The Institute of Internal Auditors Malaysia

Editor's Letter

Dear IIA Malaysia Members,

Wishing you all A Happy New Year!

NEW ANNOUNCEMENT!

We are pleased to announce the release of the Global Internal Audit Standards! The new Standards reflect a significant amount of work. The International Internal Audit Standards Board ("IIASB") thanks the IPPF Oversight Council, IIA staff, and the countless internal audit professionals and stakeholders who contribute their time and feedback.

We invite you to join us and other members of the Standards Board for a webinar Get To Know The New Global Internal Audit Standards/ on 24 January 2024, where we will discuss the contents of the new Standards and highlight the many ways in which the new Standards elevate the profession.

In this publication, our Technical Writer emphasises on the importance of soft skills alongside technical proficiency within an audit team. Such is especially so in the context of joint venture or shareholders' audits (JVA/SHA) where diverse cultures, practices, and methodologies come into play. These dynamics underscore the significance of forward-looking perspective in applying innovative approaches to auditing in weaving a strong team tapestry and navigating unity amidst diversity.

The article "Global Perspective & Insights" assists IA for organisations with AI implementations, ensures risk management assurance, addresses moral and ethical concerns, and verifies the effectiveness of AI governance structures. Internal auditors are ideal for these roles as they possess a deep understanding of organisational objectives, the capability to assess AI effectiveness, the capacity to provide internal assurance on AI risk management and serve as trusted advisors offering insights for leveraging AI in process improvement or enhancing products and services.

The "Cybersecurity" article highlights that strengthening IA team resources requires prioritising cybersecurity staffing and development. In response to the evolving landscape, IT auditors are now combining technical proficiency with an understanding of business processes, often opting for training to bridge the gap and ensure a comprehensive approach to addressing cybersecurity challenges.

The "Training Tomorrow's Internal Auditor" article thoroughly covers The IIA's International Standards for the Professional Practice of Internal Auditing, emphasising the implementation and supplementary guidance, including Practice Guides, to strengthen requirements. Additionally, the course extensively explores integrating the COSO Enterprise Risk Management framework with strategy and performance, focusing on corporate strategies that reduce risk through internal controls and align with boards' strategy synchronisation with risk appetite and tolerance.

The frameworks highlight that IA should systematically and methodically approach AI, applying the same rigour used in evaluating risk management, control, and governance processes, making these articles valuable for IA navigating the dynamic AI and business landscapes.

Alyssa Hew
Head, Technical & Quality Assurance

ABOUT THIS

On 9 January 2024, the International Internal Audit Standards Board (IIASB) has released the latest Global Internal Audit Standards™ (GIAS). This culmination of a multiyear process involved extensive research, stakeholder input, and a public comment period. Virtual attendees will hear directly from IIASB representatives about the final Standards, their structure, content, and the impact on the internal audit function and practitioners, including Chief Audit Executives.

Learning Objectives

During this session, participants will: -

- Gain insights into the framework of the new IPPF and Global Internal Audit Standards.
- Acquire knowledge about the key differences between the 2017 Standards and the latest version.
- Familiarise themselves with the content of each section within the new Standards.
- Receive information on the impact that the new Standards will have on internal auditors and internal audit functions.

PRESENTER

Naohiro Mouri, CIA, is the Executive Vice President and Chief Auditor of AIG, with prior roles at MetLife Japan, JP Morgan, Shinsei Bank, Morgan Stanley Japan, and Deutsche Bank Japan. He served as Chairman of the IIA Global Board of Directors (2018-2019) and was the first President of the Asian Confederation of Institutes of Internal Auditors (2001-2006). Mouri, an active IIA member since 1995, received The IIA's Victor Z. Brink Award in 2021 and the 2016 Outstanding Contribution in the Field of Internal Audit Award from the Asia Confederation of the IIA. He has co-authored a book on internal auditing for financial institutions in Japanese and Mandarin.

Michael Peppers, CIA, QIAL, CRMA, CPA, is the Chief Audit Executive for The University of Texas System, managing a team of over 100 professionals across fourteen institutions with an annual budget exceeding $25 billion. With 35 years of experience, he has led internal audit functions in notable not-for-profit organisations in higher education and health care. Peppers serves as The Institute of Internal Auditors' representative on the COSO Board and recently chaired the IIA International Internal Audit Standards Board. He has held key leadership roles, including global chairman (2017-18) and chairman of the IIA North American Board (2012-13). Recognitions include induction into the IIA American Hall of Distinguished Audit Practitioners and receiving the Victor Z. Brink Award. Peppers holds bachelor's and master's degrees in accountancy from the University of South Florida for Distinguished Service. Peppers holds bachelor's and master's degrees in accountancy from the University of South Florida.

Reference

1. Get To Know The New Global Internal Audit Standards/

2. Global Internal Audit Standard

Navigating Unity in Diversity for Shareholders' Audit Success

TECHNICAL WRITER
BY JAVEN KHOO AI WEE, CIA, CISA, CFE, CC
CMIIA Membership No. 211787

I usually write about my experiences in auditing, notably in the execution of engagements. However, for a change, this article focuses on how an audit team should conduct itself. The success of internal auditors **goes beyond technical proficiency and hard skills. Soft skills, including having the right mindset and behaviours** play a crucial role in influencing the effectiveness of engagements.

This article delves into the common challenges encountered in a joint venture or shareholders' audit (JVA/SHA) and highlights how mindset and behaviours of the audit team, notably their professionalism, diversity, equity, and inclusion (DEI) can significantly influence the success of the engagement. For this purpose, I have referred to two (2) joint venture or shareholders' audits (JVA/SHA) to which I was assigned in 2023 - where I led one as the *Audit Lead* and contributed in the other in an *Auditor*. The objectives of the JVA/SHA are generally to provide reasonable assurance to stakeholders that the joint venture or shareholders' agreement is being executed in accordance with **agreed-upon terms** and **industry standards**, fostering **trust** and **transparency**.

The followings are some key learnings, encompassing **best practices** that can be **emulated**, and worst practices that can serve as **"pitfalls" to avoid** in future JVA/SHA.

THE CHALLENGES IN CONDUCT OF JVA/SHA

Kindly note that some details have been generalised, aggregated, or modified due to data sensitivity.

Let's begin by acknowledging the fact that a JVA/SHA team comprises of auditors from different companies or joint venture (JV) partners, thus posing complexities and challenges that are not typically present in an ordinary audit team. Auditors from different companies often bring **diverse working cultures, practices, and methodologies.**

- Failing to appreciate and respect diverse perspectives within the JVA/SHA team may result in a lack of collaboration, trust issues, and challenges in maintaining a positive and inclusive work environment.
  - Some team members prefer to work in isolation rather than actively collaborating with others from other companies. This lack of collaboration hinders the sharing of knowledge and expertise.
- Ineffective communication, whether due to language barriers, cultural differences, or inadequate interpersonal skills can hinder collaboration and teamwork within the JVA/SHA team. Cultural insensitivity and miscommunication such as the followings may lead to misunderstandings and breakdowns in professionalism.
  - Poor communication etiquette, including interrupting colleagues during meetings, dismissive body language, and failure to actively listen to different perspectives.
- Auditors may resist adopting new methodologies or ways of working, particularly if these changes deviate from their established practices, leading to variations in the quality and rigor of audit procedures.
  - Inconsistencies can affect the reliability of audit conclusions and compromise the overall quality of the audit.

In view of the above, harmonising these diverse approaches can be challenging, requiring efforts to establish a **common understanding and alignment**.

Navigating Unity in Diversity for Shareholders' Audit Success

In addition, a JVA/SHA often involves **satisfying expectations of multiple stakeholders from different companies**, and **conflicts of interest** may be encountered with potentially **divergent priorities.**

- JVA/SHA may involve multiple reporting requirements – e.g., audit findings' classification, audit opinion rating etc, thus reflecting the interests and perspectives of each participating company hence, can be intricate.
- Inability to address conflicts and disagreements in a constructive manner may lead to toxic work environment.
- The use of different audit tools, software, or repository systems amongst the diverse auditors may create compatibility and/or control access issues.

Henceforth, ensuring objectivity and independence in such situations requires **careful management and effective leadership by the Lead Auditor** of the JVA/SHA. Failing to foster a sense of team cohesion can lead to lack of collaboration and shared responsibility.

Below are some examples of areas of challenges at different audit phases of a JVA/SHA: -

Audit Planning	❖ Determination of audit scope and audit coverage period, resource allocation by respective partner, and scope assignment to auditors. ❖ Clarify of roles and responsibilities of auditors, scope leads, and lead auditor.
Audit Fieldwork	❖ Protocols for document requests, walkthrough sessions/interviews with auditee, including periodic progress updates internally within JVA/SHA team.
Audit Reporting	❖ Methodology in developing audit findings, classification and overall audit opinion.

THE MITIGATION STRATEGY

Addressing the abovementioned complexities require a combination of effective leadership, open communication, and a commitment to fostering a positive and professional team culture. By proactively managing mindset and behaviors, JVA/SHA team can enhance their ability to work cohesively and deliver high-quality audit outcomes.

