GLOBAL PERSPECTIVES AND INSIGHTS

Artificial Intelligence – Considerations for the Profession of Internal Auditing

Special Edition

The Institute of Internal Auditors | Global

About The IIA

The Institute of Internal Auditors (IIA) is the internal audit profession's most widely recognized advocate, educator, and provider of standards, guidance, and certifications. Established in 1941, The IIA today serves more than 190,000 members from more than 170 countries and territories. The association's global headquarters are in Lake Mary, Fla., USA. For more information, visit www.globaliia.org.

Reader Feedback

Send questions or comments to globalperspectives@theiia.org.

Previous Issues

Previous issues of Global Perspectives and Insights on a variety of topics can be found at www.theiia.org/gpi.

Disclaimer

The opinions expressed in Global Perspectives and Insights are not necessarily those of the individual contributors or of the contributors' employers.

Copyright

Copyright © 2017 by The Institute of Internal Auditors, Inc. All rights reserved.

Contents

Artificial Intelligence

Considerations for the Profession of Internal Auditing

Introduction

Artificial intelligence (AI) is a broad term that refers to technologies that make machines "smart." Organizations are investing in AI research and applications to automate, augment, or replicate human intelligence — human analytical and/or decision-making — and the internal auditing profession must be prepared to fully participate in organizational AI initiatives.

There are many other terms related to AI, such as, deep learning, machine learning, image recognition, natural-language processing, cognitive computing, intelligence amplification, cognitive augmentation, machine augmented intelligence, and augmented intelligence. AI, as used here, encompasses all of these concepts.

Putting AI Into Context

AI is not new. According to the McKinsey Global Institute's (MGI) discussion paper "Artificial Intelligence: The Next Digital Frontier," the idea of AI dates back to 1950 when Alan Turing first proposed that a machine could communicate well enough to convince a human evaluator that it, too, was human.

While AI represents a series of significant advancements in technology, it was not the first, and likely will not be the last. Looking back over the last few decades, the advent of computers, PCs, spreadsheets, relational databases, sophisticated connectivity, and similar technological advancements have all impacted how organizations operate and accomplish their objectives. AI is poised to do the same with the potential to be as or more disruptive than many previous technological advances.

AI can be viewed as the latest significant advancement on a continuum of advancements that have occurred due to technology improvements. What *is* new is the advancement and scalability of technologies that have unleashed the practical application of AI.

This application was demonstrated publicly to a wide audience in 2011 when IBM's AI platform Watson won a Jeopardy! exhibition on prime time TV. According to IBM Research, IBM is "guided by the term 'augmented intelligence' rather than 'artificial intelligence,'" and focuses "on building practical AI applications that assist people with well-defined tasks." Human expertise develops technologies to make machines smart, and smart machines, in turn, augment human capabilities.

There is already widespread application of AI across diverse sectors (publicly held, privately held, government, and nonprofit) and industries. Consider, for example, that AI enables a number of new and novel capabilities that were impossible just a few years ago:

- Automobile manufacturers to develop self-driving vehicles.
- Online search engines to deliver targeted search results.
- Social media organizations to recognize faces in photographs and filter newsfeeds.
- Media companies to recommend books or shows to subscribers.
- Retailers to create customized online experiences for shoppers.
- Logistics companies to route optimal paths for deliveries.
- Governments to predict epidemics.
- Marketing professionals to deliver hyper-personalized content to customers in real time.
- Virtual assistants to use voice-controlled natural language to interface with consumers.

But it is not only new and novel activities affected by AI. More mundane tasks that have been occurring for decades are being improved by AI such as loss modeling, credit analysis, valuations, transaction processing, and a host of others.

It is critical that internal auditors pay attention to the practical application of AI in business, and develop competencies that will enable the internal auditing profession to provide AI-related advisory and assurance services to organizations in all sectors and across all industries.

AI is dependent on big data and algorithms, and it can be intimidating, especially for internal audit activities and organizations that have yet to master big data. But internal auditors do not have to be data scientists or quantitative analysts to understand what AI can do for organizations, governments, and societies at large.

This paper:

- Presents an overview of AI basics.
- Explores internal audit's roles in AI.
- Discusses AI risks and opportunities.
- Introduces a framework for internal auditors (the Framework).

This paper is Part I of a three-part series. Parts II and III will provide more detailed information on and practical application of the Framework.

AUDIT FOCUS

IIA Standard 1210: Proficiency (Excerpt)

Internal auditors must possess the knowledge, skills, and other competencies needed to perform their individual responsibilities. The internal audit activity collectively must possess or obtain the knowledge, skills, and other competencies needed to perform its responsibilities.

