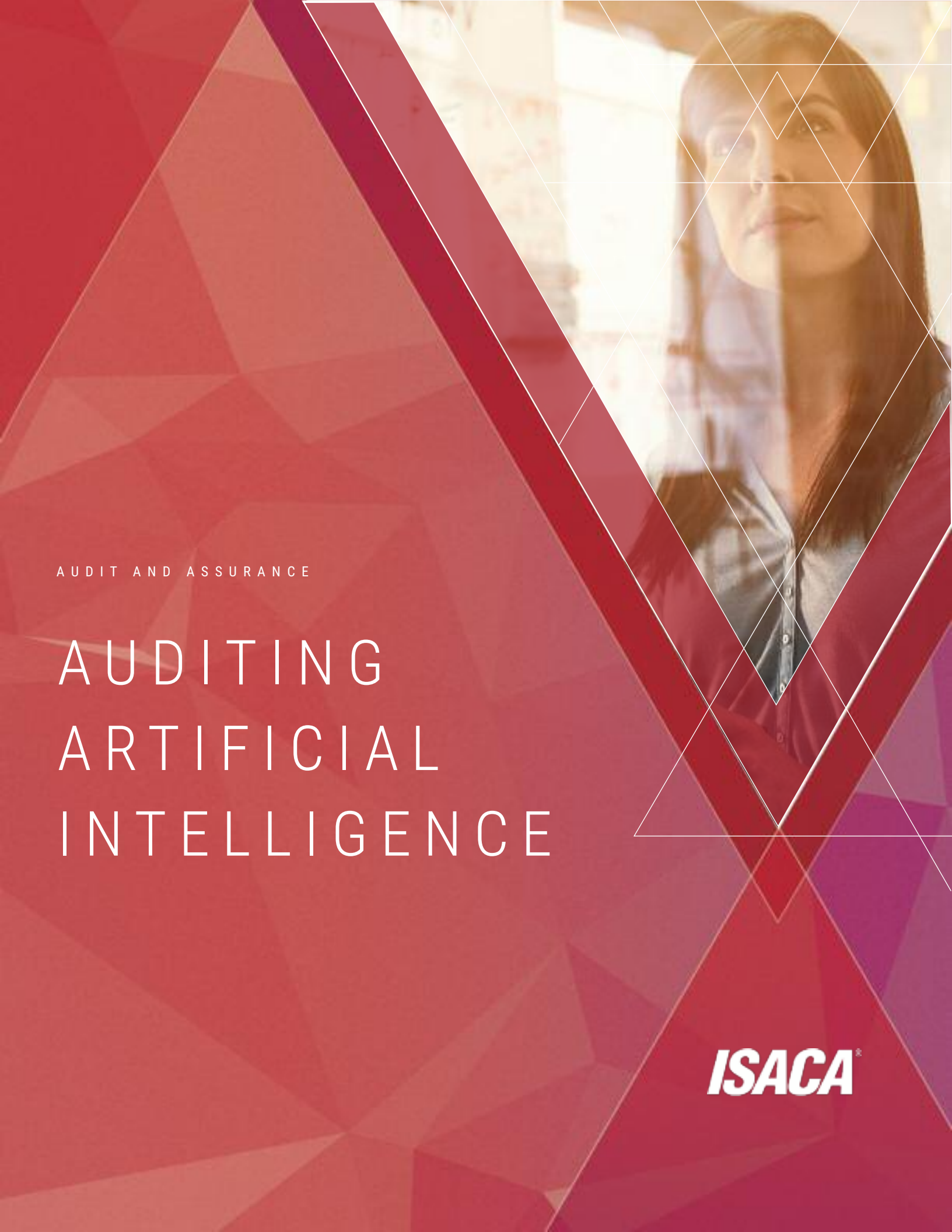


AUDIT AND ASSURANCE

AUDITING ARTIFICIAL INTELLIGENCE

ISACA®

CONTENTS

ABSTRACT

There are many potential challenges for IT auditors preparing to equip themselves to audit artificial intelligence (AI). But solutions do exist that can transform challenges into successes. This white paper focuses on what auditors need to know as they prepare to focus on AI. It explores the definition of AI, describes the challenges of auditing AI, and discusses how the current version of COBIT® (COBIT® 2019) can be leveraged to audit AI. Additionally, it identifies other frameworks that are also relevant today. Auditors will explore initial keys to successfully auditing AI and uncover relevant references.