Below are some mitigations which you could consider:-

- Encourage **collaborative leadership styles that promote inclusivity and shared decision-making**. This approach helps build consensus and a sense of shared responsibility.
- Ensure that leadership positions within the audit team are **representative of the various JV partners**. This can help build trust and credibility among auditors from different cultural backgrounds.
- Inculcate **cultural sensitivity and awareness** within the JVA/SHA team where auditors should understand and respect the cultural nuances of their colleagues from different JV partners.
- Establish **clear and well-defined roles and responsibilities for each auditor**, specifying the tasks they are accountable for during the audit.
- Establish **consistent and transparent communication channels** that allow auditors from different JV partners to share information, ask questions, and collaborate effectively.
- Conduct **regular team meetings or check-ins** to discuss progress, challenges, and updates. Use these meetings as an opportunity to reinforce individual accountability.

Navigating Unity in Diversity for Shareholders' Audit Success

- Establish **clear protocols for resolving conflicts** to ensure that auditors feel comfortable addressing and resolving issues constructively.
- Foster a **sense of unity and camaraderie** among auditors through team welcome luncheons, team gatherings, etc. as these activities can help break down cultural barriers and build stronger working relationships.
- Establish a **culture of continuous improvement** where auditors are encouraged to reflect on their work and identify areas for improvement.

KEY TAKEAWAYS

1. With businesses engaging in increasingly diverse and complex partnerships, innovative approaches to auditing are becoming a pre-requisite for success. One such differentiation lies in **cultivating the right mindset and behaviors within the JVA/SHA team.**

2. **Effective leadership, cultural sensitivity, transparent communication channels and conflict resolution protocols** are essential in improving the overall effectiveness of JVA/SHA team. Meanwhile, encouraging **collaborative leadership styles**, ensuring **representation from various JV partners** in leadership positions, and implementing clear roles and responsibilities may contribute to a positive, respectful and collaborative team culture.

   In the words of Maya Angelou, *"we all should know that diversity makes for a rich tapestry, and we must understand that all the threads of the tapestry are equal in value".* **Embracing diverse cultures** and **fostering inclusivity** are essential for weaving a strong and valuable team tapestry in JVA/SHA.

3. In navigating the complexities of JVA/SHA, the unwavering commitment to **professionalism** is of paramount importance. Regardless of the challenges encountered - be it diverse working cultures, communication hurdles, or resistance to change - maintaining a high standard of professional conduct is **non-negotiable**. Upholding integrity, adhering to established audit standards, and engaging in transparent communication are the cornerstones of a **credible audit process**.

GLOBAL PERSPECTIVES & INSIGHTS

PART I: UNDERSTANDING, ADOPTING AND ADAPTING TO AI

- **About the Expert**

Eric Wilson, CIA, CISA
Eric Wilson is the director of internal audit and CAE at Gulfport Energy. He previously led internal audit and consulting teams for various domestic and international companies in a wide range of industries, including energy, commercial real estate, and healthcare. He serves as a member of the Board of Advisors for the University of Oklahoma's Steed School of Accounting, has lectured on internal auditing at several universities, and holds active leadership positions with multiple local and nonprofit organisations. He currently serves on The Institute of Internal Auditors (IIA) Professional Knowledge Committee and North American Content Advisory Committee. He is a member of the Board of Governors of The IIA's Oklahoma Chapter.

- **INTRODUCTION**

A Growing Area

When ChatGPT was introduced in November 2022, it marked a significant advancement in artificial intelligence (AI). Many likened its impact to that of the internet, foreseeing its potential to reshape current business practices, regulations, and societal norms.

ChatGPT and its swiftly emerging counterparts exemplify generative AI. Large language models drive this type of AI, utilising neural networks modelled after the human brain, trained on vast amounts of diverse data to generate requested outputs. When prompted, it leverages its training and algorithms to create content—text, images, videos, sounds, speech, and code—that resembles human-generated output AI.

While ChatGPT garners considerable attention, it's just one instance of the myriad tools falling under the AI umbrella.

AI permeates every smart device we use and fuels more sophisticated applications transforming various industries, including business, government, and healthcare. AI replicates human analysis and decision-making in diverse fields.

The global composite AI market is anticipated to surge from $900 million in 2023 to $4.4 billion by 2028, with a compound annual growth rate of 36.5%. Business leaders, with 94% consensus, view AI as crucial to their organisations' success over the next five years, according to Deloitte's "State of AI in the Enterprise."

An article in Internal Auditor magazine suggests that AI could become the most disruptive technological development to date, presenting both opportunities and risks across all facets of business and life. Drawing on their expertise in assessing risks and opportunities, internal auditors are positioned to evaluate, understand, and communicate the impact of AI on an organisation's ability to create value, as highlighted in "Artificial Intelligence—Considerations for the Profession of Internal Auditing" from The Institute of Internal Auditors (IIA).

Given the widespread and rapid adoption of AI, it is imperative for internal auditors to swiftly gain a comprehensive understanding of its workings, practical applications, and the associated risks and opportunities it introduces to organisations. This brief will delve into these areas, offering best practices and insights to help internal auditors stay abreast of AI developments.

GLOBAL PERSPECTIVES & INSIGHTS

UNDERSTANDING AI

Machine Learning and Simulated Human Intelligence

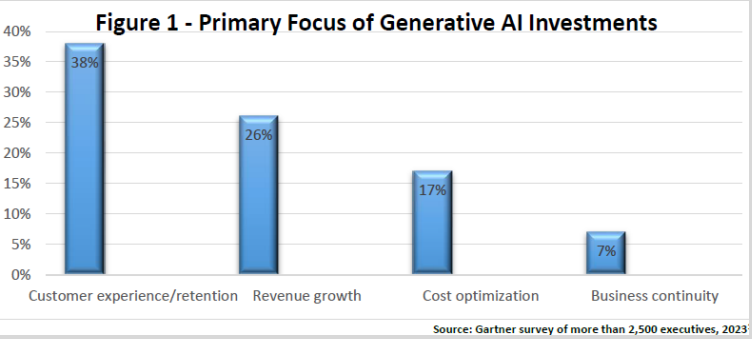
The terms AI and automation are frequently used interchangeably, indicating a limited grasp of AI's more potent and transformative capabilities. While AI can certainly automate routine tasks, its scope extends far beyond mere automation. Robotic process automation (RPA), a fundamental form of automation, relies on structured data and logic to execute repetitive, rule-based processes like accounting workflows and data collection. In contrast, more advanced AI tools can emulate human intelligence, understanding natural human communication, engaging in problem-solving, and enhancing overall performance and operational efficiency. Unlike automation, which follows predefined rules, AI leverages its training to make independent decisions.

AI and machine learning solutions fall into distinct categories:

- Descriptive: What happened?
- Diagnostic: Why did it happen?
- Predictive: What could happen next?
- Prescriptive: What should be done next?

However, current AI capabilities lack the judgment and contextual understanding that enable humans to make optimal decisions. Although technological advancements may enhance these abilities in the future.

Furthermore, the effectiveness of AI is contingent on its training. Researchers from MIT and other institutions studying cases involving rule violations found that if machine-learning models are not trained on appropriate data, they "are likely to make different, harsher judgments than humans would." The ensuing section will address the risks associated with AI's limitations.



Putting AI to Work

AI finds practical applications in various everyday tools that have been in use for years. Examples include online search engines, chatbots offering information and answering queries, voice assistants like Alexa and Siri performing tasks, navigation tools such as Google Maps for optimal travel routes, self-driving cars, customised online shopping experiences, and personalised advertising.

In business and government, AI is employed in diverse use cases, including:

- Addressing skill shortages by automating tasks.
- Enhancing IT or network performance.
- Crafting strategies to retain or appeal to specific customers, improving customer experience. An example is Brinks Home, which used AI to gain brand recognition in a competitive market.
- Identifying and preventing fraud or errors in financial information.
- Forecasting product or service demand based on customer history/feedback and market and economic activity.
- Contributing to sustainability objectives, with AI potentially supporting 79% of the UN General Assembly's Sustainable Development Goals.
- Prioritising customer opportunities or leads.
- Tracking responses to sales campaigns, market research, and search engine optimisation (SEO).
- Streamlining and enhancing customer support activities.

Currently, business investments in generative AI primarily focus on improving customer relations and increasing revenue. According to a recent Gartner survey, most organisations have yet to make significant commitments to efforts that leverage generative AI for new business opportunities or entering new markets.

GLOBAL PERSPECTIVES & INSIGHTS

Opportunities, Challenges, and Risks

In formulating and executing an AI strategy, companies must grasp not only the potential advantages but also comprehend the limitations and risks associated with this technology. As businesses rush to adopt AI solutions, opportunities include:

- Reducing the data processing cycle duration.
- Mitigating potential errors by substituting human actions with flawlessly repeatable machine actions.
- Employing process automation to decrease labor time and costs.
- Utilising robots or drones for tasks that may pose potential hazards.
- Making more precise predictions, ranging from potential sales in specific markets to forecasting epidemics and natural disasters.
- Leveraging AI initiatives and efficiencies to propel revenue and market share growth.

Despite these benefits, there are challenges in harnessing AI. According to the IBM Global AI Adoption Index, nearly one in five companies faced difficulties in:

- Ensuring data security.
- Data governance.
- Managing diverse data sources and formats
- Integrating data across any cloud

However, organisations may not fully grasp how to optimise the opportunities presented by AI. Simultaneously, a lack of comprehensive understanding regarding the functioning of AI systems, as well as the potential biases and errors ingrained in their training and output, could unknowingly expose companies to various threats. Risks with the potential for reputational or financial damage include:

- Lack of transparency: Undetected biases or errors within AI technology can result in improper decisions, leading to issues like discriminatory practices in hiring or credit provision.

