
KPMG
When trust in AI matters, system cards keep score
kpmg.com

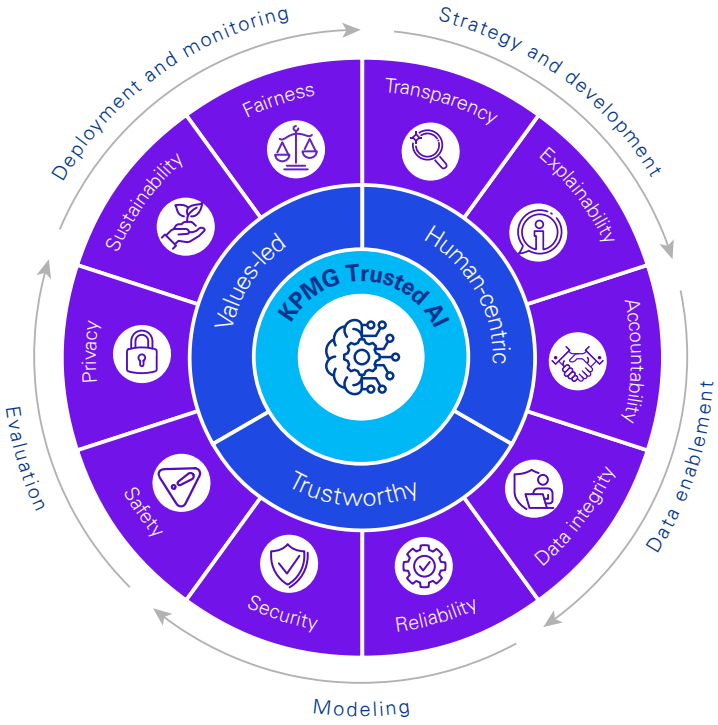
Introduction

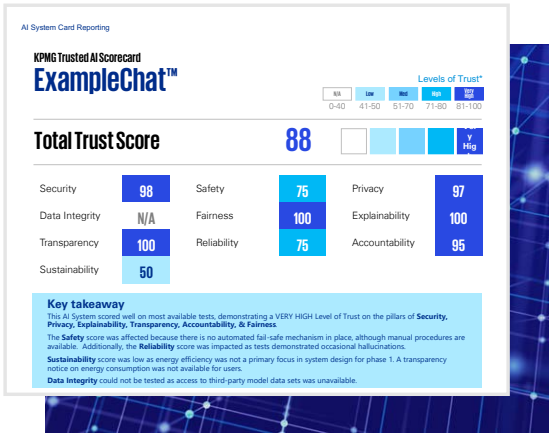
As artificial intelligence (AI) rapidly transforms nearly every sector, the path to scaling AI solutions has introduced new challenges. The current technology landscape is not immune to risks and limitations, from bad chatbot advice to slanderous hallucinations.[1] This has tempered aspirations for a quick launch of technology-enabled use cases across many businesses. What's hindering adoption? Trust in the technology's ethical foundations and confidence in its risk guardrails.

Committed to reassuring stakeholders of AI's fairness and safety, organizations are striving to share more about AI's inner workings as well as the reliability of its outputs. This is especially important as more and more businesses are leveraging complex technologies like generative AI (GenAI) and AI agents. In fact, various standards advocate such transparency, including:

- The European Union's AI Act (EU AI Act)
- The National Institute of Standards and Technology's AI Risk Management Framework
- The Open Web Application Security Project Generative AI, LLM Security Guidance and Initiatives.

Among these standards' core guidelines is the need to apply and document appropriate levels of control for high-risk use cases. Yet, most organizations lack uniform technical specifications or reporting to consistently describe their AI systems, controls compliance, or risk mitigations. A valuable tool to this end is the right AI system card. As organizations align their AI governance practices with increasing regulatory conventions and leading standards, a rigorous evaluation and reporting approach is essential. This strategy will build trust with stakeholders and regulators, helping ensure transparency and accountability in AI development and deployment.