Potential Impact of Artificial Intelligence on Organizations

There are many truths and half-truths out there concerning the impact that AI will have across a range of industries and professions. Some industries have adopted elements of the technology faster than others, with varying degrees of success and challenges. Given the hype surrounding AI we can be certain that there will be a significant impact on many areas in the business world for the foreseeable future. AI will have a far-reaching impact on the audit profession as well, given auditors' need to provide assurance around it. The purpose of this paper is to prepare auditors for what to expect and how to approach AI in a real-world audit scenario.

Why Should Auditors Care About AI?

Like many complex emerging technologies, AI is defined in many ways, by many experts. Whereas the ISACA research team has elected to retain flexibility in the definition, due to the technology's ever-changing scope and context, one general definition can serve as an indicator as to the nature and purpose of AI. Russell and Norvig, two of the leading minds in the field, call AI the study of "intelligent agents," devices that perceive their environment and take actions that maximize their chance of successfully achieving their goals.[1]

Two other concepts may also be helpful in understanding AI:

- **AI may be envisioned as a large circle with several smaller circles within it.** AI, which is machines carrying out tasks based on algorithms in an "intelligent" manner,[2] is the large circle; other, more specific types of AI, such as machine learning, are represented in the smaller circles. Machine learning is a subset of AI in that it focuses on machines' ability to receive a set of data and learn for themselves, changing their algorithms as needed as they learn more about the information they are processing.[3]
- **AI does not operate based on a set of predetermined rules.** Predetermined rules are associated with traditional software engineering. However, an excessive number of rules tends to inhibit the technology's ability to learn and adapt to its circumstances. Therefore, AI does not always operate based on a predefined set of rules.

Challenges for the Auditor

Tractica Research expects AI software revenue to grow from US $3.2 billion in 2016 to US $89.9 billion by 2025.[4] With the support of adjacent technologies (such as cloud computing and storage), AI has emerged from the so-called "AI winter" of 2010 to garner up to US $40 billion of

[1] Russell, S.; P. Norvig; *Artificial Intelligence: A Modern Approach (3rd Edition)*, Pearson, USA, 2009, https://www.pearson.com/us/higher-education/program/Russell-Artificial-Intelligence-A-Modern-Approach-3rd-Edition/PGM156683.html
[2] Venkatesan, M.; "Artificial Intelligence vs. Machine Learning vs. Deep Learning," Data Science Central, 7 May 2018, https://www.datasciencecentral.com/profiles/blogs/artificial-intelligence-vs-machine-learning-vs-deep-learning
[3] *Ibid.*
[4] Tractica Research, "Artificial Intelligence Software Market to Reach $89.8 Billion in Annual Worldwide Revenue by 2025," 21 December 2017, https://www.tractica.com/newsroom/press-releases/artificial-intelligence-software-market-to-reach-89-8-billion-in-annual-worldwide-revenue-by-2025

investment capital, at the same time production deployments have been limited.[5]

AI's rise has been accompanied by the traditional lag time between early adoption and the establishment of regulatory and compliance frameworks. There is, for example, no mature auditing framework in place detailing AI subprocesses, nor are there any AI-specific regulations, standards or mandates. Clark pioneered the cross-industry process for data mining (CRISP-DM) framework in early 2018, but individual auditors are challenged with how to perform audits successfully when there are virtually no widely adopted precedents for handling AI use cases.[6]

In addition to a lack of explicit audit standards around AI, there are additional challenges impacting the audit process. As previously noted, the definition of AI is frequently debated and the IT world, including auditors, has not reached a common definition or taxonomy on which to specify a set of world-class practices.

Moreover, AI systems and solutions vary widely from each other, and the vast set of existing and emerging technologies foundational to AI architecture give birth to complex systems. This complexity points to a high likelihood of uncertainty around the scope of AI within the business. Despite this uncertainty in the business, auditors are fairly well positioned to take on their responsibilities relative to AI. Good technology auditors are already likely to possess enough skill and understanding to effectively assess AI in the enterprise.

