GLOBAL PERSPECTIVES & INSIGHTS

The Artificial Intelligence Revolution

PART I: Understanding, Adopting and Adapting to AI

PART II: Revisiting The IIA's Artificial Intelligence Framework

PART III: Internal Audit's Role in AI Ethics

The Institute of
Internal Auditors

Contents

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 organizations. 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 released in November 2022, it was considered a significant leap forward in artificial intelligence (AI). Many compared it to the internet in terms of its potential to change and disrupt current business practices, regulations, and social norms.

ChatGPT and the rapidly emerging alternatives to it are examples of generative AI. Generative AI is powered by large language models, systems that are trained on enormous amounts of data from a variety of sources that are processed by a neural network modeled on the human brain to develop requested outputs. When prompted, it uses this training and algorithms to develop content — including text, images, videos, sounds, speech, and code — that resembles something a human might create.

While this specific system has received a tremendous amount of attention, it is only one example of the many tools that fall under the AI umbrella. AI is at the heart of every smart device that we use, and it also drives far more sophisticated applications that are transforming businesses. It is being put to work in business, government, health care, and many other fields to replicate human analysis and even decision making.

The global composite AI market is projected to increase from $900 million in 2023 to $4.4 billion by 2028, rising at a compound annual growth rate of 36.5% as the expanding availability of data and AI resources spur the use and development of new AI solutions[1]. The vast majority of business leaders (94%) believe AI will be critical to their organizations' success over the next five years, according to the most recent edition of Deloitte's "State of AI in the Enterprise".[2]

"AI may become the most disruptive technological development to date, creating new opportunities and risks in every aspect of business and life," according to an *Internal Auditor* magazine article[3]. Internal auditors are well-versed in assessing the risks and opportunities that affect whether an organization can meet its objectives. Using their insight and experience, "internal audit can help an organization evaluate, understand, and communicate the degree to which artificial intelligence will have an effect (negative or positive) on the organization's ability to create value in the short, medium, or long term," according to " Artificial Intelligence–Considerations for the Profession of Internal Auditing"[4] from The Institute of Internal Auditors (IIA).

94%

of business leaders believe AI will be critical to their organizations' success over the next five years.

Source: Deloitte - State of AI in the Enterprise, 5th Edition

Given the broad and rapid growth of AI use, it's important that internal auditors quickly develop a deep understanding of how it works, its practical applications in business and government, and the risks and opportunities it presents to organizations. This brief will examine these areas in depth and provide best practices and insights for keeping pace.

[1] "$4.4 Billion Composite AI Markets: Growing Intricacy of AI Applications for Better Performance and Accuracy to Drive Growth - Global Forecast to 2028," Research and Markets press release, June 13, 2023.

[2] "State of AI in the Enterprise, Fifth Edition," Deloitte, October 2022.

[3] "Auditing Artificial Intelligence," James Bone, *Internal Auditor*, October 14, 2020.

[4] "Artificial Intelligence—Considerations for the Profession of Internal Auditing", The Institute of Internal Auditors, 2017.

UNDERSTANDING AI

Machine Learning and Simulated Human Intelligence

Getting Beyond Simple Automation

The terms AI and automation are often used interchangeably. This reflects a limited understanding of AI's more powerful and game-changing potential. Indeed, while AI can automate routine tasks, it has much greater abilities and uses. For example, robotic process automation (RPA), a basic level of automation, uses structured data and logic to perform repetitive, rule-based processes, such as accounting workflows and data collection. In doing so, it enables people to take on higher-level tasks. It can replicate human *actions*, but more sophisticated AI tools can perform tasks that simulate human *intelligence*, such as understanding normal human communications, taking on problem solving, and offering higher performance and operational efficiency. Automation follows established rules, while AI relies on the training it has received to make its own decisions.

AI and machine learning solutions can fall into several categories, including:

- Descriptive: What happened?
- Diagnostic: Why did it happen?
- Predictive: What could happen next?
- Prescriptive: What should be done next?[5]

However, AI currently doesn't possess the kind of judgment or context that enables humans to make the best decisions, although those abilities may be enhanced as technology advances.

Additionally, AI is only as good as its training. In studying cases involving rule violations, researchers from MIT and other organizations found that if machine-learning models are not trained on the right data, "they are likely to make different, harsher judgments than humans would."[6] Risks related to AI's limitations will be discussed in another section.

[5] "AI and Machine Learning: It May Not Be as Difficult as You Think," RSM, September 7, 2022.

[6] "Study: AI Models Fail to Reproduce Human Judgements About Rule Violations," Adam Zewe, MIT News, May 10, 2023.

