Oversight Responsibility for Audit Committees?" Brian Cassidy, Ryan Hittner, and Krista Parsons, NACD 2024 Governance Outlook.

Conclusion

Technology assurance that identifies risks and roadblocks is already well integrated into internal audit's role. While maintaining a focus on some of the greatest technology-related vulnerabilities, internal audit can also promote improved coordination of efforts to ensure a fuller and more accurate picture for risk managers and stakeholders. The steps outlined in this brief can help ensure that the organization's overall approach to technology risk and the audit plan adequately address potential technology risks.

Part 2: Staying on top of the organization’s technology adoption

About the Experts

Jim Pelletier, CIA, CGAP

Jim Pelletier, CIA, CGAP, is a senior product manager with TeamMate Audit Solutions, where he works to continuously improve audit productivity while delivering strategic insights via TeamMate's best-in-class solution. He has more than 20 years of internal auditing experience in both the public and private sectors.

Previously, Jim held a number of leadership roles at The Institute of Internal Auditors, served as City Auditor for the City of Palo Alto, CA, and was Chief of Audits for the County of San Diego, CA. His diverse internal auditing background includes positions with the California State University System, PETCO Animal Supplies, Inc., State Street Corporation, and General Electric.

Dennis Wong, CIA, CFSA

Dennis Wong, CIA, CFSA, is a managing director at an international bank based in London. He is a seasoned audit and risk professional with over 20 years of experience in international banking and capital markets. His passion is to lead and drive changes through process re-engineering and technology innovation. He volunteers with The IIA's New York Chapter and serves on the global Exam Development Committee.

Introduction

Technology has become the lifeblood of organizations, a vital tool used regularly in essentially every function. But while 60% of business and risk leaders see one new technology tool, generative AI (GenAI), as an opportunity, 57% say that preparing for investments in new technology is the single biggest trigger to review the risk landscape, according to the PwC 2023 Global Risk Survey.[10]

Technology offers new benefits, but dependence on it also brings threats, ones that are growing as tech use becomes more critical and pervasive. These include risks related to the ways that technology is adopted. Internal audit can help organizations determine and carry out the best implementation strategies to minimize risk and enhance the value of new technologies. This brief discusses the steps internal audit can take to add value in this effort.

[10] "Cyber and Digital Technology Risks Are a Key Concern for Businesses and Risk Leaders, Even as 60% See GenAI as an Opportunity: PwC 2023 Global Risk Survey," PwC press release, November 20, 2023.

Develop a New Governance Framework

How does new tech fit in?

Internal audit can help guide tech adoption

New technologies always present new risk considerations. While GenAI, for example, has inspired a wealth of innovative uses for this transformative technology, it also comes with new dangers in areas that include privacy, embedded bias, and the transparency and accuracy of the information received. At the same time, risks can arise as new technologies drive changes in business operations that expose an organization to new operational risks.

For those reasons, when adopting new technologies, organizations should develop a robust project governance framework that considers how the new tools fit into the business, align with corporate strategies, and help achieve corporate goals, said Dennis Wong, CIA, CFSA, a seasoned audit and risk professional with more than 20 years of experience in international banking and capital markets. Indeed, among the companies designated as "risk pioneers" in the PwC survey, 73% were likely to have an enterprisewide technology strategy and roadmap, compared with 57% of less advanced organizations. The framework should include a broad consideration of risk, including a comprehensive risk assessment and controls that can address the threats posed by new risks, Wong said.

Internal audit can provide assurance over that project governance and how well it is working, and it can advise on technology adoption in general. At the outset, internal audit can conduct a pre-implementation review that considers the technology's suitability as well as any related risks and necessary changes in controls. Once new tools are in place, internal audit can also provide feedback on how the technology adoption is working and the impact that new tools are having throughout the organization, according to Wong. After implementation, internal audit can weigh in on whether the technology is functioning as envisioned, and why not if it isn't, including whether the expected benefits have been achieved.

Internal audit can also spot roadblocks that may hinder adoption. Companies that are heavily compartmentalized may be subject to silo thinking, in which professionals in different functions are unaware of what is going on in other areas. One area may not know that another group is exploring the same technology but has discovered different uses for it, or that a third function has faced some failures with the technology but learned valuable lessons. "That could create bifurcation when you are looking for synergy," according to Wong. Because internal audit has a holistic view of the organization, it is in a unique position to break down these silos and offer end-to-end insights that prevent duplication of efforts. "Because of its institutional knowledge, internal audit can bring a new perspective that can lead to more valuable technology usage," he said. It can also offer assurance on whether operational controls are working appropriately and ensuring safe and secure technology use. Because investment money is always scarce, organizations will value advice on whether their technology expenditures are being put to best use, Wong said.