In addition, the complexity of AI and the shortage of qualified data scientists will routinely lead to the outsourcing of AI development projects to one or more third-party resources. A coherent understanding of enterprise AI will be dispersed—and, over time, perhaps even lost—across tiers of AI providers. This will subsequently increase the challenge for the AI auditor.

While there will undoubtedly be challenges for AI auditors as they ramp up for their new responsibilities, the situation is not as dire as might be assumed. The "black box" effect often ascribed to machine learning is often cited as a source of audit challenges. However, this assumes that traditional technology auditors are responsible for auditing algorithms. This is not the case. IT auditors should look at the governance of AI and the integration among systems. Although the algorithms should be audited by model specialists, auditors having a basic understanding of the would be beneficial. In fact, auditors already do so, using information in regulations such as US Office of the Comptroller of the Currency (OCC) 2011-12.

There are also claims the challenge is due to a lack of academic research and industry publications on the topic. This, too, is inaccurate. There is a considerable amount of research, but it is highly technical and not typically aimed at the traditional auditor. Historically, traditional IT auditors have looked at governance and integration, without diving deeply into algorithms.

Most enterprises have not yet begun to think about how AI may play a role in their businesses, so they are unlikely to have a documented plan to align AI use cases to the business or to recognize return on AI investments. However, if they do decide to adopt AI, executives will demand clarity of a higher order as they begin their efforts to develop an effective AI strategy. Because the business case and strategy documents represent typical starting points on the AI journey, auditors will be challenged to cascade down the COBIT® 2019 hierarchy from the strategic to the tactical parts of the audit.

In sum, IT auditors should not go down the path of overthinking the challenges of auditing AI. Reflecting on how they first audited cloud computing or cybersecurity should provide them with a useful frame of reference. For example, it is unlikely they examined all the protocols in depth and tested that the Open Systems Interconnection (OSI) layer 5 implementation was functioning appropriately. Instead, with AI, as with those previous new technologies, auditors will focus on the controls and governance structures that are in place and determine that they are operating effectively. Auditors can provide some assurance by focusing on the business and IT governance aspects.

[5] Bughin, J.; E. Hazan; S. Ramaswamy; M. Chui; T. Allas; P. Dahlstrom; N. Henke; M. Trench; "Artificial Intelligence: The Next Digital Frontier?" McKinsey Global Institute, June 2017, https://www.mckinsey.com/~/media/McKinsey/Industries/Advanced%20Electronics/Our%20Insights/How%20artificial%20intelligence%20can%20deliver%20real%20value%20to%20companies/MGI-Artificial-Intelligence-Discussion-paper.ashx

[6] Clark, A.; "The Machine Learning Audit—CRISP-DM Framework," *ISACA® Journal*, vol. 1, 2018, https://www.isaca.org/Journal/archives/2018/Volume-1/Pages/the-machine-learning-audit-crisp-dm-framework.aspx

Mapping COBIT to Strategy: A Visual Representation of How to Apply COBIT® 2019 in the Auditing of AI

As the application of AI in the business world is still in its early stages, there is limited guidance on how to approach auditing an AI initiative for an organization. Therefore, this example leverages ISACA's COBIT® 2019 framework as a starting point. The COBIT® 2019 framework provides the auditor with tools—including process descriptions, desired outcomes, base practices and work products across virtually all the IT domains—to enable the auditor to provide assurance over the AI initiative for any organization.

