AI assessments: enhancing confidence in AI

Effective assessments of artificial intelligence can support strong governance, compliance and performance.

The better the prompt. The better the answer.
The better the world works.

EY
Shape the future with confidence

ACCA

Foreword

Marie-Laure Delarue
EY Global Vice-Chair – Assurance

Artificial intelligence (AI) is at an inflection point. Business leaders, policymakers, academics and citizens are beginning to unlock AI's transformational opportunities. At the same time, they are also grappling with how to manage AI's complexities and considerable risks.

EY teams are at the forefront of efforts to enable successful AI adoption. By conducting rigorous assessments of AI systems, these teams can help to ensure that AI is developed and deployed safely and effectively. In so doing, they can build confidence in AI across businesses, governments and entire societies.

This paper discusses how these AI assessments – whether voluntary or mandatory and if conducted in a careful and independent manner – can play a pivotal role in establishing the foundation of confidence and trust that is essential for businesses, policymakers and citizens to maximize AI's potential, and minimize its risks across all sectors and geographies.

Effective AI assessments can play an important role in supporting corporate governance, including by determining whether an AI system performs as intended, complies with applicable laws, regulations and standards, and is managed in accordance with internal policies and ethical standards.

We believe that this paper can serve as a positive and valuable contribution for business leaders and policymakers by highlighting the importance of AI governance and the role that AI assessments can play in ensuring that governance over AI systems is tailored, robust and effective.

I would like to thank the professionals at the Association of Chartered Certified Accountants and International Federation of Accountants for their collaboration on this report. I look forward to continuing to engage with them and others to support business leaders and policymakers in using AI to help build a future of great progress and prosperity.

Helen Brand
Chief Executive Officer, Association of Chartered Certified Accountants (ACCA)

As AI scales across the economy, the ability to trust what it says is not just important — it's vital for the public interest. AI assessments are an important part of this journey to create sustainable, long-term value from AI.

This policy paper explores the role that AI assessments can play. It looks at how they are currently understood, the challenges in developing robust assessments, and the key elements needed to maximize value from them in the future.

It also highlights key considerations for business leaders and policy makers, including the important role AI assessments can play in enhancing corporate governance and risk management. The value of voluntary assessments to build confidence in AI is also explored, as is the importance of clearly defined purpose and components in assessment frameworks. The paper underlines the value of recognized standards or criteria for conducting assessments.

We're delighted to be collaborating with EY and IFAC on this and hope that the paper acts as a catalyst for discussion among those seeking to further develop their views and approach. ACCA launched its refreshed Global Policy Priorities this year, spanning areas including bridging skills gaps and driving sustainable business — and AI assessments relate to these given the need for upskilling in this area and their role in driving trust within the AI ecosystem.

We see this as a longer-term agenda and look forward to collaborating with policymakers and others in this fascinating and important area.

Lee White
Chief Executive Officer, International Federation of Accountants (IFAC)

As professional accountants, the delivery of trust is our foundation. Now, as artificial intelligence becomes a core part of how businesses operate, our role in creating that trust has never been more important.

AI brings speed, scale and new possibilities. But it also brings complexity. The systems behind AI are often opaque, their decisions hard to trace.

That's why effective assessments of AI systems matter — and why this report is so timely. It reminds us that this work must be more than checklists. AI assessments should be robust, clear and meaningful. They need to be led by professionals with the right skills and ethical foundation.

No matter how advanced the technology becomes, it can't reflect, question or ask "is this right?" Whereas as professional accountants, our job has always been to step back, think critically and serve the public interest.

Accountants are already equipped to evaluate systems, interpret data, apply consistent frameworks and exercise sound judgment. As AI changes how work is done, we must evolve too, embracing technology but also deepening the human qualities that make our profession essential: skepticism and critical thinking.

Let's build a future where technology is trusted, and people remain at the heart of progress.

Contents

1 Executive summary

More and more businesses are adopting artificial intelligence (AI) to meet their strategic objectives. This adoption is accelerating transformation across enterprises and unlocking new business opportunities. As businesses' adoption of AI grows, so does their need to ensure that the AI systems they deploy are safe, reliable and effective. Confidence in AI systems is, therefore, essential so that AI can fulfill its potential to enhance innovation, productivity and growth.

To build that confidence, many business leaders, policymakers and other stakeholders are using, or are considering using, AI assessments. AI assessments are at times referred to as "AI audits" or "AI assurance." These assessments can help companies build and use AI systems that are well-governed, that comply with any applicable laws and regulations, and that meet the standards of quality that business leaders seek and expect.

This paper identifies and discusses the components of effective AI assessments. It does this by surveying relevant AI assessment frameworks – both voluntary and regulatory – in key jurisdictions where businesses and policymakers are working to build confidence in AI. Our survey identifies three emerging types of AI assessments that companies are using separately or in combination:

Governance assessments
To evaluate the internal governance structures surrounding AI systems.

Conformity assessments
To determine compliance with any applicable laws, regulations and standards.

Performance assessments
To measure AI systems against predefined quality and performance metrics.

We also identify potential challenges to the effectiveness of these AI assessments, including ambiguous terminology, insufficiently defined subjects of evaluation, methodologies and assessment criteria, and the need for qualified professionals to perform these assessments.

