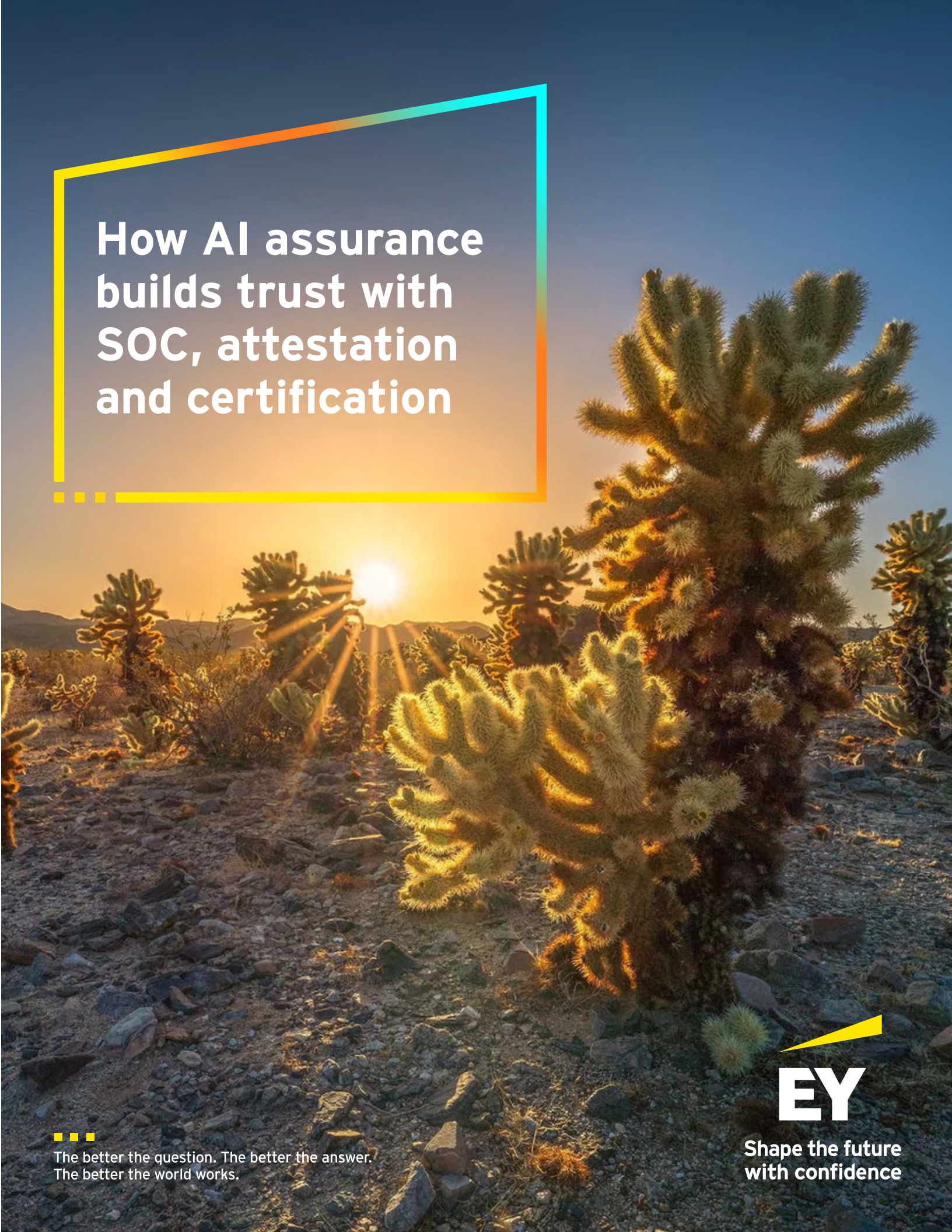




How AI assurance builds trust with SOC, attestation and certification



The better the question. The better the answer.
The better the world works.



Shape the future
with confidence



“

Trust and confidence in AI is earned through control evidence: clear governance, strong data practices and continuous risk monitoring.

Brandon Miller

EY Global and EY Americas Technology Risk System and Organization Controls, Attestation and Certification Leader

AI assurance is becoming essential as AI and generative AI (GenAI) transform how organizations make decisions and deliver services, but significant skepticism remains.

Customers want different types of assurance about how AI systems operate, what data they use and how risks are managed. Organizations using AI must also be able to show stakeholders that their AI systems are reliable and have controls around them functioning as intended. The 14th annual EY System and Organization Controls (SOC), Attestation and Certification Conference explored the growing need for AI assurance and how organizations can navigate this major change.

“Trust is becoming a new requirement in every conversation,” says Yvonne Zhu, EY Canada, Responsible AI Risks and Controls, AI Assurance Leader. “How do we scope AI assurance properly, so you are delivering trust that’s meaningful to your clients and yourself as well?”

