Addressing Emerging Audit Challenges

Challenges come in various forms, including personal, academic, professional and societal. Addressing these challenges can be a positive or negative experience and often provides the opportunity for growth, learning and development. Challenges can test one's abilities, build resilience and lead to success.

With the rapid advancement of technology, every field is undergoing various challenges, and the audit field is no exception.

Audits play a critical role in ensuring that financial information disclosed to stakeholders is fair and accurate, identifying potential threats to enterprises and ensuring compliance with regulatory requirements. An enterprise's financial records are evaluated during an audit to ensure that they adhere to accounting standards, rules and laws. Maintaining investor trust, assisting in decision-making processes and ensuring the integrity of the financial system all depend on the audit's independent assessment of the accuracy and reliability of financial statements.

The audit profession is facing new challenges related to the globalization of business operations; environmental, social and governance (ESG) expectations; the increasing complexity of data and the evolving business environment; and the emergence of new technology. In addition, cutting-edge technologies such as blockchain and artificial intelligence (AI) are revolutionizing the way audits are carried out. In this environment, traditional audit methods may no longer be adequate; auditors must keep pace with new developments and challenges and adapt their audit approaches as needed.

Globalization Challenges

Because enterprises are increasingly likely to operate globally, auditors must understand the accounting and auditing standards of other countries to provide relevant and reliable assurance services across different jurisdictions.

Each country has its own accounting and auditing standards based on its specific legal and regulatory requirements. The United States relies on generally accepted accounting principles (GAAP), but more than 100 countries worldwide require enterprises to abide by the International Financial Reporting Standards (IFRS).[1] Investors and key stakeholders in multinational enterprises must have confidence in the accuracy and reliability of those entities' financial statements, and auditors play a key role in providing that assurance.

IGNATIUS RAVI | CISA

Is a senior IT auditor in Amazon's Internal Audit Department and has worked in the field of audit and risk at Fortune 500 companies for the past eight years. Ravi is the education and program director for the ISACA® Utah (USA) Chapter and is involved in the ISACA Certified Information Systems Auditor® (CISA®) Exam Item Writing Group. He has served as a judge for several awards such as the Stevie, Globee and CODiE Awards and the ISACA OneInTech Scholarship. He is part of Criya, a highly vetted circle of tech industry professionals, and is a member of the Information Systems Security Association (ISSA) Utah Chapter.

Variations in data quality can add to the complexity of an audit, especially when structured and unstructured data are gathered from a variety of sources.

ESG Challenges

Accuracy and completeness of financials may not be the only factor important to investors and stakeholders. ESG concepts such as organizations' ethical practices, impact on climate change; ethical relationships with employees, customers, vendors, communities and other stakeholders; and governance structure and processes that guide decision-making and oversight within an organization may also need to be assessed. ESG information may not be material to an enterprise's financial statements, and reporting is often voluntary; however, ESG subjects are increasingly important to global investors and stakeholders.[2]

Auditing ESG information can be a challenge because relevant data are often complex, unstructured and hard to gather and verify. In addition, ESG issues may be subjective, making it difficult to establish objective criteria for auditing purposes. However, auditors can use various methods to assess the reliability and accuracy of subjective information including:

- Examine the documents on which the ESG data are based, including sustainability reports, social impact studies and environmental impact studies. Check the sufficiency of the data collecting and reporting processes and the completeness, accuracy and dependability of the data.
- Interview key people involved in the gathering and reporting of ESG data, including sustainability officers, environmental managers and human resources (HR) staff. They can provide information to auditors about the accuracy of the data, making it easier to spot any gaps or inconsistencies.
- Examine the ESG data to identify any unexpected patterns or discrepancies that might point to inaccuracy. For instance, utilize data analytics to compare the ESG data with industry benchmarks, historical patterns or other pertinent data sets.
- Consult outside experts such as environmental engineers, sustainability consultants or social impact analysts to gain insight into ESG data. These professionals can help auditors determine the information's reliability and accuracy and point out any potential red flags.