Organizations will need to address the interrelationship between strategic and operational risks and the underlying technology. "One impacts the other," Wong said. New technology changes how the organization operates, which brings new risks. That in turn, can drive changes in operations that can lead to additional risks. The key is having a clear understanding of the organization's goals, how they are affected by or carry new risk, and what controls can address these concerns.

Organizations will also benefit from a strong risk culture, given the changes brought forth by the new technology. Even if the organization has a robust control mindset and control framework, it still needs to depend on individuals to implement controls or take the right steps in their absence, Wong noted, so strong risk discipline and appropriate understanding of new technology risk are critical. The company culture should identify and communicate potential threats of new tools and corporate expectations for their use so that they are clear to everyone.

Consider Measured Steps

Finding a balance between speed and safety

Advising on when to embrace new tech

There is often an urgency to implement once a new technology is introduced, illustrated most recently by the rush to deploy GenAI. Because of the potential risks associated with new tools, “organizations need to find the right balance between speed and safety,” Wong said. He pointed to automobiles, which did not have seatbelts when they were first introduced, but which added more and more safety features over the years as cars began to move faster. Given the current rate of change in technology and the complexity of the systems involved, an internal audit can help examine whether management has implemented proper safety features — or controls. “The risk, whether it is identified or not, starts on day one,” Wong said. “It may not crystallize into a loss or threat immediately, but once you start using a technology, you are already exposed to the risk.”

As an example, GenAI is a sophisticated tool with layers of complexity; it is easy for bad actors to exploit it for malicious purposes. In addition, a staff that hasn’t been properly trained on GenAI risks may unwittingly load in confidential or sensitive data, which could be incorporated into the program’s training and could be accessible to outsiders.

Organizations should consider whether to be first to market and face risks from unexpected sources and potential business or reputational damage, or whether they should adopt a quick follower strategy to learn from others’ experiences and mistakes.

Understanding Technical Debt

Infrastructure, staff, culture may not be able to handle latest tech

Identifying tech debt and steps to correct

Organizations will also need to determine whether their existing infrastructure can handle new tech tools. When technology is adopted, time pressures, cost considerations, or other obstacles often force organizations to cut corners to meet a deadline, or other challenges may cause them to fail to reach optimal implementation. This technical debt can build up over time if the organization fails to upgrade to new software versions or new hardware, to implement patches, or to take other key maintenance steps, said Jim Pelletier, CIA, CGAP, senior product manager with TeamMate Audit Solutions. As the organization constantly adopts new workarounds to keep the system going, its technical agility falls further behind.

Technical debt can prevent the organization from making the best use of existing software or even make it impossible to effectively adopt new technologies, Pelletier said. The problem may not be well communicated by the IT team because they are unaware of it, reluctant to discuss the system's failings, or consider the technology too complex to explain to non-technology professionals. As a result, internal auditors may not be cognizant of this technical debt or its impact on the organization's ability to adopt new technology.

Questions to Ask on New Technology

In providing assurance or advice, some of the questions that internal audit can ask include:

- What impact will the new technology have on the organization and its business processes, including risks, benefits, and new opportunities?
- How does the technology fit into the organization's enterprise risk management and governance, risk, and compliance approaches?
- How should the technology be integrated with existing controls? Has there been an evaluation of the impact on internal controls? If so, what changes should be made in controls and processes? Should internal audit work with each business unit to reevaluate their risk and controls and prepare to document new risks and controls?
- Do we need to do technology upgrades, business process changes, or upskilling of our people?
- What new risks does it introduce, including threats to privacy, customer data, proprietary information, and others?
- Where is the new system used and by whom?
- What happens to the data that the technology gathers or produces? Where is it stored and how is it protected?
- Will the organization now be sharing data that it shouldn't be or otherwise exposing itself to new data privacy risks?

Although internal audit does not need the same expertise as the organization's technology team, it can address the problem of technical debt by taking steps to ensure its people maintain sufficient skills to have productive dialogues with the IT team that can reveal the current state of the organization's systems, Pelletier said. Armed with this knowledge, internal audit team members can have fruitful conversations that respect IT team members' time and expertise.

