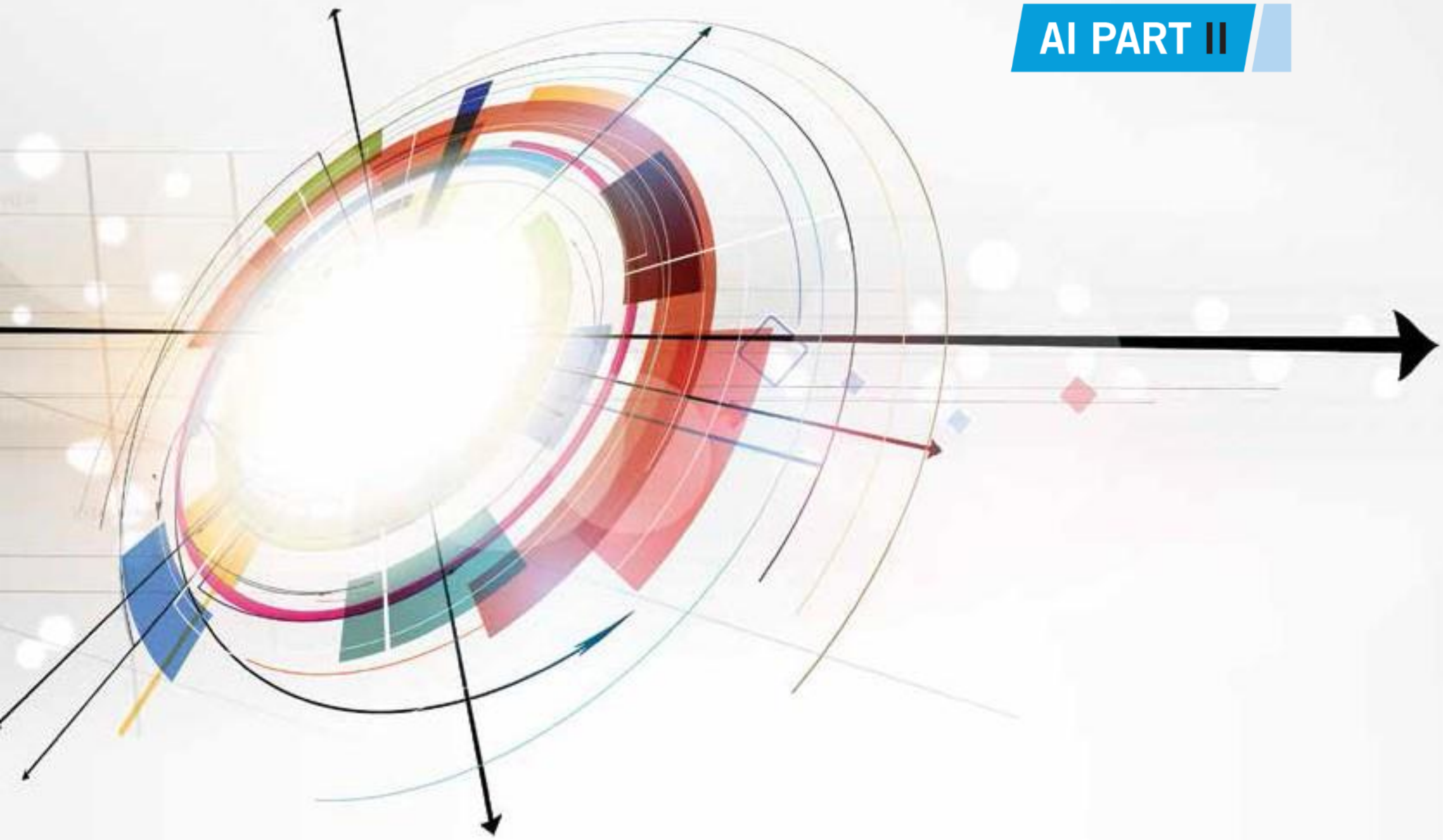
AI PART II



GLOBAL PERSPECTIVES AND INSIGHTS

The IIA's Artificial Intelligence Auditing Framework

Practical Applications, Part A

Special Edition

The Institute of Internal Auditors | Global

Table of Contents

Advisory Council

Previous Issues

To access previous issues of Global Perspectives and Insights, visit www.theiia.org/gpi.