Auditors can plan meaningful audits by identifying risk factors, evaluating existing controls, documenting control gaps or process failures, and sharing their findings with key stakeholders. For example, a control may be designed to avoid lending to businesses that use unfair labor practices or to those that emit an unacceptable level of greenhouse gases. If any exception is found during control testing, that issue should be captured in the official audit findings. Auditors must use their professional judgment to assess ESG information and provide reasonable assurance that it is reliable and accurate and that clients have adequate controls to manage ESG-related risk.[3]

Complex Data Challenges

The volume and complexity of data that organizations produce and process have risen dramatically in recent years as organizations have become more complex and implemented increasingly sophisticated technologies. As a result, auditors now have to evaluate the correctness and completeness of vast and varied data sets, which has created new obstacles.

Auditors may find it difficult to process and analyze big data effectively if they lack the necessary technical skills, access to advanced analytical tools, and specialized computing storage and processing capabilities. If auditors do not have access to adequate bandwidth, it severely limits their ability to analyze data in a short time frame. Moreover, meaningful insights from big data cannot be obtained with the use of limited tools such as Excel.

Variations in data quality can add to the complexity of an audit, especially when structured and unstructured data are gathered from a variety of sources. The quality of big data may be variable, and the data may contain errors or inaccuracies, affecting the accuracy and reliability of audit results.

Moreover, big data may contain sensitive and confidential information (e.g., US Social Security numbers, protected health information [PHI], payment card information) that is not made available to auditors to prevent unauthorized access or

disclosure. For example, auditors are required to undergo specialized training and may be required to pass a US Health Insurance Portability and Accountability Act (HIPAA) assessment before gaining access to such sensitive and highly protected data as PHI.[4] HIPAA prohibits the disclosure of PHI outside US borders unless certain conditions are met. One of those conditions is that the entity receiving the PHI must be subject to privacy and security regulations similar to those in HIPAA.

Auditors must have a good understanding of the differences in data quality if they are to gather relevant, complete and accurate information. They must also have a solid understanding of privacy laws and regulations to ensure that they comply with them.

Auditors should consider taking deep dives to understand emerging technology, complete a risk assessment, collaborate with experts, and invest in continuous learning.

Emerging Technology Challenges

New technologies such as AI, robotic process automation (RPA),[5] the Internet of Things (IoT), blockchain and quantum computing can rapidly transform business operations, but they also pose new challenges for auditors. Emerging technologies may introduce new security and privacy risk factors such as hacking, data breaches and unauthorized access, which may change how transactions are recorded and tracked and make it more difficult to establish a clear audit trail. Emerging technologies require specialized technical expertise, which may be outside the scope of traditional auditing skills.

Blockchain Example

Blockchain is a digital ledger technology that enables the safe, open and decentralized recording of transactions.[6] Although it was initially created for cryptocurrency transactions, it is now used in a broad variety of fields and situations. Blockchain allows many parties to record and verify transactions without the need for a central authority or middleman.

Auditing blockchain transactions involves several challenges including:

- Blockchain transactions are pseudonymous, which means that users are recognized by their public keys rather than their actual identities. This makes it difficult to determine who is responsible for a certain transaction and whether that user has a history of fraud.
- Blockchains are decentralized, which means that there is no single entity in charge of regulating the transactions. Therefore, it is difficult to identify who is to blame for fraudulent transactions.
- Some blockchains are private, and only specific parties have access to their data. This can prevent auditors from gathering the data they need to complete a thorough audit.
- The method of substantive testing using samples may soon become obsolete, and auditors might be required to examine all blockchain transactions within the observation period.

When auditing blockchains, practitioners should follow these steps:

1. Understand the blockchain's purpose and scope before beginning the audit. This helps determine what types of data are being kept and any possible threats related to the blockchain.
2. Determine the essential elements that comprise the blockchain, such as the nodes, consensus algorithm and smart contracts.
3. Confirm the blockchain's integrity by checking the blocks on the chain to ensure that they are authentic and unaltered. This can be achieved by examining the blocks' cryptographic signatures.
4. Verify that the blockchain complies with all applicable regulations.[7]
5. Ensure that smart contracts, which are automated applications, work as intended and are secure.
6. Validate that access controls are designed and operating effectively, allowing access only to authorized personnel.

