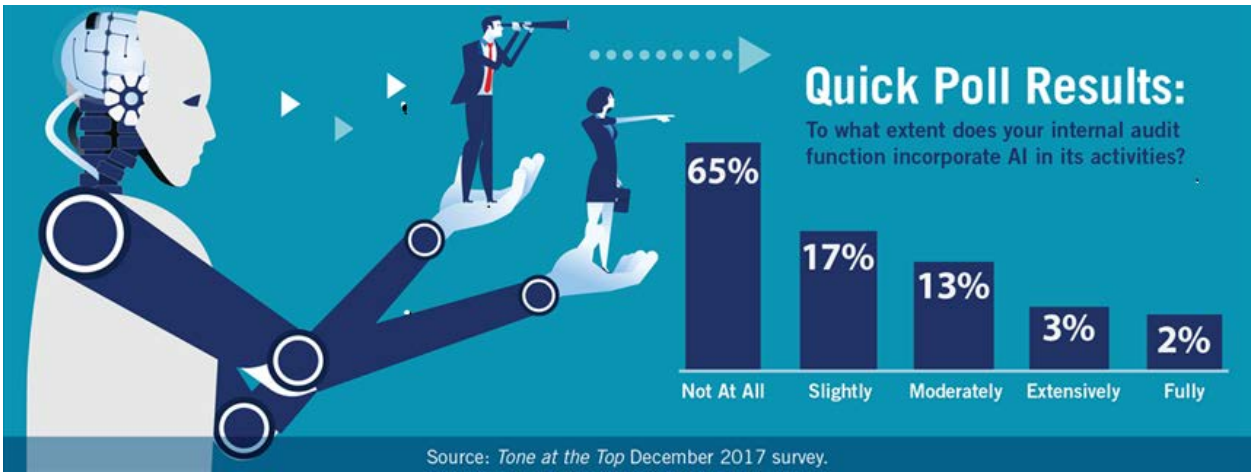
ARTIFICIAL INTELLIGENCE (AI) AND INTERNAL AUDIT



Artificial intelligence: Where do we stand?

Companies are fast approaching the most significant technological revolution of the 21st century, namely artificial intelligence (AI). This emerging paradigm, which is just starting to transform our lives and our organizations, is not some fleeting trend that we can afford to underestimate. The impact of AI will be immense, to an extent never before seen!

What is AI?

It has been said that AI is the latest in a series of advancements made possible by technological improvements (increased power, lower prices). We have seen many technological advances over the years, but the capacity to process "Big Data" using AI is an unparalleled game-changer.

The use of AI affects every sector of activity and every industry. It has already led to the development of a certain number of new capabilities and the automation of others.

Organizational impact

Regardless of the sector, the size or the type of organization, AI will represent a fundamental and significant change in the way things are done – both internally and in dealing with external stakeholders.

This fundamental change will have as yet unforeseen repercussions on our operating methods. What is commonly referred to as "Industry 4.0" has arrived, and nothing will ever be the same again. We must prepare ourselves, and we must do it now!

How does it work?

AI allows machines to learn from their experience, integrate new data that allows them to learn on a continuous basis and execute tasks similar to those carried out by humans. Most examples of AI that we hear about today – from chess-playing computers to self-driving cars – rely heavily on deep learning and natural language processing (NLP).

NLP is a branch of AI that helps computers to understand, interpret and manipulate human language. NLP was inspired by a variety of disciplines, including informatics and computational linguistics, with a view to closing the gap between human communication and the ability of computer systems to understand.

With the help of these technologies, computers can be trained to execute specific tasks by processing massive quantities of data and recognizing trends within the data.

Algorithms are the key!

AI is powered by algorithms that are fueled by Big Data. Therefore, it is essential to develop a strong foundation in Big Data in order to maximize the benefits derived from implementing AI processes. The IIA study titled "Global Perspectives and Insights, Artificial Intelligence – Considerations for the Profession of Internal Auditing, Special Edition (2017)" defines Big Data as follows:

- Large amounts of data;
- Such high volume, variety, velocity and variability of data that organizations invest in system architectures, tools and practices specifically designed to handle them;
- Data that may be generated by the organization, whether they are publicly available or purchased.

To put big data to good use, organizations develop algorithms.

What is an algorithm?

An algorithm is a finite and unambiguous set of operations or instructions that allow for a problem to be resolved or a result to be obtained. It is a set of rules that a computer must follow in order to quickly process vast amounts of data that a human cannot reasonably process, or even comprehend.