While expectations among customers, regulators and boards are high, in many cases, stakeholders are not looking for perfection, say EY leaders. They want assurance that the right considerations are being

addressed. They want to know how AI systems are defined and tested and that they are monitored regularly, because AI systems and the risks they introduce are evolving.

As Natalie Deak Jaros, EY Americas Assurance Financial Services Managing Partner, noted during the conference, “Technology is advancing, and trust must keep up. The conversation has shifted from what AI can do to how organizations can demonstrate trust in AI systems through transparency, governance and evidence.” This shift is increasing demand for AI assurance approaches that provide stakeholders with independent evidence that AI systems are governed responsibly, monitored effectively and supported by appropriate controls, creating a stronger foundation for trust.

How attestation and certification strengthen AI assurance

With the advancement of AI, demand for transparency, governance and reliability continues to rise. Today, customers want tested evidence, not assumptions. The standard for AI assurance has moved from “Does it work?” to assessing “Can we explain and defend it?”

System and Organization Controls (SOC) reports and International Organization for Standardization (ISO) certifications have traditionally helped bridge the gap between service providers and customers by offering standard ways to demonstrate that information systems are reliable and well controlled. As AI raises new questions about governance, monitoring and risk management, these reports and certifications can continue to help organizations communicate trust and confidence in their responsible AI practices in a format that customers, regulators and boards already recognize.

Unlike traditional systems, AI is not a series of control points or a checklist of independent items. It can include data, models, platforms, applications and operations, which makes attestation even more complex. Providers may need to show lifecycle controls, monitoring and oversight, while customers may need controls over how the system performs in their own environment.

“

From a customer’s point of view, ‘trust me’ is not enough. I need hard evidence and any kind of trust without evidence is just hope. Unfortunately, hope is not a control.

Jatin Sehgal

EY Global ISO Leader; EY CertifyPoint Managing Partner,
Ernst & Young CertifyPoint B.V





How AI improves SOC reporting and attestations

As organizations work to provide stronger evidence around AI, they are also exploring how AI can help improve the attestation process itself. AI can already deliver value across the SOC lifecycle and in audit-adjacent work by improving consistency, visibility and speed across documentation, evidence collection, mapping and response processes.

Conference speakers pointed to six practical areas where AI can support SOC and attestation work today:

1. Consolidate process and procedure documentation to draft control descriptions, establish consistent terminology and map completeness against the American Institute of Certified Public Accountants (AICPA) Trust Services Criteria.

2. Draft structured management responses, helping to address root cause analysis, remediation actions, timelines and ongoing monitoring commitments.

3. Convert meeting notes into structured action items, audit documentation and clarify control areas.

4. Collect evidence continuously to generate real-time compliance snapshots and identify gaps.

5. Draft tailored responses to customers' security questionnaires, learning from issued SOC reports and approved answers over time.

6. Track evidence collection, escalations and project completion on AI-powered dashboards.

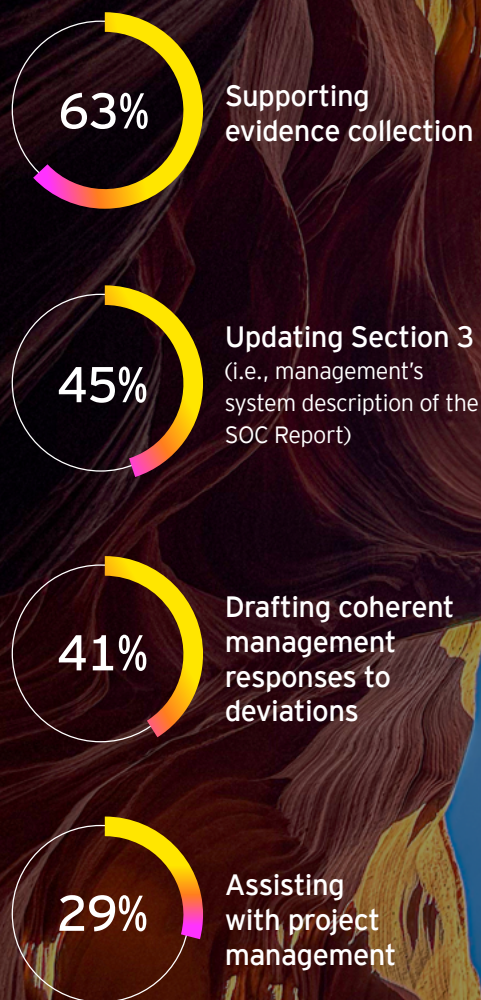
In framework and control mapping, AI can compare internal control data sets with process and control frameworks, laws and regulations. AI can also be used to monitor AI system performance, pinpointing problems like model drift detection at an early stage. For SOC report recipients, AI can be used to review SOC reports, compare reports to their risk assessments, identify changes from prior periods and call out control deviations. However, EY leaders emphasize that even as accuracy improves, AI-generated outputs and processes still require human oversight. AI may invent details and fill in blanks, even when instructed to ignore them. AI agents may rewrite themselves and change their behavior to work around anomalies.