In other cases, even if an organization's tech infrastructure is adequate, technology may get ahead of the company and its people. That can happen when organizations modernize their technology without bringing their workforces or business processes up to date. The company may be implementing the technology to enhance efficiency, but it fails to take the time to align and understand how processes will be affected or need to change. "People don't know how to use it, which wastes time, energy, and money," Pelletier said. "There's a missed opportunity to make significant improvements." Once again, internal audit has the institutional knowledge needed to ask the right questions to ensure that technology and the business's goals and assets are equally matched.

Finally, as technology hurtles forward, it may be easy to forget the value of the human touch, but human review and assessment will remain critical to the process, Wong noted. Not only does a tool like GenAI sometimes make mistakes or make things up, if used in customer or other human interactions, it may miss signals that a person would have understood or provide unworkable answers that a human familiar with the customer would have known were inappropriate.

Addressing Some GenAI Limitations

GenAI was met with wild enthusiasm when it was first introduced, but its shortcomings, as discussed in this report, have raised concern. It can be a valuable tool in addressing technology adoption in an organization, if used properly. Jim Pelletier identifies two options for internal auditors who want to enhance their GenAI use.

- In some cases, GenAI makes up answers, or hallucinates, if it can't answer a query, or it makes mistakes because it only knows what it has been trained on. To address that problem, Retrieval-Augmented Generation (RAG) is a technique that makes available accurate, timely data to augment what's in a GenAI system. RAG optimizes the output of large language models, such as GenAI, by referencing an authoritative knowledge base outside of GenAI's training data sources before a response is generated. And while GenAI sources have not been transparent, RAG makes it possible to identify source materials.
- Getting the best output from GenAI depends in part on giving the right directions, known as prompts. Prompts should specify details such as how long the response should be, the audience for it if it will be shared with others, the style, and the tone. Pelletier provides an example:

  You are an experienced internal audit manager with expertise in technology risk management in the financial services industry. You evaluate technology risk based on the impact to business operations and the likelihood that the risk will occur.

  - In table format, identify the top 10 risks related to the adoption of new technology in a large bank.
  - Include columns for Risk Name, Risk Description, and Rationale, describing why the risk is a top priority.
  - Prioritize the rows of the table from high risk to low risk.

Conclusion

While adopting new technologies can bring risk, it’s also important to remember the dangers of failing to stay up to date on new tools. The many disadvantages of doing so include:

- Missing out on benefits that new technology can offer.
- Failing to keep up with competitors because of the advantages they gain from digital transformation.
- Missing out on improved efficiencies and productivity or failing to innovate new products and services.
- Losing potential or existing customers, valued business partners, or talented employees who prefer to work with more technologically advanced organizations.

“Technology underlies all that we do every day,” Pelletier said. Internal audit can play a role in ensuring that new tools have the maximum positive impact.

Part 3: Internal Audit's Tech Talent Challenge

About the Experts

Jim Pelletier, CIA, CGAP

Jim Pelletier, CIA, CGAP, is a senior product manager with TeamMate Audit Solutions, where he works to continuously improve audit productivity while delivering strategic insights via TeamMate's best-in-class solution. He has more than 20 years of internal auditing experience in both the public and private sectors.

Previously, Jim held a number of leadership roles at The Institute of Internal Auditors, served as City Auditor for the City of Palo Alto, CA, and was Chief of Audits for the County of San Diego, CA. His diverse internal auditing background includes positions with the California State University System, PETCO Animal Supplies, Inc., State Street Corporation, and General Electric.

Dennis Wong, CIA, CFSA

Dennis Wong, CIA, CFSA, is a managing director at an international bank based in London. He is a seasoned audit and risk professional with over 20 years of experience in international banking and capital markets. His passion is to lead and drive changes through process re-engineering and technology innovation. He volunteers with The IIA's New York Chapter and serves on the global Exam Development Committee.

Nisha Nair, CIA, FCCA, UAECA, CFE, ACMA, CGMA

Nisha Nair works as an internal audit specialist for the Federal Authority for Nuclear Regulation in the United Arab Emirates. She has accumulated more than 10 years of experience as a financial and business risk advisory professional which includes working at the risk consulting practice of a 'Big 4' consulting firm. She is a member of various professional qualification bodies and is passionate about promoting and unlocking the true value of the internal audit profession. Additionally, she serves as a subject matter expert in the Global Professional Knowledge Group for IIA Global, with expertise that stretches across various subjects related to internal audit including risk management, data analytics, governance, fraud risk management, ethics, and external audit.