To help meet these challenges and facilitate effective and useful AI assessments, we conclude with several considerations for business leaders and policymakers.

Specifically, we suggest that business leaders consider the following:

- The role AI assessments can play in enhancing corporate governance and risk management.
- Whether – even in the absence of regulatory requirements – voluntary assessments can build confidence in AI systems among employees and customers; and, where voluntary assessments are used,
- What the most appropriate type of assessment is (e.g., governance, compliance or performance assessment) and whether it should be conducted internally or by a third party.

For policymakers, we suggest:

- Consider what role voluntary (or mandated) AI assessments can play to build confidence in AI systems, support successful adoption and contribute to the governance of AI.
- Clearly define the purpose and components of the assessment framework and, where possible, the recognized standards or criteria by which the assessment should be conducted.
- Address any expectation gaps in what AI assessments entail and their limitations.
- Identify appropriate measures to build the capacity of the market to provide high-quality and consistent assessments.
- Endorse assessment standards that are, to the extent practicable, consistent and compatible with standards in other jurisdictions to reduce AI assessment costs and promote cross-border confidence in the credibility of the assessments.

2 Introduction

In November 2022, OpenAI released ChatGPT, generating widespread public recognition of AI's existing and potential capabilities, while also raising concerns about risks related to AI's development and deployment. Since that time, companies, policymakers and others have increased their efforts to address a common and fundamental challenge: how to develop and deploy AI applications that are fit for purpose and trusted by employees, customers, the market and society as a whole.

The development and deployment of AI — including generative AI systems like ChatGPT and, more recently, agentic AI — will continue to increase given the significant opportunities AI presents. EY Parthenon, for example, estimates that generative AI alone could boost global GDP by anywhere from US$1.7 trillion to US$3.4 trillion by 2033.[1] However, successful adoption depends on trust and confidence in the technology, particularly considering the rise in harmful incidents related to AI. Indeed, the Organisation for Economic Co-operation and Development (OECD) reports that the monthly average rate of adverse incidents continues to increase, having grown almost twenty-fold from 32 in November 2022 to 614 in January 2025.[2] The EY AI Sentiment Index Study from April 2025 found that 58% of surveyed citizens are concerned that organizations are failing to hold themselves accountable for negative uses of AI, and 52% are concerned that organizations are failing to comply with AI internal policies and regulatory requirements.[3]

Amidst the rapid development of AI, business leaders, policymakers, academics, investors, insurers and other stakeholders are asking urgent and fundamental questions, such as:

- How do we assess whether an AI system is reliable and effective?
- How do we identify and manage its risks?
- How do we determine if an AI system meets applicable regulatory and other standards for effectiveness and quality?

Numerous AI governance frameworks are emerging to help address these questions. Many of these frameworks incorporate assessments designed to validate the technology's governance, compliance with applicable policies, operational integrity or effectiveness.[4] In this paper, we use the term "AI assessments" to refer to "structured evaluations of a defined subject matter[5] to produce an outcome, judgment, or conclusion."[6]

AI assessments can be tailored to meet the needs and requirements of diverse stakeholders, including regulators, business leaders, investors, insurers and consumers. AI assessments can be voluntary or mandatory, qualitative or quantitative, and conducted by internal or external parties, with a range of reporting and disclosure metrics. AI assessments can also be specific to certain use cases, risk levels or operating domains of the technology.

Rigorous assessments of AI systems can enhance confidence in the technology by validating that its development and deployment meet applicable criteria for governance, compliance or effectiveness.

1 How global business leaders can harness the power of GenAI, EY, 1 August, 2024.
2 AI Incidents and Hazards Monitor, OECD, January, 2025.
3 How a license to lead can transform human potential in an AI world, EY, 9 April, 2025; How responsible AI can unlock your competitive edge, EY, 3 June, 2025.
4 Compliance can include adherence to applicable laws and regulatory guidelines, internal policies or standards.
5 In the context of assurance, "subject matter" refers to the specific information, process or set of controls that the assurance practitioner is evaluating.
6 The terminology used in policy texts and discussions to describe "AI assessments" is wide-ranging and inconsistent across texts. Terms including "assurance," "audits," "benchmark testing," "certification," "conformity assessments" and "verifications" are at times used interchangeably. The term "audit" is sometimes used in the AI domain to refer to any form of third party evaluation, including investigative journalism, compliance and bias assessment, and conformity assessments. For the purposes of this publication, all these terms will be broadly referred to as forms of "AI assessments."

3 The current public policy landscape of AI assessments

This section examines relevant AI policies and summarizes some of the challenges for companies, AI assessment providers and other stakeholders in implementing these policies.

Policymakers are active in this emerging space, developing both mandatory and voluntary policy frameworks for AI assessments. As of January 2025, policymakers from nearly 70 countries have proposed over 1,000 AI policy initiatives, including legislation, regulations, voluntary initiatives and agreements, according to the OECD.[7] A 2025 report from Stanford University found that over 39 countries have enacted 204 of those initiatives into law.[8] While it is difficult to get an exact account, AI assessments are part of a number of AI policy initiatives that have either been proposed or enacted into law.[9] In July 2025, the Trump administration in the United States unveiled its AI Action Plan, which observes that evaluations can be a critical tool in measuring the performance and reliability of AI systems.[10] The table below highlights some well-known AI assessment policy frameworks and illustrates how policymakers are taking a range of approaches. A broader list of policy initiatives from around the world can be found in Appendix II.