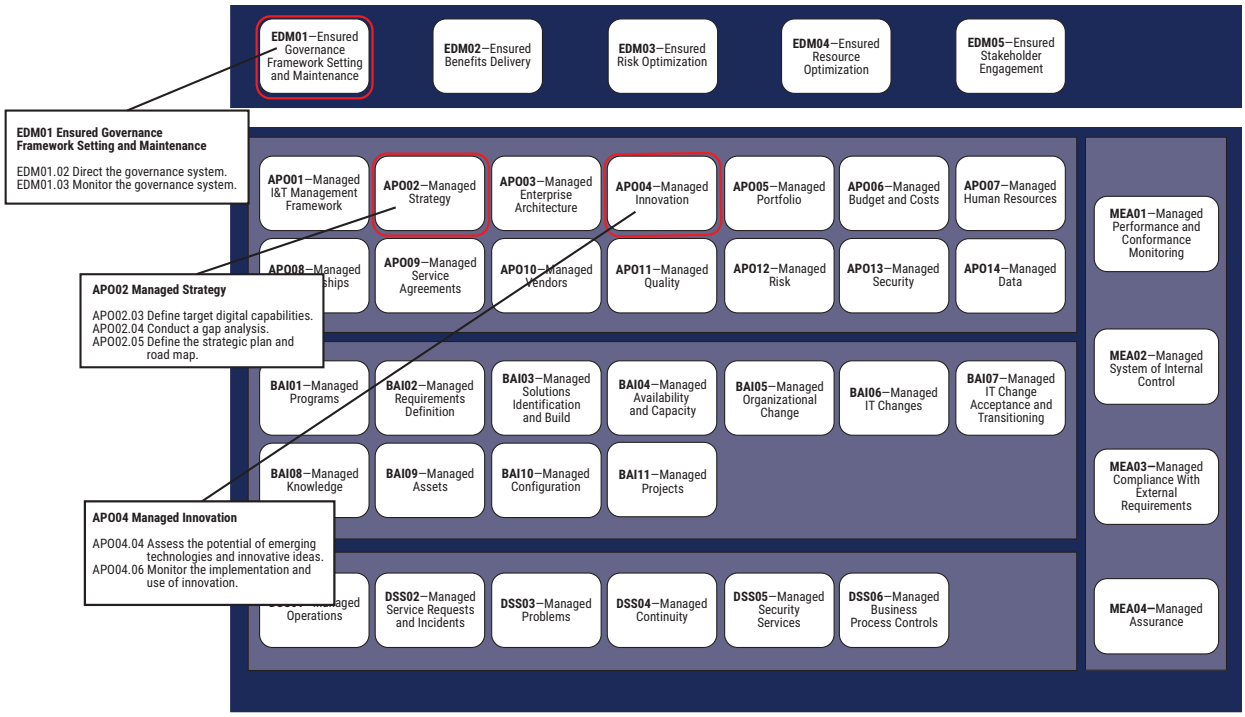
A starting point for an audit of an organization's AI is to define the scope and objectives of the audit and consider risk to the organization related to the AI initiative. These areas of risk should then be compiled in a document such as a risk and control matrix (RCM), which lists each risk and related controls. COBIT® 2019 provides a good framework for considering the risk of any initiative or process within an organization.

There are several examples of risk related to AI strategy:

- Lack of alignment between IT plans and business needs
- IT plans that are inconsistent with the organization's expectations or requirements
- Improper translation of IT tactical plans from the IT strategic plans
- Ineffective governance structures that fail to ensure accountability and responsibility for IT processes related to the AI function

Figure 1 highlights several examples of processes within COBIT® 2019 that may provide help in compiling a list of risks and controls for the AI initiative within an organization.

FIGURE 1: Select COBIT® 2019 Governance and Management Objectives Relevant to AI Risk and Controls Review



Source: ISACA, *COBIT® 2019 Framework: Introduction and Methodology*, USA, 2018

DSS06 provides a more in-depth example of how the auditor can leverage COBIT® 2019 during the course of an AI assurance review.

DSS06 *Managed Business Process Controls* includes management practice DSS06.05 *Ensure traceability and accountability for information events*, which could be used to ensure AI activity audit trails provide sufficient information to understand the rationale behind every AI decision made within the organization. The DSS06.05 description (**figure 2**) follows: "Ensure that business information can be traced to an originating business event and associated with accountable parties. This discoverability provides assurance that business information is reliable and has been processed in accordance with defined objectives."[7]

FIGURE 2: COBIT® 2019: Relevance of DSS06 to AI

A. Component: Process *(cont.)*	
Management Practice	**Example Metrics**
DSS06.05 Ensure traceability and accountability for information events. Ensure that business information can be traced to an originating business event and associated with accountable parties. This discoverability provides assurance that business information is reliable and has been processed in accordance with defined objectives.	a. Number of incidents in which transaction history cannot be recovered b. Percent of completeness of traceable transaction log
Activities	**Capability Level**
1. Capture source information, supporting evidence and the record of transactions.	2
2. Define retention requirements, based on business requirements, to meet operational, financial reporting and compliance needs.	3
3. Dispose of source information, supporting evidence and the record of transactions in accordance with the retention policy.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	

Source: ISACA, *COBIT® 2019 Framework: Governance and Management Objectives*, USA, 2018

Process outcomes in COBIT 2019 are derived from the practice itself, and for DSS06.05, can be articulated as "Business information is traced to an originated business event and is associated with accountable parties."