In an article that was published in The Conversation entitled "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: The simplest types of AI systems are purely reactive, and do not allow for memories to be developed or for past experiences to be used to inform future decisions. Reactive machines respond to a given situation the same way every time.

Type II. Limited memory: Limited memory AI machines can look to the past, but cannot build memories or "learn" from past experience. The memory cannot be created instantaneously, but rather requires the identification of specific objects and the monitoring of those objects over time.

Type III. Theory of mind: This type of AI represents the point between the machines we have now and the machines we will be constructing in the future. Machines of this type, which are more advanced, not only form perspectives on the world, but also on other agents or entities within the world. Type III AI is able to understand that the people, creatures and objects in the world may have thoughts and emotions that affect their own behavior.

Type IV. Self-awareness: The final step in the development of AI involves creating systems that can form self-representations. Ultimately, AI researchers must not only understand the concept of consciousness, but also construct conscious machines. Such a machine would be self-aware, understand its internal state and be able to predict the feelings of others.

Most of the systems we see 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**, or what we commonly call "the black box"!

Opportunities for organizations

The potential benefits of AI for any organization are literally limitless. AI will enable companies to accelerate and improve their processes and reduce the risk of human error. AI will also allow companies to collect data generated by their activities that has never before been usable by reason of sheer volume.

This capacity for analyzing data will also provide companies with a competitive advantage to the extent that organizations will be able to optimize their operations and products in accordance with their respective investment in and commitment to AI. This advantage will be even more enhanced through the machine learning[1] associated with AI.

[1] *Machine learning* is based on statistical approaches that allow computers to improve their performance in terms of resolving tasks using available data without being explicitly programmed for each task. This approach covers the design, assessment, development and implementation of the corresponding methods.

Benefits for companies that use AI:

- The risk of error is practically nonexistent, and accuracy is enhanced;
- Smart machines can replace human beings in many areas of work; robots can carry out certain laborious tasks;
- Using AI allows for fraud detection in systems that use smart cards;
- Emotion, which often interferes with rational thinking among human beings, is not a consideration for AI systems, because they do not experience emotions; robots apply reason and logic to make proper decisions, because they are not influenced by the types of moods that affect human effectiveness;
- Smart machines can be used to carry out certain dangerous tasks;
- The risk to the health and safety of individuals is reduced when AI is used to carry out dangerous tasks,
- The ability to make more accurate predictions;
- The ability to drive revenue and increase market share through AI initiatives.

Risks to be considered (*not an exhaustive list*)

- Governance framing the use of AI may not exist or may be inadequate;
- Unidentified human bias may be imbedded in AI technology;
- Human logic errors may be imbedded in AI technology;
- Inadequate testing and oversight of AI may result in ethically questionable results;
- AI products and services may cause harm, resulting in financial and/or reputational damage;
- Clients or other stakeholders may not accept or adopt the organization's AI initiatives;
- Questionable results may be obtained due to inadequate testing or supervision.

Ultimately, one of the most significant risks is that, with the eventual appearance of the black box, AI will evolve in such a way that computers take control over humans.

Fraud

Fraud is an ever-present risk for any company. AI relies on algorithms developed by humans, and therefore, human bias (intentional or not) may affect the data that fuels the algorithms. The consequences of this may be devastating.

Intention, pressure and rationalization are some of the factors that may incite an individual to commit an act of fraud. Therefore, in order to grasp the power and the impact associated with this technology

and reduce risks, especially of cyberattack and fraud, it is important to have a strategic and technical understanding of how AI is designed and how it works.

This highly advanced technology requires an in-depth mastery of the control environment.

How to prepare: Essential resources for this type of project, and the role of Internal Audit (IAu)

The success of any digital transformation project, and in the case of AI, projects that have significant impact, will depend in part on those who are responsible for developing the projects. The level of success will also depend on the company's ability to evolve in step with the progress of the project over time, because new jobs and new areas of expertise will emerge throughout the process of creating transformative AI projects.

For companies today, it is important to begin to envision the possibilities that will be opened up in terms of jobs because, as stated in the Creative Destruction theory developed by Schumpeter in 1912, the arrival of this new technology will cause many existing jobs to disappear and will create others in their place. The upheaval will be such that, if we are to believe the study published in 2017 by the Institute for the Future and Dell Technologies, more than 85% of the jobs that will exist in 2030 do not exist today.

In light of this, it seems that it would be more than desirable to include experts in project management, information technologies (IT), AI, IAu, fraud and ethics as essential resources for such a project.