How Can Auditors Prepare?

Organizations are investing heavily in new and robust technology to make their operations more efficient and increase their return on investment (ROI). But are they investing enough resources to address the risk associated with emerging technologies?

LOOKING FOR MORE?

- Read *Blockchain Framework Audit Program. www.isaca.org/blockchain-framework-audit-program*
- Learn more about, discuss and collaborate on audit and assurance in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

To address the challenges they are faced with and continue to perform their duties effectively, auditors must attain the knowledge and technical expertise needed to work with new technologies and ensure that clients' internal controls and financial reporting methods are accurate, reliable and secure. To do so, auditors should consider taking deep dives to understand emerging technology, complete a risk assessment, collaborate with experts, and invest in continuous learning.

Auditors must work closely with IT professionals and other stakeholders to ensure that they have a comprehensive understanding of emerging technologies and their impact on financial reporting

Complete a Deep Dive to Understand the Technology

Diving deep into emerging technologies can be challenging because they are often complex and tend to evolve rapidly. But by diving deep into emerging technologies, auditors can better understand how they work and how they can be used. This understanding can aid the auditor in identifying potential vulnerabilities and weaknesses that may threaten business operations and assets. It is important to understand both external and internal technologies as they emerge:

- **Third-party (external) emerging technologies**—It is imperative for auditors to stay up to date and learn about new technologies being used by competitors. This can be accomplished through reading published articles and news reports, joining online communities and discussion groups, watching tutorial videos, and making connections with industry experts or specialists. Attending webinars and conferences is another way to gain knowledge about recent advances while exchanging ideas and experiences with others. User guides, technical manuals and design materials can also facilitate comprehension of the functionality and underlying architecture of new technologies.
- **In-house (internal) emerging technologies**—Auditors should examine the architecture, data flows, security measures and user interfaces of new technologies to see how they were designed and implemented; analyze their performance and functionality; and observe any areas that need improvement. It is also helpful to involve relevant parties such as developers, quality assurance professionals, business users and process owners throughout the auditing process. To ensure that all viewpoints are considered during the audit, feedback should be requested and incorporated.

Conduct a Risk Assessment

Conducting an effective risk assessment during the audit planning phase can identify significant risk factors and reduce the resources spent on insignificant threats. First, auditors should determine which assets are most vulnerable and evaluate the possibility that a threat will materialize. During a risk assessment, auditors should consider:

- **Absence of security testing**—If new technologies have not undergone thorough security testing, hackers may gain access to sensitive information or systems by taking advantage of their flaws.
- **Sensitive data**—Given the amount of personal data gathered by emerging technologies, questions about data privacy and possible exploitation may arise. Because of the complex and dynamic regulatory environment, it may be challenging to guarantee that emerging technologies comply with pertinent rules and regulations such as the EU General Data Protection Regulation (GDPR) or the US State of California Consumer Privacy Act (CCPA).[8] Emerging technologies' impact on employment, social inequality and human rights are only a few of the ethical issues that might come up.
- **Compatibility issues**—Emerging technologies might not be properly integrated with current systems and procedures, which could harm business operations and result in downtime.

Identifying potential risk factors, creating an efficient audit plan, allocating resources wisely and evaluating the efficiency of internal controls are all aided by learning about emerging technologies and performing effective risk assessments. This makes it possible for auditors to carry out thorough audits that

give key stakeholders reasonable assurance that existing controls are designed and operating effectively and are managing any significant risk related to emerging technologies.

Collaborate With Experts

Auditors must work closely with IT professionals and other stakeholders to ensure that they have a comprehensive understanding of emerging technologies and their impact on financial reporting. For example, cybersecurity specialists can offer insight into the security risk related to new technologies and can help evaluate the efficacy of policies intended to reduce such risk. They can also assist auditors in locating potential security weaknesses in programs and systems that cybercriminals could use to their advantage.

