The Impact of Poor IT Audit Planning and Mitigating Audit Risk

IT auditors provide reasonable assurance that business processes and their supporting technology are secure and comply with enterprise policies, standards, and applicable statutory and regulatory mandates. Auditors' IT competence and experience vary, and that expertise increases with an individual's knowledge of information security and technical environments.[1] The lack of IT audit plans and the absence of appropriate technical resources can cause deficiencies in safeguards and conformance with external mandates such as the US Health Insurance Portability and Accountability Act (HIPAA), the Payment Card Industry Data Security Standard (PCI DSS), and the EU General Data Protection Regulation (GDPR). Today, data protection, compliance and privacy are major concerns for enterprises and consumers, and inadequate plans can lead to breaches in consumer data and personally identifiable information (PII).[2]

Development of IT Auditors in a Changing Landscape

The audit profession must continually develop and adapt to a landscape where technology and risk are always evolving. Adopting a risk-based approach to audits involves determining and applying the enterprise's risk appetite, tolerance and expectation for compliance.[3] Risk appetite is the level of risk an enterprise is willing to accept in pursuit of its goals, objectives and mission and how much deviation is tolerable.[4] Before conducting assessments, IT auditors should talk with enterprise executives to understand their perspective on risk and to establish risk thresholds. Afterward, the auditors can involve subject matter experts to ensure the accurate interpretation and employment of technical controls.[5]

Similar to compliance-oriented assessments, risk-based audits utilize questionnaires to ensure that controls are operating and comply with internal and external mandates. However, IT auditors do not rely solely on "yes" or "no" responses to questions. They weigh each response against the enterprise's risk appetite and expectations.[6] Additionally, risk-based approaches can utilize open-ended questions to obtain information about the control environment. This strategy allows auditors to obtain a clearer understanding of an enterprise's security posture and associated risk. Likewise, risk-based methods involve an in-depth analysis based on the client's responses. However, because risk-based tactics evaluate responses against expectations, the auditor is in a better position to determine the need for an investigation than would be the case with a subjective assessment of "yes" or "no" responses. Risk-based inquiries are comparable to an instructor giving students an exam. To grade each student's

Blake Curtis, CISA, CRISC, CISM, CGEIT, CISSP
Began his IT career in 2009 and has more than 10 years of experience in engineering, networking, virtualization, IT service management, cybersecurity and risk management. Curtis currently serves as an information security and compliance adviser for Cigna's global security assurance team. He advocates for continuous education and has more than 15 industry certifications across diverse disciplines. His primary interests exist within governance, risk and compliance, and he emphasizes the significance of acting as the bridge between the enterprise and information technology. Curtis is currently completing his doctorate degree in cybersecurity at Capitol Technology University (Washington DC, USA). He can be reached at *https://www.linkedin.com/in/reginaldblakecurtis/*.

exam fairly and consistently, the instructor must determine beforehand what answers the students are expected to give for each question.

Suggested Solutions

Enterprises should reinforce compliance with audit standards and support their auditors by providing ongoing education and motivation. Standards such as those developed by ISACA® and the Institute of Internal Auditors (IIA) exist to ensure that professionals conduct audits in a consistent and organized fashion.[7,8] Continuing education ensures that auditors are aware of the risk associated with modern technologies.[9] Employee motivation reduces the risk of deficient audit processes and encourages collaboration among subject matter experts.

Compliance With Audit Standards

Enforcing conformance with standards ensures that auditors plan audits properly; possess a comprehensive understanding of the technology, processes and knowledge required to perform competent audits; and collaborate with subject matter experts to develop review criteria that encompass compliance with laws, regulations and enterprise standards. In turn, proper audit preparation guarantees that auditors employ appropriate processes to collect, validate and comprehend the data used as evidence.[10] Compliance with standards also offers clients transparency and ensures that enterprises are aware of the techniques, procedures and resources IT auditors use to perform audits.[11]

Some IT audit assurance functions may disaffirm or repudiate IT audit standards. However, individuals holding the Certified Information Systems Auditor® (CISA®) credential must conform to ISACA's Code of Professional Ethics, which requires auditors to be competent, have an adequate understanding of IT, and engage in activities that can be accomplished with their current skills and knowledge.[12] Violations can result in disciplinary measures and the loss of credentials.