7 These initiatives have emerged at different levels including multi-lateral organizations, national governments, city and state levels and are aimed at different objectives. National AI policies & strategies, OECD, January, 2025.
8 "The AI Index 2025 Annual Report", Stanford Human-Centered Artificial Intelligence, April, 2025.
9 "Global AI Law and Policy Tracker", IAPP, November, 2024.
10 "America's AI Action Plan: Winning the Race", 23 July, 2025, pg. 10.

Table 1: Examples of public policy frameworks that incorporate AI assessments

Framework	EU AI Act	G7 AI Code of Conduct	UK Toolkit on AI Assurance	New York City Local Law 144
Overarching policy objective	Protect the safety, security and fundamental rights of individuals.	Promote safe, secure and trustworthy AI worldwide.	Provide resources and guidance for AI assurance practitioners.	Protect job applicants against possible bias in automated employment decision tools (AEDT).
Purpose of the assessment(s)	Assessment of conformity of the AI system with EU AI Act obligations.	Ensure trustworthiness, safety and security of AI systems.	Proposes assessments to measure, evaluate and communicate AI risks.	Assessment of the AEDT's impact on people based on demographic data categories such as race, ethnicity or sex.
Subject matter of assessment	AI quality management system and technical documentation, including processes and governance.	Not specified.	Varies based on technique; can evaluate data, AI model or governance processes.	AI system outcomes.
Methodologies for assessment	Conformity assessment demonstrating compliance with EU AI Act requirements.	Assessments not detailed in depth.	Defined AI assurance techniques and mechanisms.	Bias audit including calculations of selection or scoring rates across categories.
Assessment provider	Self-assessments; third party assessments for certain AI applications.	Not specified.	Multiple options considered depending on assessment type.	Independent third party assessment.
Terminology used to describe assessment(s)	Conformity assessment; risk assessments.	Independent external testing measures; assessment of effects and risks.	AI assurance includes compliance and bias audits, formal verification and other terms.	Bias audit.

Themes identified in current policy landscape:

Three categories of AI assessments are emerging

The purpose of AI assessments varies significantly, from validating compliance with regulations and standards, determining if the results of an AI system are free from bias, to measuring the accuracy of AI outcomes. Clearly defining the purpose of an AI assessment is crucial, as it shapes the requirements and expectations surrounding the assessment. AI assessments can generally be grouped into three categories and may be performed separately or in combination, such as:[11]

- **Governance assessments:**
  These assessments determine whether appropriate internal corporate governance policies, processes and personnel are in place to manage an AI system, including in connection with that system's risks, suitability and reliability.
- **Conformity assessments:**
  These assessments determine whether an organization's AI system complies with relevant laws, regulations, standards, or other policy requirements.
- **Performance assessments:**
  These assessments measure the quality of performance of an AI systems' core functions, such as accuracy, non-discrimination and reliability. They often use quantitative metrics to assess specific aspects of the AI system.

11 These categories should not be interpreted as fully distinct from one another. For example, an assessment that evaluates governance over an AI system may also be an assessment of conformity such as an assessment of an organization's AI Management System against the ISO/IEC 42001 standard.

There is significant variation across the policy frameworks for AI assessments

We currently observe significant variations in all aspects of both mandatory and voluntary AI assessment policy frameworks, including the scope, subject matter, methodologies, specified provider competence and qualifications, and the level of confidence the assessment is intended to deliver.

The scope of assessments can be narrow or very broad and can vary widely. For instance, their scope may cover the bias in AI systems' outcomes, as outlined in NYC Local Law 144; organizational governance and control processes around an AI system, as seen in the EU Digital Services Act and Australia's assurance framework; or data governance properties, such as those included in the EU AI Act's conformity assessments. This variation can be explained in part by differences in the jurisdictions' overarching policy goals and objectives, or the needs of the stakeholders whom the assessment is intended to serve.

Moreover, even when the objectives of AI assessments align, the specific requirements of AI assessment frameworks may still differ across jurisdictions. For example, various US cities and states have policies that include assessments for bias in the AI systems used in hiring and employment.[12] However, the specific requirements of those assessments vary greatly. NYC Local Law 144, for example, has different requirements for measuring bias than the state laws requiring bias assessments in Colorado and Illinois.[13]

AI assessments also provide varying levels of confidence based on the design of their specific requirements, such as the extent of evidence required or the requirements for the providers of the assessments. Assessments conducted by third parties may be viewed as more credible than those conducted by internal teams, especially if third party providers adhere to standards of professional responsibility, ethics and public reporting that internal teams might not be obligated to follow.[14]

Finally, mandatory AI assessments that evaluate compliance with a regulation, for example, will often be very different from voluntary assessments against a governance standard, such as the voluntary AI Risk Management Framework of the US National Institute of Standards and Technology (NIST).[15]

As stated in the December 2024 findings by the UN's International Panel on the Information Ecosystem (IPIE), the diversity of approaches for AI assessments makes it difficult to ensure consistent quality and accountability.[16]

12 "A running list of states and localities that regulate AI in hiring", HR Dive, 20 May, 2024.
13 The Trump administration intends to review state AI policy to determine how it aligns with the AI Action Plan, including when making decisions on federal funding and grants, which may influence the development of state AI policy going forward.
"America's AI Action Plan: Winning the Race", 23 July, 2025, p. 3.
Schlemmer, Michael D., Morgan Lewis, "AI in the Workplace: The New Legal Landscape Facing US Employers", 1 July, 2024.
14 "Enhancing AI Accountability: Effective Policies for Assessing Responsible AI, Business Software Alliance", 23 October, 2024.
15 "AI Risk Management Framework", NIST, January 2023.
16 The IPIE refers to AI assessments as "AI audits".
"Recommendations for a Global AI Auditing Framework: Summary of Standards and Features", IPIE, December 2024.