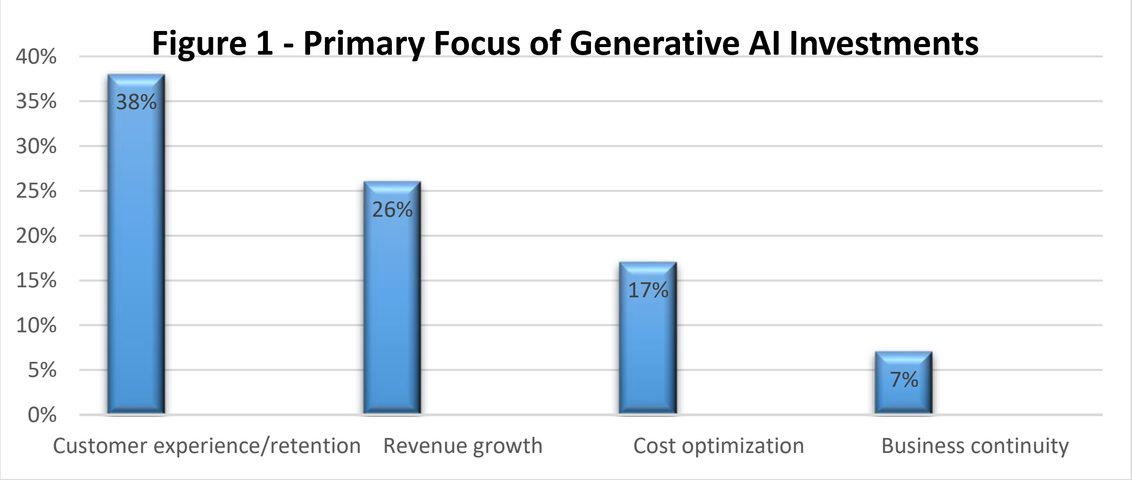
Putting AI to Work

Practical applications of AI include everyday tools that have been in use for years, such as online search engines; chatbots that provide simple information and answers to questions; voice assistants, such as Alexa and Siri, that respond to commands and perform tasks; Google Maps and similar tools to select the best travel and delivery routes; self-driving cars; customized online shopping experiences; and personalized advertising. Gartner cites examples of the ways that generative AI, for example, can be used in drug design, material science, chip design, synthetic data, and part design.[7]

Other business and government use cases of AI include:

- Solving skill shortages by automating tasks.
- Enhancing IT or network performance.
- Designing strategies to retain or appeal to specified customers and improve customer experience. For example, a recent *Harvard Business Review* article noted that Brinks Home, a smart-home-technology company, used AI to gain brand recognition in a competitive market.[8]
- Identifying and preventing fraud or errors in financial information.
- Forecasting product or service demand based on customer history/feedback, along with market and economic activity.
- Addressing sustainability objectives. AI can help achieve 79% of the UN General Assembly's Sustainable Development Goals, according to Nature Communications.[9]
- Prioritizing customer opportunities or leads.
- Tracking responses to sales campaigns, market research, and search engine optimization (SEO).
- Streamlining and enhancing customer support activities.

At present, generative AI investments in business remain largely focused on improving customer relations and growing revenue. Most organizations have yet to commit significantly to efforts that drive new business opportunities or new markets using generative AI, according to a recent Gartner survey (see Figure 1).



Source: Gartner survey of more than 2,500 executives, 2023[10]

[7] "Beyond ChatGPT: The Future of Generative AI for Enterprises," Jackie Wiles, Gartner, January 26, 2023.
[8] "Customer Experience in the Age of AI," David C. Edelman and Mark Abraham, Harvard Business Review, March-April 2022.
[9] "The Role of Artificial Intelligence in Achieving the Sustainable Development Goals," Ricardo Vinuesa, et al., Nature Communications, January 13, 2020.
[10] "Gartner Experts Answer the Top Generative AI Questions for Your Enterprise," Gartner, 2023.

Opportunities, Challenges, and Risks

In developing and implementing an AI strategy, companies must understand not only the possibilities, but also the limitations and threats that this technology can pose. As companies scramble to implement AI solutions, examples of AI opportunities include the ability to:

- Shorten the data processing cycle.
- Minimize potential errors by replacing human actions with perfectly repeatable machine actions.
- Use process automation to lower labor time and costs.
- Employ robots or drones for potentially dangerous work.
- Make more accurate predictions about topics that can range from potential sales in specific markets to predicting epidemics and natural catastrophes.
- Use AI initiatives and efficiencies to drive revenue and market share growth.[11]

For all its benefits, there may be challenges to harnessing AI. According to the IBM Global AI Adoption Index, nearly one in five companies cited difficulties in:

- Ensuring data security.
- Ensuring data governance.
- Managing disparate data sources and formats.
- Integrating data across any cloud.[12]

Organizations may not recognize how best to benefit from the opportunities of AI. At the same time, failure to fully understand the workings of these systems and the biases and errors that may infiltrate their training and output could leave companies unknowingly vulnerable to a variety of threats. Risks that may cause reputational or financial damage, among other threats, include:

- **Lack of transparency.** Unidentified biases or errors incorporated into AI technology can lead to a range of improper decisions, including discrimination in hiring or providing credit, for example.
- **Maintaining security and confidentiality of information.** "The potentially disastrous effects of a cybersecurity breach involving AI cannot be overstated," according to The IIA's Artificial Intelligence—Considerations for the Profession of Internal Auditing. The IIA recommended that if organizations don't already have sufficient cybersecurity, CAEs should continuously inform stakeholders that it must be built up rapidly. As organizations move to gather and store increasingly large volumes of data, they may be vulnerable to breaches, privacy violations, loss of data, or system failure caused by internal errors and the acts of hackers or other cybercriminals. Tactics used by cybercriminals can also include "model poisoning,"

Initial Steps Toward Regulating AI

The rapid rise and the potential risks of AI have prompted calls for greater regulation. The European Parliament has approved a draft of the Artificial Intelligence Act, which calls for greater transparency and safeguards. The law establishes three levels of AI risk: applications and systems considered unacceptable risk, which are banned; high-risk applications, which are subject to stated legal requirements; and those of limited risk, which could comply with minimal transparency regulation. Generative AI would also have to comply with transparency requirements. Fines range up to $33 million, or 6% of a company's annual global revenues.

In the U.S., the White House has issued a fact sheet and a blueprint for an AI Bill of Rights aimed at ensuring safe and effective systems. China has also drafted regulations setting potential guardrails on generative AI. In addition, Sam Altman, the CEO of OpenAI, the creator of ChatGPT, has called for coordinated international regulation of generative AI and signed a statement on AI risk along with hundreds of other AI experts and public figures.

[11] Artificial Intelligence—Considerations for the Profession of Internal Auditing, Institute of Internal Auditors, 2017.