Introduction

The chink in internal audit's armor

According to the 2024 North American Pulse of Internal Audit, cybersecurity and IT were selected by internal audit leaders as the two highest risk areas in their organizations, with 78% and 58% of respondents respectively rating them as a high or very high risk. This should not come as a surprise; indeed, technology has dominated the risk landscape for the last several years. However, year after year it becomes more evident that internal audit faces serious challenges in this area that will only get worse if not addressed.

Cybersecurity and IT efforts combined make up nearly 20% of audit plans, according to Pulse survey respondents, who are primarily North American audit leaders. These together create the highest percentage of any other risk area, but Pulse data also indicate that both cyber and data security and IT were the areas most outsourced or co-sourced. Additionally, although about 2 in 10 respondents indicate that technology would be the top priority, nearly half of audit functions prioritize in-house staff increases. This is even though audit functions continue facing a variety of issues with recruiting, with 29% of Pulse respondents citing compensation expectations as the most significant challenge followed by 17% who say job candidates lack needed competencies.

Taken together, these findings paint a picture that shows that internal audit itself, while addressing technology risks to the best of its ability through outsourcing and co-sourcing, is overall not in an ideal place to bring technology competencies in-house. Long term, this approach can have significant repercussions not just for risk coverage, but also for audit functions' abilities to leverage the technology to improve all aspects of their role.

As the final installment of this three-part series on innovation and technology sponsored by TeamMate, this knowledge brief examines a number of facets of what can be called internal audit's "tech challenge," such as the struggle to build tech-savvy teams. It will also, through the input of selected industry experts, provide some best practices and strategies teams regardless of industry, budget, or function size can use to provide assurance and advisory services that can keep pace with technology's accelerating and relentless march.

Tech Team Building

Prepare Now for a Tech Future

The funding issue

Internal audit is not alone in the race to acquire tech-literate talent. Indeed, nearly every department in every organization in every industry is experiencing the same challenge, creating fierce competition to hire from what was already a limited recruiting pool. Following the mass layoffs in tech sectors during the COVID-19 pandemic, many analysts expected the roughly 20,000 tech-industry workers looking to work to sate this need somewhat. However, in testament to the rapid evolution of technology, the gap between needed positions and adequately skilled talent has widened — and what talent is available to hire does not come cheap. With 51% of audit functions, according to Pulse data, seeing their budgets stay about the same from the previous year, clearly, any audit function that wants to wade into the tech hiring pool has a steep challenge ahead of them.

“The most recurring topic that always pops up when various IA leaders talk about technology deployment struggles is the need for adequate funding,” says Nisha Nair, an internal audit specialist for the Federal Authority for Nuclear Regulation in the United Arab Emirates. “This includes funding for IT tools, funding for technology training for internal audit department's staff, and funding for hiring the right tech resources within the team. Very often when you try to recruit an individual from say a particular field such as the cyber industry, their expectations from a remuneration package standpoint is going to be much higher than a typical IA remuneration package, many of whom also prefer to work and grow in their niche specialized field of work that pays them more as opposed to being employed in a generalist internal audit role.”

Facing this harsh reality, to even come close to maintaining pace with the tech-driven risk landscape, internal audit has had to get creative in filling these necessary skill gaps. “Skillset strategy is not one-size-fits-all,” says Dennis Wong, managing director of internal audit at an international bank. “The right mix is different for every audit department. It’s a combination of growing/upskilling organically, co-sourcing with consultancies, and, when possible, hiring externally.”

Each element of this three-pronged strategy is worthy of discussion:

Hiring Externally

As previously mentioned, given current budget levels and lack of additional funding, implementing this strategy might come across as somewhat unrealistic thinking and even be discounted entirely. However, while certainly a challenge, advancement in this area is possible — and it starts with the audit committee.

Because the Board and/or the Audit Committee, do have a strong role to play for the approval of an internal audit’s annual budget, the goal for an internal audit leader should be to make a strong business case as to why additional funding for technical staff hiring is necessary in light of technology deployment and innovation. This goes beyond quoting data; rather, the goal should be to “deliver a compelling story” that is hard to refuse, says Nair. “IA leaders have to get the Audit Committee and the Senior Management's buy-in on the need for tech talent within the IA department, the value it shall provide to the organization, and explain the need for appropriate remuneration package and career path to attract such talent within the IA department,” says Nair.