What types of threats should internal auditors be concerned about?

By definition, regardless of the manner in which it is used to manage or monitor diverse operations, there is no question that AI will dramatically change the way internal auditors perform their function. In theory, having access to intermediaries who act as "trusted agents" will become less and less necessary, because this new technology will result in a high level of security and transparency.

Why should AI be of interest to the Internal Audit function?

These days, organizational transformation is a commonplace occurrence. With the arrival of AI, this trend will be intensified, and organizational transformations will be larger and more costly. Within a context of large scale projects that carry significant risks of loss, internal auditors, as experts in identifying risk and the means to manage it, are ideally positioned to play a crucial role in this new reality!

On the other hand, in order to remain relevant in our new world, the profile of IAu must evolve, both in terms of training and in the ability to evaluate the risks associated with emerging situations. More than ever, the IAu function (IAF) can act as a precursor and facilitator for AI within its organization, but only

if it begins to adapt now. If The IAF acts quickly, it can continue to prove that it generates added value, and is not exclusively a control mechanism. The role of the IAF:

- Help the organization to identify opportunities for incorporating AI into its operating methods;
- Continue to play its traditional role of identifying risk and the means to manage it, and as a specialist in business processes;
- Adapt its audit procedures;
- Incorporate resources with varied profiles.

In its role as a business partner, the IAF can be a key player in the planning, implementation and optimization phases of the organization's business processes.

In order to properly prepare, internal auditors must understand the basics of AI, the roles that the IAF should play and the risks and opportunities associated with AI. The IAF should take advantage of the IIA's AI Auditing Framework (see below) to develop a systematic and disciplined approach for evaluating and improving the efficiency of AI risk management, control and governance processes.

Responsibilities of the IAF:

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

(Source: https://global.theiia.org/knowledge/Public%20Documents/GPI-Artificial-Intelligence-Part-II.pdf)

AI strategy
Cyber resilience – AI competencies

Governance
Data quality – measuring performance – data architecture and infrastructure

Human factor
Ethics – the black box

These types of competencies will be needed in all of the three lines of defense. The management team and the Board of Directors should also know how AI works and understand the risks and opportunities associated with it. The IAF can help an organization to evaluate, understand and communicate the degree

to which AI will have an effect (negative or positive) on the organization's ability to create value over the short, medium or long term.

Responsibilities of the IAF:

- Understand the organization's strategic objectives and the processes that are implemented to achieve those objectives;
- Be in a position to evaluate whether AI activities are accomplishing their objectives;
- Provide internal assurance concerning the management team's risk management activities with respect to AI risks;
- Maintain its position as a trusted advisor that can support the adoption of AI to improve business processes or enhance the product and service offer.

Actions to be taken by the IAF:

- Include AI in its risk assessment, and consider whether AI should also be included in its risk-based audit plan;
- Actively participate in AI projects from their beginning, providing advice and insight that contribute to successful implementation;
- Provide assurance concerning the management of risks related to the reliability of the underlying algorithms and the data on which they are based;
- Ensure that the moral and ethical issues that may surround the organization's use of AI are being addressed;
- As is the case with any other major initiative, provide assurance concerning governance structures.

However, in order to avoid any hindrance to its independence and objectivity, whether perceived or real, the IAF should not be in charge of or responsible for the implementation of AI processes, policies or procedures

The IAF should treat AI as it treats every other field: with a systematic and disciplined approach aimed at evaluating and improving the effectiveness of AI risk management, control and governance processes.

Enhancing cyber resilience

According to the IIA report entitled "Global Perspectives and Insights, Artificial Intelligence – Considerations for the Profession of Internal Auditing, Special Edition" (2017), cybersecurity threats are more prevalent than ever. The adoption and evolution of AI will force organizations to enhance their

cyber resilience capabilities, an approach that is currently being adopted by organizations[2]. With AI, decisions are increasingly being entrusted to new, complicated and opaque algorithms that use huge data sets. Protecting these systems from malevolent external forces is critical. Cyber resilience is critical for organizations that increasingly rely on AI.

As complex a concept as cybersecurity is, the document defines four key areas where the IAF can have an immediate impact:

- Provide assurance concerning the organization's level of readiness and its response to cyber threats;
- Inform the management team and the Board with respect to the level of risk to the organization and the efforts to address this risk;
- Work in partnership with IT and other parties to ensure that effective defenses and responses are in place;
- Facilitate communication and coordination among all parties in the organization with respect to the risk.