[12] IBM Global AI Adoption Index 2022.

where a machine learning model's training data is deliberately polluted. This can corrupt systems, produce incorrect data, trigger denial of service, or initiate malware attacks that can paralyze organizations.[13]

- **Legal challenges.** Plagiarism, copyright infringement, or intellectual property violations are potential pitfalls if the content that AI generates is not original. Additionally, inadequate testing and oversight of AI can lead to ethically questionable results.
- **Vendor or supplier dependency**. This can be a particular threat as AI becomes key to a wide range of organizational systems and functions.[14] Among other concerns, organizations should ensure that risk-assessment indicators properly address the dangers involved in using or integrating third-party tools, given the associated concerns about vendor or supplier actions and behaviors.
- **Employment losses.** Organizations could face tough decisions if AI replaces workers who can't be reassigned or are unable to find similar jobs. In addition to the toll for individuals, unemployment in an area or industry can lead to economic and social disruption.
- **Regulatory risks.** As governments attempt to understand and address AI's use, organizations may have to pivot their AI strategies to an evolving regulatory landscape. There may also be legal risks if issues with their AI systems cause financial losses for others or if they violate human rights or ethical standards.
- **Environmental considerations.** The systems that power AI use large amounts of electricity, which can counteract organizations' sustainability efforts and hinder achievement of their environmental, social, and governance (ESG) goals.
- **Investment decision making and results.** The organization may be at a competitive disadvantage due to insufficient investment in AI initiatives or resistance to these initiatives from customers, employees, or other stakeholders. Return on AI investment (infrastructure, research and development, and talent acquisition) may not be adequate. Without a robust AI strategy, these issues may stymie an organization's effort to make the best use of AI tools.

[13] "Do Free AI Tools Pose a Security Risk to Your Business?", Rebecca Neubauer, Business News Daily, May 16, 2023.

[14] "Artificial Intelligence and The Top 6 Business Risks," Chandu Gopalakrishnan, April 28, 2023, The Cyber Express.

THE ROLE OF INTERNAL AUDIT

Assessing Risk and Providing Foresight

Trusted Techniques and Proven Skills Support AI Risk Management

Internal audit is well-equipped to help organizations assess and communicate AI's impact on value creation and achievement of goals. Internal audit leaders can incorporate AI considerations into their risk assessments and determine how AI should be included in a risk-based audit plan. Practitioners should take an active role in AI projects from the outset. Acting as trusted advisors, internal auditors can offer advice and insight on implementation. This assumes proficiency has been or will be acquired in the relevant areas. Additionally, internal audit can provide assurance over related risk areas, such as AI's impacts on readiness and response to cyber threats. It's important to note that, to maintain independence and objectivity, internal auditors should not take ownership or responsibility for AI implementation or other steps.

If an organization already has implemented AI into its operations or a product or service, internal audit can:

- Offer assurance over risk management related to the reliability of the underlying algorithms and the data on which they are based.
- Ensure that related moral and ethical issues are being addressed.
- Offer assurance on AI governance structures.

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 Center, 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.

Internal auditors are equipped to perform these roles because of their:

- Understanding of the organization's strategic objectives and how they are achieved.
- Ability to assess whether AI activities are accomplishing their objectives.
- Ability to offer internal assurance over management's AI risk management efforts.
- Position as a trusted advisor that can offer insights on using AI to improve business processes or enhance product and service offerings.

Best Practices for Putting AI to Work

As daunting as AI may sound**,** the best approach for internal auditors is to embrace it as quickly and as much as possible.

"Don't hide from advanced technologies such as AI," advised Eric Wilson, CIA, CISA, director of internal audit and CAE at Gulfport Energy Corporation. For many companies, AI has already appeared on their risk profiles for several years, but some decide to put off tackling it due to lack of understanding of it and how it should be audited. However, Wilson notes that auditors will have to develop expertise in tools that their organizations are already using or may be taking on soon.

The best way to get started is by trying it out, something that's easy to do with generative AI such as ChatGPT or Bard. "See how it works, interact with the system," Wilson recommended. As part of the process, if the system utilizes an interactive language model, ask it to explain the logic it used to produce its answers. This is an option that's only available with a generative AI system, because it is language based, so it's worth giving it a try.

To gain a better understanding of systems that aren't as easily interfaceable as ChatGPT, Wilson recommends asking to shadow people within the organization who are using them. This can offer a practical understanding of how the system is being applied to different functions and uses. On a basic level, "find out if the people who are using it can explain it or describe how it is making a difference in the organization." Wilson said. "If they can't, this lack of expertise or gap in understanding on how the system works at a fundamental level may be an opportunity for improved utilization that internal audit can point out to the organization."

CONCLUSION

"This is an exciting time for internal audit to play a leadership role in providing assurance for AI," according to the *Internal Auditor* magazine article.[15] The initial hype is expected to abate as organizations wrestle with actual understanding and implementation, but its impact will expand as people and businesses find more innovative ways to put it to work.[16] Now is the time for internal auditors to understand the opportunities and risks for their organizations so that they can offer valuable assurance and insights on AI initiatives.

[15] "Auditing Artificial Intelligence," James Bone, *Internal Auditor*, October 14, 2020.

[16] "Gartner Experts Answer the Top Generative AI Questions for Your Enterprise," Gartner, 2023.

Part II: Revisiting The IIA's Artificial Intelligence Framework

About the Expert

Eric Wilson, CIA, CISA

Eric Wilson, CIA, CISA, is the director of internal audit and CAE for 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 is a member of The Institute of Internal Auditors' (IIA) Professional Knowledge Committee and North American Content Advisory Committee. He has served on the IIA's Advocacy Committee and is a member of the Board of Governors for The IIA's Oklahoma Chapter. In addition to his work with The IIA, Eric serves as a member of the Board of Advisors for the University of Oklahoma's Steed School of Accounting, has lectured on internal audit at several universities, and holds active leadership positions with multiple local and nonprofit organizations.

