GLOBAL KNOWLEDGE BRIEF

The Artificial Intelligence Revolution

Part 2: Revisiting The IIA's Artificial Intelligence Framework

The Institute of Internal Auditors

Contents

INTRODUCTION **3**

KEY COMPONENTS **4**

Building Strategies on Capabilities, Risk, Opportunities 4

THE SIX COMPONENTS **5**

AI Governance 5

Data Architecture and Infrastructure 5

Data Quality 7

Measuring Performance of AI 7

The Human Factor 7

The Black Box Factor 8

ETHICAL CONSIDERATIONS **9**

Internal Audit Must Remain Vigilant 9

INTERNAL AUDIT'S ROLE **10**

Picking Up the Assurance Challenge 10

CONCLUSION **11**

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."[1]

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.

[1] "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.[2]

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.

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.[3] Human error and biases (both intentional and unintentional) will have an impact on 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:

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

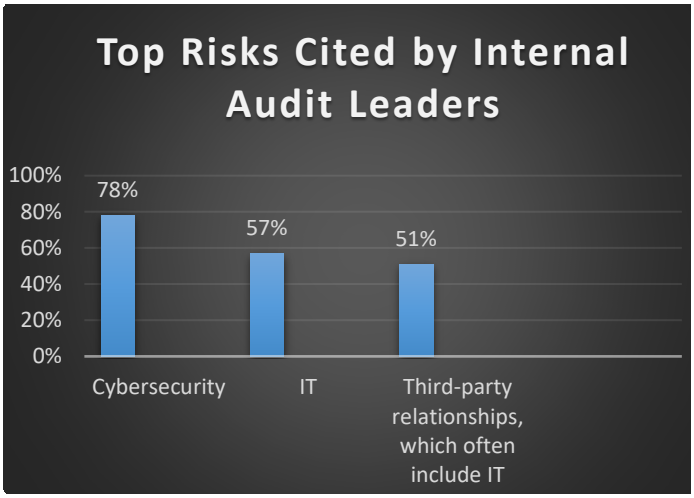
- Monitoring and managing the risk of human error or bias in the system.
- Testing to ensure that AI results reflect the original objective.
- Ensuring sufficient transparency in AI technologies given the complexity involved.
- Verifying AI output is being used legally, ethically, and responsibly.

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.

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

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

August 2023

December 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