Challenges to the effectiveness of current AI assessments

Beyond variations across jurisdictions, several common factors are currently hindering the robustness and effectiveness of some AI assessment frameworks — and thus their ability to achieve their intended purpose.

These challenges primarily relate to the lack of clarity and sufficient definition of the following critical elements of the AI assessment, such as:

- Purpose of the AI assessment
- Subject matter of the assessment
- Methodologies, criteria against which the assessment is to be performed, evidence and reporting requirements
- Required qualifications, accountability and absence of conflicts of interest for the AI assessment providers

The nature of AI technologies can also complicate assessments. AI systems are often complex, integrated into larger environments and involve multiple stakeholders. These factors can complicate the identification of the appropriate subject matter of an assessment. Additionally, model drift — the variation in a model's results over time — can also render assessment outcomes outdated and misleading, and the variability of AI systems can complicate reproducibility. Lastly, the rapid advancement of AI technology may outpace the development of technical standards for evaluating performance.

Furthermore, the use of ambiguous, inconsistent and subjective terminology can result in differing interpretations of key concepts and suitable criteria, which may result in assessments that do not address their intended purpose. Broad terms like "fairness," "trustworthiness" and "transparency" can create ambiguity unless specified further[17], and may limit the feasibility and usefulness of certain assessments.[18]

Lastly, insufficiently developed standards and methodologies pose challenges for the rigor and comparability of AI assessments. Stakeholders are increasingly focusing on the need for greater clarity, consistency, objectivity and methodological rigor in setting and applying standards for AI assessments. The International Association of Algorithmic Auditors (IAAA), for instance, was established to bring together experts and "lay the foundation for algorithmic auditing standards." Standards development organizations, such as ISO/IEC[19], CEN-CENELC[20] and NIST, have also taken up this challenge and are working on both adapting existing standards and developing new AI standards.[21] In the UK, regulators have outlined a roadmap for an effective "AI assurance" ecosystem,[22] and launched initiatives to provide detailed guidance on AI assessments.[23] In February 2025, the UN's IPIE released a comprehensive global "AI auditing" framework[24] setting-out technical considerations, providing guidance on assessment scope, assessor qualifications, assessment criteria and methodologies.[25]

Addressing the challenges detailed above is essential for developing coherent and effective policy and business frameworks for AI assessments.

17 UK's Information Commissioner's Office guidance on Explaining decisions made with AI identified six main types of explanations.
18 Vague and subjective criteria may render it difficult to provide assurance in certain instances.
19 Joint work of the International Standards Organization (ISO), the International Electrotechnical Commission (IEC), 2025.
20 Joint work of the European standards bodies CEN and CENELEC under the banner CEN-CENELEC, 2025.
21 For instance, ISO/IEC developed the new ISO/IEC 42001:2023 standard for AI Management Systems, and CEN-CENELEC published EN ISO/IEC 25059:2024 on quality for AI systems based on a pre-existing ISO/IEC standard for software quality.
22 "The roadmap to an effective AI assurance ecosystem," UK Department for Science, Innovation and Technology, 8 December, 2021.
23 UK DSIT refers to AI assurance accordingly: "The term 'assurance' originally derived from accountancy but has since been adapted to cover areas including cyber security and quality management. Assurance is the process of measuring, evaluating and communicating something about a system or process, documentation, a product or an organization. In the case of AI, assurance measures, evaluates and communicates the trustworthiness of AI systems."
24 "Towards A Global AI Auditing Framework: Assessment and Recommendations", IPIE, February 2025.
25 UN IPIE refers to AI audit accordingly: "Auditing an AI system can help evaluate its interactions with individuals, communities, and organizations and assess whether these systems are properly developed, deployed, operated and managed. An audit can check whether an AI system adheres to vital social, ethical and legal norms, such as fairness, data privacy and environmental sustainability."

4 How to make AI assessments more effective

Three fundamental elements of AI assessment frameworks need to be more clearly and consistently defined in order to make AI assessments effective: what is to be assessed, how to perform the assessment and who performs the assessment.[26]

What is to be assessed

For an AI assessment framework[27] to be effective, it should have a well-specified business or policy objective. A clear objective is crucial to avoid misalignments between the information provided by the assessment and the purpose that the AI assessment is intended to serve. The purpose of an assessment should also guide the selection of appropriate methodologies and reference standards.

Importantly, AI assessment frameworks should have a clear and sufficiently defined scope, including the type of assessment (e.g., governance, conformity or performance), the subject matter, and guidance regarding when the assessment should occur. For instance, it is important to determine whether the assessment should evaluate the entire AI system – including training data, algorithms and safeguards – or only its outcomes.