INTRODUCTION

In 2017, The Institute of Internal Auditors (IIA) published a landmark examination of an important topic that has only burgeoned in significance since then, "Artificial Intelligence – Considerations for the Profession of Internal Auditing." This three-part work described the internal auditor's role in artificial intelligence (AI), set forth a framework of issues to be considered in addressing AI in the context of internal audit, and discussed the practical application of this multifaceted technology.

Despite tremendous advancement in AI during the ensuing six years, the framework remains largely relevant and useful in most internal audit areas. This brief begins by reviewing some of the key elements of the framework and their continuing applicability. It also reviews other issues to consider and concludes by examining the internal auditor's role in AI going forward.

KEY COMPONENTS

Framework Addresses Critical Factors

Building Strategies on Capabilities, Risk, Opportunities

The framework addresses six components, all incorporated within the organization's strategy. The framework notes that each organization will need a unique AI strategy based on its own existing capabilities as well as its approach to managing risks and capitalizing on opportunities. In assessing where organizations stand in their AI strategy, internal audit must consider questions such as:

- Does the organization have a defined AI strategy?
- Is it investing in AI research and development?
- Does it have plans to identify and address AI threats and opportunities?

The framework notes that AI can provide a competitive advantage for organizations, and that internal audit should help management and the board realize the importance of developing a considered AI strategy consistent with the organization's objectives. These observations certainly remain true today. Strategic planning for AI is also unique because of the technology's rapid and constant evolution and the breadth and depth of its potential impact. As a starting point, internal auditors should be sure that they fully comprehend the magnitude of AI systems. "Some critical components are so starkly different from systems that we've used *and audited* before, *that both end users and auditors* may not understand what the system is doing and how it's doing it," said Eric Wilson, CIA, CISA, director of internal audit and CAE for Gulfport Energy.

One key difference when it comes to AI is meaning making, which refers to how people understand or make sense of themselves, the events they experience, and the world around them. It is a concept that also applies to advanced technologies. "Meaning making in the AI era starts with an appreciation of what machines can and cannot do. It may be possible, for example, for a machine to make certain kinds of [medical] diagnoses more accurately than a person can. But it will be up to nurses, doctors, and therapists to help patients understand the implications and manage the consequences. It's the difference between knowledge and meaning."[17]

With AI, technology has gone past the point of being able to simply gather and sort data to being better able to take information and contextualize it. It is a step forward that offers organizations completely new abilities, risks, and opportunities. Wilson recommends that internal auditors engage in an ongoing conversation, both internally and with their peers, about auditing AI strategy to appropriately monitor its effectiveness.

[17] "Putting Lifelong Learning on the CEO Agenda," A. Edmonson and B. Saxberg, *McKinsey Quarterly* 2017 Number 4.

THE SIX COMPONENTS

Governance, Performance, and More

AI Governance

This component encompasses the structures, processes, and procedures that are used to direct, manage, and monitor the organization's AI activities undertaken to achieve its objectives. Once again, the appropriate formality and structure of AI governance will vary based on each company's circumstances and characteristics. In every case, the framework notes, AI governance addresses accountability and oversight and considers whether those in charge of AI have the necessary skills and expertise to monitor its use and if its AI activities reflect its values. Given advancements in AI's impact, it is critical that related actions and decisions align with the organization's ethical, social, and legal responsibilities.

Data governance is always important, but once again, the approach is a little different when dealing with AI. For example, because generative AI systems are trained on specific information, it's much easier to introduce not only errors, but also bias early on in their development if they are not trained on reliable data. If traditional systems are taught that a certain specific shade of red is actually blue, they will always think that shade is blue. AI in that situation, on the other hand, will think that any shade of red is blue.

Once a small bias or inaccuracy is fed into the technology, the system will continue to be trained on that error, expanding its impact potentially exponentially, so the bias must be spotted and removed upfront before it is used in decision making, in a customer-facing communication, or in any other manner that could damage the organization's finances or reputation. "One wrong data point could completely change how the system views and contextualizes the data it's trying to work through," Wilson said.

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.

Data Architecture and Infrastructure

The framework established that AI data architecture and infrastructure will likely resemble those used for big data. Issues that fall under these areas encompass how data is accessed, along with information privacy and security concerns throughout the data lifecycle – from collection and use to storage and destruction. Other considerations include data ownership and use throughout the data lifecycle.

When it comes to AI, cybersecurity must be a top consideration for chief audit executives within their teams. As the volume and complexity of data grows with expanding AI use, consider, as well, that the information AI and generative AI use is only as good as what they are given or trained on. "Organizations will have to know down to data point level that the information being fed into the system is accurate, and that it reflects actual activities," Wilson said. "Good data architecture is the foundation of how AI systems will interpret the world around them that we're asking them to operate in," he said.

Controls will also differ for AI systems. When working with a former employer, Wilson helped develop a system that linked together data science, robotic process automation (RPA), and AI to develop intelligent automation. The company created a control set for each part of the system, much like the general IT controls it had always used. However, when considering that the goal AI system would be one that improved its own performance over time, Wilson's team quickly realized that there needed to be globalized controls over the entire system. These controls are essential to govern how the various system components interacted and what limits would be placed on the AI system in regard to its ability to modify the data science or RPA algorithms and processes. "We needed to see holistically how the system, composed of multiple technologies and integrations, interacted and provided answers to our questions," Wilson said. It was not only a new concept, but a new problem to solve. "We spent a lot of time on it because it touches all the systems and has to dovetail into IT general controls," he said.

In his internal audit role, Wilson also often asks about efficiency boundaries in place with AI systems. "You can only let the system get so efficient, because we need to understand what it is doing and not let it get away from us," he said. Because limiting efficiency in technology is a new concept, it may take trial and error to develop a new way of thinking about AI.