“We have to get audit committee buy-in and make them realize that such talent is niche, and that the remuneration package that applies to the internal audit team may not actually be sufficient for someone in the cyber field,” she says.

This might also require the audit committee to reconsider how effective internal audit teams are structured for today’s risk environment. What is required of the audit staff today is very different than it was even 15 years ago. “Looking at the big picture, we need to think about what our teams need to look like," says Jim Pelletier, senior product manager with TeamMate Audit Solutions. "Today, you're not hiring a traditional internal auditor, you're hiring a cybersecurity expert — so maybe that's the role you need to have. Audit leaders need to explain to their committees they can't offer internal audit rates, because they're not hiring an internal auditor. They might not even have 'audit' in their job title."

As part of the pitch, such a cybersecurity expert does not have to be reserved explicitly for internal audit. "They can be used wherever their skill set fits," says Pelletier. "When I do a cybersecurity audit, I would do it comprehensively, but I might not need to do it continuously, so I might just need cybersecurity skills maybe a couple of times a year. It's time internal audit gets creative. I may not need to bring a cyber specialist on my team full time, but if I can use a cyber specialist that normally works in the second line as an auditor when necessary, that's incredibly valuable and efficient as long as I can manage any concerns with independence and objectivity."

Such conversations shouldn't end with the Audit Committee or the Board, however, the internal audit leader should use their position as a trusted advisor to communicate the value of skilled tech talent. "Leaders in the audit department can become the bearers of change," Nair continues. "They need to have technology oriented communication with the management team and facilitate navigation of the whole organization towards a more technology-enabled future." Having such communications at the top, she says, will trickle down to other departments within the organization. This shall help creating an environment that encourages collaboration to develop or enable technological solutions to reach a common goal. With enough organizational buy-in, funding inevitably follows.

Equally important in external talent searches is to take advantage of every avenue to widen the pool, if and when possible. This can be accomplished in a few ways. For example, maintaining a focus on diversity, equity, and inclusion (DEI) initiatives not only promotes cognitive intelligence within the department and organization but also makes organizations more attractive to younger generations of skilled talent. Additionally, departments posting vacant positions should be strongly considering widening the pool to include remote work options. According to Pulse, an astonishing 95% of Millennial (1981-1996) internal audit leaders expect remote work levels to remain the same, which implies there is an expectation that future hires will be looking for such options.

Finally, when hiring, be cognizant that technology is advancing so quickly that many of the competencies one might place in a job description could become outdated in a matter of years or even months. Therefore, hiring managers should not be so rigid in checking skillset boxes for candidates. What is key is not how well one knows a particular tech skill, but rather their ability to continually build new skills. "We don't suggest you hire an individual for a particular technology, but rather somebody who can grasp new technology easily," says Nair. "IA functions needs people who are adaptable, in terms of being able to absorb new skills like a sponge."

These are the kinds of individuals who will benefit most from team pairings that put them in a position to learn and succeed. "It's very rare to find a unicorn individual who 'singularly' has all the risk, business knowledge, audit, and data science and technology skills. It's not impossible, but it's rare," says Wong. "So, priority should really be about the creation of the team that has people working together collectively, like data scientists working alongside internal auditors who can learn and grow through the audit process."

Outsourcing and Co-Sourcing for Upskilling

As previously mentioned, many audit functions today are opting to outsource and co-source their cyber and IT auditing responsibilities. This trend obviously stems from necessity given the challenges and constraints of hiring, but especially in tech areas such as cybersecurity, it is also a necessity.

"Internally, it's very hard to get knowledge of the latest, greatest technology," says Wong. "You've got to go out of your company to look for that expertise. That is where consultancies and specialists come in."

However, when bringing in these outside firms, it can sometimes be overlooked how that outsourced talent can have an impact on the audit function beyond the length of their contract.

"What works really well is when IA Departments make use of their existing IA suppliers, IA partners, and/or consultancy firms in upskilling their own departmental IA staff, while the outsourced/co-sourced talent executes the prescribed audit work," says Nair.

“It’s good to pair the external outsourced/co-sourced talent/partners/consultants up with inhouse IA staff to enable knowledge transfer whilst the engagement is being executed. On the job learning definitely proves to be more effective.”