Reader Feedback

Send questions or comments to globalperspectives@theiia.org.

Note: This is the second report in a three-part series. For more information, see the first report: Artificial Intelligence – Considerations for the Profession of Internal Auditing.

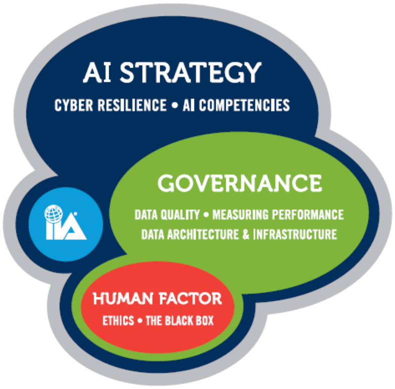
Introduction

A new Google project called AutoML is poised to take artificial intelligence (AI) — a broad term that refers to technologies that make machines "smart" — to another level. ML, short for machine learning, refers to computer algorithms that analyze data to learn to perform tasks. AutoML is a machine-learning algorithm that learns to build other machine-learning algorithms.

Google engineer Jeff Dean describes the project as a way for companies to build systems with AI even if they do not have extensive expertise. Only a few thousand companies today have the right talent for building AI, he estimates, but many more have the necessary data. "We want to go from thousands of organizations solving machine learning problems to millions," he told *The New York Times*.

Google is one of many organizations investing in AI research and applications to automate, augment, or replicate human intelligence — human analytical and/or decision-making. Following the creation path blazed by computer science, Microsoft recently unveiled a tool to help coders build "deep neural networks," a type of computer algorithm that eliminates "a lot of the heavy lifting," according to Joseph Sirosh, a vice president at Microsoft, in *The Times*. This focus on facilitating organizational AI initiatives means it is even more critical for the internal auditing profession to fully prepare for AI now.

There are many other terms related to AI besides machine learning, such as deep learning, image recognition, natural-language processing, cognitive computing, intelligence amplification, cognitive augmentation, machine augmented intelligence, and augmented intelligence. AI, as used in The IIA's AI Auditing Framework (Framework), encompasses all of these concepts.


AI STRATEGY
CYBER RESILIENCE • AI COMPETENCIES
GOVERNANCE
DATA QUALITY • MEASURING PERFORMANCE
DATA ARCHITECTURE & INFRASTRUCTURE
HUMAN FACTOR
ETHICS • THE BLACK BOX

The IIA's AI Auditing Framework

As explained in Artificial Intelligence – Considerations for the Profession of Internal Auditing, internal audit's role in AI is to "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."

To help internal audit fulfill this role, internal auditors can leverage The IIA's AI Auditing Framework in providing AI-related advisory, assurance, or blended advisory/assurance services as appropriate to the organization. The Framework comprises three overarching components — AI Strategy, Governance, and the Human Factor — and seven elements: Cyber Resilience; AI Competencies; Data Quality; Data Architecture & Infrastructure; Measuring Performance; Ethics; and The Black Box.

Internal audit should consider numerous engagement or control objectives, and activities or procedures in implementing the Framework and providing advisory, assurance, or blended advisory/assurance internal audit services related to the organization’s AI activities. Relevant objectives and activities or procedures that address the Strategy (Cyber Resilience and AI Competencies elements) and Governance (Data Architecture & Infrastructure, and Data Quality elements) of the Framework are provided in this document. Relevant objectives and activities or procedures that address Governance (Measuring Performance element) and the Human Factor (Ethics and The Black Box elements) will be provided in Part III of this three-part series.

AI Strategy

AI STRATEGY
GOVERNANCE
HUMAN FACTOR

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. The AI strategy should clearly articulate the intended result of AI activities. AI strategies should be developed collaboratively between the organization’s business leaders who can articulate the intended result of AI activities and how those results relate to the organization’s goals, and technology leaders who understand the organization’s AI technology capabilities, constraints, and aspirations. Both business leaders and technology professionals also need to be involved in managing the execution of the AI strategy.

AI is dependent on big data, so an organization’s big data strategy should be fully developed and implemented before it considers AI. Indeed, AI can help organizations capture insights from big data. As described in The IIA’s Global Technology Audit Guide: Understanding and Auditing Big Data, by using these insights, “the organization can make better decisions, target new customers in creative and differentiating ways, service existing customers with a targeted and improved delivery model unique to the individual, and offer new services and capabilities that truly distinguish the company from its competitors.” Organizations that capitalize on AI opportunities can develop a lasting competitive advantage, and the AI strategy should be developed and implemented against a backdrop of cyber resilience and AI competencies.