Data Quality

With that in mind, it's clear to see, as The IIA's framework established, that the reliability of the data on which AI algorithms are built is critical. Unfortunately, a survey taken last year by open source data quality tool Great Expectations found that 77% of data professionals felt their organizations had data quality issues, and 91% said they were affecting company performance. Only 11% said they had no data quality issues. The company defined the six dimensions of data quality as:

- Accuracy.
- Completeness.
- Uniqueness.
- Consistency.
- Timeliness.
- Validity.[18]

Data quality may be challenged because systems may not communicate with each other well or may do so through complicated add-ons or customizations. "How this data is brought together, synthesized, and validated is crucial," the framework notes.

77%

OF DATA PROFESSIONALS FEEL THEIR ORGANIZATIONS HAVE DATA QUALITY ISSUES, AND

91%

SAID THEY WERE AFFECTING COMPANY PERFORMANCE.

Great Expectations survey, June 2022

Measuring Performance of AI

How well are AI systems performing? What contributions are they making? The framework established that, as organizations integrate AI into their activities, they should identify appropriate performance metrics that link activities to business objectives and clearly show if AI is helping achieve goals. At the same time, it's critical that management actively monitors the performance of its AI activities.

The Human Factor

Under the automation paradox, the more efficient an automated system is, the more important it is for humans to be involved in the process. In some cases, humans are needed to spot and address errors that other humans have made. Indeed, a total of 88% of data breach incidents were a result of human error.[19] Human error and biases (both intentional and unintentional) will have an impact on

[18] "Data Governance vs. Data Quality: Where Do They Overlap?, Sam Bail, Great Expectations, June 10, 2022.
[19] "'Psychology of Human Error' Could Help Businesses Prevent Security Breaches," *CISO Magazine*, Sept. 12, 2020.

the performance of both the algorithms and the training that are the drivers of AI systems. The framework establishes that addressing the human factor means:

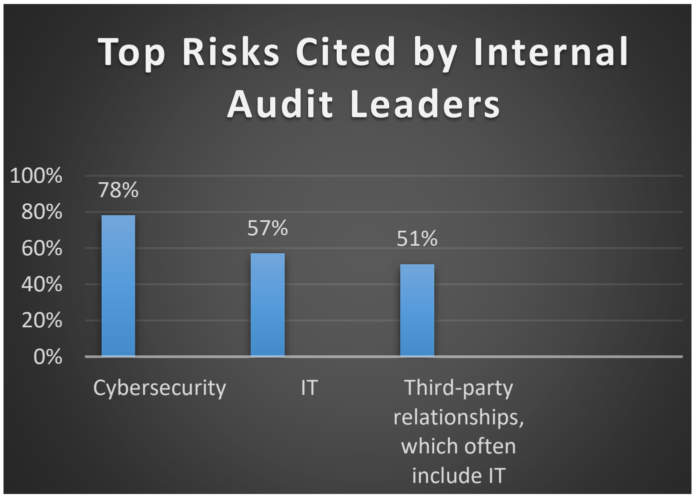
- Monitoring and managing the risk of human error or bias in the system.
- Testing to ensure that AI results reflect the original objective.
- Ensuring sufficient transparency in AI technologies given the complexity involved.
- Verifying AI output is being used legally, ethically, and responsibly.

The Black Box Factor

The term "black box" generally refers to a complicated electronic device whose internal workings are not visible to or understood by the user. Anticipating generative AI and other advanced systems, the framework notes that, as organizations implement new AI technologies, using machines or platforms that can learn on their own or communicate with each other, the workings of the algorithms become less transparent or understandable. The black box factor will become more and more of a challenge as an organization's AI activities become more sophisticated. Advancements in AI since the framework was first published certainly validate and underscore that point and all of the observations about 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.

ETHICAL CONSIDERATIONS

Ensuring AI Systems Remain True

Internal Audit Must Remain Vigilant

The framework establishes that internal audit should ensure the organization 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 organization'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 new technologies also raise questions about their potential to take work away from humans. AI is not going to replace internal auditors, but it may have the potential to replace those who don't use AI and drive its value, Wilson believes. With that in mind, he urges auditors to get to know existing and emerging AI technologies. AI has languished on many organizations' risk profiles for a while, but many have postponed action due to lack of understanding or available expertise. He urges internal auditors to get ahead of the process by getting their feet wet. "Jump in and accept it as part of the culture," he advises.

Internal auditors are well-equipped to use their experience in assessing risks and opportunities that may impact an organization's ability to meet its objectives. The framework cites several critical activities for internal auditors related to AI:

- In any organization, internal audit should include AI in its risk assessment and consider including it in its risk-based audit plan. The numerous risks associated with AI include data breaches, plagiarism or copyright infringement in content created by generative AI tools, and model data poisoning, in which bad actors tamper with the data used to train large language models.
- For organizations exploring AI, internal audit should be engaged from the outset in AI projects, offering advice and insights for successful implementation. Keep in mind that, to avoid impairment of independence or objectivity, internal audit should not own, nor be responsible for, the implementation of AI processes, policies, or procedures.
- In companies that have partially implemented AI, either within their operations or in a product or service, internal audit should provide assurance on how risks relate to the reliability of the underlying algorithms and the data on which they are based are managed.
- Internal audit should ensure that steps are being taken to address the moral and ethical issues surrounding the organization's use of AI.
- Internal audit can also provide assurance on proper governance structures related to AI use.

CONCLUSION

In summing up internal audit's role, the framework concluded that "internal auditing should approach AI as it approaches everything — with systematic, disciplined methods to evaluate and improve the effectiveness of risk management, control, and governance processes related to AI." The 2017 framework was ahead of its time, according to Wilson. It still stands as a valuable resource for internal auditors moving forward into a rapidly and constantly changing AI environment.