- Ensuring the security and confidentiality of information is crucial, with The IIA's "Artificial Intelligence- Considerations for the Profession of Internal Auditing" underscoring the potentially devastating impact of a cybersecurity breach involving AI. The IIA advises that organisations lacking adequate cybersecurity should swiftly reinforce it, with continuous communication from Chief Audit Executives (CAEs) to stakeholders emphasising the need for rapid enhancement. As organisations amass increasing volumes of data, they become susceptible to threats such as breaches, privacy violations, data loss, or system failures, arising from internal errors or the actions of hackers and cybercriminals. Cybercriminal tactics, including "model poisoning," intentionally polluting machine learning model training data, can lead to system corruption, inaccurate data, denial of service, or malware attacks capable of crippling organisations.

- Legal challenges, including the potential for plagiarism, copyright infringement, and intellectual property violations due to non-original AI-generated content, pose significant risks. Insufficient testing and oversight of AI may further give rise to ethical concerns.

- Vendor or supplier dependency becomes a notable threat as AI assumes a crucial role in organisational systems, necessitating careful consideration of risk-assessment indicators for third-party tool integration.

- Organisations may confront tough decisions related to employment losses if AI replaces workers without suitable reassignments, potentially leading to economic and social disruption in affected areas or industries.

GLOBAL PERSPECTIVES & INSIGHTS

- Regulatory risks emerge as governments seek to understand and regulate AI use, requiring organisations to adapt their strategies to an evolving regulatory landscape. Legal challenges may arise if AI systems cause financial losses or violate human rights.

- Environmental considerations, such as the substantial electricity consumption of AI systems, present challenges to organisations' sustainability efforts and hinder the achievement of environmental, social, and governance (ESG) goals.

- Investment decision-making and results may be compromised by insufficient investment in AI initiatives or resistance from stakeholders, placing organisations at a competitive disadvantage without a robust AI strategy. Achieving a satisfactory return on investment in AI infrastructure, research and development, and talent acquisition becomes challenging without strategic planning.

Initial step in regulating AI

The swift ascent and associated risks of AI have spurred demands for increased regulation. The European Parliament has endorsed the Artificial Intelligence Act, advocating for enhanced transparency and safeguards. This legislation categorises AI risk into three levels: banning applications and systems deemed unacceptable, imposing legal requirements on high-risk applications, and applying minimal transparency regulation to those of limited risk, including generative AI. Fines can reach up to $33 million or 6% of a company's annual global revenues. In the U.S., the White House has proposed an AI Bill of Rights for secure and efficient systems. China has also outlined regulations to establish potential boundaries for generative AI. Sam Altman, CEO of OpenAI, the developer of ChatGPT, has called for coordinated international regulation of generative AI and joined a statement on AI risk alongside numerous AI experts and public figures.

THE ROLE OF INTERNAL AUDIT
Assessing Risk and Providing Foresight

Trusted Techniques and Proven Skills Support AI Risk Management

Internal audit plays a crucial role in helping organisations evaluate and communicate the impact of AI on value creation and goal achievement. Internal audit leaders should incorporate AI considerations into risk assessments and integrate it into a risk-based audit plan. Active involvement in AI projects allows internal auditors to function as trusted advisors, providing guidance on implementation, assuming proficiency in relevant areas. However, to maintain independence, internal auditors should refrain from taking ownership or responsibility for AI implementation.

For organisations that have already implemented AI, internal audit can:

- Provide assurance on risk management related to the reliability of underlying algorithms and data.
- Ensure that moral and ethical issues related to AI are addressed.
- Offer assurance on the effectiveness of AI governance structures.

Internal auditors are well-suited for these roles due to their:

- Understanding of organisational strategic objectives
- Ability to assess AI activities' effectiveness.
- Capacity to provide internal assurance on AI risk management,
- Position as trusted advisors offering insights on leveraging AI for process improvement or enhancing products and services.

GLOBAL PERSPECTIVES & INSIGHTS

AI Frameworks and Standards

In 2017, The Institute of Internal Auditors published one of the first frameworks for auditing artificial intelligence. Other relevant guidelines on AI include: An AI Risk Management Framework from the U.S. National Institute of Standards and Technology (NIST), which includes related research and standards. The Trustworthy & Responsible Artificial Intelligence Resource Centre, part of NIST, is a repository for current U.S. federal guidance on AI. The U.K. Information Commissioner's Office provides guidance and resources on AI. The Organisation for Economic Co-operation and Development provides a framework, as well as information on principles and policies.

Best Practices for Putting AI to Work

Despite the perceived challenges of AI, internal auditors are encouraged to wholeheartedly embrace it. Eric Wilson, CIA, CISA, Director of Internal Audit and CAE at Gulfport Energy Corporation, advises against avoiding advanced technologies like AI and emphasises the need for auditors to develop expertise in tools already in use or soon to be adopted by their organisations. Wilson suggests that auditors should take a hands-on approach, experimenting with generative AI like ChatGPT or Bard to understand its functionality. With generative AI systems, it's even possible to interact with the model and ask for explanations of the logic behind its answers. Additionally, for systems that may not be as easily approachable, Wilson recommends shadowing individuals within the organisation who are using them to gain practical insights into their applications. Auditors should seek to understand how these systems contribute to various functions and inquire whether users can articulate their impact on the organisation. Identifying gaps in understanding or expertise can present opportunities for internal audit to enhance utilisation and provide valuable insights to the organisation.

CONCLUSION

The Internal Auditor magazine article states that this is a thrilling moment for internal audit to take on a leadership role in providing assurance for AI. While the initial excitement is predicted to diminish as organisations grapple with the real challenges of understanding and implementing AI, its influence will grow as individuals and businesses discover more innovative applications. It is now imperative for internal auditors to comprehend the opportunities and risks associated with AI initiatives, enabling them to deliver valuable assurance and insights for their organisations.

GLOBAL PERSPECTIVES & INSIGHTS

PART II: Revisiting The IIA's Artificial Intelligence Framework

About the Expert

Eric Wilson, CIA, CISA

Eric Wilson is the director of internal audit and CAE at Gulfport Energy. He previously led internal audit and consulting teams for various domestic and international companies in a wide range of industries, including energy, commercial real estate, and healthcare. He serves as a member of the Board of Advisors for the University of Oklahoma's Steed School of Accounting, has lectured on internal auditing at several universities, and holds active leadership positions with multiple local and nonprofit organisations. He currently serves on The Institute of Internal Auditors (IIA) Professional Knowledge Committee and North American Content Advisory Committee. He is a member of the Board of Governors of The IIA's Oklahoma Chapter.

INTRODUCTION

In 2017, the Institute of Internal Auditors (IIA) released a significant examination on the increasingly relevant topic of "Artificial Intelligence – Considerations for the Profession of Internal Auditing." This comprehensive three-part work outlined the internal auditor's responsibilities in the realm of artificial intelligence (AI), presented a framework addressing AI-related issues within internal audit, and explored practical applications of this complex technology.

Despite the substantial progress in AI over the subsequent six years, the established framework remains largely pertinent and valuable across various internal audit domains. This summary initiates by revisiting key components of the framework and their sustained relevance. Additionally, it delves into other pertinent considerations and concludes by assessing the evolving role of internal auditors in the context of AI.

KEY COMPONENTS

Framework Addresses Critical Factors

Building Strategies on Capabilities, Risk, Opportunities

The framework encompasses six components integrated into the organisation's strategy. It emphasises the need for a tailored AI strategy based on the organisation's existing capabilities, risk management approach, and the pursuit of opportunities. Internal audit's evaluation of an organisation's AI strategy should involve considerations such as:

- Does the organisation have a clearly defined AI strategy?
- Is there investment in AI research and development?
- Are there plans to identify and address both threats and opportunities related to AI?

The framework underscores that AI can confer a competitive advantage, emphasising the role of internal audit in guiding management and the board to recognise the importance of crafting a thoughtful AI strategy aligned with organisational objectives. These insights remain relevant today. Strategic planning for AI is distinctive due to its rapid evolution and broad potential impact.

Internal auditors are urged to ensure a comprehensive understanding of the magnitude of AI systems, given their significant differences from traditional systems. Eric Wilson, Director of Internal Audit and CAE for Gulfport Energy, highlights the challenge in grasping the workings of AI systems, noting that both end users and auditors may struggle to comprehend their operations.

GLOBAL PERSPECTIVES & INSIGHTS

A key divergence in AI lies in "meaning making," a concept applicable to advanced technologies. Understanding what machines can and cannot do is crucial in the AI era. While machines may excel in certain diagnostic tasks, the interpretation and management of implications require human intervention, emphasising the distinction between knowledge and meaning.

In the realm of AI, technology has progressed beyond mere data gathering and sorting to the capability of contextualising information. This advancement introduces new abilities, risks, and opportunities for organisations. Wilson advises internal auditors to engage in ongoing conversations, both internally and with peers, to effectively audit AI strategy and monitor its efficacy.

1. **AI Governance**

This element encompasses the structures, processes, and procedures utilised to guide, manage, and oversee the organisation's AI activities aimed at achieving its objectives. Once again, the appropriate level of formality and structure for AI governance will vary based on the unique circumstances and characteristics of each company. The framework emphasises that AI governance, in every instance, addresses accountability and oversight, ensuring that those responsible for AI possess the requisite skills and expertise to monitor its use, and that AI activities align with the organisation's values. Given the evolving impact of AI, it is crucial that related actions and decisions adhere to the organisation's ethical, social, and legal responsibilities.