Before internal audit attempts to evaluate the organization’s AI strategy, it should determine its own strategy for covering AI by including the topic in its risk assessment and considering whether AI should be included in the risk-based audit plan.

Cyber Resilience

The organization’s ability to resist, react to, and recover from cyberattacks, including the intentional misuse of an organization’s AI technologies for nefarious means, is becoming increasingly important (see Facebook’s Corrective Actions on page 12). CAEs need to rapidly build cybersecurity competencies within their teams, continuously monitor AI/cybersecurity risks, and communicate to executive management and the board the level of risk to the organization and efforts to address such risk.

Relevant objectives and activities or procedures identified by The IIA do not comprise a prescribed audit plan, but are examples that should be useful in identifying engagement or control objectives, and in planning and performing AI audit engagements.

AI audit engagements should conform with IIA Standard 2200: Engagement Planning. AI audit plans and AI engagement objectives and procedures should always be customized to meet the needs of the organization.

AI Competencies

As noted in Artificial Intelligence – Considerations for the Profession of Internal Auditing, the pool of talent for technology professionals with AI expertise is reportedly small. Even if projects such as AutoML (see page 2) succeed, enabling organizations to build systems with AI even if they don't have extensive expertise, organizations will still need to fill a *knowledge* gap with staff who have a deep understanding of AI even if they cannot "do" AI. Staff need to:

- Know how AI works.
- Understand the risks and opportunities AI presents.
- Determine whether AI outcomes are as expected.
- Be capable of recommending or taking corrective action if needed.

Such competencies will be needed within internal audit and among the first and second lines of defense. Senior management and the board also should know how AI works and understand the risks and opportunities that AI presents.

Internal audit also should have the capability to determine if third-party providers of AI technologies are competent.

Relevant AI Strategy Objectives and Activities or Procedures

Engagement or Control Objective(s)	Activities or Procedures
Be actively involved in AI projects from their beginnings, providing advice and insight contributing to successful implementation.	**Attend** AI project team meetings.
The organization has a defined AI strategy.	**Determine** whether an AI strategy has been documented and if so, **verify** that the strategy: ■ Articulates the intended results of AI activities (strategic objectives). ■ Articulates at a high level how the AI objectives will be accomplished (strategic plan).
Provide assurance over the readiness and response to cyber threats.	**Leveraging** an established cybersecurity framework, **work** collaboratively with IT and other parties to ensure effective defenses and responses are in place.
There are sufficient resources (staff and budget) to implement the AI strategy.	**Review** process for determining staff and budget needs to support AI.
Advise on whether the strategy adequately considers AI threats and opportunities.	**Review** any existing assessments of AI threats and opportunities. If no assessments exist, **make recommendations** for moving forward (how the organization could plan to identify AI threats and opportunities).

Governance

AI governance refers to the structures, processes, and procedures implemented to direct, manage, and monitor the AI activities of the organization. Governance structure and formality will vary based on the specific characteristics of the organization. AI governance:

- Establishes accountability, responsibility, and oversight.
- Helps to ensure that those with AI responsibilities have the necessary skills and expertise.
- Helps to ensure that AI activities and AI-related decisions and actions are consistent with the organization's values, and ethical, social, and legal responsibilities.

AI policies and procedures should be established for the entire AI life cycle — from inputs to outputs. Policies and procedures also should be established for training, measuring performance, and reporting.

AI STRATEGY
GOVERNANCE
HUMAN FACTOR

Accountability, Responsibility, and Oversight

AI has the potential to do great good and great harm. Ultimately, stakeholders will likely hold the board and senior executives accountable (answerable) for their organization's AI outcomes. When assessing AI governance, internal auditors can leverage the three lines of defense model. The three lines of defense, along with senior management, the governing body, external auditors, and regulators all have roles in AI. Internal auditors should understand the role of each party, and how internal audit interfaces with that role.

