GLOBAL KNOWLEDGE BRIEF

Innovation and Technology

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

Wolters Kluwer

The Institute of Internal Auditors

Contents

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.[1]

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.

[1] "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.

About The IIA

The Institute of Internal Auditors (IIA) is a nonprofit international professional association that serves more than 245,000 global members and has awarded more than 195,000 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 only. This material is not intended to provide definitive answers to specific individual circumstances and as such is only intended to be used as peer-informed thought leadership. It is not formal IIA Guidance. 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.

Global Knowledge Briefs are intended to address topics that are timely and relevant to a global internal audit audience, and each topic covered is vetted by members of The IIA's volunteer North American Content Advisory Committee. Subject-matter experts are primarily identified and selected from The IIA's list of Global Guidance Contributors.

To apply to be added to the Global Guidance Contributors list, email Standards@theiia.org. To suggest topics for future Global Knowledge Briefs, email Content@theiia.org.

Copyright

February 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