While data governance is always crucial, the approach differs when dealing with AI. For instance, generative AI systems, being trained on specific information, are more susceptible to introducing errors and bias early in their development if not trained on reliable data. In contrast to traditional systems, which may consistently interpret a specific shade of red as blue if trained as such, AI systems might generalise any shade of red as blue.

Once a minor bias or inaccuracy is introduced into the technology, the system continues to be trained on that error, potentially magnifying its impact exponentially. Therefore, it is imperative to detect and rectify bias at the outset before the technology is applied in decision-making, customer-facing communication, or any other context that could harm the organisation's financial standing or reputation. As Eric Wilson noted, "One incorrect data point could fundamentally alter how the system perceives and contextualises the data it is processing.

AUDIT FOCUS

Key IIA Standards

The IIA's *International Standards for the Professional Practice of Internal Auditing* include several standards that are particularly relevant to AI, including:

- IIA Standard 1100: Independence and Objectivity
- IIA Standard 1210: Proficiency
- IIA Standard 2010: Planning
- IIA Standard 2030: Resource Management
- IIA Standard 2100: Nature of Work
- IIA Standard 2110: Governance
- IIA Standard 2120: Risk Management
- IIA Standard 2130: Control
- IIA Standard 2200: Engagement Planning
- IIA Standard 2201: Planning Considerations
- IIA Standard 2210: Engagement Objectives
- IIA Standard 2220: Engagement Scope
- IIA Standard 2230: Engagement Resource Allocation
- IIA Standard 2240: Engagement Work Program
- IIA Standard 2310: Identifying Information
- IIA Standard 2400: Communicating Results
- IIA Standard 2410: Criteria for Communicating
- IIA Standard 2420: Quality of Communications
- IIA Standard 2440: Disseminating Results

Complete text of the *Standards* is available at theiia.org. Each standard is complemented by a related Implementation Guide.

GLOBAL PERSPECTIVES & INSIGHTS

2. Data Architecture and Infrastructure

The framework establishes that the architecture and infrastructure for AI data are likely to resemble those used for big data. Areas falling under these considerations include data access, information privacy, and security throughout the data lifecycle—from collection and use to storage and destruction. Additional factors to ponder encompass data ownership and utilisation across the data lifecycle.

In the realm of AI, cybersecurity emerges as a paramount concern for chief audit executives and their teams. With the expanding use of AI and the growing volume and complexity of data, it is crucial to recognise that the effectiveness of AI and generative AI is contingent upon the quality of the information they are provided or trained on. Eric Wilson emphasises the necessity for organisations to ensure the accuracy of information at the data point level fed into AI systems, emphasising that sound data architecture forms the basis for how these systems interpret the operational environment.

Controls for AI systems also present unique challenges. Wilson shares his experience in developing a system that integrated data science, robotic process automation (RPA), and AI for intelligent automation. While controls were initially developed separately for each component, the realisation that the AI system aimed to enhance its own performance over time necessitated globalised controls for the entire system. These controls play a crucial role in governing interactions among system components and establishing limits on the AI system's ability to modify data science or RPA algorithms and processes. Wilson underscores the importance of a holistic understanding of the system's functioning, which involves addressing new challenges and integrating with IT general controls.

Efficiency boundaries are another aspect Wilson emphasises in his audit role, questioning the extent to which AI systems are allowed to become efficient. He highlights the need to strike a balance between efficiency and the imperative to comprehend the system's operations, recognising that limiting efficiency in technology is a novel concept that may require trial and error in reshaping perspectives on AI.

3. Data Quality

Considering this, it becomes evident, as outlined in The IIA's framework, that the dependability of the data upon which AI algorithms rely is of utmost importance. Regrettably, a survey conducted last year by the open-source data quality tool Great Expectations revealed that 77% of data professionals believed their organisations grappled with data quality issues, with 91% asserting that these issues had a detrimental impact on company performance. Merely 11% claimed to have no data quality concerns. The survey defined six dimensions of data quality:

- Accuracy.
- Completeness.
- Uniqueness.
- Consistency.
- Timeliness.
- Validity.

Challenges to data quality may arise due to inadequate communication between systems or reliance on intricate add-ons and customisations. The framework underscores the critical nature of how data is brought together, synthesised, and validated.

GLOBAL PERSPECTIVES & INSIGHTS

4. Measuring Performance of AI

To gauge the effectiveness of AI systems and assess their contributions, the framework suggests that organisations, as they integrate AI into their operations, should define suitable performance metrics. These metrics should establish a clear connection between AI activities and business objectives, providing transparent insights into whether AI is facilitating the achievement of goals. Simultaneously, the framework underscores the importance of proactive management oversight in actively monitoring the performance of AI activities.

5. The Human Factor

Within the automation paradox, the more efficient an automated system becomes, the greater the need for human involvement in the process. Human engagement is essential, particularly in identifying and rectifying errors made by other humans. Notably, 88% of data breach incidents stem from human error. Human errors and biases, whether intentional or unintentional, significantly influence the performance of both algorithms and the training that propels AI systems.

The framework emphasises addressing the human factor by:

- Monitoring and managing the risk associated with human error or bias in the system.
- Conducting tests to ensure that AI outcomes align with the initial objectives.
- Guaranteeing adequate transparency in AI technologies due to their inherent complexity.
- Verifying that AI output is employed legally, ethically, and responsibly.

GLOBAL PERSPECTIVES & INSIGHTS

6. The Black Box Factor

The term "black box" commonly refers to a complex electronic device whose internal mechanisms are not visible or comprehensible to the user. In anticipation of advanced systems like generative AI, the framework highlights that, as organisations adopt new AI technologies involving machines or platforms capable of independent learning or communication, the inner workings of the algorithms become increasingly opaque and challenging to understand. The black box aspect poses a growing challenge as an organisation's AI activities evolve and become more sophisticated. The advancements in AI since the initial publication of the framework undoubtedly affirm and emphasise this point, along with all the insights regarding the six key components.

Technology Remains Top Risk

When asked what issues were a high/very high risk to their organizations, internal audit leaders who responded to the 2023 North American Pulse of Internal Audit survey gave the top three spots to technology-related risks. Pulse survey respondents' choices were largely consistent across privately held and publicly traded companies, financial and public sectors, as well as not-for-profit organizations. Technology risk will likely remain top of mind as AI tools and systems become more complicated and multifaceted.

Note: The IIA's North American Pulse of Internal Audit Survey, Oct. 20 to Dec. 2, 2022. Q26: How would you describe the level of risk in your organization in the following risk areas? *n* = 562.

GLOBAL PERSPECTIVES & INSIGHTS

ETHICAL CONSIDERATIONS
Ensuring AI Systems Remain True

- **Internal Audit Must Remain Vigilant.**

The framework establishes that internal audit should ensure the organisation is addressing the moral and ethical issues related to its AI use. Some might question how ethics considerations figure into a computer system, but AI and generative AI go well beyond the technology systems of the past in their reach and potential impact. Indeed, the reliance on these systems may become so great that an organisation's entire operations are built on answers that they provide. Without appropriate training and monitoring, output may reflect the most expedient answer, but not necessarily one that is acceptable for any number of reasons. Internal auditors will have to ask what has been done to ensure AI systems continue to follow proper ethical, legal, and regulatory guidelines, Wilson said.

INTERNAL AUDIT'S ROLE
Driving AI's Value

- **Picking Up the Assurance Challenge.**

These emerging technologies prompt concerns about their potential impact on human employment. While AI is not poised to replace internal auditors, Eric Wilson suggests that it may replace those who fail to leverage AI and harness its value. To address this, he encourages auditors to familiarise themselves with both existing and emerging AI technologies. Although AI has been a part of many organisations' risk profiles, lack of understanding or available expertise has delayed action. Wilson advocates for internal auditors to proactively engage with AI, advising them to embrace it as part of the organisational culture.

Internal auditors, drawing on their expertise in assessing risks and opportunities, play a crucial role in the context of AI, according to the framework, which outlines key activities for internal auditors:

- In any organisation, internal audit should integrate AI into its risk assessment and consider its inclusion in the risk-based audit plan. Various risks associated with AI, such as data breaches, plagiarism, and model data poisoning, should be carefully examined.
- For organisations exploring AI, internal audit should be involved from the project's inception, providing guidance and insights for successful implementation. However, to maintain independence and objectivity, internal audit should not own or be responsible for implementing AI processes, policies, or procedures.
- In companies with partial AI implementation, either within operations or in a product or service, internal audit should offer assurance on how risks related to the reliability of underlying algorithms and data management are addressed.
- Internal audit should ensure that measures are in place to address moral and ethical considerations in the organisation's use of AI.
- Internal audit can also provide assurance on the proper governance structures related to AI utilisation.

CONCLUSION

In summarising the role of internal audit, the framework emphasises that AI should be approached with the same systematic and disciplined methods employed for evaluating and enhancing the effectiveness of risk management, control, and governance processes. Eric Wilson notes that the 2017 framework was ahead of its time and remains a valuable resource for internal auditors navigating the dynamic and ever-evolving AI landscape.

GLOBAL PERSPECTIVES & INSIGHTS

PART III: INTERNAL AUDIT'S ROLE IN AI ETHICS

About the Expert

Andrew Clark, Ph.D., CAP, GSTAT
Andrew is co-founder and chief technology officer at Monitaur. A trusted domain expert on the topic of ML auditing and assurance, he built and deployed ML auditing solutions at Capital One. He has contributed to ML auditing standards at organisations including ISACA and ICO in the UK. Before Monitaur, Andrew also served as an economist and modeling advisor for several very prominent crypto-economic projects while at Block Science.