PART III: INTERNAL AUDIT'S ROLE IN AI ETHICS

About the Experts

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 organizations 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 issues have prompted some to recommend a hiatus or slowdown in further development.[20] But despite calls for temporary halts, many organizations are ramping up AI use or planning to do so. Internal auditors will clearly have an important assurance and advisory role as organizations wrestle with AI choices and their implications.

Previous briefs in this series have focused on what internal auditors need to understand about AI and have revisited a landmark publication on the topic, The Institute of Internal Auditors' (IIA) *Artificial Intelligence – Considerations for the Profession of Internal Auditing*. Although it was published in 2017, this framework generally remains relevant and useful in most internal audit areas. "Internal audit can help an organization evaluate, understand, and communicate the degree to which artificial intelligence will have an effect (negative or positive) on the organization's ability to create value in the short, medium, or long term," according to the framework[21].

This third and final brief in the AI series addresses the ethical issues surrounding this multifaceted technology and what those issues mean to organizations and internal auditors. This brief also includes recommendations and insights from management and internal auditors already working on the frontlines of AI use.

[20] https://futureoflife.org/open-letter/pause-giant-ai-experiments/

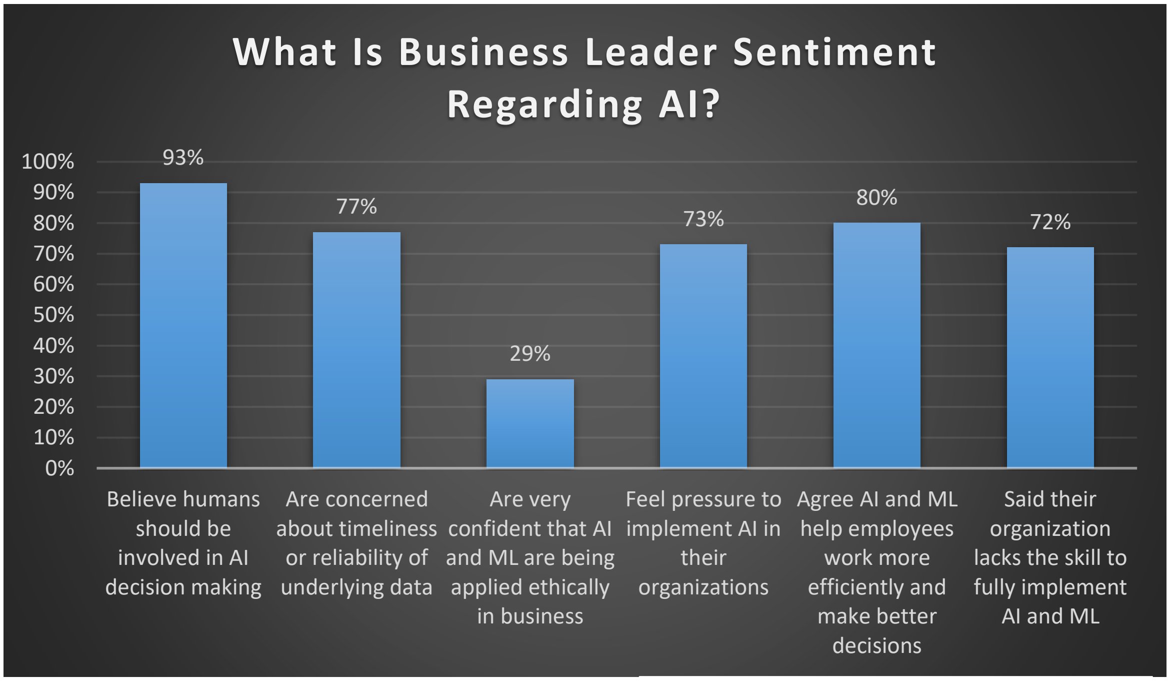
[21] *Artificial Intelligence - Considerations for the Profession of Internal Auditing, Special Edition*, The Institute of Internal Auditors, 2017.

Risks and Opportunities

Internal Audit's Role as Adviser

Excitement Over AI Could Overshadow Ethical Considerations

The global artificial AI market size was valued at $136.55 billion last year and was expected to grow by a 37% compound annual growth rate from 2023 to 2030, according to Grand View Research, Inc.[22] This surge in interest, and the excitement and hype surrounding technologies such as generative AI, have spurred many software developers and organizations to rush ahead in their AI research or efforts. However, amid rapid advancements, many serious and distinct risks, including ethical and performance issues, may be overlooked. Internal auditors are well positioned to alert their organizations to these issues and to offer advice on the efficacy of current controls and the need for enhanced controls or guardrails. Indeed, the Partnership on AI, led by Google executives, published a paper that calls for internal audit to play a leading role in providing assurance over the processes involved in AI creation and deployment and ensuring they meet ethical expectations and standards.[23]



Source: Workday Survey, June 2023.

With that in mind, it's important for organizations and internal auditors to understand AI's risks and limitations, and what impact they might have on a business's use of AI. "There's a misconception that AI is really smart," said Andrew Clark, co-founder and CTO,

[22] *Artificial Intelligence Market Size, Share & Trends Analysis Report By Solution, By Technology (Deep Learning, Machine Learning), By End-use, By Region, And Segment Forecasts, 2023 – 2030*, Grand View Research, Inc., June 2023.

[23] "Closing the AI Accountability Gap: Defining an End-to-End Framework for Internal Algorithmic Auditing," The Partnership on AI, January 2020.

Monitaur, an AI governance software company. Unfortunately, generative AI, which is receiving much of the current focus among the media and organizations, is only as smart as the data that it has been trained on and, at least in the technology's early stages, that training may include random social media posts, web content, and other material that has not been authenticated.