Pelletier agrees.

“If we’re outsourcing or co-sourcing, that’s fine, but are you improving?” he asks. “Are you embedding your staff into their projects so that they’re learning? Are you taking full advantage of the time you have to build internal skill sets a bit more?”

It is also a useful idea to spread basic tech competencies from outsourced and co-sourced talent in a more structured manner. This can take the form of workshops or group sessions where individuals from all departments can see firsthand the possibilities of technology, and then they can bring the newfound knowledge back to their respective areas.

However, once the team is upskilled or expertise is brought in full-time, co-sourcing should always be a part of an organization’s skillset strategy. “Once highly skilled talent is brought in as a full-time employee, inevitably they lose their edge,” says Wong. “In cybersecurity, for example, let’s say you bring in a white hat hacker with the latest tech expertise to do things like penetration testing. But if they are no longer ‘hacking,’ they are no longer going to be on that cutting edge of the field. So, no matter the internal team’s skill level, you’re always going to want to hire an outside firm to some extent because they’re always going to know the latest vulnerabilities.”

Upskilling From the Inside Out

While so much of the discussions on technology revolve around bringing talent in, it is critical not to overlook the talent that is already in-house. Through positive relationships and collaboration among internal audit, senior management, and the IT team, internal audit should work to develop a clear understanding of both the skills and tools other departments possess. Data analytics or continuous monitoring software, for example, can have broad applications that could fit seamlessly into audit tasks with a little training.

“You should work together with other teams and explore the various avenues where you can collaborate — and if the relationship is good, they might be able to say something like, ‘Okay, we have these tools in place, so why don’t we use them for an internal audit purpose?’” says Wong.

This is true for senior management, as well. As the second line, they might have access to data analytics tools, continuous auditing continuous monitoring (CACM) tools, and tools that deal with ISOs and procedures — all of which can be useful in an internal audit context.

Of course, the need for upskilling goes far beyond just internal audit. To be sure, the drive to increase baseline tech competencies organization wide needs to be omnipresent in today’s environment. Again, leveraging their role as a bearer of change, internal audit leaders should advocate in all their department interactions for mandatory training on current technology trends and techniques. “An effective approach would be to define the bare minimum level of technology or data related knowledge and skills along with levels of progress/expertise for each position within the IA competency framework,” says Nair. “We need to encourage each IA professional to undergo the minimum required training to learn at least the basic IT skills for their job position and progress thereon.”

Wong expresses a similar sentiment. “There’s a constant need for upskilling in all roles,” he says. “It’s a must just to stay relevant and keep pace with markets. There are always new tools and techniques to be aware of.”

Getting such skills does not always have to involve increasing training budgets. Many of these skills can be learned either individually via free online courses or inter-departmental knowledge sessions — ideally both. “Very often when a non-technical person reads technical articles online, the technical jargon tends to put them off,” says Nair. “Having individuals within the department or the organization to just help IA Staff through with understanding such tech jargons and concepts is quite helpful in terms of creating a desire for exploring various facets of technology.”

Keep in mind, however, that once a “bare minimum” is established, that bar will need to be raised in short order. When assessing these frameworks through an audit, internal auditors need to focus not just on whether the skills are being taught but also on seeing how those skills are continuously and effectively implemented and built on as the knowledge base grows.

"An effective upskilling strategy should include some measurement of 'digital fitness,'" says Nair. "Departmental performance measures shouldn't be restricted to implementation of technology; it should also include KPI's that measure how the department continuously evolves with regards to usage of that particular technology. Hence, internal audit leaders need to advocate in favor of upgrading KPI's that indicate how departments are transforming rather than just deploying a particular technology. Without continuous evolution or transformation, everyone risks remaining stagnant."

Pelletier adds, "Technology is integrated into everything we do, so we have to constantly advocate for raising that bar. Technology is constantly changing, so really, we're already in catch-up mode. If we don't move, the gap is going to continue to grow. As an audit leader, your goal is to manage how broad or narrow you and your board are willing to have that gap be."

Hail, King Data

The Foundation of All Tech Progress

Finding quality data and understanding it

Data is king, the cliché goes, and it gets truer by the day. No matter the strategy used to create effective digital teams, none of them will have any kind of effect without access to quality data.

“Data is imperative to audit work, especially with the prevailing use of system and automated controls,” says Wong. “Given the abundance of data today, the opportunities to leverage them in internal audit is immense — provided one knows how to use it, which makes the lack of it all the more problematic.”