26 Established assessment frameworks in sectors, such as information technology (IT), automotive, pharmaceuticals and cybersecurity can offer insights for AI assessments, as long as accommodations are made for the unique aspects of AI. For example, in IT, assessments (commonly referred to as "audits") are often used to support the security and effectiveness of an organization's IT infrastructure, and involve a comprehensive evaluation of the organization's ability to protect its data, manage risks and comply with relevant industry regulations.

27 Inclusive of assessment frameworks as required in regulation or undertaken voluntarily.

How to perform the assessment

Methodologies and suitable criteria determine how a subject matter is assessed, and it is essential that similar AI assessments use clearly defined and consistent approaches. Some assessments, for instance, may include explicit opinions or conclusions, while others may only provide a summary of procedures performed. A lack of clearly defined methodologies, criteria, evidence and reporting requirements can undermine assessment outcomes and create misunderstandings with the users of the assessments. Consistency, combined with clear terminology, allows users to compare assessment outcomes and to understand how they were reached. Suitable criteria — relevant, objective, measurable and complete — facilitate consistent, comparable and decision-useful assessment results.

Methodologies may include reference to standards like ISAE 3000 (Revised),[28] which guides assurance engagements, or other evaluation processes such as formal verification, red teaming, or quality assurance (see Appendix I for more on ISAE 3000 (Revised)). Evaluation methods should also address challenging properties of AI systems, such as the range of variability in AI system outputs that is acceptable for the use cases and context that the assessment seeks to cover.

Criteria for assessment can be defined directly in the policy framework or referenced through technical standards. The criteria should be suitable and available to users of the assessment to facilitate understanding of the assessment outcomes. When selecting methodologies and criteria, they must align with the assessment's purpose, subject matter and desired confidence level. Some methodologies may be better suited for specific assessments.

Who performs the assessment

The choice of provider is crucial for effective AI assessments because their objectivity, expertise and adherence to transparent methodologies directly influence the credibility, reliability and overall integrity of the evaluation process. Key considerations for selecting assessment providers include:

- Competency and qualifications: Credible AI assessments require professionals with technical knowledge of AI and competency regarding assessment procedures, as well as an understanding of ethical and regulatory frameworks.
- Objectivity: The objectivity of the provider — including its ability to demonstrate the absence of conflicts of interest — impacts the credibility of an assessment and can help foster confidence among stakeholders.
- Professional accountability: Professional accountability requirements can be based on publicly available and accepted standards and guidelines, such as the International Ethics Standards Board for Accountants (IESBA) Code of Ethics for the audit profession.[29] Providers that follow these standards and guidelines enable confidence and help stakeholders understand how assessments are provided.

28 International Standard on Assurance Engagements (ISAE) 3000 Revised, Assurance Engagements other than Audits or Reviews of Historical Financial Information, December 2013.
29 International Code of Ethics for Professional Accountants, IESBA, 2024.

5 Considerations for business leaders

- **Consider the role AI assessments can play in enhancing corporate governance and risk management.** AI assessments can help business leaders identify and manage evolving risks associated with their AI systems and help indicate whether AI systems perform as intended.
- **Evaluate whether — even in the absence of any regulatory obligations — to conduct voluntary assessments to build confidence in AI systems among employees, customers and other important stakeholders.** Market dynamics, investor demand or internal governance considerations may make a voluntary AI assessment advisable to build confidence in a business's AI systems. Moreover, if some AI systems are subject to regulatory obligations, business leaders may choose to use assessments to help measure and monitor compliance.
- **Where voluntary assessments are used, determine the most appropriate assessment.** Business leaders will want to determine whether to conduct a governance, compliance or performance assessment, and whether it should be conducted internally or by a third party.

6 Considerations for policymakers

- **Consider what role voluntary (or mandated) AI assessments can play to build confidence in AI systems**, support successful adoption and contribute to the governance of AI.
- **Clearly define the purpose and components of the assessment framework**, and where possible, the recognized standards or criteria by which the assessment should be performed.
- **Address any expectation gaps** in what AI assessments entail, as well as their limitations. This information can enhance public awareness and confidence by setting realistic expectations about the significance of those assessments.
- **Take steps to build capacity of the market to provide high-quality, consistent assessments.** Policymakers may want to determine if there is sufficient capacity in their jurisdictions to conduct effective AI assessments. If not, they should work with AI assessment providers, professional bodies and others to build capacity, including by supporting the development of assessment quality criteria and accredited training courses.
- **Endorse assessment standards that are, to the extent practicable, consistent and compatible with standards in other jurisdictions.** Policymakers should consider aligning their AI assessment standards with those set by international organizations or major jurisdictions in order to reduce assessment costs and promote cross-border confidence in the credibility of assessments.

7 Conclusion

As businesses continue to develop and deploy AI systems, AI assessments can play an important role in maximizing AI's benefits and mitigating its risks. If properly designed, and if conducted by qualified assessment providers, AI assessments can promote the confidence in AI that business leaders, policymakers and the public seek in order to realize the full potential of this important technology.

