GLOBAL KNOWLEDGE BRIEF

Innovation and Technology

Part 1: Internal Audit’s Role in Technology Assurance

Wolters Kluwer

The Institute of Internal Auditors

Contents

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

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 assurance efforts by determining if the risk management, compliance, internal audit, and other functions each have their own systems

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%.

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

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.

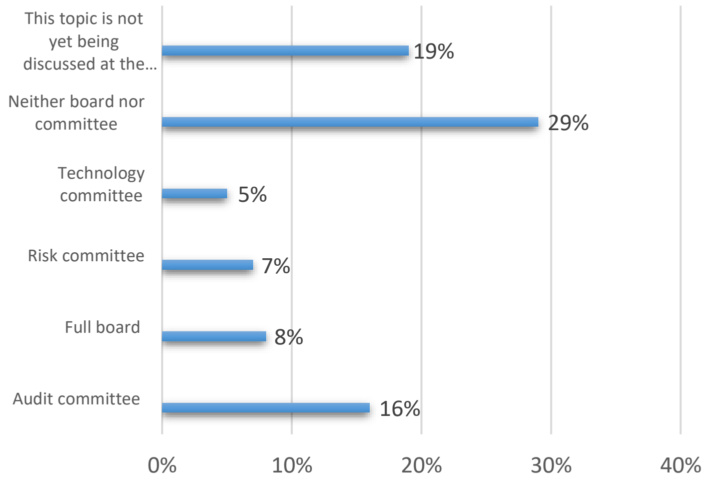
Keeping an eye on AI

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.

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

January 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