Use of public generative AI programs can expose private or confidential company, customer, or business partner data. And because generative AI is so easy to use, these capabilities are accessible to everyone from veteran cybercriminals to amateur hackers. While cybersecurity efforts can mitigate some of the potential damage these efforts can cause, awareness of the elevated risk, from organizational level to the individual employee, is essential for proper cybersecurity.

Generative AI can also incorporate intentional or unconscious biases. When a regulatory organization works to identify problematic activity, for example, there are ethical and legal considerations about whether the data approaches being used might be biased against certain members or types of trading activity, noted Ellen Taylor-Lubrano, machine learning team lead--regulatory, Cboe Global Markets. On another front, researchers have found high error rates in using AI facial recognition systems to identify people of color, women, and young people, making misidentification more likely and increasing the chances for people to be wrongly accused of crimes. AI may also be subject to knowledge gaps and inaccuracies. For example, while AI systems can be trained to detect illnesses, they may not recognize a disease such as melanoma in someone with skin characteristics that were not included in its original data set.[24]

Current generative AI models also are not transparent about their sources, so without knowing the origins of the information it generates, users may expose themselves to legal, copyright, and intellectual property risks. Equally alarming, it may produce "facts" that the system has made up (called hallucinations) when trying to respond to a prompt. Generative AI, "is meant to mimic a human, not to be correct," Clark said. Internal auditors can advise organizations on the best ways to address such errors or omissions or their unintended consequences.

The user friendliness of generative AI can be another risk for organizations. In the past, models were typically built by people with advanced degrees or knowledge of systems who had expertise in automating those models, Clark said. Today, it's possible for people with little or no understanding of models, systems, or the data they are using to leverage a tool such as generative AI and ask it to make a prediction or a decision using information that may be incomplete or lacks proper context.

In addition to monitoring potential concerns with internal use of AI, organizations should also consider external threats. The same models behind technologies such as ChatGPT can be used to create tools that can produce malicious software and code, scam pages, and phishing emails. They can also be used to identify organizational vulnerabilities, as well as train new types of cybercrime tools, among other functions.[25] What's more, AI could make it easier for hackers to develop malware that can steal data or exert control over it.

While these threats may sound daunting, there are also risks in failing to embrace AI. If others surge ahead in AI use, an organization may be perceived as less tech-oriented or future-focused by current or potential customers or talent, giving competitors an advantage. AI also offers tangible benefits that can enable companies to streamline and enhance processes, thereby boosting productivity, improving customer service, minimizing costs, and potentially opening new service, market, or product opportunities. In addition, in many situations AI can help organizations identify risks or threats or spot new opportunities. AI may offer organizations access to a huge internal knowledge base faster and more efficiently than a straight search would do, according to Tim Lipscomb, senior vice president and chief technology officer at Cboe Global Markets. If an organization is using a manual information-gathering process, it may not be able to make the best decisions or respond to threats or opportunities as would be the case if it were using AI.

[24] "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification," Joy Buolamwini and Timnit Gebru, *Conference on Fairness, Accountability and Transparency*, 2018.

[25] "Surge in Generative AI Tools for Cybercrime Sparks Concerns," GRC Report, August 10, 2023.

Turn to Fundamental Auditing Concepts

Adapting Three Lines and Other Existing Models

Using Fundamental Assurance Approaches for New Technology

While a technology may be new, many of the details of putting it to work may not be. For example, decision models and machine learning have long been used in the financial sector, noted Jim Enstrom, senior vice president and chief audit executive, Cboe Global Markets. (See the sidebar on "Minding Your Model Risk Management" on page 7.) IT auditors have had to address a myriad of risks, including ethical uses in the past, and AI is no different in this regard. It is critical, therefore, to ensure internal audit has a seat at the table to understand the strategic use of AI within the organization.

If we view AI systems through the lens of software development processes, internal auditors can go back to fundamental concepts, Enstrom said. Traceability, for example, should be a consideration if the AI system will be making decisions or working autonomously, while auditability will also be key. Just as internal auditors work with teams across their organizations to understand their work, the internal audit team will also have to work with engineers, data scientists, and programmers to understand what the systems are doing, the sources of data used as inputs, what requirements were used to build the model, and what artifacts can be used to defend decisions the model makes. "We have to think about new ideas for auditing AI, fueled by agile and iterative approaches, and working collaboratively with the first and second lines. Yet we also have a clear opportunity to leverage existing tools, methodologies, and approaches as a starting point," he said.

Taylor-Lubrano notes that because organizations have long used statistical models, they can regard machine learning and other examples of AI as a new version of those models. If approaches to ethical issues or other risks that were used in the past are no longer adequate, organizations will have to rethink their approaches. "We have a nice opportunity to add ethics to the debate now that AI has put a spotlight on it," Enstrom added.

That includes applying existing review criteria to AI systems. Because his organization is currently using AI as an assistive technology, with humans reviewing output, "we're treating AI essentially as a vendor," said Lipscomb. "We go through the appropriate vender onboarding processes and control structures around that, then we would expect a third-line review of the process."

The Three Lines Model

Under the IIA's Three Lines Model[26], effective risk management starts at the top, with management, as the first line, as risk owners and further clarifies roles, including those of the board. This governance framework can serve as a tool to help a company consider how to navigate opportunities and risks presented by AI. "We use it as part of our governance framework," Enstrom said. Among other things, it can aid in understanding roles and responsibilities for AI, including board oversight. As the independent, objective third line, internal audit reports to the audit committee, but can also offer perspective to the full board on ethics and other concerns. It can also advise on how changes driven by AI might alter the organization's risk profile.