The potentially disastrous effects of a cybersecurity breach involving AI must be managed through the implementation of cybersecurity measures by IAu teams.

Regulatory bodies

There are currently no laws dedicated exclusively to AI, but certain sections of some existing laws may be relevant to AI activities. Regulatory and standardization bodies around the world have expressed their concern in the form of research, discussion documents, recommendations and guidelines. The IIA's AI Auditing Framework can facilitate their task.

In addition, *Université de Montréal* and a number of luminaries in the field from the Montréal community, including Yoshua Bengio, have developed a document entitled "Montreal Declaration for a Responsible Development of Artificial Intelligence" (https://www.montrealdeclaration-responsibleai.com/the-declaration), which sets forth ethical principles for the use of AI.

Creating a sub-committee of the Board of Directors

We believe that it would be wise to consider creating a sub-committee of the Board dedicated to the proper functioning of AI. This committee could adopt the mission of ensuring the proper use of AI by

[2] The Cyber Resilience Blueprint: A New Perspective on Security
https://www.symantec.com/content/en/us/enterprise/white_papers/b-cyber-resilience-blueprint-wp-0814.pdf

exercising its functions in an objective and independent manner. The sub-committee must include at least one expert in each of the following fields: internal audit, crisis management, fraud, ethics, information technology and cybersecurity/cyber resilience.

Preparations for internal auditors: Added-Value certifications

In addition to the skills that internal auditors must possess, the following is a non-exhaustive list of certifications that can better equip the IAF to deal with AI:

- CIA: Certified Internal Auditor;
- CRMA: Certification in Risk Management Assurance;
- CISA: Certified Information Systems Auditor;
- CFE: Certified Fraud Examiner.

The internal audit profession is highly susceptible to the robotization and automation of its functions, which is why we must develop an in-depth understanding of what AI really entails, along with expertise related to the associated risks. Now, more than ever, internal auditors must adapt and acquire the knowledge required to manage the AI control environment.

In addition to technical competencies and past experiences, internal auditors must be prepared to explore new horizons related to transformation and robotization. Toward this end, they must demonstrate a capacity for analysis and integration, along with a willingness and hunger for learning.

On top of the added-value certifications attesting to this type of expertise, internal auditors must be proactive in educating themselves with respect to AI. It is safe to assume that the "tone at the top" will play an important role in the education of internal auditors on the subject of AI. Therefore, it is up to management to bring all of the necessary stakeholders on board with the IAF for their transformation projects.

In effect, while an auditor examines a sample in order to test a control, AI analyzes the entire population, thus reflecting the actual condition of the population.

Conclusion

The IIA's AI Auditing Framework will help internal auditors to 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 the use of tools like AutoML or by a third party, the IAF should be prepared to advise the Board and the management team, coordinate with the first and second lines of defense and provide assurance concerning AI risk management, governance, and controls.

Next subject – Progress Report #2

Understanding the use of AI in organizations and acting accordingly

Progress Report #1 produced by: Pierre Taillefer, Partner at BDO Canada LLP; Florian Bodart, Consultant, Risk Advisory Services at BDO Canada LLP; and Pascal Théoret, Director, Internal Audit Office at Université de Montréal

References

https://www.declarationmontreal-iaresponsable.com/the-declaration

Global Perspectives and Insights, Artificial Intelligence – Considerations for the Profession of Internal Auditing, Special Edition (2017):

https://na.theiia.org/periodicals/Public%20Documents/GPI-Artificial-Intelligence.pdf

https://global.theiia.org/knowledge/Public%20Documents/GPI-Artificial-Intelligence-Part-II.pdf

https://global.theiia.org/knowledge/Public%20Documents/GPI-Artificial-Intelligence-Part-III.pdf

https://na.theiia.org/periodicals/Public%20Documents/GPI-Agility-and-Innovation.pdf

https://docs.ifaci.com/wp-content/uploads/2018/03/tone-at-the-top-85-AI.pdf

https://mag.ifaci.com/les-metiers-de-laudit-et-du-controle-internes-vont-se-reinventer-avec-lintelligence-artificielle/

http://theconversation.com/understanding-the-four-types-of-ai-from-reactive-robots-to-self-aware-beings-67616

http://www.iftf.org/future-now/article-detail/realizing-2030-dell-technologies-research-explores-the-next-era-of-human-machine-partnerships/

The Cyber Resilience Blueprint: A New Perspective on Security:
https://www.symantec.com/content/en/us/enterprise/white_papers/b-cyber-resilience-blueprint-wp-0814.pdf