> "The IIA's Artificial Intelligence Auditing Framework is a practical tool for helping internal audit to provide independent assurance over AI risk management, control, and governance processes."
>
> Nur Hayati Baharuddin,
> Member, IIA–Malaysia

Regulators

Regulators inform and control specific activities (such as banking, health care, or food safety) at national, regional/state, and local levels. Regulators "inform" through activities such as conducting research, participating in the development of standards and guidance, and communicating with stakeholders. Regulators "control" through activities such as supervising, and setting and enforcing regulations. As stated in The IIA's Position Paper: The Three Lines of Defense in Effective Risk Management and Control, regulators sometimes set requirements intended to strengthen controls in an organization and on other occasions perform an independent and objective function to assess the whole or some part of the first, second, or third line of defense with regard to those requirements.

To date, there are no regulations dedicated exclusively to AI. However, parts of existing regulations may be particularly relevant to AI activities, and regulators and standard setting bodies around the world have signaled their concern through research, discussion papers, recommendations, and guidance (see Regulatory Compliance on page 7).

Regulators already recognize the importance of AI audits. For example, in its guidance on Off-The-Shelf Software Use in Medical Devices, the U.S. Food and

Drug Administration recognizes the importance of auditing OTS knowledge-based software (for example, artificial intelligence, expert systems, and neural net software), stating that the manufacturer is expected to provide assurance "that the product development methodologies used by the OTS Software developer are appropriate and sufficient for the intended use…" and "recommends this include an audit of the OTS Software developer's design and development methodologies used in the construction of the OTS Software. This audit should thoroughly assess the development and qualification documentation generated for the OTS Software."

Auditors should keep apprised of the work of regulators and standard-setters in the area of AI, advise management and the board of matters of importance, and assess whether the organization's regulatory control objectives reflect emerging regulations, standards, and guidance.

Governing Body/Board/Audit Committee

The board is responsible for the ultimate oversight of the organization's AI activities. The board should be involved with senior management in defining the organization's AI strategy.

Internal audit must understand and be well-informed about AI generally, and the organization's AI activities specifically. In addition to providing assurance over AI activities, internal audit should offer advice and insights to help ensure that the board is prepared for its role.

> "In addition to providing assurance over AI activities, internal audit should ensure audit committees and boards are equipped to understand their role in navigating the benefits and risks associated with AI in the companies they serve."
>
> Carolyn Saint, CAE,
> University of Virginia

Senior Management

Working with the board, senior management defines the organization's AI strategy. Senior management also sets AI objectives and develops plans to implement the AI strategy.

Internal audit should be represented on the senior management team, and should keep well-informed of senior management's AI initiatives. Regarding AI risk management, governance, and controls, internal audit should be a trusted advisor to senior management.

First Line of Defense

Operational managers should own and manage AI risks on a day-to-day basis. Internal audit should assess operational-level AI policies and procedures, verifying that control objectives are adequate and working as designed.

Second Line of Defense

Compliance, ethics, risk management, and information privacy/security are some of the second line of defense functions that likely will oversee some aspect of AI risks. Internal audit should assess second line of defense AI-related policies and procedures, verifying that control objectives are adequate and working as designed.

Third Line of Defense

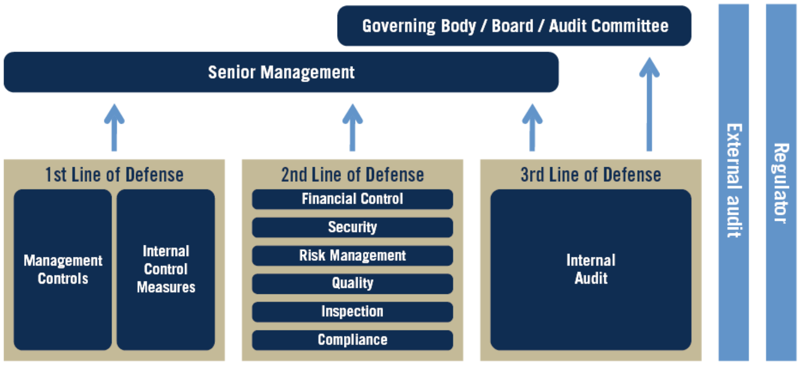
Internal audit should provide independent assurance over AI risks, governance, and controls. The IIA's AI Auditing Framework can facilitate this role. Regulators and standard-setters have recognized the potential of AI in risk management and compliance. According to the Financial Stabilities Board (FSB) report Artificial intelligence and machine learning in financial services, "The use of AI and machine learning in financial services may bring key benefits for financial stability in the form of efficiencies in the provision of financial services and regulatory systemic risk surveillance… The internal (back-office) applications of AI and machine learning could improve risk management, fraud detection, and compliance with regulatory requirements, potentially at lower cost." Similarly, the most advanced internal audit departments will start to use algorithms to fuel their continuous auditing and continuous monitoring initiatives, gaining both effectiveness and efficiency.