The following activities are listed for DSS06.05:

1. Capture source information, supporting evidence and the record of transactions.
2. Define retention requirements, based on business requirements, to meet operational, financial reporting and compliance needs.
3. Dispose of source information, supporting evidence and the record of transactions in accordance with the retention policy.

Figure 3 shows the inputs and outputs from DSS06.05.

[7] ISACA, *COBIT® 2019 Framework: Governance and Management Objectives*, USA, 2018, http://www.isaca.org/COBIT/Pages/COBIT-2019-Framework-Governance-and-Management-Objectives.aspx

FIGURE 3: COBIT® 2019: DSS06 Inputs and Outputs

C. Component: Information Flows and Items (see also Section 3.6) *(cont.)*				
Management Practice	**Inputs**		**Outputs**	
DSS06.04 Manage errors and exceptions.	**From**	**Description**	**Description**	**To**
			Error reports and root cause analysis	Internal
			Evidence of error correction and remediation	MEA02.04
DSS06.05 Ensure traceability and accountability for information events.			Record of transactions	Internal
			Retention requirements	Internal; APO14.09
DSS06.06 Secure information assets.			Reports of violations	DSS05.03
Related Guidance (Standards, Frameworks, Compliance Requirements)		**Detailed Reference**		
National Institute of Standards and Technology Special Publication 800-37, Revision 2, September 2017		3.1 Preparation (Task 10, 11): Inputs and Outputs		

Source: ISACA, *COBIT® 2019 Framework: Governance and Management Objectives*, USA, 2018

Audits should evaluate the work products, retention requirements and records of transaction as part of fieldwork testing. Criteria the auditor would use for testing include, "Does the decision made by AI seem appropriate, given the decision inputs and use case?"

Challenges and Solutions for the AI Auditor

While there are several potential challenges for IT auditors preparing to equip themselves to audit AI, solutions do exist that can convert the challenges into successes. The list in **figure 4** provides examples.

FIGURE 4: Challenges and Solutions for AI Auditing

CHALLENGES FOR THE AUDITOR OF AI	KEYS TO THE SUCCESSFUL AUDITING OF AI
1. Immature auditing frameworks or regulations specific to AI	1. Adopt and adapt existing frameworks and regulations.
2. Limited precedents for AI use cases	2. Explain and communicate proactively about AI with stakeholders.
3. Uncertain definitions and taxonomies of AI	3. Explain and communicate proactively about AI with stakeholders.
4. Wide variance among AI systems and solutions	4. Become informed about AI design and architecture to set proper scope.
5. Emerging nature of AI technology	5. Become informed about AI design and architecture to set proper scope.
6. Lack of explicit AI auditing guidance	6. Focus on transparency through an iterative process. Focus on controls and governance, not algorithms.
7. Lack of strategic starting points	7. Involve all stakeholders.
8. Possibly steep learning curve for the AI auditor	8. Become informed about AI design and engage specialists as needed.
9. Supplier risk created by AI outsourcing to third parties	9. Document architectural practices for cross-team transparency.

The following information expands on the keys to success listed in **figure 4**, to help auditors address the challenges of auditing AI:

- **Become informed about AI design and architecture to set proper scope.** AI includes a large set of technologies, people and processes and, therefore, will require significant attention to controls, policies and governance. AI architecture may combine programming, data warehousing, stream processing platforms, machine learning tool kits, algorithms, cloud computing, cloud storage, computing clusters, compute kernels, application software testing and debugging, data process and modeling, and commercial off-the-shelf (COTS) software. From a skills perspective, AI projects may require data scientists, data engineers, data architects and programmers capable in Python, R, Java and matrix laboratory (MATLAB).[8]