The Three Lines Model can also help organizations recognize the necessity for each line to assess and monitor risk within its own purview, Enstrom noted. If AI is being used autonomously without rigorous human review of its output or decision making, the risk might be high, which may mean that management should implement enhanced quality assurance procedures or other controls within

[26] *The IIA's Three Lines Model: An Update of the Three Lines of Defense*, The Institute of Internal Auditors, 2020.

the first line. For the second line, chief risk or compliance officers may need to determine how best to establish adequate assurance and control, which would also be a consideration for internal audit's assurance role, as the third line. In light of any new changes, internal audit could also raise questions on how autonomous technology is being rolled out, if it is a priority on the board's agenda, and how it may be managed going forward.

The bottom line is that no matter how many changes AI may drive, "we have an opportunity to add value by positioning internal audit as a key element of the AI governance framework, leveraging our knowledge and experience around controls, and what we know as a profession; this all carries forward," Enstrom said.

Minding Model Risk Management

Model risk management addresses the risks that may result when decisions are made using models that are incorrect or improperly used. The goal of model risk management is to identify, measure, and mitigate or prevent the use of inaccurate data, assumptions, methodologies, processes, or interpretations. The banking sector has well established model risk management paradigms that are used to monitor models for credit, finance, and marketing activities, Clark noted. (See OCC 2011-12, Supervisory Guidance on Model Risk Management, from the Office of the Comptroller of the Currency.) As an Office of the Comptroller handbook on the topic notes, "sound model governance includes board and management oversight, policies and procedures, a system of internal controls, internal audit, a model inventory, and documentation."[27] Organizations can leverage these recommendations aimed at the banking industry, Clark advised, and avoid having to build their own risk model management systems from scratch. Effective model risk management is one factor in speeding adoption of AI and machine learning, "by creating stakeholder trust and accountability through proper governance and risk management," according to EY.[28]

[27] *Safety and Soundness: Model Risk Management*, Version 1.0, Comptroller's Handbook, Office of the Comptroller of the Currency, August 2021.

[28] "Understand Model Risk Management for AI and Machine Learning," Gagan Agarwala, et al., May 13, 2020, EY.

Understanding AI Privacy and Accountability Considerations

In addition to understanding the AI implications for their organizations, internal auditors will also have to consider how best to use generative AI and other tools in their own audits, and what kinds of privacy risks to consider. For example, in working with generative AI, "it is essential to ensure that the data entered into ChatGPT is anonymized and that sensitive information is not shared or stored on the platform," according to an Internal Auditor article[29]. "Additionally, internal auditors need to ensure they have the appropriate consent and authorization to use the data in ChatGPT." The article details how internal auditors can use AI in planning, testing, reporting, and monitoring, and underscores the importance of leveraging the capabilities of tools such as ChatGPT while protecting the confidentiality and privacy of sensitive data.

Key Questions to Consider

Clark recommends that organizations develop a strategic understanding of what AI does or can mean to them. Internal audit can recommend that organizations address issues such as:

- Where and how is AI being used?
- What is the company trying to model? What is the purpose of that model?
- Are there solutions other than machine learning tools that can help us reach our goals?
- What risks are involved?
- How is or should the organization be automating decision making with models?
- Are there adequate monitors and risk management controls around AI?
- Is there a second line function dedicated to model risk management? If so, are there existing model-risk-management systems that can be used with AI tools?
- How does AI affect the audit scope and process?

Organizations should be certain to address ethical issues if an algorithm is being used in a process that makes consequential decisions about people. When that is the case, they should ask:

- Are there protections or laws in place? If so, how can the organization ensure that processes using AI are complying.
- If there are no external compliance considerations, are there still steps that should be followed to ensure the company is doing the right thing, according to its own values?

Internal audit can treat these considerations with the same care as external mandates, making sure there is a process to monitor and validate compliance and reporting on related compliance concerns.

[29] "On the Frontlines: AI in 'IA,'" Alex Rusate, *Internal Auditor*, May 17, 2023.

Conclusion

Because of weighty ethical issues related to AI, Clark advises that organizations that are not confident in the outcomes that the systems may produce should take a step back before implementing them. Instead, he recommends tackling AI initially as a research and development (R&D) project, giving the company a chance to explore how the technology fits its needs and identify potential risks.

Digital transformation is exciting, but internal auditors should keep a clear-eyed view of any technology's risks and limitations and focus on providing relevant advice and assurance. Amid the hype surrounding any new technology, "we need to be the ones asking which business problems it will actually solve and which data privacy issues and other risks may be involved," Clark said.

About The IIA

The Institute of Internal Auditors (IIA) is a nonprofit international professional association that serves more than 235,000 global members and has awarded more than 190,000 Certified Internal Auditor (CIA) certifications worldwide. Established in 1941, The IIA is recognized throughout the world as the internal audit profession's leader in standards, certifications, education, research, and technical guidance. For more information, visit theiia.org.

Disclaimer

In Part III: Internal Audit's Role in AI Ethics, the views and opinions expressed are offered by the experts in their personal capacities and do not reflect the views and opinions of Cboe Global Markets, Inc., and its subsidiaries.

The IIA publishes this document for informational and educational purposes only. This material is not intended to provide definitive answers to specific individual circumstances and as such is only intended to be used as peer-informed thought leadership. It is not formal IIA Guidance. The IIA recommends seeking independent expert advice relating directly to any specific situation. The IIA accepts no responsibility for anyone placing sole reliance on this material.

Global Knowledge Briefs are intended to address topics that are timely and relevant to a global internal audit audience, and each topic covered is vetted by members of The IIA's volunteer North American Content Advisory Committee. Subject-matter experts are primarily identified and selected from The IIA's list of Global Guidance Contributors.

To apply to be added to the Global Guidance Contributors list, email Standards@theiia.org. To suggest topics for future Global Knowledge Briefs, email Content@theiia.org.

Copyright

November 2023

The Institute of Internal Auditors®

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101