> "Emerging use of AI requires that audit needs specifically to address the logic used in the design of the algorithms."
>
> Hans Nieuwlands, CEO,
> IIA–Netherlands

External Audit

External auditors are third parties with no vested interest in the organization, and express an opinion on whether financial statements are prepared in accordance with applicable financial reporting frameworks and/or regulations. Regarding AI, external auditors will most likely focus on outcomes — for example, the algorithms behind model risk management or valuation, and whether those algorithms have a material impact on the organization's financial statements.

The Three Lines of Defense Model



Adapted from ECIIA/FERMA *Guidance on the 8th EU Company Law Directive, article 41*

Regulatory Compliance

Regulations typically lag technological change, and AI is no exception. However, as reported by The Hill, Tesla CEO Elon Musk warned the National Governors Association (U.S.) that regulations are needed sooner rather than later. In addition, privacy regulations such as the U.S. Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the EU's General Data Protection Regulation (GDPR), effective May 2018, may complicate AI implementation. Both regulations protect personally identifiable information, which typically are inputs to AI technologies.

For example, the HIPAA Privacy Rule "set national standards for the protection of health information, as applied to the three types of covered entities: health plans, health care clearinghouses, and health care providers who conduct certain health care transactions **electronically** [emphasis added]." And according to the FSB report Artificial intelligence and machine learning in financial services, "several sections of the GDPR are particularly relevant to AI: Article 11 provides a right to 'an explanation of the decision reached after [algorithmic] assessment"; Article 9 prohibits the processing of "special [sensitive] categories of personal data"; Article 22 provides for a data subject's qualified right not to be subject to a decision with legal or significant consequences based solely on automated processing; and Article 24 provides that decisions shall not be based on special categories of personal data.

Other generally recognized regulatory concerns include compliance with anti-discrimination laws and legal liabilities, especially with regard to third parties who provide the organization with AI services. The FSB summed up concerns regarding third parties by saying "Many current providers of AI and machine learning in financial services may fall outside the regulatory perimeter or may not be familiar with applicable law and regulation. Where financial institutions rely on third-party providers of AI and machine learning services for critical functions, and rules on outsourcing may not be in place or not be understood, these servicers and providers may not be subject to supervision and oversight. Similarly, if providers of such tools begin providing financial services to institutional or retail clients, this could entail financial activities taking place outside the regulatory perimeter."

Organizations should not wait until the regulatory environment catches up to the technology environment. Even if existing regulations do not specifically address AI, the *letter* of the law, organizations should ask whether or not their AI activities are consistent with the *spirit* of existing laws. One approach is to perform scenario and "what if?" analyses to determine if AI activities could potentially be used for malicious or criminal activities, or result in unintended consequences that cause harm. Those responsible for governance also should consider that AI activities may potentially diminish internal controls if the AI learns to override established rules or if AI systems learn how to communicate with each other and "work" together without the organization's knowledge. A proactive approach in considering the spirit of existing laws will help organizations be agile as new regulations are enacted and become effective.