Jim Enstrom, CIA, CRISC, CISA
Jim is senior vice president and chief audit executive, internal audit, at Cboe Global Markets, Inc. An accomplished business leader, he has extensive audit, compliance and risk management experience in areas such as financial reporting, business operations, and information technology. Prior to joining Cboe in 2009, Jim spent 13 years in public accounting, having worked at Arthur Andersen and Deloitte.

Tim Lipscomb
Tim is senior vice president, chief technology officer for Cboe Global Markets, Inc. He oversees software engineering and quality assurance for Cboe equities, options, and futures markets, as well as its Data and Access Solutions business. Previously, Tim was chief operating officer of Cboe Europe, where he oversaw the company's software engineering, infrastructure, and operational teams.

Ellen Taylor-Lubrano, Ph.D.
Ellen is machine learning team lead in the regulatory division of Cboe Global Markets, Inc. She joined Cboe in 2020 as the founder of the regulatory division's ML program, which applies ML/AI in the surveillance of financial markets. Prior to that, Ellen worked in fundamental scientific research and production software development.

INTRODUCTION

Amid rapid advancements in artificial intelligence (AI), concerns about ethics and related matters have led some to propose a temporary halt or slowdown in further development. However, despite these calls for a pause, numerous organisations are actively increasing their use of AI or planning to do so. As organisations grapple with AI choices and their implications, internal auditors are poised to play a crucial assurance and advisory role. Previous briefs in this series have focused on enhancing internal auditors' understanding of AI, revisiting The Institute of Internal Auditors' (IIA) landmark publication, "Artificial Intelligence – Considerations for the Profession of Internal Auditing," published in 2017. While from 2017, this framework remains generally relevant and useful in most internal audit areas. The framework emphasises that internal audit can assist organisations in evaluating, understanding, and communicating the impact of artificial intelligence on their ability to create value over the short, medium, or long term. This third and final brief in the AI series delves into the ethical issues surrounding this multifaceted technology and explores their implications for organisations and internal auditors. The brief also offers recommendations and insights from professionals actively engaged in the frontline of AI implementation.

GLOBAL PERSPECTIVES & INSIGHTS

Risks and Opportunities

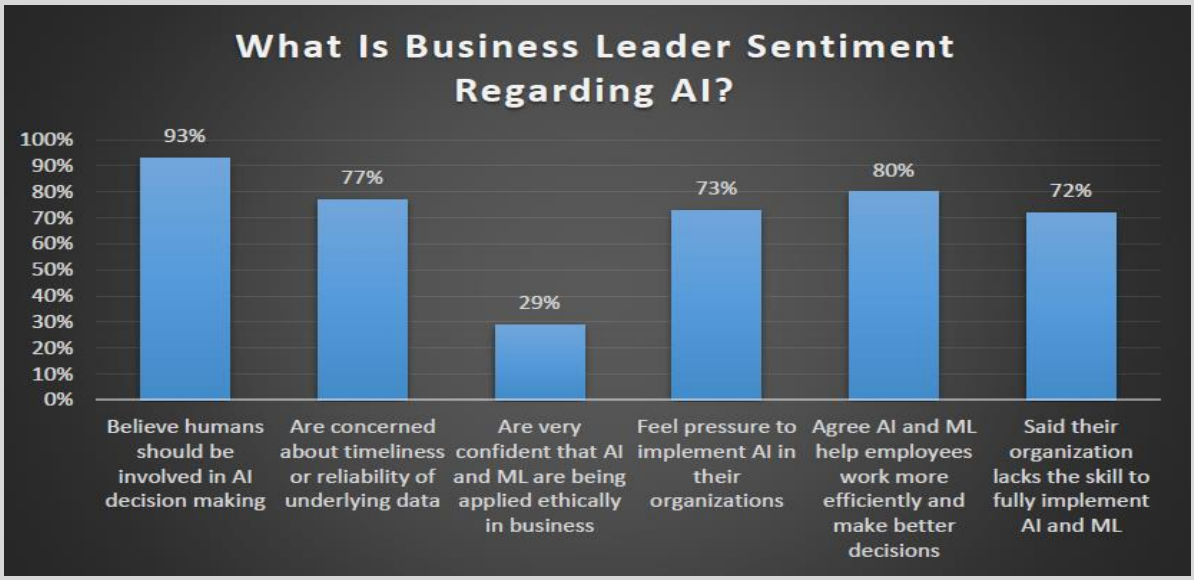
Internal Audit's Role as Adviser

- **Excitement Over AI Could Overshadow Ethical Considerations**

The global artificial intelligence (AI) market reached a valuation of $136.55 billion last year, with an anticipated compound annual growth rate of 37% from 2023 to 2030, as per Grand View Research, Inc. This heightened interest in AI, particularly in technologies like generative AI, has prompted software developers and organisations to rapidly advance their AI research and initiatives. However, the rapid progress also raises concerns about potential risks, including ethical and performance issues, that may be overlooked. Internal auditors are in a prime position to bring attention to these issues, providing valuable insights on the effectiveness of current controls and advocating for enhanced controls or guardrails. Notably, the Partnership on AI, led by Google executives, has emphasised the pivotal role of internal audit in assuring the processes involved in AI creation and deployment, ensuring they align with ethical expectations and standards.

Recognising and addressing the risks and limitations of AI is essential for both organisations and internal auditors. Despite the current emphasis on generative AI, its intelligence is contingent on the quality of training data, which, in its early stages, may include unverified content. Public use of generative AI introduces the risk of exposing private data to cyber threats, while biases, knowledge gaps, and inaccuracies are concerns. Additionally, the lack of transparency in AI models raises legal and intellectual property risks.

The user-friendly nature of generative AI allows individuals with limited expertise to leverage its capabilities, posing organisational risks. External threats, such as the malicious use of AI models, necessitate ongoing vigilance. However, refraining from embracing AI also entails risks, including falling behind in technological advancements and missing out on benefits such as streamlined processes and efficient identification of opportunities or threats. Tim Lipscomb underscores the role of AI in providing rapid access to extensive internal knowledge for informed decision-making.



GLOBAL PERSPECTIVES & INSIGHTS

Turn to Fundamental Auditing Concepts

Adapting Three Lines and Other Existing Models

- **Using Fundamental Assurance Approaches for New Technology**

Even though AI is a new technology, the principles of putting it to use often have familiar aspects. Decision models and machine learning, which are integral to AI, have been employed in the financial sector for a long time.

Jim Enstrom emphasises the need for internal auditors to be actively involved in understanding the strategic use of AI within the organisation. Applying traditional concepts from software development processes is crucial for effective AI auditing. Traceability and auditability become essential considerations, requiring collaboration with engineers, data scientists, and programmers to comprehend the AI systems' operations and decision-making processes.

Enstrom suggests leveraging existing tools, methodologies, and approaches while embracing new ideas, considering agile and iterative approaches. Addressing ethical issues becomes paramount, offering an opportunity to enhance ethical considerations in AI applications, according to Taylor-Lubrano. Existing review criteria can be applied to AI systems, treating AI as a vendor when used alongside human reviews.

Lipscomb highlights the importance of following appropriate vendor onboarding processes and control structures, emphasising the need for a third-line review of the process.

The Three Lines Model

The IIA's Three Lines Model focuses on effective risk management, starting with management as the first line and delineating roles for each line, including the board. This framework, integrated into AI risk considerations, helps organisations navigate opportunities and risks. Internal audit, as the third line, reports to the audit committee and provides perspectives to the board, particularly on ethical concerns from AI changes.

The Three Lines Model aids in recognising the need for each line to assess and monitor risks within its domain. For autonomous AI usage without robust human review, the first line (management) may need to enhance quality assurance procedures. Internal audit, as the third line, plays a vital role in aligning with the second line (chief risk or compliance officers) and inquiring about AI rollout, prioritisation, and future management.

Enstrom emphasises internal audit's opportunity to add value by positioning itself as a key element in the AI governance framework, leveraging knowledge and experience around controls, remaining crucial in the evolving landscape.

Minding Model Risk Management

Model risk management aims to address the risks associated with incorrect or improper use of models in decision-making. The objective is to identify, measure, and mitigate the use of inaccurate data, assumptions, methodologies, processes, or interpretations. Established paradigms in the banking sector, particularly for credit, finance, and marketing activities, provide guidance for model risk management. Organisations can benefit from existing recommendations, such as those outlined in the "OCC 2011-12 Supervisory Guidance on Model Risk Management", to build robust model governance, including oversight, policies, internal controls, audit, model inventory, and documentation. Implementing effective model risk management contributes to building trust and accountability, expediting the adoption of AI and machine learning.

GLOBAL PERSPECTIVES & INSIGHTS

Using AI Within Internal Audit

Adapting Improving Effective Assurance with New Technology

Understanding AI Privacy and Accountability Considerations

Internal auditors must not only grasp the implications of AI for their organisations but also determine the optimal utilisation of generative AI and other tools in their audits, considering privacy risks. For instance, when working with generative AI like ChatGPT, it is crucial to anonymise the entered data and prevent the sharing or storage of sensitive information on the platform. Obtaining appropriate consent and authorisation for using data in ChatGPT is also emphasised. An Internal Auditor article outlines how internal auditors can incorporate AI in planning, testing, reporting, and monitoring. It stresses the significance of harnessing the capabilities of tools like ChatGPT while safeguarding the confidentiality and privacy of sensitive data.