Continuing Education

Continuing education provides auditors with the techniques and skills required to perform audits across various technologies, and it makes them aware of the risk factors associated with new technologies and applications.[13] Emerging technologies such as artificial intelligence (AI), data science and investments in cloud infrastructure introduce ambiguity and new risk factors that can challenge IT audit professionals. To stay up to date, enterprises should require that IT auditors undergo training and obtain credentials in cloud technologies such as Microsoft Azure and Amazon Web Services (AWS). Additionally, entry-level certifications in networking, storage and operating systems can diversify auditors' skill sets. This strategy better enables auditors to identify and interpret technical risk factors that could have a significant impact on the enterprise. Furthermore, IT auditors with diverse skill sets can foster teamwork and facilitate effective communication between the business and technical teams. ISACA's 2001 Audit Charter guidelines recommend that the audit function provide continuing education with a minimum of 40 hours of practice each year, and its 1006 Proficiency standard requires IT auditors to maintain competency through ongoing training.[14] Audit functions must evaluate the expertise and competency of their auditors, determine the causes of deficiencies, and develop training plans to mitigate weaknesses.

> "AUDIT FUNCTIONS MUST EVALUATE THE EXPERTISE AND COMPETENCY OF THEIR AUDITORS, DETERMINE THE CAUSES OF DEFICIENCIES, AND DEVELOP TRAINING PLANS TO MITIGATE WEAKNESSES."

Some enterprises may fail to see the benefit of requiring continuing education or may struggle with the cost of providing such training, finding it difficult to justify based on the return on investment (ROI). However, audit functions must ensure that their practitioners abide by the applicable code of ethics

and standards. The IIA's Code of Ethics states that auditors must continuously improve their competencies through training and adopt best practices.[15] An auditor's skills and technical capacity can impact an audit's quality.[16] Because financial considerations can impede auditors from obtaining the necessary skills to conduct audits involving intricate technologies, ISACA recommends that auditors accept tasks only if they are confident that reasonable measures exist to ensure a successful audit.[17] For example, the audit function can provide on-the-job training or stewardship or hire third parties skilled in the auditing of specific environments. Internal IT audit functions can work alongside third parties to acquire the applicable skills and reduce future costs associated with outsourcing.

Motivation

Apathetic auditors are likely to produce substandard audits that may jeopardize an enterprise's security posture. Therefore, audit functions should offer incentives to their employees to promote self-sufficiency and teamwork. According to ISACA's Professional Independence standard, enterprises should utilize rewards and penalties based on auditors' performance.[18] IT auditors who conduct only specific types of assessments in areas such as PCI DSS or HIPAA may get bored, which could cause them to overlook material misstatements. Over time, auditors can develop a myopic perspective toward their jobs, and they may fail to consider risk factors associated with underlying technologies or the implications of emerging solutions. Failure to adapt and modify IT audit practices can create knowledge gaps and impede effective communication. Furthermore, these failures can result in the inability to identify and interpret risk associated with new technology. To address these potential shortcomings, enterprises can institute job rotation and incentive programs to reduce the monotony associated with familiarity.

Some enterprises may argue that motivational solutions are not feasible, owing to their reliance on personnel resources and their lack of versatility. The adoption of COBIT® is feasible because it focuses on current business processes and knowledge. Enterprises can develop both organizational goals and IT goals, mapping focused issues to the COBIT® framework to define motivational processes based on organizational needs.[19] Additionally, by means of a constant review of employee performance, enterprises can identify listless individuals and develop solutions to diversify their skill sets and engender allegiance. ISACA's professional independence and proficiency standards emphasize that job rotation and continuing education can contribute to motivation and flexibility.[20]

> "RISK-BASED TACTICS ADDRESS EXPERIENCE VARIATIONS AMONG IT AUDITORS BY ESTABLISHING EXPECTATIONS FOR BOTH RISK AND COMPLIANCE."

Conclusion

Data constitute an enterprise's most valuable commodity, and enterprises transfer and store data across complex systems, making effective cybersecurity and assurance processes paramount.[21] It is therefore vital to ensure that IT audits are conducted by those with the requisite expertise and experience.[22] Risk-based tactics address experience variations among IT auditors by establishing expectations for both risk and compliance. This strategy enables IT auditors to remain objective and ensures a consistent interpretation of clients' responses. This approach also addresses variances in IT audit skills and competencies by providing auditors with better direction and the ability to evaluate their expectations for technical responses. Enterprises must ensure that IT auditors utilize suitable resources, competencies and skills to conform to legal mandates and protect the enterprise's and consumers' data.[23]