[8] *Op cit* Tractica

- **Involve all stakeholders.** AI not only integrates a variety of enterprise technologies but also involves multiple internal teams and external third parties. Internal stakeholders involve engineering and security teams on the technical side and business leaders engaged with the AI strategy. The use of cloud computing is widespread with AI and implies that third parties will control part of the infrastructure. Where cloud computing is used, for example, auditors must address risk (such as vendor lock-in and partitioned knowledge) differently from the on-premise applications.
- **Explain and communicate proactively about AI with stakeholders.** Due to the immature state and limited deployment of AI, enterprise stakeholders may be uninformed about its use and strategy. AI auditors must be proactive to address AI concerns and be able to break down and simplify complex designs and issues into terms stakeholders can understand. Auditors must be aware of the different contexts for AI discussions and be able to adjust the level of the conversation appropriately.
- **Adopt and adapt existing frameworks and regulations.** The lack of new frameworks specific to AI should not be an impediment to a successful audit. COBIT 2019 and other existing frameworks can be adopted to handle most of the existing AI use cases that will be encountered in the field. Also, from a regulatory perspective, existing charters such as the United States Health Insurance Portability and Accountability Act (HIPAA) and Fair Lending Act and the European Union's General Data Protection Regulation (GDPR) can be adopted to provide legal guidance. The existing frameworks and regulation (adapted by an auditor who knows the AI landscape) and legal consultation will suffice until more specific AI standards are implemented.
- **Focus on transparency through an iterative process.** Transparency is an essential aim for the AI auditor due to the complexity of the AI environment. Algorithms require multiple rounds of tuning by data scientists and data engineers. Some enterprise-based commercial off-the-shelf solutions may already contain components of machine learning. Likewise, the auditing process must ensure vigilance of current and new AI developments and promote continuous improvement and explicit documentation throughout the AI life cycle. AI itself can, in fact, become a tool for the AI auditor.

Conclusion

Artificial intelligence promises to transform more than just the way enterprises do business. It will touch every corner of society.

Auditors should ask themselves whether organizations and audit teams are ready for the tough questions around AI and the approach for auditing it. The key points covered in this white paper can be helpful in getting off to a successful start.

Despite ambiguity around a conceptual definition, AI continues to proliferate across business, academic and social environments. Initial disruptions being caused by emerging AI technologies will evolve and affect the way people work until machines act like human beings for all conceivable functions. This emerging phase offers a great opportunity for the business and information technology community to step up, prepare and establish sound governance around auditing AI. COBIT® 2019, a powerful and time-tested methodology, can be leveraged to pave the way.

Resources and References for Auditing AI

The Association for the Advancement of Artificial Intelligence, Digital Library, Conference Proceedings, https://aaai.org/Library/conferences-library.php

Azoff, M.; "2017 Trends to Watch: Artificial Intelligence," Ovum, 26 January 2017, https://ovum.informa.com/~/media/Informa-Shop-Window/TMT/Files/Whitepapers/2017-trends-to-watch-in-AI.pdf

Bughin, J.; E. Hazan; S. Ramaswamy; M. Chui; T. Allas; P. Dahlstrom; N. Henke; M. Trench; "Artificial Intelligence: The Next Digital Frontier?" McKinsey Global Institute, June 2017, https://www.mckinsey.com/~/media/McKinsey/Industries/Advanced%20Electronics/Our%20Insights/How%20artificial%20intelligence%20can%20deliver%20real%20value%20to%20companies/MGI-Artificial-Intelligence-Discussion-paper.ashx

Clark, A.; "The Machine Learning Audit—CRISP-DM Framework," *ISACA® Journal*, vol. 1, 2018, https://www.isaca.org/Journal/archives/2018/Volume-1/Pages/the-machine-learning-audit-crisp-dm-framework.aspx

Conitzer, V.; W. Sinnot-Armstrong; J. S. Borg; Y. Deng; M. Kramer; "Moral Decision Making Frameworks for Artificial Intelligence," Association for the Advancement of Artificial Intelligence, 2017, https://users.cs.duke.edu/~conitzer/moralAAAI17.pdf

Cummings, M. L.; "Artificial Intelligence and the Future of Warfare," Chatham House, January 2017, https://www.chathamhouse.org/sites/default/files/publications/research/2017-01-26-artificial-intelligence-future-warfare-cummings-final.pdf