1210.A3 – Internal auditors must have sufficient knowledge of key information technology risks and controls and available technology-based audit techniques to perform their assigned work. However, not all internal auditors are expected to have the expertise of an internal auditor whose primary responsibility is information technology auditing.

AI – The Basics

Big Data and Algorithms

AI is powered by algorithms, and algorithms are fueled by big data, so before an organization embarks on AI, it should have a strong foundation in big data. And before internal audit can think about addressing AI, it should already have a strong foundation in big data. For comprehensive guidance on understanding and auditing big data, including a discussion of opportunities and risks, and a sample work program, see The IIA's "GTAG: Understanding and Auditing Big Data," available free to IIA members and available to non-members through The IIA Bookstore (*www.theiia.org*).

Big data means more than just large amounts of data — big data refers to data (information) that reaches such high volume, variety, velocity, and variability that organizations invest in system architectures, tools, and practices specifically designed to handle the data. Much of this data may be generated by the organization itself, while other data may be publicly available or purchased from external sources.

To put big data to good use, organizations develop algorithms. An algorithm is a set of rules for the machine to follow. An algorithm is what enables a machine to quickly process vast amounts of data that a human cannot reasonably process, or even comprehend. The performance and accuracy of algorithms is very important. Algorithms are initially developed by humans, so human error and biases (both intentional and unintentional) will impact the performance of the algorithm. Faulty algorithms can produce minor undesirable glitches in an organization's operations, or major catastrophic outcomes. It is generally recognized that flawed algorithms, at least in part, fueled the 2008 global financial crisis.

Types of AI

In *The Conversation's* "Understanding the four types of AI, from reactive robots to self-aware beings," Arend Hintze, assistant professor of Integrative Biology & Computer Science and Engineering at Michigan State University, outlines four types of AI:

Type I. Reactive machines: This is AI at its simplest. Reactive machines respond to the same

situation in exactly the same way, every time. An example of this is a machine that can beat world-class chess players because it has been programmed to recognize the chess pieces, know how each moves, and can predict the next move of both players.

Type II. Limited memory: Limited memory AI machines can look to the past, but the memories are not saved. Limited memory machines cannot build memories or "learn" from past experiences. An example is a self-driving vehicle that can decide to change lanes because a moment ago it noted an obstacle in its path.

Type III. Theory of mind: Theory of mind refers to the idea that a machine could recognize that others it interacts with have thoughts, feelings, and expectations. A machine embedded with Type III AI would be able to understand others' thoughts, feelings, and expectations, and be able to adjust its own behavior accordingly.

Type IV. Self-awareness: A machine embedded with Type IV AI would be self-aware. An extension of "theory of mind," a conscious or self-aware machine would be aware of itself, know about its internal states, and be able to predict the feelings of others.

In other words, a Type II self-driving vehicle would decide to change lanes when a pedestrian is in its path, simply because it recognizes the pedestrian as an obstacle. A Type III self-driving vehicle would understand that the pedestrian would expect the vehicle to stop, and a Type IV self-driving vehicle would *know* that it should stop because that is what the self-driving vehicle would want if it (the self-driving vehicle) were in the path of another oncoming vehicle. Wow.

Most "smart machines" today are manifestations of Type I or Type II AI. Ongoing research and development initiatives will enable organizations to advance toward practical applications of Type III and Type IV AI.

AI Opportunities and Risks

The first step toward understanding the organization's AI opportunities and risks is to thoroughly understand the organization's big data opportunities and risks. Again, for comprehensive guidance on understanding and auditing big data, including a discussion of opportunities and risks, and a sample work program, see The IIA's "GTAG: Understanding and Auditing Big Data," available free to IIA members and available to non-members through The IIA Bookstore (*www.theiia.org*).

Examples of AI opportunities and risks include:

Opportunities

- The ability to compress the data processing cycle.
- The ability to reduce errors by replacing human actions with perfectly repeatable machine actions.
- The ability to replace time-intensive activities with time-efficient activities (process automation), reducing labor time and costs.
- The ability to have robots or drones replace humans in potentially dangerous situations.
- The ability to make better predictions, for everything from predicting sales of certain goods in particular markets to predicting epidemics and natural catastrophes.
- The ability to drive revenue and grow market share through AI initiatives.

Risks

- The risk that unidentified human biases will be imbedded in the AI technology.
- The risk that human logic errors will be imbedded in the AI technology.
- The risk that inadequate testing and oversight of AI results in ethically questionable results.
- The risk that AI products and services will cause harm, resulting in financial and/or reputational damage.
- The risks that customers or other stakeholders will not accept or adopt the organization's AI initiatives.