Relevant AI Governance Objectives and Activities or Procedures

Engagement or Control Objective(s)	Activities or Procedures
Provide assurance that AI governance structures have been established, documented, and are working as designed.	**Review** business models and organizational structure; **determine** if business models and organizational structure reflect the organization's AI strategy. **Review** AI policies and procedures; **determine** whether organizational policies and procedures clearly identify AI roles and responsibilities related to AI strategy, governance, data architecture, data quality, ethical imperatives, and measuring performance.
Assess whether those with AI responsibilities have the necessary competencies to be successful. For example, those responsible for ethical imperatives should be competent in assessing the ethical behavior of those who provide human input into the AI, and should be independent of the AI activity.	**Interview** those with AI responsibilities. **Review** AI job descriptions, requisite skills, etc., and **verify** whether those responsible have their stated qualifications.
Provide assurance that AI policies and procedures have been established and documented.	**Review** AI policies and procedures and **determine** if they sufficiently address AI risks. **Determine** if policies and procedures provide for periodic "what if" analysis or scenario planning.
Provide assurance that AI activity audit trails provide sufficient information to understand what AI decisions were made, and why.	**Review** AI audit trails. **Determine** whether audit trails provide sufficient information to understand what decisions were made, and why.
Provide assurance that policies and procedures have been implemented and are working as designed, and that employees are compliant.	**Observe** employees implementing AI procedures. **Review** helpline/hotline reports and **follow up** on any reports alleging noncompliant or malicious activities related to AI. **Interview** a random sample of employees and **determine** if they are knowledgeable about AI policies and procedures. **Identify** and **review** AI access policies and procedures. **Evaluate** access policies and **test** access controls. **Assess** whether regulatory control objectives reflect emerging regulations, standards, and guidance.

Data Architecture & Infrastructure

AI data architecture and infrastructure will likely be one and the same, or at least nearly 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 life cycle.

According to InfoWorld, organizations should focus on three major areas of software development to ensure the success of AI integration:

- Data integration — data from multiple sources must be integrated before AI can be incorporated into the organization's applications and systems.
- Application modernization — software updates will need to be made on a regular basis. Frequent, less intensive updates should replace infrequent, more intensive updates that slow down or disrupt systems.
- Employee education — software developers, project managers, and other technology staff need to keep up with machine learning and every aspect of the technology "stack" (the software and components that run AI).

In addition, data should be reconciled so that nuances such as rounding, demographics, and other variables are normalized before input.

> "Data Infrastructure & Architecture and Data Quality are often intertwined. Relevant engagement or control objectives, and activities and procedures in one area, may overlap or impact objectives, activities, and procedures in the other area."
>
> Lesedi Lesetedi,
>
> Deputy Executive Director (Deputy CEO) – Strategy & Corporate Services
>
> Botswana College of Distance & Open Learning (BOCODOL)

Relevant Data Architecture & Infrastructure Objectives and Activities or Procedures

Engagement or Control Objective(s)	Activities or Procedures
Provide assurance that the organization is cyber resilient. Cyber resilience includes, but is broader than, cybersecurity alone. Cyber resilience encompasses security (resistance), reaction, and recovery.	**Understand** and audit big data (see The IIA's Practice Guide: Understanding and Auditing Big Data). **Assess** whether the organization is preparing for compliance with new technology regulations, such as the EU's General Data Protection Regulation (GDPR). **Assess** whether the organization's disaster recovery protocols include AI failures, including the breakdown of controls that maintain the rules set forth by AI governance.
Provide assurance that the data infrastructure has the capacity to accommodate the size and complexity of AI activity set forth in the AI strategy.	**Assess** whether the infrastructure is capable of handling structured and unstructured data.
Provide assurance that the organization has established a data taxonomy. **Evaluate** the quality, completeness, and consistency of use for the enterprisewide data taxonomy.	**Assess** whether the taxonomy is robust enough to accommodate the size and complexity of AI activities.

Data Quality

The completeness, accuracy, and reliability of the data on which AI algorithms are built are critical. For AI to be successful, organizations need access to vast amounts of high quality data — data that is well-defined and in standardized formats. Often, systems do not communicate with each other or do so through complicated add-ons or customizations. How this data is reconciled, synthesized, and validated is also critical, so systems that do not communicate with each other or do so through complicated add-ons or customizations may thwart an organization's AI activities.

In addition to data that is well-defined in standardized formats (structured data), AI technologies may be dependent on unstructured data (such as social media posts). As described in The IIA's "Global Technology Audit Guide: Understanding and Auditing Big Data," unstructured data is "typically more difficult to manage, due to its evolving and unpredictable nature, and it is usually sourced from large, disparate, and often external data sources. Consequently, new solutions have been developed to manage and analyze this data."

Ironically, organizations can turn to machine learning — a form of AI — to improve data quality. For example, there may be multiple versions of a vendor's name across an organization's many business units, data bases, and spreadsheets. A computer program could scan and reconcile all variations of the name in a matter of hours or minutes.

Internal audit also should look at how data that is used in internal audit reports has been reconciled, synthesized, and validated.