With AI agents becoming part of the scene, organizations are encouraged to start by building and testing simple AI automations in controlled environments and then expanding into multi-agent capabilities under close oversight as programs mature and governance has been implemented.

If a task involves creating insights, gathering knowledge from a range of sources, recognizing complex patterns and analyzing readily available data, it may be a good use case for AI. On the other hand, if judgment is needed or nuance is involved, if explaining how the AI model produces output in specific step-by-step detail is required, or if a business case can't be made for setting up the AI system to address the problem defensibly and ethically, the problem may not be a good fit for AI.

"Organizations that are just getting started in AI are advised to start with governance and an AI inventory now," says John McLain, EY Americas, Assurance AI Deputy Leader and Technology Risk AI Leader.

Participants' top four use cases for AI usage in SOC reporting



Source: Live polling of attendees at the 2026 Annual EY SOC, Attestation and Certification Conference; multiple selections were possible.

“

When you think about AI, the sky is the limit. Whatever you're doing, thinking about or reviewing, it can help tremendously. There's significant upside, but there are also risks.

John McLain

EY Americas, Technology
Risk Leader and Assurance
AI Deputy Leader

Why data readiness is critical for AI assurance

AI performance depends heavily on accessible, centralized, high-quality data, which means the return on investment from AI is directly tied to data and infrastructure investment. Organizations are hiring chief data strategy officers to manage strategy, governance and controls.

“If you have good data governance, you can unlock value from all that data very quickly with the use of AI,” says Ryan Ward, EY, US-East Technology Risk AI Leader. Fixing data now is the most important investment that can be made, because AI learns from data, and bad data will be replicated. When problems arise, organizations may have to answer not only how a model performed, but what data it used, how that data moved through the system and who was responsible for managing it.



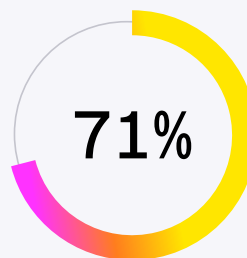
Managing AI risks through continuous assurance

Risk management and control processes help organizations fulfill contractual commitments and maintain stakeholder trust.

Most organizations don't struggle because they ignore regulation. They struggle because different rules apply at the same time – and often to the same AI system. While many of these controls tend to be IT-centric, other dimensions of risk include operational, enterprise, financial and people risks.

Risk assessment may sound straightforward: define the organization's risk appetite, identify inherent risk, apply controls and reduce the risk profile. However, the risk landscape is constantly changing because of technological upgrades, regulatory shifts, evolving customer expectations, acquisitions, disruptions and changes in data or model performance. That means risk assessment cannot be treated as a static or annual exercise. Organizations need to determine how often their risk assessment cycle should refresh based on their AI use cases, regulatory exposure, business environment and risk tolerance.

"Controls that were sufficient last year may not hold up today," says Daryl Box, EY Americas Assurance Technology Risk Leader. "The organizations that get this right will treat risk assessment as a living process, not a checkbox – reviewing it regularly as models, data and regulations change."



of conference participants rank the maturity of their risk management practices as a 7 or lower out of 10.



“

Trust is becoming a new requirement in every conversation.

Yvonne Zhu

EY Canada, Responsible AI Risks and Controls, AI Assurance Leader

Three ways to strengthen AI assurance and build trust

1

Map AI use now: Build an inventory across tools, pilots and vendor solutions to create the foundation for governance and assurance.

2

Fix the data first: Strengthen data ownership, quality and governance before scaling AI maturity.

3

Reassess risk often: Revisit AI risks as models, data, regulations and business priorities evolve.

Our Ernst & Young team

Authors



Brandon R. Miller

EY Global and EY Americas Technology Risk System and Organization Controls, Attestation and Certification Leader

brandon.miller@ey.com



Nate Adler

Senior Manager, Technology Risk

Ernst & Young LLP
nate.adler@ey.com



Jatin Sehgal

EY Global ISO Leader; EY CertifyPoint Managing Partner, Ernst & Young CertifyPoint B.V

jatin.sehgal@ey.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.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

© 2026 EYGM Limited
All Rights Reserved.

SCORE 115096-26-GBL
2602-10679-CS
ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, legal or other professional advice. Please refer to your advisors for specific advice.

ey.com