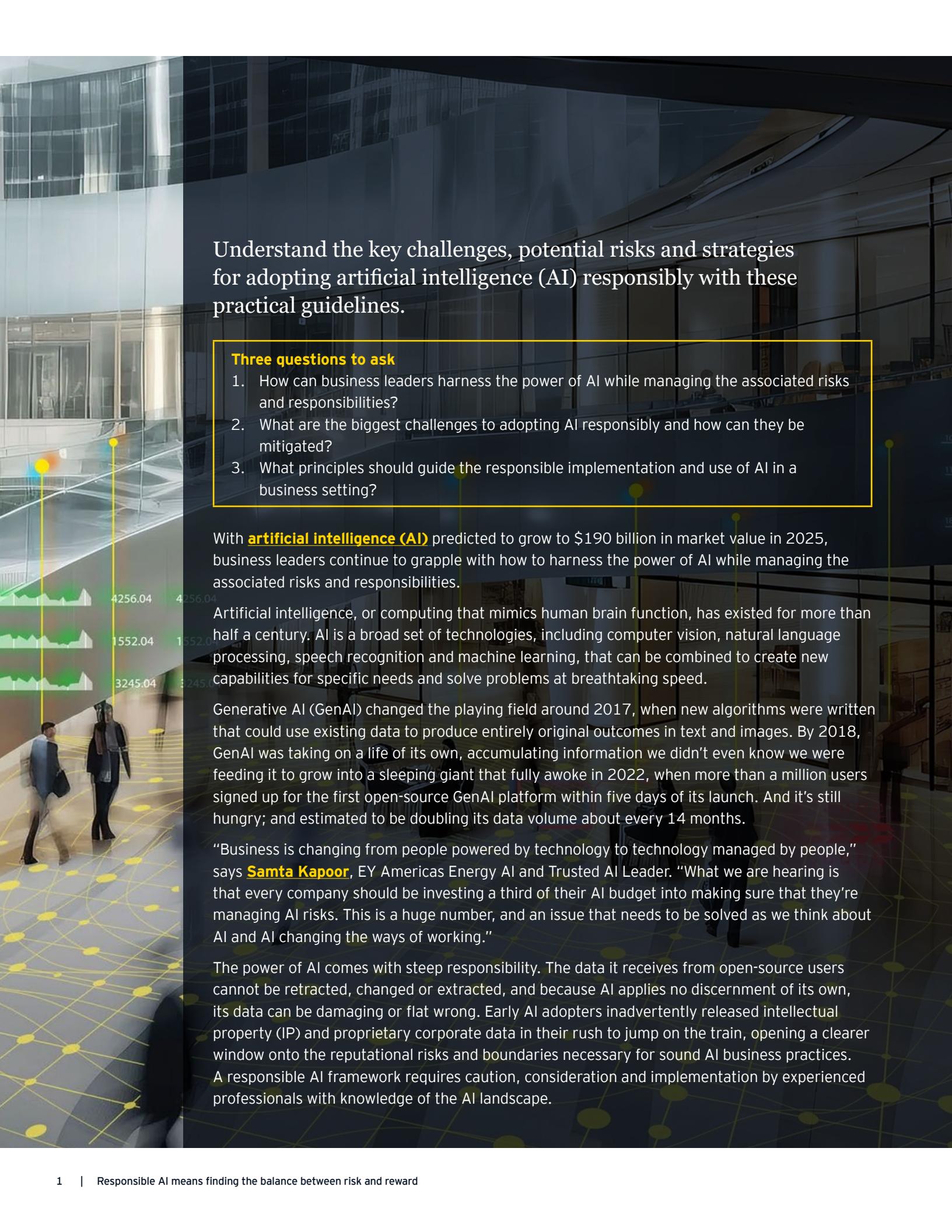




Building a better  
working world

Responsible AI  
means finding the  
balance between  
risk and reward





Understand the key challenges, potential risks and strategies for adopting artificial intelligence (AI) responsibly with these practical guidelines.