- The risk that the organization will be left behind by competitors if it does *not* invest in AI.
- The risk that investment in AI (infrastructure, research and development, and talent acquisition) will not yield an acceptable ROI.

More in-depth information on AI risks will be presented in Parts II and III of this three-part Global Perspectives and Insights series, which will provide recommendations on leveraging the Framework to provide AI-related assurance and advisory services.

Internal Audit's Role

Internal audit is adept at evaluating and understanding the risks and opportunities related to the ability of an organization to meet its objectives. Leveraging this 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. Internal audit can engage through at least five critical and distinct activities related to artificial intelligence:

- For all organizations, internal audit should include AI in its risk assessment and consider whether to include AI in its risk-based audit plan.
- For organizations exploring AI, internal audit should be actively involved in AI projects from their beginnings, providing advice and insight contributing to successful implementation. However, to avoid the perception of or actual impairments to both independence and objectivity, internal audit should not own, nor be responsible for, the implementation of AI processes, policies, or procedures.
- For organizations that have implemented some aspect of AI, either within its operations (such as a manufacturer using robotics on a production line) or incorporated into a product or service (such as a retailer customizing product offerings based on purchase history), internal audit should provide assurance on management of risks related to the reliability of the underlying algorithms and the data on which the algorithms are based.

AUDIT FOCUS

IIA Standard 2120: Risk Management (Excerpt)

The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes.

2120.A1 – The internal audit activity must evaluate risk exposures relating to the organization's governance, operations, and information systems regarding the:

- Achievement of the organization's objectives.
- Reliability and integrity of financial and operational information.
- Effectiveness and efficiency of operations and programs.
- Safeguarding of assets.
- Compliance with laws, regulations, policies, procedures, and contracts.

- Internal audit should ensure the moral and ethical issues that may surround the organization's use of AI are being addressed.
- Like the use of any other major system, proper governance structures need to be established and internal audit can provide assurance in this space.

Regardless of the specific activities performed, internal audit is well-suited to be a key contributor to an organization's AI-related activities. Internal audit:

- Understands the strategic objectives of the organization, and the processes implemented to achieve those objectives.
- Is able to evaluate whether AI activities are accomplishing their objectives.
- Can provide internal assurance over management's risk management activities relevant to AI risks.
- Is perceived as a trusted advisor that can positively support the adoption of AI to improve business processes or enhance product and service offerings.

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.

AI Competencies: Filling the Understanding Gap

The pool of talent for technology professionals with AI expertise is reportedly small. Organizations who want to participate in the AI revolution need to grow or acquire talent with competencies in a multitude of areas such as:

- Natural language processing.
- Application program interfaces (APIs) such as facial recognition, image analytics, and text analytics.
- Algorithms and advanced modeling.
- Probabilities and applied statistics.
- Data analytics.
- Software engineering.
- Programming language.
- Machine learning.
- Computer vision.
- Robotics.

While a handful of organizations in the technology, automotive, manufacturing, financial services, and utilities industries seem to be leading the AI revolution, it is hard to imagine an organization that will not be impacted by AI. Just as computers, spreadsheets, and distributed processing were a focus of select industries in their early stages, ultimately all organizations adopted aspects of these technologies. As AI becomes more mainstream, it is hard to imagine any internal audit activity that will not need to be ready to provide its organization with AI-related assurance and advisory services.

How can CAEs upskill the internal audit activity to be ready for the challenge? The first step is recognizing that new skillsets are required. Collectively, the internal audit activity must have a sufficient understanding of AI, how the organization is using it, and the risks that AI represents to the organization. The CAE must be able to communicate this understanding to senior management, the board, and the audit committee. A good place to start is with The IIA's thought leadership on AI, and The IIA's supplemental guidance on topics like big data and talent management.

Reemphasizing Cyber Resilience

Cybersecurity threats continue to define our times. The adoption and evolution of AI will force organizations to reemphasize their cyber resilience capabilities. As AI becomes more powerful and more decisions are handed off to new, complicated, and opaque algorithms, using huge data sets, protecting these systems from outside, malevolent forces is critical to success. A 2014 EY report defined cyber resilience as the ability to resist, react to, and recover from cyberattacks — and modify an environment to increase security and sustainability over time. Cyber resiliency is critical for any organization relying increasingly on AI.