Key Questions to Consider

Clark suggests that organisations develop a strategic understanding of AI's implications for them. Internal audit can advise on key issues, including:

- Identification of AI applications and usage areas.
- Purpose and modelling objectives.
- Exploring alternative solutions beyond machine learning.
- Evaluation of associated risks.
- Automation of decision-making processes with models.
- Implementation of adequate monitoring and risk management controls for AI.
- Presence of a second-line function for model risk management.
- Impact of AI on the audit scope and process.

Furthermore, organisations must address ethical concerns when algorithms influence consequential decisions about individuals. In such cases, they should inquire about:

- Existing protections or legal frameworks and ensuring compliance.
- In the absence of external compliance considerations, steps to align processes with the organisation's values.

Internal audit should handle these considerations diligently, treating them with the same rigor as external mandates, ensuring processes for monitoring, validating compliance, and reporting on related concerns.

CONCLUSION

Due to significant ethical concerns associated with AI, Clark suggests that organisations lacking confidence in system outcomes should approach AI cautiously. Instead, he recommends treating AI as an initial research and development (R&D) project. This approach allows companies to explore how the technology aligns with their needs and identify potential risks.

While digital transformation is captivating, internal auditors should maintain a realistic perspective on the risks and limitations of any technology. Their focus should be on providing pertinent advice and assurance. Amid the excitement surrounding new technology, Clark emphasises the importance of questioning its actual impact on solving business problems and addressing potential data privacy issues and other risks.

GLOBAL PERSPECTIVES & INSIGHTS

What Should an Internal Auditor Do?

Standard 2110 – Governance

Internal auditors, guided by Performance Standard 2110 – Governance, hold a pivotal position in navigating the complexities of AI implementation within organisations. Their responsibilities span strategic alignment, ethical considerations, and effective governance.

The strategic engagement of internal auditors involves evaluating AI-related structures, processes, and procedures, ensuring alignment with the organisation's objectives. Ethical considerations take precedence, necessitating proactive assessments of moral and ethical issues related to AI use. Model risk management is pivotal, requiring internal auditors to identify and address risks associated with AI models.

Adopting the Three Lines Model, internal auditors navigate AI-related risks and opportunities, collaborating with management, risk, and compliance functions. Addressing the human factor in AI, they actively consider and mitigate risks associated with human error or bias. Embracing agile approaches, internal auditors adapt to the dynamic AI landscape.

In essence, Performance Standard 2110 – Governance guides internal auditors to ensure effective AI governance. Their strategic engagement, ethical considerations, model risk management, and adherence to established models collectively contribute to the responsible and beneficial integration of AI technologies within organisations. As organisations embrace AI, internal auditors stand as guardians of ethical standards and effective governance, facilitating a seamless and responsible integration of AI technologies.

Reference

Global Perspectives Insights: The Artificial Intelligence Revolution

Cybersecurity

Part 1: Staffing and Development for the Next Generation

About the Expert

Aneta Waberska, CISA
Aneta Waberska is Director of Information Security and Compliance Products at Audit Board. She has more than 15 years of experience across IT audit and compliance domains and joined Audit Board to focus on product development efforts serving IT risk and compliance users, leveraging her industry experience. Aneta started her career at KPMG and PwC, where she helped clients implement and assess frameworks such as SOC 1 and SOC 2. She has worked with companies of different sizes to implement and manage compliance programs of varying complexity, including managing company-wide policies and third-party risk management programs. Aneta has worked closely with management to implement controls to meet security framework requirements, as well as with executive management to ensure compliance supports the company's strategic objectives.

Uday Gulvadi, CIA, CPA, CAMS, CISA
Uday Gulvadi is a Managing Director in the Disputes, Compliance, and Investigations group at Stout, and co-leads its regulatory compliance and financial crimes practice nationally. Uday is a financial crime, internal audit, information systems audit, and risk advisory practice leader with more than 20 years of experience. He specialises in advising boards, audit committees, and senior management on their most challenging financial crime compliance, IT, and cyber risk, governance and risk, and compliance matters, including enterprise risk management, AML and sanctions program governance, model validations, risk-based internal audits, information technology, and cybersecurity audit and controls. Uday's clients range from some of the world's largest banks and financial institutions to smaller financial services companies.

INTRODUCTION

Cybersecurity poses a significant threat for organisations of any size. Recent incidents illustrate the swift escalation of problems. Ace Hardware Corporation experienced disruptions in shipments due to a cyberattack, leading to a temporary suspension of customer online ordering. A ransomware attack on a major Chilean telecom company disrupted various services, including data centres, internet access, and voice-over-IP. Furthermore, even smaller entities like Cabarrus County, N.C., faced cyber threats, with a cyberattack interrupting public online access to land records and vital indexes.

While internal audit is well-positioned to play a vital role in managing cyber risks, adequate resources are essential for fulfilling this role. Internal audit teams need the knowledge and skills to identify and advise on the organisation's cyber threats. In conducting a cybersecurity assessment, involving audit professionals with the requisite technical expertise and awareness of the current risk landscape is crucial, as highlighted by Deloitte. These brief initiates a three-part series on cybersecurity, addressing challenges faced by internal auditors and their organisations and exploring options and strategies for internal audit leaders to ensure they have the necessary talent to tackle ongoing cyber risks.

Cybersecurity

Part 1: Staffing and Development for the Next Generation

A Clear Threat

Cybersecurity remains a top risk.

- **Internal Audit's Cybersecurity Efforts Are Growing**

"Internal auditors must approach organisation-wide assessments with a holistic, risk-based perspective," emphasised Aneta Waberska, CISA, Director of Information Security and Compliance Products at Audit Board. Recognising cybersecurity as a top priority, internal auditors are tuned into the prevailing threat landscape. A global survey by the Internal Audit Foundation found that cybersecurity is the foremost risk entering 2024, with 73% of respondents placing it among their top five risks. In North America, The Institute of Internal Auditors' 2023 North American Pulse of Internal Audit revealed that 78% of internal audit leaders viewed cybersecurity as a high or very high risk. These auditors allocated 10% of their audit plans to cybersecurity, complemented by an additional 9% for IT concerns. Almost 70% of functions reviewed high-risk areas, encompassing cybersecurity and IT, annually or continuously, according to the Pulse survey findings.

Key cybersecurity threats to consider encompass:

- Breaches facilitating the theft of vital information or the exposure of customer and business partner data.
- Ransomware attacks rendering organisations unable to execute essential functions or access crucial information without paying a ransom to cybercriminals.
- Malware capable of causing severe disruptions to a system.

The repercussions of cyberattacks extend beyond immediate consequences, encompassing financial losses due to impaired business functions or a loss of trust from customers and business partners. Following the discovery of a cyber incident, organisations must invest time and resources in forensic investigations, remediation efforts, and assessing the material impact on financial and operational aspects to meet regulatory reporting requirements.

Reflecting the growing awareness of these risks, global cybersecurity spending was expected to surge by 13.2% in 2023, reaching a potential $224 billion. Companies recognise the tangible business and financial consequences associated with these threats, prompting increased scrutiny and assurance from internal audit, particularly from audit committees.

The Challenges

Cybersecurity approach, maturity impact staffing.

- **Clear-eyed Understanding of Cyber Environment Is Fundamental.**

Hiring the right talent for internal audit to support cyber risk management requires a comprehensive understanding of the organisation's unique cybersecurity circumstances and risks. Factors and challenges include:

1. Manual Mindset:

    - Many internal audit teams traditionally approach internal controls and processes from a manual perspective.
    - Digital transformation demands awareness of how digital solutions can enhance internal audits, including cybersecurity.
    - Understanding risks associated with digital transformation and exposure to relevant technologies are crucial.

2. Internal Controls:

    - Internal auditors focus on ensuring the organisation has proper controls to protect against cyber risks.
    - Familiarity with IT security controls specific to the organisation's technologies, such as those used in the cloud, is essential.

Cybersecurity

Part 1: Staffing and Development for the Next Generation

3. Disclosure Regulations and Data Protection:

    - Compliance with disclosure regulations, like the U.S. SEC's Cybersecurity Risk Management rule, is crucial.
    - Understanding and evaluating compliance needs related to data security and privacy laws, including GDPR, is necessary.

4. IT Systems:

    - Prioritising IT systems based on criticality to the organisation, sensitivity of processed data, and uniqueness of data.
    - Recognising that not all systems can have the same level of controls; setting priorities is essential.

5. Third Parties:

    - Assessing third parties' cybersecurity processes before sharing data and monitoring their controls.
    - Reviewing third-party attestation reports, such as SOC 2, to ensure data protection standards align with the organisations.

6. Ensuring Secure Access and Availability:

    - Balancing data protection and system availability for business objectives.
    - Choosing controls, such as multifactor authentication and encryption, based on the level of security required for different systems.

Strengthening Internal Audit Resources

Cybersecurity staffing remains a top priority.

- **Hiring and Developing Internal Audit's Cyber Talent**

Given these risks, how can internal audit build and maintain a team that can address them? The specifics of the answer will vary by organisation, but there are a few recommendations that apply to all.

Look for a Blend of Skills

To effectively manage cyber risk, internal audit teams must understand both the technical aspects of cybersecurity and the potential business consequences. Traditionally, IT auditors focused on technical proficiency, but the evolving landscape emphasises the need to articulate how these risks impact business objectives. Teams are now blending technical expertise with an understanding of business processes, with some opting for training to bridge the gap between these disciplines. This approach ensures a comprehensive approach to addressing cybersecurity challenges.