While recognizing that lack of data is problematic, even today, access to quality data is not a given. And equally worrisome, says Nair, is when IA departments use their perceived inability to acquire data as an excuse to not move forward towards technological deployment within IA activities. This cannot be the case. Instead, the journey to acquire and leverage data should be used as a critical part of the internal audit’s business case for tech advancement. “When it comes to data integrity, IA functions should not restrict themselves to mere identification or categorization of data as good or bad,” she says. “Instead, IA functions should grasp this opportunity to bring it to the attention of the executive management, provide recommendations to improve data quality, and get the ball rolling. Halting use of technology in audits for such concerns may result in IA functions never moving forward in its technology endeavors."

Data does not necessarily require investment for collection. Too often, it can be just a matter of having the knowledge to leverage the data that is already on hand. Even information tracked within an Excel spreadsheet can be considered quality data depending on the situation. The keys to unlocking it are simple: the right skill to notice it and highlight it and leverage it, and the right culture to foster the development of such a skill. In other words, where the talent is nurtured and developed, the data follows.

In the right environment, the data does not even have to be perfectly ideal to be considered valuable. “My view is that having data is always better than not having any data,” says Wong. “Even an incomplete set of data is still better than not having any data at all. What is more important than data completeness is having the mindset of getting every data analytics opportunity out of what you do have. Let’s say I give you $10, but I give it to you in pennies. You’ll still accept it on the basis that it’s still $10, even if it’s somewhat cumbersome.”

However, internal audit must do more than just understand how data is used. According to Pelletier, data knowledge comes down to answering four questions:

- Where is it coming from?
- Where is it stored?
- What is being done with it?
- How is it being disposed of?

For the most part, answering these questions does not require a particularly high degree of technical knowledge.

“Data governance is something I think every auditor should become experts at,” says Pelletier. “Some aspects may require deeper technical knowledge, but every auditor should be equipped to ask challenging questions and understand underlying processes and pull in the technical expertise just on the parts you need.”

Conclusion

Tech is opportunity, not loss

For all the talk about the incredible benefits technology can bring, it can bring just as much anxiety. It is natural to see it as overwhelming — even to the point where one might even start to question their own job security. At some point as tech evolves, is there going to be a place for human work at all?

This is an understandable concern, but it is a concern that stems from the wrong kind of organizational culture. Technology should not be looked upon as a competitor or threat — it should be viewed with enthusiasm as an opportunity to accomplish more, provide more value to the organization, and indeed even improve the individual workers' day-to-day.

"While not a majority, there may still be a number of people who may believe that automation would take away their job or those who are behaviorally anchored towards maintaining their set ways in executing audits, such as doing what you are comfortable with, let's say use of the good old spreadsheets," says Nair. "IA leaders should encourage discussions about the need to remain agile in this dynamic technology driven era, adopting a learning mindset and the potential benefits of technology, particularly framed as means to reduce department workload or increase efficiencies rather than as a means to replace auditors. "

Internal audit can and should be technology's biggest advocate in the organization. It is the change-bearer, the partner, the bringer of good news. As the tech challenge continues, organizations could use a few more of those.

About The IIA

The Institute of Internal Auditors (IIA) is a nonprofit international professional association that serves more than 235,000 global members and has awarded more than 190,000 Certified Internal Auditor (CIA) certifications worldwide. Established in 1941, The IIA is recognized throughout the world as the internal audit profession's leader in standards, certifications, education, research, and technical guidance. For more information, visit theiia.org.

About Wolters Kluwer TeamMate

Wolters Kluwer TeamMate Audit Management Solutions is a world-leading internal audit and assurance expert solution with over 25 years dedicated to advancing corporate, commercial, and public sector auditors. As internal audit teams evolve to deliver deeper insights, greater risk assurance, and improve efficiency, they require purpose-build and future-ready solutions. TeamMate provides expert solutions internal auditors rely on to drive value into their organizations. For more information, visit www.teammatesolutions.com.

Disclaimer

The IIA publishes this document for informational and educational purposes. This material is not intended to provide definitive answers to specific individual circumstances and as such is only intended to be used as a guide. The IIA recommends seeking independent expert advice relating directly to any specific situation. The IIA accepts no responsibility for anyone placing sole reliance on this material.

Copyright

May 2024

The Institute of
Internal Auditors

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101