Davenport, T.; J. Raphael; 10Rule; "Creating a Cognitive Audit," *CFO*, 12 July 2017, http://ww2.cfo.com/auditing/2017/07/creating-cognitive-audit/

Faggella, D.; "What is Artificial Intelligence? An Informed Definition," TechEmergence, 15 May 2017, https://www.techemergence.com/what-is-artificial-intelligence-an-informed-definition/

The Institute of Internal Auditors, "Global Perspectives and Insights Series, Artificial Intelligence—Considerations for the Profession of Internal Auditing," 2017, https://na.theiia.org/periodicals/Public%20Documents/GPI-Artificial-Intelligence.pdf

The Institute of Internal Auditors, "Global Perspectives and Insights Series, The IIA's Artificial Intelligence Auditing Framework—Practical Applications, Part A," 2017, https://na.theiia.org/periodicals/Public%20Documents/GPI-Artificial-Intelligence-Part-II.pdf

The Institute of Internal Auditors, "Global Perspectives and Insights Series, The IIA's Artificial Intelligence Auditing Framework—Practical Applications, Part B," 2017, https://na.theiia.org/periodicals/Public%20Documents/GPI-Artificial-Intelligence-Part-III.pdf

The Institute of Internal Auditors, "Artificial Intelligence: The Future for Internal Auditing," *Tone at the Top*, December 2017

Internal Audit Foundation, "Request for Proposals, Artificial Intelligence Research Project," 2017, https://na.theiia.org/iiarf/Public%20Documents/RFP-Artificial-Intelligence.pdf

International Standards Organization (ISO), "ISO/IEC 27000:2018(en), Information technology—Security techniques—Information security management systems—Overview and vocabulary," https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:e

ISACA, *COBIT® 2019 Framework: Governance and Management Objectives*, USA, 2018, http://www.isaca.org/COBIT/Pages/COBIT-2019-Framework-Governance-and-Management-Objectives.aspx

ISACA, COBIT 4.1 Brochure, http://www.isaca.org/Knowledge-Center/cobit/Documents/CobiT-4.1-Brochure.pdf

Issa, H.; T. Sun; M. Vasarhelyi; "Research Ideas for Artificial Intelligence in Auditing: The Formalization of Audit and Workforce Supplementation," *Journal of Emerging Technologies in Accounting*, vol. 13, no. 2, 2016, http://aaapubs.org/doi/pdf/10.2308/jeta-10511?code=aaan-site

Koenig, M.; S. Bee; D. Applegate; *Artificial Intelligence: The Data Below*, Internal Audit Foundation, 2018

KPMG, "Capitalizing on robotics: Driving savings with digital labor," 2017, https://assets.kpmg.com/content/dam/kpmg/is/pdf/2017/03/capitalizing-robotics-digital-labor-savings.pdf

Kuang, C.; "Can A.I. Be Taught to Explain Itself?" *The New York Times Magazine*, 21 November 2017, https://www.nytimes.com/2017/11/21/magazine/can-ai-be-taught-to-explain-itself.html

Meek, T.; "How Humans and AI Will Share the Auditing Function of the Future," *Forbes*, 10 July 2017, https://www.forbes.com/sites/workday/2017/07/10/how-humans-and-ai-will-share-the-auditing-function-of-the-future/#63d3bf774fa1

Peter Davis and Associates, www.pdaconsulting.com/

Russell, S.; P. Norvig; *Artificial Intelligence: A Modern Approach (3rd Edition)*, Pearson, USA, 2009

Sandvig C.; K. Hamilton; K. Karahalios; C. Langbort; "Auditing Algorithms: Research Methods for Detecting Discrimination on Internet Platforms," Paper Presented at the "Data and Discrimination: Converting Critical Concerns into Productive Inquiry" preconference of the 64th Annual Meeting of the International Communication Association, http://www-personal.umich.edu/~csandvig/research/Auditing%20Algorithms%20—%20Sandvig%20—%20ICA%202014%20Data%20and%20Discrimination%20Preconference.pdf

Tegmark, M.; *Life 3.0: Being Human in the Age of Artificial Intelligence*, Knopf, USA, 2017