#### Three questions to ask

1. How can business leaders harness the power of AI while managing the associated risks and responsibilities?
2. What are the biggest challenges to adopting AI responsibly and how can they be mitigated?
3. What principles should guide the responsible implementation and use of AI in a business setting?

With **artificial intelligence (AI)** predicted to grow to \$190 billion in market value in 2025, business leaders continue to grapple with how to harness the power of AI while managing the associated risks and responsibilities.

Artificial intelligence, or computing that mimics human brain function, has existed for more than half a century. AI is a broad set of technologies, including computer vision, natural language processing, speech recognition and machine learning, that can be combined to create new capabilities for specific needs and solve problems at breathtaking speed.

Generative AI (GenAI) changed the playing field around 2017, when new algorithms were written that could use existing data to produce entirely original outcomes in text and images. By 2018, GenAI was taking on a life of its own, accumulating information we didn't even know we were feeding it to grow into a sleeping giant that fully awoke in 2022, when more than a million users signed up for the first open-source GenAI platform within five days of its launch. And it's still hungry; and estimated to be doubling its data volume about every 14 months.

"Business is changing from people powered by technology to technology managed by people," says **Samta Kapoor**, EY Americas Energy AI and Trusted AI Leader. "What we are hearing is that every company should be investing a third of their AI budget into making sure that they're managing AI risks. This is a huge number, and an issue that needs to be solved as we think about AI and AI changing the ways of working."

The power of AI comes with steep responsibility. The data it receives from open-source users cannot be retracted, changed or extracted, and because AI applies no discernment of its own, its data can be damaging or flat wrong. Early AI adopters inadvertently released intellectual property (IP) and proprietary corporate data in their rush to jump on the train, opening a clearer window onto the reputational risks and boundaries necessary for sound AI business practices. A responsible AI framework requires caution, consideration and implementation by experienced professionals with knowledge of the AI landscape.



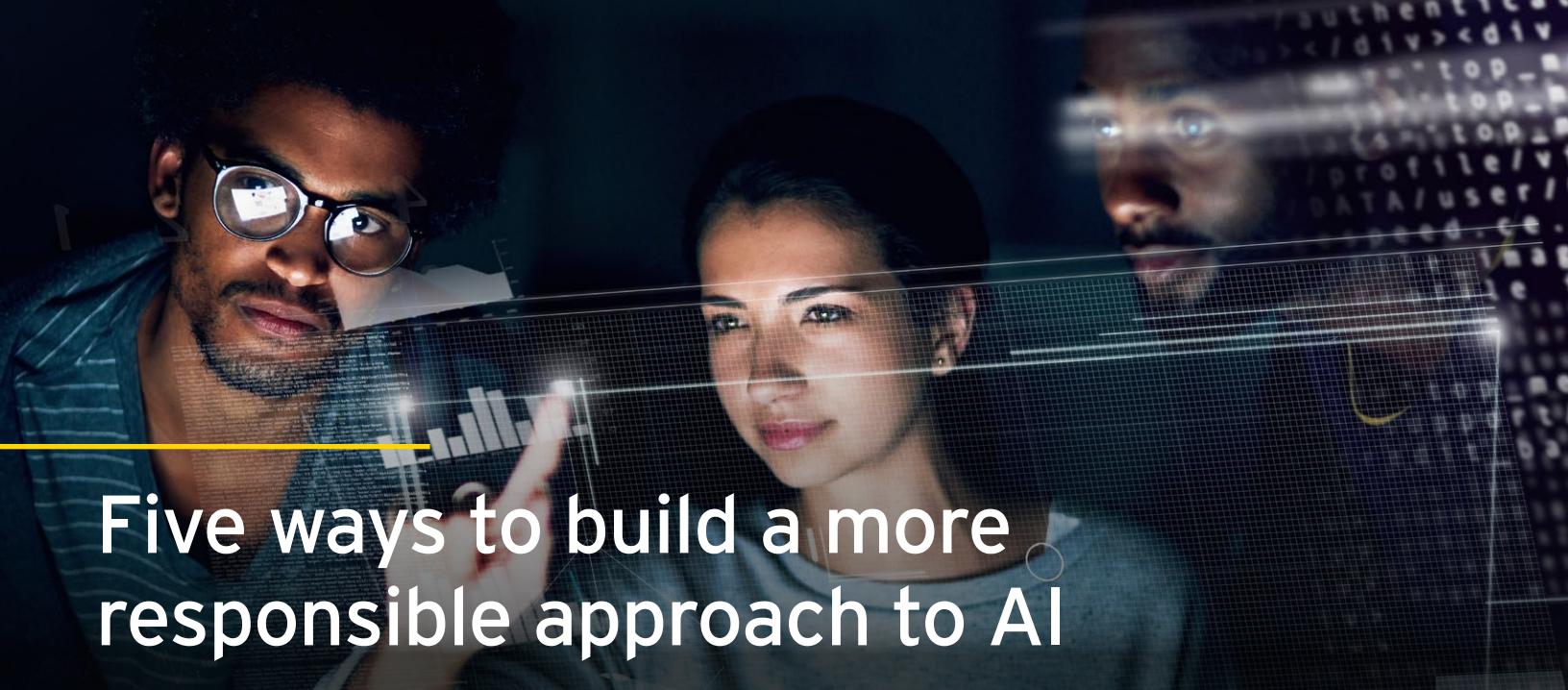
# Five challenges to adopting AI responsibly:

- 1. Data:** Lack of preparation of organizational data, risking access by external parties, such as outside collaborators and sources.
- 2. Performance:** Decentralized AI policies that widen access to the tools too soon, before proper training and governance are established.
- 3. Algorithms:** Complex technologies that may allow unique AI outputs for individual prompts, without tracking and retaining AI training data.
- 4. Design:** Inscrutable practices, such as blackbox AI solutions and data changes within models.
- 5. Training:** Lack of thorough knowledge-led training and comprehensive understanding of GenAI and its associated risks that can lead to inadvertent misuse.

"One of the trickiest parts of channeling AI for business is the human bias factor," says Kapoor. "AI absorbs everything it receives without judgment, so individual user choices, however innocent or inadvertent, can easily affect AI outcomes, becoming a permanent part of the AI universe. That's why it is advisable to create a protected internal space for practice and experimentation before applying AI capabilities to external business deliverables."

There is no one off-the-shelf business solution for AI governance. At this stage, it remains a collective, yet largely siloed, endeavor within individual organizations, and the investment required depends on the stage of AI maturity. Those responsible for guiding AI implementation require deep knowledge of the evolving technology, understanding of the business risks and a high level of leadership trust.

"A responsible approach to AI balances the power of innovation with the associated risks and challenges," says [Kapish Vanvaria](#), EY Americas Risk Leader. "It is up to chief risk officers (CROs) and risk management teams to create an environment where AI can bring benefit without compromising organizational data. That requires sophisticated understanding of the technology, its potential – and its pitfalls – and an advanced framework to support the collective business objectives and oversight. The strategy should come from the C-suite and be communicated clearly and directly to everyone who has access to AI use on behalf of the business."