Endnotes

1 Brazel, J. F.; "How Do Financial Statement Auditors and IT Auditors Work Together?" *CPA Journal*, vol. 78, iss. 11, 2008, p. 38–41, *https://pdfs.semanticscholar.org/8144/6735e950b2bc3a53d529f616a45124694a32.pdf*

2 Bassett, J.; "Security in Management's Terms: By Translating Audit Findings About Technology Weaknesses Into Actions CEOs Can Take, Auditors Can Make IT Governance a Top Business Priority," *Internal Auditor*, June 2007, p. 27

3 Jana, V. W.; R. Rudman; "COBIT 5 Compliance: Best Practices Cognitive Computing Risk Assessment and Control Checklist," *Meditari Accountancy Research*, vol. 27, iss. 5, 2019, p. 761–788, *https://doi.org/10.1108/MEDAR-04-2018-0325*

4 Drew, M.; "Information Risk Management and Compliance—Expect the Unexpected," *BT Technology Journal*, vol. 25, iss. 1, 2007, p. 19–29, *https://doi.org/10.1007/s10550-007-0004-x*

5 Hux, C. T.; "Use of Specialists on Audit Engagements: A Research Synthesis and Directions for Future Research," *Journal of Accounting Literature*, vol. 39, 2017, p. 23–51, *https://doi.org/10.1016/j.acclit.2017.07.001*

6 *Op cit* Jana, Rudman

7 ISACA®, "Standards, Guidelines, Tools and Techniques," 2020, *https://www.isaca.org/resources/isaca-journal/issues/2020/volume-1/standards-guidelines-tools-and-techniques*

8 Institute of Internal Auditors: North America, "International Standards for the Professional Practice of Internal Auditing (Standards)," 2017, *https://na.theiia.org/standards-guidance/Public%20Documents/IPPF-Standards-2017.pdf*

9 D'Onza, G.; R. Lamboglia; R. Verona; "Do IT Audits Satisfy Senior Manager Expectations? A Qualitative Study Based on Italian Banks," *Managerial Auditing Journal*, vol. 30, iss. 4, 2015, p. 413–434, *https://www.emerald.com/insight/content/doi/10.1108/MAJ-07-2014-1051/full/html*

10 *Op cit* ISACA

11 Chang, C.; Y. Luo; L. Zhou; "Audit Deficiency and Auditor Workload: Evidence from PCAOB Triennially Inspected Firms," *Review of Accounting and Finance*, vol. 16, iss. 4, 2017, p. 478–496, *https://doi.org/10.1108/RAF-03-2017-0050*

12 *Op cit* ISACA

13 Lindsay, J. B.; A. Doutt; C. Ide; "Emerging Technologies Risk and the Auditor's Focus," Harvard Law School Forum on Corporate Governance, 8 July 2019, *https://corpgov.law.harvard.edu/2019/07/08/emerging-technologies-risk-and-the-auditors-focus/*

14 *Op cit* ISACA

15 Institute of Internal Auditors: North America, "Code of Ethics," 2020, *https://na.theiia.org/standards-guidance/mandatory-guidance/Pages/Code-of-Ethics.aspx*

16 Roussy, M.; M. Brivot; "Internal Audit Quality: A Polysemous Notion?" *Accounting, Auditing and Accountability Journal*, vol. 29, iss. 5, 2016, p. 714–738, *https://doi.org/10.1108/AAAJ-10-2014-1843*

17 *Op cit* ISACA

18 *Ibid*.

19 Putu Wulan, W. S.; I. M. Sukarsa; E. P. I. Putu Agus; "The Improvement of IT Processes at Office X in One of the Cities in Indonesia," *International Journal of Information Engineering and Electronic Business*, vol. 11, iss. 6, 2019, p. 1, *www.mecs-press.org/ijieeb/ijieeb-v11-n6/IJIEEB-V11-N6-1.pdf*

20 *Op cit* ISACA

21 Short, J.; S. Todd; "What's Your Data Worth?" *MIT Sloan Management Review*, vol. 58, iss. 3, 2017, p. 17–19, *http://ilp.mit.edu/media/news_articles/smr/2017/58331.pdf*

22 Kim, S. L.; T. S. Teo; A. Bhattacherjee; K. Nam; "IS Auditor Characteristics, Audit Process Variables, and IS Audit Satisfaction: An Empirical Study in South Korea," *Information Systems Frontiers*, vol. 19, iss. 3, 2017, p. 577–591, *https://doi.org/10.1007/s10796-015-9612-z*

23 *Op cit* Chang *et al*.