Tractica Research, "Artificial Intelligence Software Market to Reach $89.8 Billion in Annual Worldwide Revenue by 2025," 21 December 2017, https://www.tractica.com/newsroom/press-releases/artificial-intelligence-software-market-to-reach-89-8-billion-in-annual-worldwide-revenue-by-2025

Venkatesan, M.; "Artificial Intelligence vs. Machine Learning vs. Deep Learning," Data Science Central, 7 May 2018, https://www.datasciencecentral.com/profiles/blogs/artificial-intelligence-vs-machine-learning-vs-deep-learning

Acknowledgments

ISACA would like to recognize:

Lead Developers

ISACA Phoenix Chapter

John Livingston, CISA, ITIL v3, Lean Six Sigma Black Belt
Advisor, Information Security Compliance & Audit Governance , USA

Joe Norris, CGEIT, COBIT, ITIL v3
Director, Enterprise Risk Management, USA

Jon Oppenhuis, CCSK, CCSP, CISSP, ITIL SS/SD, TOGAF
Client Solutions Architect, USA

Expert Reviewers

Andrew Clark

Michael J. Podemski
CIPM, CIPT, USA

Marc Vael
CISA, CRISC, CISM, CGEIT, Belgium

ISACA Board of Directors

Rob Clyde, Chair
CISM
Clyde Consulting LLC, USA

Brennan Baybeck, Vice-Chair
CISA, CRISC, CISM, CISSP
Oracle Corporation, USA

Tracey Dedrick
Former Chief Risk Officer with Hudson City Bancorp, USA

Leonard Ong
CISA, CRISC, CISM, CGEIT, COBIT 5 Implementer and Assessor, CFE, CIPM, CIPT, CISSP, CITBCM, CPP, CSSLP, GCFA, GCIA, GCIH, GSNA, ISSMP-ISSAP, PMP
Merck & Co., Inc., Singapore

R.V. Raghu
CISA, CRISC
Versatilist Consulting India Pvt. Ltd., India

Gabriela Reynaga
CISA, CRISC, COBIT 5 Foundation, GRCP
Holistics GRC, Mexico

Gregory Touhill
CISM, CISSP
Cyxtera Federal Group, USA

Ted Wolff
CISA
Vanguard, Inc., USA

Tichaona Zororo
CISA, CRISC, CISM, CGEIT, COBIT 5 Assessor, CIA, CRMA
EGIT | Enterprise Governance of IT (Pty) Ltd, South Africa

Theresa Grafenstine
ISACA Board Chair, 2017-2018
CISA, CRISC, CGEIT, CGAP, CGMA, CIA, CISSP, CPA
Deloitte & Touche LLP, USA

Chris K. Dimitriadis, Ph.D.
ISACA Board Chair, 2015-2017
CISA, CRISC, CISM
INTRALOT, Greece

About ISACA

Nearing its 50th year, ISACA® (isaca.org) is a global association helping individuals and enterprises achieve the positive potential of technology. Technology powers today's world and ISACA equips professionals with the knowledge, credentials, education and community to advance their careers and transform their organizations. ISACA leverages the expertise of its half-million engaged professionals in information and cyber security, governance, assurance, risk and innovation, as well as its enterprise performance subsidiary, CMMI® Institute, to help advance innovation through technology. ISACA has a presence in more than 188 countries, including more than 217 chapters and offices in both the United States and China.

DISCLAIMER

ISACA has designed and created *Auditing Artificial Intelligence* (the "Work") primarily as an educational resource for professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, professionals should apply their own professional judgment to the specific circumstances presented by the particular systems or information technology environment.

RESERVATION OF RIGHTS

ISACA®
1700 E. Golf Road, Suite 400
Schaumburg, IL 60173, USA

Phone: +1.847.660.5505

Fax: +1.847.253.1755

Support: support.isaca.org

Website: www.isaca.org

Provide Feedback:

www.isaca.org/auditing-AI

Participate in the ISACA Online Forums:
https://engage.isaca.org/onlineforums

Twitter:
www.twitter.com/ISACANews

LinkedIn:
www.linkd.in/ISACAOfficial

Facebook:
www.facebook.com/ISACAHQ

Instagram:
www.instagram.com/isacanews/