# Five ways to build a more responsible approach to AI

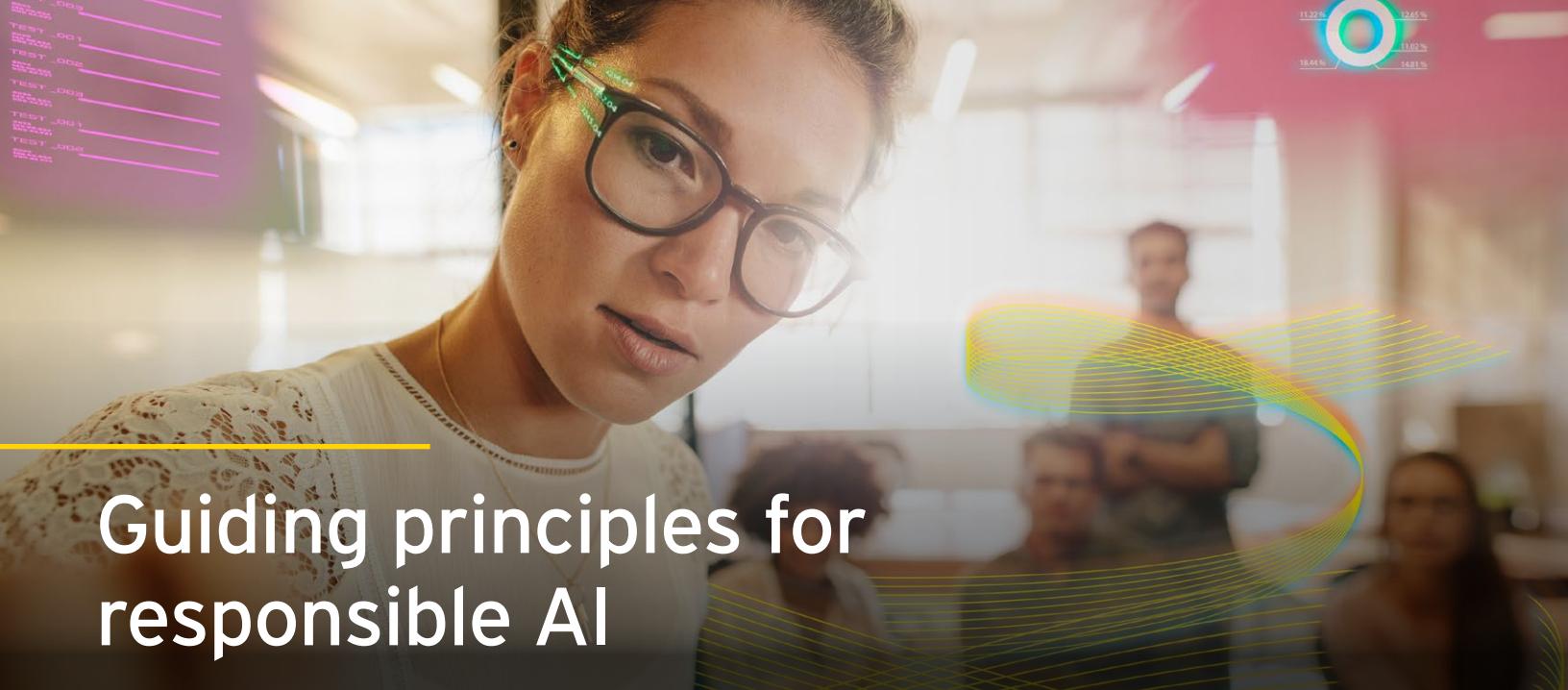
AI is hardly new news, but its full story is still unfolding. A responsible AI framework can help mitigate AI risks while complying with rapidly emerging global AI regulations. The EU, China and Canada have led the charge with the US's Biden administration following closely, issuing an executive order (EO) outlining AI regulations in October 2023.

The sweeping EO, which aims to promote the “safe, secure, and trustworthy development and use of artificial intelligence,” will impact organizations across all sectors of the economy, from the most mature AI implementers to first-time adopters.

By following these steps, businesses can evaluate AI risks and build controls across critical business functions

1. Define a responsible AI framework to validate compliance of AI models from design to implementation with a rigorous feedback mechanism.
2. Establish an AI operating model, a multidisciplinary AI organization structure comprising business, technology and various compliance functions to implement AI at scale responsibly.
3. Employ specialized cybersecurity controls to meet the unique challenges presented by AI systems and mitigate risk to your organization.
4. Prepare your data. AI requires vast amounts of unstructured and structured **data**, and a mature data management program with robust governance is necessary to deploy transformative AI solutions.
5. Activate your enterprise across functions, defining roles and responsibilities for each and establishing a process to educate, train and inspire users.