8 Authors

Shawn Maher
EY Global Vice Chair Public Policy
Ernst & Young LLP
shawn.maher@eyg.ey.com

Dr. Ansgar Koene
EY Global AI Ethics and Regulatory Leader
Ernst & Young LLP
ansgar.koene1@be.ey.com

Anne McCormick
EY Global Digital Technology Public Policy Leader
Ernst & Young LLP
anne.mccormick@uk.ey.com

Tate Ryan-Mosley
EY Assistant Director, Technology and Geopolitics
Global Public Policy
Ernst & Young LLP
tate.e.ryan-mosley@ey.com

Richard Jackson
EY Global Assurance AI Leader
Ernst & Young LLP
richard.jackson@ey.com

Cathy Cobey
EY Global Responsible AI Leader, Assurance
Ernst & Young LLP
cathy.r.cobey@ca.ey.com

Narayanan Vaidyanathan
Head of Policy Development
ACCA
narayanan.vaidyanathan@accaglobal.com

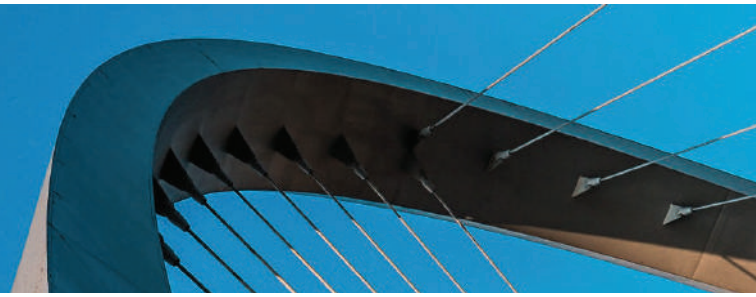
Acknowledgements

We would like to thank the following individuals from the EY organization for their contributions to this work: Katie Kummer, Amy King, Marc Ryser, Yvonne Zhu, Julia Tay, Yi Xie, Denise Schalet, Bridget Neill, John Hallmark, Antonio Quintanilla, Andrew Hobbs, Tim Volkmann, Ambrose Murray, Dean Protheroe, Frank de Jonghe, Detmar Ordemann, Brent Simer, Brandon Miller, Kelly Devine, Dan Albanese and Krista Walpole.

We would like to thank the following ACCA members for their contributions to this work: Alex Panait, Andrew Chong, Fahad Riaz and James Best.

9 Appendices

Appendix I: Case study: Applying ISAE 3000 (Revised) to ISO 42001



Policymakers are considering whether existing assessment, assurance or certification frameworks in use in other domains (such as ISO CASCO Toolbox[30], ISO/IEC 17067[31], ISAE 3000 (Revised)[32], IFRS standards[33]) could, with modifications, be applied to AI. The use of existing frameworks could allow policymakers to avail themselves of the established quality control and accreditation processes.

For example, the ISAE 3000 (Revised) standard established by the International Auditing and Assurance Standards Boards (IAASB)[34], outlines requirements and a methodology for an assurance engagement in domains beyond the scope of a financial statement audit and details steps to compare a certain subject matter against applicable criteria. ISAE 3000 (Revised) is a principles-based standard that is capable of being applied to a broad range of underlying subject matters. This global standard has been a foundation for assurance engagements across a broad set of domains, including sustainability, internal controls and regulatory compliance. The requirements for the assurance provider, as outlined in ISAE 3000 (Revised) include the following:

- Being compliant with relevant ethical requirements, including the absence of conflicts of interest
- Having a sufficient understanding of the subject matter and scope of the assurance ("reasonable" vs. "limited")
- Obtaining necessary evidence to evaluate subject matter against applicable criteria
- Expressing a conclusion regarding the outcome of the evaluation

An assurance provider could use ISAE 3000 (Revised) to evaluate an AI management system against a recognized standard, such as ISO/IEC 42001.[35] Such an engagement could be used to evaluate an AI management system's compliance with an internationally recognized standard.

ISO/IEC 42001 specifies requirements for establishing, implementing, maintaining and continually improving an AI management system (AIMS) within organizations. It is designed for entities providing or utilizing AI-based products or services, and for ensuring responsible development and use of AI systems. ISO/IEC 42001 addresses some of the challenges that AI poses, such as ethical considerations, transparency and continuous learning.

Ongoing work at CEN-CENELEC JTC21 toward developing a Conformity Assessment framework to support compliance with the EU AI Act is referencing the ISO CASCO toolbox and ISO/IEC 17067:2013 "Conformity assessment – Fundamentals of product certification and guidelines for product certification schemes" as primary references. This will provide businesses with means to build on their existing conformity assessment procedures – as used for non-AI systems – when preparing for compliance with the obligations for high-risk AI systems in the EU AI Act.

30 Conformity Assessment tools to support public policy, ISO CASCO toolbox – Conformity Assessment tools to support public policy, 2024.
31 ISO/IEC 17067:2013 - Conformity assessment – Fundamentals of product certification and guidelines for product certification schemes, August 2013.
32 International Standard on Assurance Engagements (ISAE) 3000 Revised, Assurance Engagements other than Audits or Reviews of Historical Financial Information, December 2013.
33 International Financial Reporting Standards (IFRS), 2025.
34 International Auditing and Assurance Standards Boards (IAASB), 2025.
35 ISO/IEC 42001:2023 -Information technology – Artificial intelligence – Management system, ISO/IEC 42001:2023 - AI management systems, December 2023.