Among all the complexity surrounding cybersecurity, there are four key areas where internal audit can have an immediate impact:

- Provide assurance over readiness and response to cyber threats.
- Communicate to executive management and the board the level of risk to the organization and efforts to address such risks.
- Work collaboratively with IT and other parties to ensure effective defenses and responses are in place.
- Facilitate communication and coordination among all parties in the organization regarding the risk.

The potentially disastrous effects of a cybersecurity breach involving AI cannot be overstated. If not already in place, CAEs need to rapidly build cybersecurity within their teams.

AI Auditing Framework

The Framework is comprised of six components, all set within the context of an organization's AI strategy.

Strategy

Each organization's AI strategy will be unique based on its approach to capitalizing on the opportunities AI provides. An organization's AI strategy might be an

obvious extension of the organization's overall digital or big data strategy — organizations with a well-developed and implemented digital/big-data strategy are one step ahead in AI. According to MGI, organizations that "combine strong digital capability, robust AI adoption, and a proactive strategy see outsize financial performance."

Internal audit must consider an organization's AI strategy first. Does the organization have a defined strategy toward AI? Is it investing in AI research and development? Does it have plans in place to identify and address AI threats and opportunities? AI can become a competitive advantage for organizations, and internal audit should help management and the board realize the importance of formulating a *deliberate* AI strategy consistent with the organization's objectives.

Components

AI Governance

AI governance refers to the structures, processes, and procedures implemented to direct, manage, and monitor the AI activities of the organization in pursuit of achieving the organization's objectives. The level of formality and structure for an organization's AI governance will vary based on the specific characteristics of that organization. Regardless of the specific approach, however, AI governance establishes accountability and oversight, helps to ensure that those responsible have the necessary skills and expertise to effectively monitor AI, and helps to ensure the organization's values are reflected in its AI activities. This last point should not be overlooked or given little attention. AI activities must result in decisions and actions that are in line with the ethical, social, and legal responsibilities of the organization.

Data Architecture and Infrastructure

AI data architecture and infrastructure will likely be one in the same as the organization's architecture and infrastructure for handling big data. It includes considerations for:

- The way that data is accessible (metadata, taxonomy, unique identifiers, and naming conventions).
- Information privacy and security throughout the data lifecycle (data collection, use, storage, and destruction).
- Roles and responsibilities for data ownership and use throughout the data lifecycle.

Data Quality

The completeness, accuracy, and reliability of the data on which AI algorithms are built are critical. Unfortunately, it is not unusual for organizations to have a poorly defined, incoherent structure to their data. Often, systems do not communicate with each other or do so through complicated add-ons or customizations. How this data is brought together, synthesized, and validated is crucial.

Measuring Performance of AI

As organizations integrate AI into their activities, performance metrics should be defined to tie AI activities to business objectives and clearly illustrate whether AI is effectively supporting the achievement of those objectives. Management must actively monitor the performance of its AI activities.

The Human Factor

Algorithms are developed by humans. Human error and biases (both intentional and unintentional) will impact the performance of the algorithm. The human factor component considers whether:

- The risk of unintended human biases factored into AI design is identified and managed.
- AI has been effectively tested to ensure that results reflect the original objective.
- AI technologies can be transparent given the complexity involved.
- AI output is being used legally, ethically, and responsibly.

It is widely recognized that human error is the most common cause of information privacy and security breaches. Similarly, the human factor component addresses the risk of human error compromising the ability of AI to deliver the expected results.

The Black Box Factor

According to the *Merriam-Webster* online dictionary, a black box is "a usually complicated electronic device whose internal mechanism is usually hidden from or mysterious to the user; *broadly*: anything that has mysterious or unknown internal functions or mechanisms."

As organizations advance to implementing Type III and Type IV AI technologies — utilizing machines or platforms that can learn on their own or communicate with each other — how the algorithms are operating becomes 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.

Closing Thoughts

The internal auditing profession cannot be left behind in what may be the next digital frontier — artificial intelligence. To prepare, internal auditors must understand AI basics, the roles that internal audit can and should play, and AI risks and opportunities. To meet these challenges, internal auditors should leverage the Framework to deliver systematic, disciplined methods to evaluate and improve the effectiveness of risk management, control, and governance processes related to AI.

This paper is Part I of a three-part series. Part II will provide more detailed information and recommendations regarding the AI Governance; Data Architecture and Infrastructure; and Data Quality components of the Framework. Part III will provide more detailed information and recommendations regarding the Measuring Performance, Human Factor, and the Black Box Factor components of the Framework. Parts II and III will include relevant engagement objectives and procedures which internal audit activities can use to customize an AI audit program to fit their organizations' risk profile and strategic objectives.

AUDIT FOCUS

Key IIA Standards

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

- 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 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

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