Integrate Skills in Emerging Technologies

As internal audit teams shift from sample-based testing, they are incorporating professionals skilled in data analytics, artificial intelligence (AI), and machine learning (ML). Utilising AI allows for comprehensive population testing and improved anomaly detection, boosting efficiency and reliability. This strategic move helps internal auditors stay ahead of cybercriminals who leverage sophisticated technologies.

Cybersecurity

Part 1: Staffing and Development for the Next Generation

Investigate Outsourcing.

Internal audit teams can bolster technical or business skills by incorporating outsourced professionals with specialised expertise in cyber or IT security. These experts may join the internal audit team on a project or longer-term basis, collaborating with internal audit members to enhance their knowledge and navigate company processes. Exposure to external experts contributes to expanding the internal audit team's knowledge base. When considering outsourcing, it's crucial to assess team members' certifications and prior experience to ensure alignment with or enhancement of current team skills.

Consider Collaboration

In some cases, the necessary expertise may be available in-house, particularly in IT, security, or compliance departments. Maintaining auditor independence, internal audit teams can form partnerships that introduce members to new insights and knowledge about the organisation's technology ecosystem and risks. This collaboration sets the stage for future audits, demonstrating shared goals in protecting the organisation and achieving objectives. Open communication helps dispel any anxiety about internal audit objectives, facilitating a risk-focused conversation with IT and security teams.

Build Internal Relationships

Building and maintaining relationships with professionals from the organisation's security, compliance, and IT teams benefit all internal audit team members. Even if not collaborating on a specific project, understanding current work in the company's environment is crucial. These relationships ensure timely updates, allowing the team to stay informed about changes, trends, and emerging threats. While specific audits reveal trends and threats, it's advantageous to know about changes as soon as possible.

Make Use of Available Resources

To stay current on modern technologies and associated risks, internal audit teams should dedicate time to learning at least at a high level. Utilising available resources, such as The IIA's Cyber Resource Centre and Audit Board's cybersecurity materials, provides guidance, research, certificate programs, and information about relevant conferences. The Risk in Focus 2024 report from the Internal Audit Foundation explores cybersecurity risks globally, offering unique regional perspectives on how organisations view and manage cybersecurity and other top risks worldwide.

CONCLUSION

The 2023 IIA Pulse survey indicates a gradual increase in internal audit staff growth, though it has not yet reached pre-COVID levels. Recognising that incoming generations are digitally adept, internal audit leaders should strategically leverage their digital skills. In a competitive staffing environment, internal audit teams can distinguish themselves by providing opportunities for the new generation to apply emerging technologies like AI/ML, offering valuable insights to address critical business issues. As internal audit teams rebuild or enhance their expertise, incorporating the advice and insights from this brief into their planning can be beneficial.

Cybersecurity

Part 1: Staffing and Development for the Next Generation

What should Internal Auditors do?

Standard 1210 – Proficiency and Due Professional Care

Amid growing cybersecurity threats, internal auditors must align their actions with the International Professional Practices Framework (IPPF) standards, with a focus on Standard 1210 – Proficiency and Due Professional Care.

In response to dynamic cyber threats, Standard 1210 emphasises the need for auditors to continually update their knowledge and skills, ensuring proficiency in addressing emerging risks. The standard directs auditors to tailor their approach based on the organisation's unique circumstances, necessitating a thorough assessment of cybersecurity maturity and prevalent threats.

To effectively address challenges, auditors must integrate technical proficiency with a broader understanding of business processes. Standard 1210 guides auditors to ensure their teams possess skills in IT security controls, data protection regulations, and prioritisation of critical IT systems.

Moreover, collaboration with other assurance functions is encouraged. By forming partnerships with IT, security, and compliance teams, auditors can gain valuable insights into the organisation's technology ecosystem, enhancing the effectiveness of their audits.

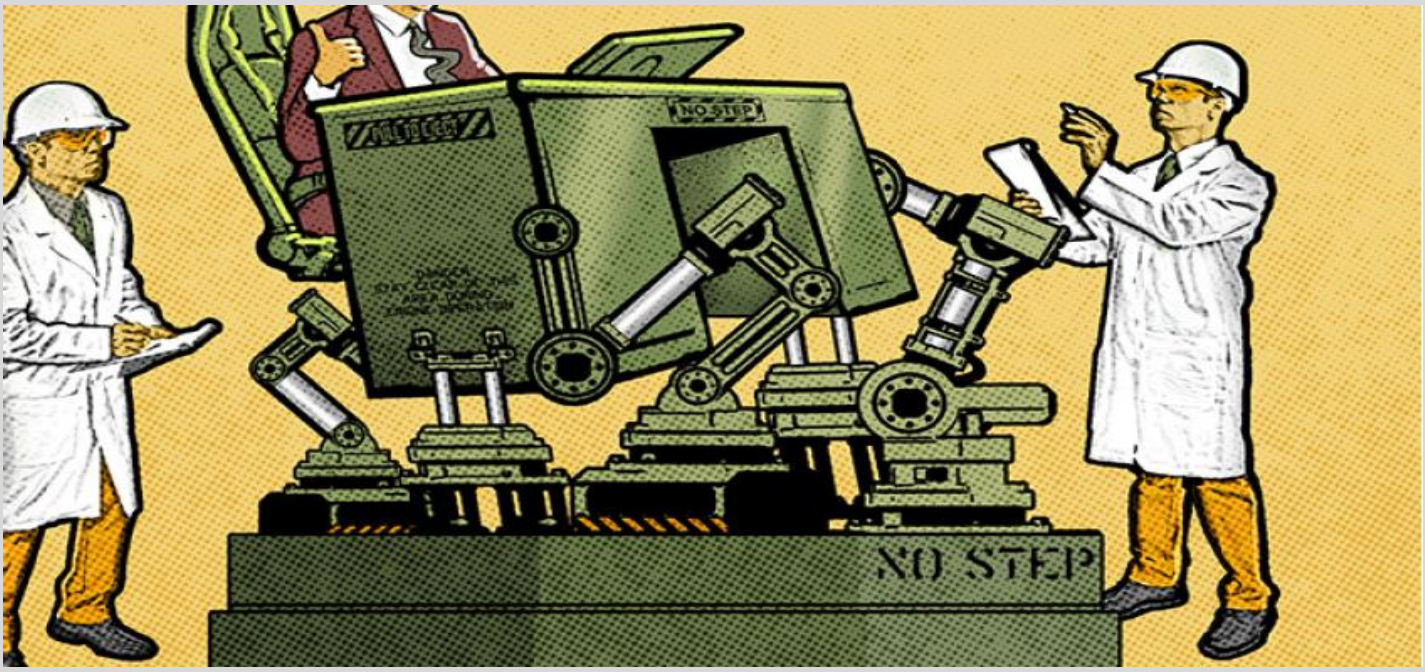
In conclusion, internal auditors, guided by Standard 1210, play a crucial role in enhancing cybersecurity resilience. Upholding proficiency and due professional care, auditors contribute significantly to safeguarding organisational assets against evolving cyber risks.

Reference

Cybersecurity Part 1: Staffing and Development for the Next Generation

Training Tomorrow's Internal Auditor

ARTICLES | DENNIS APPLEGATE, CIA, CPA, CMA, CFE | OCT 09, 2023



The Internal Audit Foundation's 2022 report, "Internal Audit: A Global View," highlights a concerning trend of a shrinking number of early career internal audit practitioners, with practitioners aged 50 and above representing a larger proportion of the workforce. To address this talent gap, colleges and universities are playing a crucial role by introducing students to the rewarding possibilities within the internal audit profession.

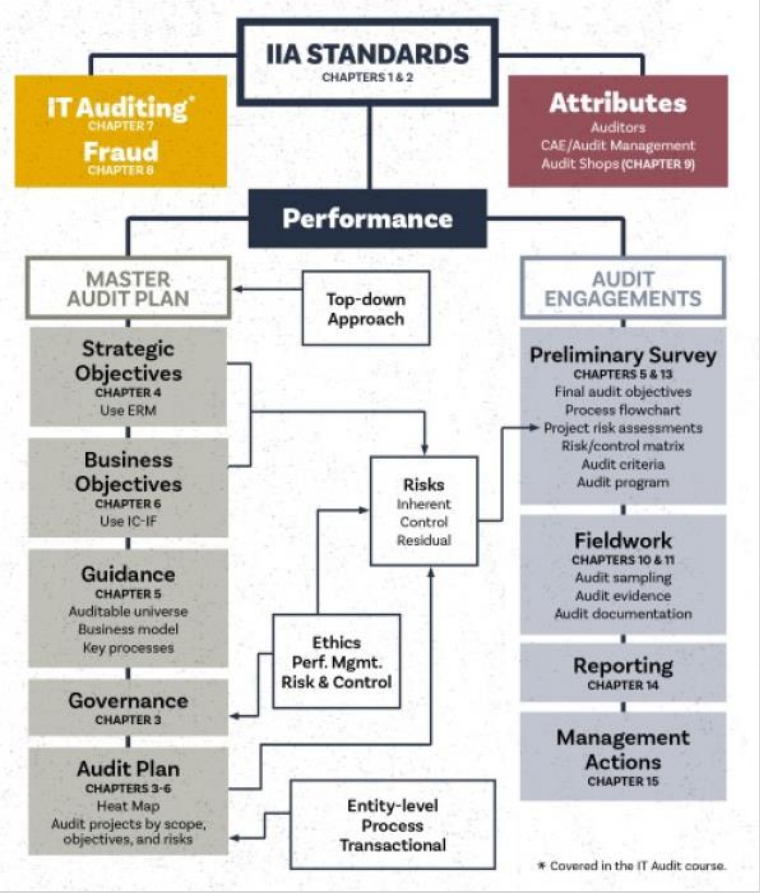
Universities often refer to The IIA's Global Model Internal Audit Curriculum for guidance on course coverage. This curriculum provides sample learning objectives and content recommendations for core and supplemental courses. The IIA recognises and endorses universities through programs like the Internal Auditing Education Partnership Program (IAEP) and Internal Audit Awareness Program (IAAP). The classification of an IAEP school depends on the internal audit curriculum it offers, ranging from Internal Auditing Foundation to Comprehensive Internal Auditing or Centre for Internal Auditing Excellence.