Appendix II:
Examples of policy initiatives related to AI assessments

There has been significant activity by policymakers across jurisdictions since 2022, at supranational, national and local levels. The examples below provide further insights on the range of objectives and approaches related to both voluntary and mandated AI assessments.

Policy initiative	Status and objective of the policy initiative	Geographic scope	Terminology used to describe the assessment	Function of the assessment and details
Singapore AI Verify certification	Released to the public in May 2022. This voluntary AI governance testing framework and toolkit is designed to verify the performance of an AI system against the developer's claims, and with respect to internationally accepted AI ethics principles.	Globally available to the public, for voluntary use (no restrictions). Released by Singapore Infocom Media Development Authority (IMDA) and Personal Data Protection Commission (PDPC).	"Testing and assurance," which includes "external validation" and "third-party testing."	"AI governance testing framework to help companies assess the responsible implementation of their AI system against 11 internationally recognized AI governance principles." The governance principles (including transparency, robustness and fairness) are consistent with AI frameworks, such as those from EU and OECD. AI Verify helps organizations validate the performance of their AI systems against these principles through a standardized testing report.

Policy initiative	Status and objective of the policy initiative	Geographic scope	Terminology used to describe the assessment	Function of the assessment and details
EU Digital Markets Act (DMA)	Entered into force in November 2022, and into application from 2 May 2023. Aims to ensure "fair and open" digital markets.	Large digital platforms operating in the EU with a market position that meets the DMA criteria for designation as "gatekeeper platform."	"Independent audit."	Provide the regulatory authority (European Commission) an independently audited description of any techniques for profiling of consumers that the digital "gatekeeper" platform applies to its core platform services.
EU Digital Services Act (DSA)	Entered into force in November 2022. Aims to comprehensively protect the fundamental rights of users on the internet.	Large digital platforms operating in the EU with a number of active users that meets the DSA criteria for designation as "Very Large Online Platform" or "Very Large Online Search Engine" is the scope.	Varies based on technique; can evaluate data, AI model or governance processes.	AI system outcomes.
NIST Risk AI Management Framework (NIST AI RMF)	Released January 2023. Aims to provide a voluntary risk management framework to "better manage risk to individuals, organizations, and society associated with AI."	US NIST has performed several crosswalks with policy frameworks in other jurisdictions (such as EU, Japan and Singapore) to guide non-US users.	"Risk management," "Risk assessment," "Impact assessment," "Performance assessment"	Developed to help individuals, organizations and society manage AI's risks, promote the trustworthy development and responsible use of AI, and the evaluation of AI products, services and systems.
EU Digital Operational Resilience Act (DORA)	Entered into force January 2023, and application started in January 2025. Aims at strengthening the IT security of financial entities and ensuring that the financial sector is resilient.	All financial entities operating within the EU.	Verification (voluntary). External audits (voluntary). Testing through external or internal testers (mandatory).	(Voluntary) Verification of compliance with ICT risk management framework and requirements. Audit of contractual arrangements with ICT third party service providers. Digital operational resilience testing of financial entities' ICT tools and systems.

Policy initiative	Status and objective of the policy initiative	Geographic scope	Terminology used to describe the assessment	Function of the assessment and details
German Institute of Public Auditors in Germany (IDW) PS 861 standard on auditing AI systems.	The most current version of the standard was issued in March 2023. Aims to provide a voluntary framework for the auditing of AI systems. The goal is to enhance trust in AI technologies by establishing a systematic approach to auditing, thereby supporting organizations in managing risks associated with AI implementation.	Primarily pertains to Germany, with potential implications for applications in the EU and beyond (e.g., if applied to organizations with a broader European or global reach).	"Voluntary audits," "Assessment criteria," "Adequacy audit," "Effectiveness audit" of AI systems, "Reasonable assurance."	Clarifies "the requirements for voluntary audits of AI systems outside the scope of financial audits, and sets out the professional understanding according to which public auditors should plan, conduct and report on such engagements while maintaining auditors' own responsibility." The standard sets interrelated assessment criteria for AI systems on the basis of ethical, legal, traceability, IT security and performance requirements. The subject of such an AI audit is the description of the given AI system, including managements commentary on its compliance with the selected assessment criteria. The AI audit is either to be carried out in the form of an "adequacy audit" or an "effectiveness audit," both with reasonable assurance.
Bletchley Declaration	Agreed upon in November 2023. An international agreement that outlines key principles and commitments for the safe development and use of AI, including for robust safety measures, rigorous testing and continuous monitoring of AI systems.	28 signatory countries: Australia, Brazil, Canada, Chile, China, France, Germany, India, Indonesia, Ireland, Israel, Italy, Japan, Kenya, Saudi Arabia, Netherlands, Nigeria, Philippines, S. Korea, Rwanda, Singapore, Spain, Switzerland, Türkiye, Ukraine, UAE, UK, USA and EU.	"Safety testing."	Recommends that firms implement measures, including safety testing, evaluations, and accountability and transparency mechanisms to measure, monitor and mitigate potentially harmful capabilities of frontier AI. The details of such safety testing and accountability mechanisms are not detailed in the Declaration.