# Guiding principles for responsible AI

"Reliability can go two ways. One is your AI system is performing as expected. And the other is that it is able to respond safely to new situations," says Kapoor. "Companies need to have a strong monitoring framework with the tools and infrastructure necessary to make the platform easy to update and monitor platforms, and also generate reports. Automating analytics and reporting is key. AI is continually learning; it is not one and done."

The National Institute of Standards and Technology (NIST) will develop the guidelines and leading practices for developing and deploying safe, secure and trustworthy AI systems. In support of these efforts, NIST is establishing the U.S. Artificial Intelligence Safety Institute (USAISI)<sup>1</sup>, served by the U.S. AI Safety Institute Consortium. The consortium brings together more than 200 organizations, including the EY organization, to develop science-based and empirically backed guidelines and standards for AI measurement and policy. This lays the foundation for AI safety and preparing the US to address the capabilities of the next generation of AI models or systems, from frontier models to new applications and approaches, with appropriate risk management strategies.

Guided by the NIST risk management framework and professional experience, the EY organization developed these basic principles to help our clients build confidence and trust in the evolving understanding, regulation, cross-sector coordination and risk mitigation that will define the future optimization of AI.

- ▶ **Accountability:** Establish clear and delineated internal ownership over AI systems and their impacts across the AI development lifecycle. Open the access pipeline slowly as user success builds.
- ▶ **Transparency:** Communicate openly with users about the purpose, design and impact of AI systems, so that designers and users can evaluate and appropriately deploy AI outputs. Help them appreciate and better understand the benefits and the risks.
- ▶ **Fairness:** AI systems should be designed with consideration for the needs of all relevant stakeholders, with the objective of promoting inclusiveness and positive impact. The broader impact of this technology should fully align with your organizational mission and ethics.
- ▶ **Reliability:** AI systems should meet stakeholder expectations and perform with precision and consistency, remaining secure from unauthorized access, corruption and attacks. If an AI application is behaving unexpectedly and raising questions, it's best to pull back use immediately for internal evaluation.
- ▶ **Privacy:** Data privacy, including collection, storage and usage, is paramount as AI systems are being deployed to internal members of any organization. A gradual, carefully planned approach to AI access and usage can minimize data risk.
- ▶ **Clarity:** Anyone using AI on behalf of your organization should receive explicit communication regarding potential risks, formal policies and expectations so they are equipped to assess, validate and challenge if necessary.
- ▶ **Sustainability:** The design and deployment of AI systems are compatible with the goals of sustaining physical safety, social wellbeing and planetary health.

The views reflected in this article are the views of the author and do not necessarily reflect the views of the global EY organization or its member firms.

## About EY AI capabilities:

EY professionals guide businesses toward responsible AI use by listening and developing customized options. Learn more by visiting [EY.ai](https://www.EY.ai)

## Summary

The possibilities of artificial intelligence are seemingly endless, and while they have immense potential to empower your business, preparation is critical to avoid exposing or creating weaknesses. GenAI already has the ability to build empires in seconds and to tear them down just as swiftly. But with the right guiding principles – including purposeful design, agile governance and vigilant supervision – this technology can blow minds without endangering future business.

## Contacts



**Sinclair Schuller**  
Partner, Ernst & Young LLP



**Samta Kapoor**  
EY Americas Energy AI and Trusted AI Leader



**Kapish Vanvaria**  
EY Americas Risk Leader



**Dan Diasio**  
EY Global Artificial Intelligence Consulting Leader

### References:

<sup>1</sup>U.S. Artificial Intelligence Safety Institute (USAISI)

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

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](http://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](http://ey.com).

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

© 2024 Ernst & Young LLP  
All Rights Reserved.

2408-4588941  
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](http://ey.com)