Relevant Data Quality Objectives and Activities or Procedures

Engagement or Control Objective(s)	Activities or Procedures
Provide assurance over the reliability of AI's underlying algorithms and the data on which algorithms are based.	**Obtain** a sample of the raw data that are inputs to AI. **Verify** that the organization has implemented methodologies to validate AI outcomes with actual, real-world outcomes, and that policies and procedures are in place to continuously measure, monitor, escalate, and rectify inconsistencies between the two.
Provide assurance that data input is reconciled and normalized to maximize accuracy.	**Verify** that the organization has policies and procedures in place to continuously measure, monitor, escalate, and rectify data accuracy and integrity issues. **Confirm** that the organization is consistently following and monitoring a formalized data reconciliation framework, which includes a rationale for differing methodologies and results should they exist.
Provide assurance that aggregated data is complete.	**Verify** that the organization has policies and procedures in place to limit data input bias.
Provide assurance that the completeness of data is measured and monitored and that any material exceptions that impact decision-making are identified and explained. This should be done whether the exceptions are determined by humans or AI.	**Review** AI metrics and metric reports. **Assess** whether those responsible for decision-making have received and considered explanations on material exceptions related to data quality.

Facebook’s Corrective Actions

Facebook’s challenges with AI have been widely reported. The behemoth social network has been under scrutiny over how its algorithm-fueled technologies have been used — or misused — for malicious means.

Timeline of Major Concerns:

- In Fall 2016, ProPublica reported that advertisers could use Facebook’s ad-targeting tools to exclude certain races — a potential violation of federal housing and civil rights regulations.
- In September 2017:
  - Facebook disclosed that holders of fake accounts based in Russia purchased sizeable ads on divisive issues leading up to the 2016 presidential election.
  - ProPublica reported that Facebook’s ad targeting tools enabled advertisers to target self-described ethnic “haters.”
- In October 2017, concerns about fake news resurfaced when Facebook (and Google) posted false information about the mass shooting in Las Vegas.
- In testimony to a Senate judiciary subcommittee in late October, Facebook said the reach of Russia-backed ads stretched much further than they had originally known, reaching as many as 126 million Americans before and during the 2016 presidential election.

Facebook’s Response

In a Sept. 20, 2017, post, Facebook Chief Operating Officer Sheryl Sandberg announced three corrective actions:

1. Facebook is clarifying its advertising policies and tightening its enforcement processes to ensure that content that goes against Facebook’s community standards cannot be used to target ads. (Policies and processes relate to the Governance component of the Framework. Among other things, AI Governance should establish accountability for and oversight of enforcement.)

2. Facebook is increasing “human review and oversight” of its automated processes. (Human review and oversight relates to the Ethics component of the Framework. Among other things, Ethics addresses whether AI results reflect the original objective and whether AI output is being used legally, ethically, and responsibly.)

3. Facebook is working on a program that will encourage Facebook users to report potential abuses of its ads systems. (Reporting systems relate to the Measuring Performance component of the Framework. Reporting systems help management monitor the performance of AI activities. Measuring Performance will be covered in a future Global Perspectives and Insights report.)

By utilizing The IIA’s AI Auditing Framework, internal auditors can provide assurance and advisory services to help organizations separate truth from fiction and address reporting, operations, and compliance risks associated with AI.

Using the Standards to Audit AI

Internal auditors should conform with all applicable IIA standards when planning or performing AI engagements. Key IIA standards that are particularly relevant to AI are highlighted in the sidebar, but others may apply as well.

Each standard is complemented by an Implementation Guide. Implementation guides assist internal auditors in applying the *Standards*. They collectively address internal auditing's approach, methodologies, and consideration, but do not detail processes or procedures.

Closing Thoughts

The IIA's Artificial Intelligence Auditing Framework will help internal auditors approach AI advisory and assurance services in a systematic and disciplined manner. Whether the organization's AI technologies and activities are developed in-house, through a facilitative technology such as AutoML, or by a third party, internal audit should be prepared to advise the board and senior management, coordinate with the first and second lines of defense, and provide assurance over AI risk management, governance, and controls.

This paper is Part II of a three-part series. It provides suggestions for implementing the AI Strategy and Governance components of The IIA's AI Auditing Framework. Part III will provide further suggestions for implementing the Governance component, and the Human Factor component.

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

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.

Disclaimer

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

Copyright

The Institute of Internal Auditors | Global

globaliia.org