Policy initiative	Status and objective of the policy initiative	Geographic scope	Terminology used to describe the assessment	Function of the assessment and details
ISO/IEC 42001:2023 AI Management Systems	Published in December 2023. Aims to ensure the responsible development and use of AI systems by entities providing or utilizing AI-based products or services.	Global.	"Risk assessment," "Impact assessment," "Conformity assessment," "Assurance," and "Internal audit."	"ISO/IEC 42001 specifies requirements for establishing, implementing, maintaining and continually improving an artificial intelligence management system (AIMS) within organizations. It is designed for entities providing or utilizing AI-based products or services, ensuring responsible development and use of AI systems."
UN Panel on Global Standards for AI Auditing (IPIE) – Recommendations for a Global AI Auditing Framework: Summary of Standards and Features, and Assessment and Recommendations	Two reports on AI Assessment have been published by the IPIE (December 2024 and February 2025). The IPIE aims to define criteria and methodologies for AI audits to "establish global standards and foster discussions focused on AI's public impact."	Global scope. Produced by the UN as part of International Panel on the Information Environment (IPIE).	"AI auditing."	Audits as a means to test whether algorithmic or AI systems engender the outcomes they are expected, or whether they have significant – possibly adverse – societal and technological impacts. The audits are seen as mechanisms for assessing AI systems' alignment with norms and principles of AI responsibility, accountability, trustworthiness or safety. These audits probe an AI system's design, development and operations, often examining the model(s) and data used in it. The audits are used to describe how the audited AI system performs against certain established criteria and to report on its impacts.

Policy initiative	Status and objective of the policy initiative	Geographic scope	Terminology used to describe the assessment	Function of the assessment and details
US National Telecommunications and Information Administration (NTIA) **AI Accountability Policy Report**	Published in policy paper March 2024, and is non-binding. Aim is to promote innovation and adoption of trustworthy AI, highlighting the need for new and more widely available accountability tools and information and promoting an ecosystem of independent AI system evaluation.	Produced by NTIA (US agency in the executive branch). Published under the Biden administration. It's currently unclear whether the Trump administration will continue with similar recommendations.	"AI accountability mechanisms," "AI System Assurance."	Advocates for the broader application of AI audits, though it stops short of specifying enforcement mechanisms. The report recommends that (future federal) AI policymaking not lean entirely on purely voluntary best practices; rather, some AI accountability measures should be required. In the past, the NTIA has also called for the creation of a national registry for AI system audits and a "pre-release review and certification" for select systems or models.
Colorado AI Act	Passed in May 2024. It is set to come into effect in February 2026. A set of amendments to the act were proposed in April 2025, but failed to pass before the May 7 closure of Colorado Legislature. A cross-sectoral AI governance law covering the public sector, focused on high-risk AI systems and preventing bias in automated decision-making systems.	Deployers and developers in the state of Colorado (US).	"Impact assessments," "Risk assessments."	Requires developers and deployers of high-risk AI systems to conduct impact and risk assessments, including for bias and discrimination. Impact assessments must include: 1. A statement disclosing the system's purpose, intended use cases, deployment context. 2. Analysis of risks of algorithmic discrimination and mitigation steps taken. 3. A description of categories of data processed. 4. Metrics used to evaluate the system's performance and known limitations. 5. A description of transparency measures taken. 6. Description of post-deployment monitoring and user safeguards to address issues arising from deployment.

Policy initiative	Status and objective of the policy initiative	Geographic scope	Terminology used to describe the assessment	Function of the assessment and details
EU AI Act's General Purpose AI (GPAI) Code of Practice	Passed as part of the EU AI Act. The development is ongoing. Related AI Act obligations take effect on 2 August 2025. Use of the Code of Practice is voluntary. Aim is to provide additional guidance and clarify obligations for the developers of GPAI models. Following the GPAI Code of Practice can help users demonstrate compliance with some EU AI Act requirements.	The Code will support EU AI Act compliance for any company that develops, distributes or otherwise deploys an AI system in the EU (including a company that is headquartered outside of the EU).	"Risk assessment," "Systemic risk assessment."	(The details of the assessment are still to be confirmed. However, the assessments are already outlined at a high-level in the EU AI Act and include establishing measures, procedures and modalities for the assessment and management of the GPAI systemic risks, including documentation thereof.)[36]

36 At the time of publication of this paper, the AI Act's GPAI Code of Practice has not yet been published.

About ACCA

We are ACCA (the Association of Chartered Certified Accountants), a globally recognized professional accountancy body providing qualifications and advancing standards in accountancy worldwide.

Founded in 1904 to widen access to the accountancy profession, we've long championed inclusion and today proudly support a diverse community of over 252,500 members and 526,000 future members in 180 countries.

Our forward-looking qualifications, continuous learning and insights are respected and valued by employers in every sector. They equip individuals with the business and finance expertise and ethical judgment to create, protect, and report the sustainable value delivered by organizations and economies.

Guided by our purpose and values, our vision is to develop the accountancy profession the world needs. Partnering with policymakers, standard setters, the donor community, educators and other accountancy bodies, we're strengthening and building a profession that drives a sustainable future for all.

Find out more at accaglobal.com

EY | Building a better working world

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fueled by sector insights, a globally connected, multidisciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

All in to shape the future with confidence.

EYG no. 005038-25Gbl

BMC Agency
GA 151335318

ED None

ey.com