Organizations place a strong emphasis on cybersecurity, privacy and compliance. However, many enterprises are uneducated when it comes to identifying, assessing, responding to and monitoring these domains. Auditors provide value in these areas and address these deficiencies via various techniques and approaches. IT audits play a significant role in protecting technology, enterprises and the economy; in turn, audit quality influences how the public and investors perceive an enterprise's reputation based on its effectiveness in preventing breaches of personally identifiable information (PII). Audits also play a significant role in an enterprise's cyberresilience. For example, IT auditors are responsible for ensuring that IT protects and optimizes business objectives. Moreover, IT audits ensure that technical controls are designed and operating effectively to mitigate threats to the enterprise's mission, vision and objectives. The need for IT audits is growing as technology evolves at an unprecedented velocity; the complexity of new technologies such as big data and containerization demands a unique set of skills and collaboration among IT specialists and IT auditors. The interaction between IT auditors and subject matter experts (SMEs) is vital to ensure that enterprises implement the appropriate safeguards and countermeasures. Audits enhance cyberresilience by ensuring that IT processes meet business goals and external requirements 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).

Industries of all sizes and types are exposed to risk; however, enterprises may not utilize their resources effectively to identify the likelihood of threats materializing and the potential impact if they do. For example, in the case of a new statutory or regulatory requirement, such as the US State of California Consumer Privacy Act (CCPA), the enterprise must effectively translate compliance risk throughout the strategic, operational and tactical tiers of the business. IT audits interpret risk by identifying the applicable requirements and communicating with senior management and subject matter experts within the enterprise to determine risk thresholds and implement required controls.

**Compliance vs. Risk**

Enterprises must employ best practices to reduce the frequency of cybersecurity incidents and breaches of sensitive data. There are two methods of protecting against such events: compliance-based audits and risk-based audits. Compliance-based audits substantiate conformance with enterprise standards and verify
compliance with external laws and regulations such as GDPR, HIPAA and PCI DSS. Risk-based audits address the likelihood of incidents occurring because of vulnerabilities such as deficient safeguards, technologies, policies and procedures. Although risk-based audits include the risk of noncompliance, compliance-based audits do not identify and enforce risk thresholds. Both audit strategies aim to support enterprise objectives and compliance requirements, but the approaches vary in purpose, technique and execution. The juxtaposition of these two methodologies highlights their respective strengths and weaknesses. Additionally, this comparison provides insight for enterprises that need to support contrasting stakeholder interests and reduce risk to an acceptable level.

**Compliance-Based Audits**

Compliance-based audits evaluate compliance with laws, regulations and internal policies. These audits are necessary to establish a reasonable level of assurance that an enterprise is conforming with external requirements and internal processes. The risk of noncompliance, such as fees and penalties, necessitates compliance with industry standards and recognized practices. For example, in 2019, the US Department of Health and Human Services and the Office for Civil Rights (OCR) imposed a US$2.154 million penalty against an organization that violated HIPAA’s security and breach notification rules.

Compliance-focused audits use frameworks such as those created by the US National Institute of Standards and Technology (NIST) and the International Organization for Standardization (ISO) to support enterprise objectives and comply with external requirements. IT auditors then utilize questionnaires based on these frameworks to establish statutory and regulatory compliance. IT auditors provide auditees with yes-or-no questions to ascertain whether adequate controls are in place to comply with laws, regulations and enterprise policy. Based on the responses, IT auditors perform substantive testing such as inspections, sampling and evidence gathering to obtain better assurance of compliance. This strategy is analogous to a physician asking a patient to complete a yes-or-no questionnaire to determine whether a more extensive examination is warranted. Modern IT audits leverage compliance-based tactics to ensure that enterprises conform to internal and external mandates. However, the increase in breaches highlights this methodology's inconsistency, limitations and inherent risk.

**Risk-Based Audits**

Risk-based audits also use industry frameworks to ascertain support of organizational goals and conformance to external parameters. In contrast to compliance-based audits, they also apply the enterprise’s risk appetite, risk tolerance and expectation of compliance. Risk appetite is the level of risk the enterprise is willing to accept in pursuit of its goals, objectives and mission and how much deviation is tolerable. First, IT auditors should consult senior management to establish risk thresholds. Then the auditors should involve subject matter experts to guarantee the accurate interpretation and employment of technical controls. At the strategic level, auditors should discuss risk factors that impact the enterprise’s mission, vision, strategy and objectives.