Similarly, experts in data analytics can help auditors analyze the enormous amounts of data produced by cutting-edge technologies and identify trends and abnormalities that might indicate threats or weak points. They can also assist in creating prediction models to find potential problems before they occur. Internal audit teams should collaborate with data analysts to gather, analyze and understand the significant amounts of data produced by the enterprise's systems and procedures. Data analysts can help find abnormalities, spot risk factors and pinpoint opportunities to improve controls. Using data analytics enables the internal audit team to detect patterns and trends that might not be readily apparent through conventional audit procedures, allowing auditors to provide more insightful and value-added recommendations to management. Data analytics can also help auditors test big data sets rapidly and effectively, minimizing the time and effort needed to complete an audit.

Experts in AI and machine learning (ML) can help auditors evaluate the efficacy of AI systems and algorithms utilized in emerging technologies. In addition, they can offer insight into the moral and societal ramifications of AI and ML systems and spot potential biases in algorithms.

Professionals with expertise in cloud computing can help evaluate the security and dependability of cloud-based systems employed in new technologies. They can also assist auditors in locating any risk factors linked to the transfer of data and systems to cloud-based settings.

Invest in Continuous Learning

Auditors can acquire the technical expertise required to audit emerging technologies, identify and evaluate risk, and assure stakeholders that an enterprise's technologies and systems are secure, reliable and compliant by investing in training offered by organizations such as ISACA®. Credentials often give auditors an advantage in the job market and can boost their earning potential.

Conclusion

As emerging technologies continue to transform the global business landscape, auditors will face new challenges in the effort to ensure the accuracy and reliability of financial information. The rapid pace of technological innovation means that auditors must keep abreast of new developments and adapt their audit approaches accordingly. Key challenges include understanding the risk associated with emerging technologies and ensuring that audit procedures are effective in detecting and preventing fraud in the digital age. Auditors must possess a deep understanding of an emerging technology and relevant accounting standards and regulations to perform effective audits.

Ultimately, auditors who can effectively navigate these new challenges will be best positioned to provide value to their clients and stakeholders and ensure the integrity of financial information in the digital age.

Endnotes

1 Parker, A.; "The Globalization of Accounting and Auditing Standards," Thomson Reuters, 26 July 2016, *https://www.thomsonreuters.com/en-us/posts/tax-and-accounting/globalization-accounting-auditing-standards-ifrs/*

2 Brightest, "The Top Seven Sustainability Reporting Standards in 2023," *https://www.brightest.io/sustainability-reporting-standards*

3 Santos, V.; "Thirteen Ways Internal Audit Can Play an Essential Role in ESG Reporting for Insurance Companies," PKF O'Connor Davies, 9 March 2022, *https://www.pkfod.com/insights/13-ways-internal-audit-can-play-an-essential-role-in-esg-reporting-for-insurance-companies/*

4 US Centers for Disease Control and Prevention, "Health Insurance Portability and Accountability Act of 1996 (HIPPA)," 27 June 2022, *https://www.cdc.gov/phlp/publications/topic/hipaa.html*

Auditors who can effectively navigate these new challenges will be best positioned to provide value to their clients and stakeholders and ensure the integrity of financial information in the digital age.

5 Nallasivam, A.; "Boosting RPA Security: Concerns, Solutions, and Best Practices," CiGen, 28 January 2022, *https://www.cigen.com.au/security-risks-robotic-process-automation-rpa-how-prevent-them*

6 Hayes, A.; "Blockchain Facts: What Is It, How It Works, and How It Can Be Used," Investopedia, 23 April 2023, *https://www.investopedia.com/terms/b/blockchain.asp*

7 Folk, E.; "How Emerging Technology Creates Issues for Compliance," Datafloq, 23 March 2020, *https://datafloq.com/read/how-emerging-technology-creates-issues-compliance/*

8 Menon, S.; "Solving Security and Privacy Concerns in Emerging Technology," ISACA® Now, 7 November 2022, *https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2022/solving-security-and-privacy-concerns-in-emerging-technology*