The "Principles of Internal Auditing" course, a core component across IAEP programs, prepares students for the Certified Internal Auditor exam's first two parts. A flowchart detailing the course overview is provided, emphasising two key audit process streams: audit engagements and annual audit planning.

While the course should cover all content recommendations, instructors often prioritise specific topics relevant to prospective internal auditors. For instance, at Seattle University, the emphasised topics include the internal audit value proposition, the three pillars of internal audit services, risk and materiality, auditor bias, annual audit risk assessments, and audits of ethics and values within organisations.

Training Tomorrow's Internal Auditor

ARTICLES | DENNIS APPLEGATE, CIA, CPA, CMA, CFE | OCT 09, 2023



The Pillars of Effective Internal Auditing

The "Principles of Internal Auditing" course thoroughly covers The IIA's International Standards for the Professional Practice of Internal Auditing, delving into Implementation and Supplementary guidance, including Practice Guides, to elucidate and strengthen requirements. Special emphasis is given to Standard 1100: Independence and Objectivity, and Standard 1200: Proficiency and Due Professional Care—fundamental to effective internal audit services.

The course incorporates real-world examples, such as examining the impact of market price declines on executive bonuses with a current purchase commitment. This case illustrates how internal auditors, beyond being auditors, showcase proficiency as consultants during assurance engagements.

Students are crucially informed that internal auditors engage in "consulting" when enhancing client conditions or circumstances without controlling outcomes—emphasising a key distinction under IIA Standards. When discussing Standard 1000: Purpose, Authority, and Responsibility, including components of an internal audit charter, instructors tackle the challenge that people generally dislike audits due to a lack of understanding of the internal audit value proposition. Students learn to articulate this value during the audit entrance conference and throughout the process, emphasising transparency to foster employee cooperation.

A Deep Dive Into COSO

In response, the course delves extensively into the COSO Enterprise Risk Management (ERM) framework, particularly its integration with strategy and performance. While COSO ERM outlines four management responses to risk—accept, avoid, share, and reduce—the course emphasises corporate strategies that reduce risk through internal controls. This emphasis aligns with corporate boards' tendency to synchronise strategy with risk appetite and tolerance.

A thorough exploration of the COSO Internal Control–Integrated Framework is essential for connecting assessed risks of a material nature to the controls designed for mitigation. The course emphasises the crucial distinction between documented control components and actual control execution, highlighting research indicating that control failures often result from employee behaviour rather than control design.

Recognising the importance of evidence gathering in a successful audit engagement, the course underscores the need to avoid introducing any form of auditor bias, which could compromise the quality of the audit result.

Training Tomorrow's Internal Auditor

ARTICLES | DENNIS APPLEGATE, CIA, CPA, CMA, CFE | OCT 09, 2023

Students are familiarised with three common types of auditor bias:

1. **Availability Bias:** This involves focusing the audit on readily accessible information or what comes to mind immediately, rather than prioritising information with the most probative value.

2. **Anchoring Bias:** This bias is exhibited when prior audits serve as the starting point for a current audit, irrespective of changed circumstances. It may also involve relying on the first audit evidence encountered, regardless of its accuracy or relevance.

3. **Confirmation Bias:** In this bias, auditors pursue data that aligns with pre-existing views about an audit matter, while ignoring or rejecting contrary evidence.

A Group Project

IIA Standard 2010: Planning plays a crucial role in guiding the annual risk assessment for the audit plan and schedule. In our group project, "Annual Audit Risk Assessment and Master Audit Plan/Schedule," students apply knowledge gained from Chapters 3 through 6 of the textbooks to analyse the risk profile of a publicly held firm. Utilising internet research and other sources, students identify events that may impact the risk profile. The project aims to provide hands-on training in annual risk assessment practices and audit plan development for prospective internal auditors.

To enhance the learning experience, students present and defend their annual risk assessment and master audit plan to a hypothetical "audit committee," consisting of internal audit professionals. Senior audit managers from notable firms such as Boeing, Deloitte, Microsoft, and Protiviti participate in evaluating each presentation. The committee assesses the thoroughness of the risk assessment, including its underlying rationale and supporting facts and data. Additionally, the logic of the relationship between key risks affecting the firm's business objectives and the proposed audit plan projects is evaluated.

8 Elements of a Well-defined Ethics Program

1. Written Code of Conduct: Clearly defined and documented guidelines outlining expected behaviour and ethical standards for employees.

2. Tone at the Top (Middle and Bottom): Ensuring a strong ethical tone throughout the organisation, starting from top-level leadership, and extending to middle management and all employees.

3. Employee Certifications: Documentation confirming that employees have read, comprehended, and commit to complying with the established code of conduct.

4. Recurring Employee Ethics Training: Regular training sessions to educate employees on ethical standards, dilemmas, and best practices.

5. Ethics Hotline: A dedicated channel, such as a hotline, for employees to report ethics violations, ensuring confidentiality and protection for whistleblowers.

6. Investigations of Ethics Violations: A systematic process for thoroughly investigating reported ethics violations to determine facts and take appropriate actions.

7. Disciplinary Procedures: Established procedures outlining the consequences and disciplinary actions for individuals found guilty of ethics violations.

8. Periodic Internal Audits: Regular internal audits to assess and ensure the adequacy and effectiveness of the ethics program within the organisation.

Students are encouraged to present and defend their audit plan and schedule to the audit committee, emphasising its alignment with assessed risks. This exercise, applied to companies like Alaska Airlines, Costco, Expedia, Nordstrom, Paccar, Starbucks, and T-Mobile, provides valuable real-world training for internal audit professionals.

Training Tomorrow's Internal Auditor

ARTICLES | DENNIS APPLEGATE, CIA, CPA, CMA, CFE | OCT 09, 2023

An Ethics Case Study

Given ongoing corporate scandals, class time is dedicated to Standard 2110: Governance, focusing on the internal audit's role in assessing and recommending improvements to the organisation's governance processes, including ethics and values. This ensures that students not only grasp the elements of a robust ethics program but also comprehend how to audit such a program effectively.

To stimulate discussion, the class reviews recent ethical failures in corporate governance, such as Wells Fargo's fraudulent marketing, Airbus's foreign bribery case, Kraft-Heinz's inflated cost-savings from its merger, and EY and KPMG's ethics exam scandals. Analysing these cases sparks a dynamic exchange on how internal audit can contribute to enhancing corporate governance. This discussion sets the foundation for an IIA ethics case study assignment called "Auditing the Compliance and Ethics Program," aligning with the course textbook.

The case study delves into ethics and business conduct as a governance process, prompting students to consider internal audit's practical role in the corporate ethics program. Before tackling the case study, the class reviews standard elements of an ethics program, emphasising the connections between corporate intentions, integrity, compliance, and accountability. Student study teams then apply these elements to the assigned case, identifying risks, proposing process controls, and preparing an audit report—a process aligned with the principles outlined in the "Principles of Internal Auditing Flowchart" and covered in the textbook's chapters 12 through 15.

Navigating the path to effectively teach a Principles of Internal Auditing course is challenging in a rapidly evolving audit environment, compounded by ongoing changes in The IIA's Standards. Colleges and universities venturing on this journey are advised to maintain close ties with The IIA and senior internal audit leaders in their region to ensure that class content remains focused on key topics relevant to the profession.

Credentialed readers of Internal Auditor, in collaboration with their local IIA chapter, are encouraged to consider partnering with business schools at nearby colleges and universities.

Developing and teaching internal auditing curricula aligned with The IIA's Standards, internal audit procedures, and professional practices can establish these institutions as reputable educators producing graduates knowledgeable in business risk, control, and internal audit. Such efforts contribute to cultivating a pool of competent graduates ready to enter the field of internal audit.

What should Internal Auditors do?

Standard 2130 – Control

Standard 2130 – Control Environment significantly shapes the proficiency of internal auditors, guiding them in assessing an organization's control environment. Aligning university curricula with this standard is crucial. In courses like "Principles of Internal Auditing," integrating real-world examples and projects, such as the Annual Audit Risk Assessment, mirrors practical application, preparing students for professional complexities.

Exploring COSO ERM and Internal Control reinforces Standard 2130, emphasizing interconnectedness with risk management and governance. An ethics case study, aligned with recent scandals, prompts students to evaluate governance processes and recognize the control environment's impact on ethics.

Championing Standard 2130, auditors contribute to resilient control environments. Collaborating with educational institutions ensures future professionals can evaluate and fortify governance and control processes, embodying excellence in internal audit.

Reference

Training Tomorrow's Internal Auditor