Second, IT auditors must communicate with management and business owners to identify risk factors that affect the enterprise at the operational level. The operational tier plays an imperative role by providing major business processes and services that support the strategic level’s business objectives and goals. Last, IT auditors must identify the underlying infrastructure that supports operations at the tactical level. The tactical or technical tier provides the infrastructure and technology that optimize and sustain the core services and processes in the operational tier. IT auditors must understand how risk factors at each level relate to and endanger the overall mission and business objectives. For example, frameworks such as COBIT® 2019 and NIST Special Publication 800-53 help auditors translate strategic and operational risk into technical risk and vice versa. This strategy enables auditors to have conversations at each tier and educate management on how risk factors identified at one level can affect other levels.

Similar to compliance-based audits, risk-based audits use questionnaires to ensure that controls are operating and in compliance with internal and external mandates. However, in this case, IT auditors do not rely solely on yes-or-no responses;
they weigh each response against the enterprise’s risk appetite and expectations. Additionally, risk-based questionnaires utilize open-ended questions to obtain information about the control environment. This strategy allows auditors to gain a clearer understanding of the enterprise’s security posture and associated risk. Risk-based methods also include an in-depth analysis based on the auditee’s response. However, because risk-based tactics evaluate responses against expectations rather than subjectively evaluating yes-or-no answers, the auditor is in a better position to determine the need for an investigation. Risk-based inquiries are comparable to an instructor presenting students with an examination. To grade each student’s paper fairly and consistently, the instructor must already know the answers to each question.

Modernizing IT Audits

Although risk-based audits provide several advantages over the compliance-based approach (see figure 1), today’s environment necessitates a modern methodology to keep up with continuous changes in the threat landscape, information security and technology. Technologies such as containerization and microservices solutions present new risk factors for enterprises. Therefore, it is paramount that IT auditors continuously advance the profession and utilize tools and techniques such as data analytics, continuous auditing and continuous monitoring, which are indispensable. They better illuminate threats in real time and empower management to make informed decisions about control maturity and residual risk.

Figure 1—Threat Intelligence Data Feeds

<table>
<thead>
<tr>
<th>COMPLIANCE AUDITS</th>
<th>VS.</th>
<th>RISK AUDITS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliance Risk</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compliance-Based Audits</td>
<td>• Addresses risk of penalties and fines</td>
<td>• Addresses strategic, operational and tactical risk</td>
</tr>
<tr>
<td></td>
<td>• Reviews yes-or-no questionnaires to gain reasonable assurance</td>
<td>• Identifies risk thresholds</td>
</tr>
<tr>
<td></td>
<td>• Interpretation of technical responses vary among auditors</td>
<td>• Works with management and SMEs to establish expectations for control maturity</td>
</tr>
<tr>
<td>Data Analytics</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Continuous Auditing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Continuous Monitoring</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Conclusion

Questionnaires present their own limitations during the audit process. For example, respondents may not answer truthfully or may skew their responses. Moreover, the IT auditor may not possess the skills or background to determine whether the responses are appropriate for a given situation.

Risk-based and compliance-based audits can benefit enterprises and protect them in several ways. For example, traditional compliance audits help enterprises conform to various mandates and prevent fines associated with noncompliance. However, compliance-based approaches do not take into account risk-based expectations or ensure that auditors have an adequate understanding of safeguards and technology. Most important, compliance-oriented strategies are ineffective and inconsistent in addressing risk factors other than compliance issues. Risk-based tactics, in contrast, address variations in experience 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 responses. Furthermore, this approach addresses different levels of IT audit skills and competencies by providing auditors with better direction and a better ability to evaluate responses to technical questions based on expectations.

Significant business collapses such as Enron, WorldCom and Tyco forced the US Congress to enact standards such as the US Sarbanes-Oxley Act (SOX). However, more recent events such as the Equifax breach highlight weaknesses in the compliance-oriented approach. As the number of breaches continues to increase, enterprises should be concerned about how much reliance they place on compliance certifications. Although compliance is vital, it is crucial to emphasize that many enterprises that have experienced breaches, such as Equifax and Target, were compliant and had been certified by reputable auditing and accounting firms. Therefore, enterprises should reevaluate and modify their audit strategies to address risk factors distinct from compliance to reduce the likelihood of breaches.

Endnotes

3 Ibid.
5 Op cit Haapamäki, Sihvonen
6 Ibid.
9 Op cit De Smet, Mention


© 2020 ISACA. All rights reserved. www.isaca.org