AI System Card Reporting

KPMG Trusted AI Scorecard

ExampleChat™

Levels of Trust*

N/A	Low	Med	High	Very High	
0-40	41-50	51-70	71-80	81-100	

Total Trust Score 88

Security	98	Safety	75	Privacy	97
Data Integrity	N/A	Fairness	100	Explainability	100
Transparency	100	Reliability	75	Accountability	95
Sustainability	50				

Key takeaway

This AI System scored well on most available tests, demonstrating a VERY HIGH Level of Trust on the pillars of **Security, Privacy, Explainability, Transparency, Accountability, & Fairness**.

The **Safety** score was affected because there is no automated fail-safe mechanism in place, although manual procedures are available. Additionally, the **Reliability** score was impacted as tests demonstrated occasional hallucinations.

Sustainability score was low as energy efficiency was not a primary focus in system design for phase 1. A transparency notice on energy consumption was not available for users.

Data Integrity could not be tested as access to third-party model data sets was unavailable.

> This strategy will build trust with stakeholders and regulators, helping ensure transparency and accountability in AI development and deployment.

[1] Olavsrud, "12 famous AI disasters," CIO, October 2, 2024.

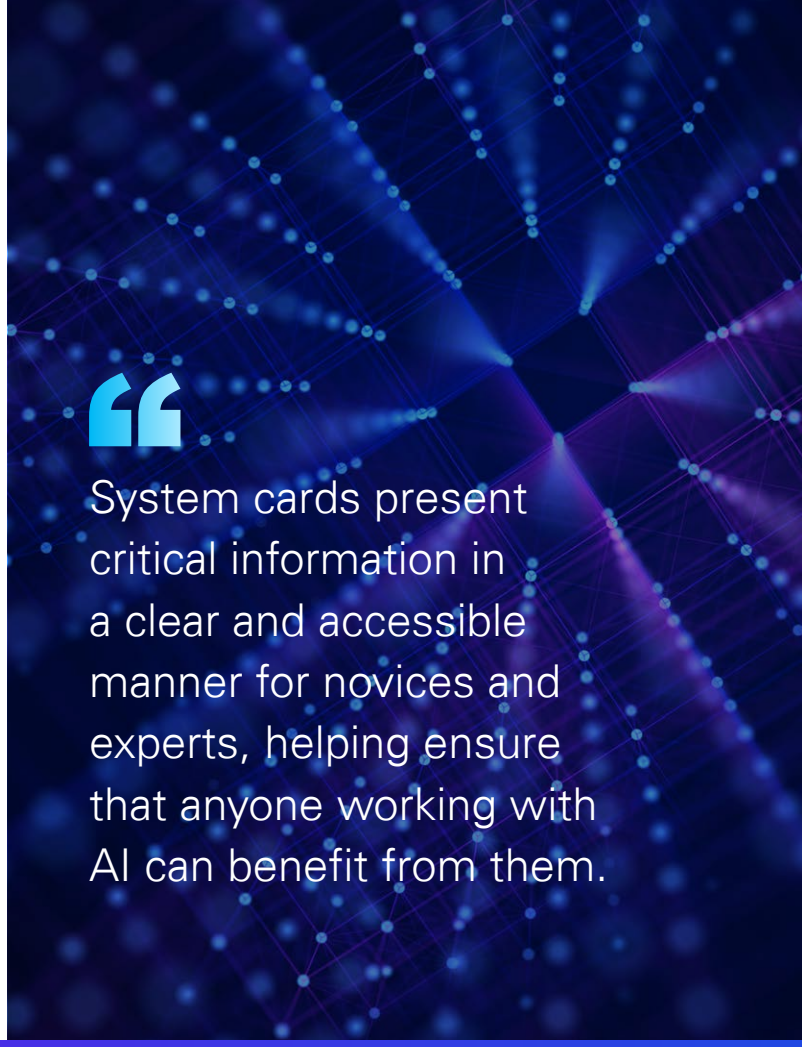
© 2025 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The value of system cards

System cards document how technology is used within an organization, viewed through a business, technology, and risk lens. They present critical information in a clear and accessible manner for both novices and experts, helping ensure that anyone working with AI can benefit from them.

Acting as a single, authoritative source, these transparency reports evaluate entire AI systems by detailing intended use, data considerations, AI components, and limitations, ultimately contributing to a trust score that reflects adherence to an organization's responsible AI principles.

Unlike model cards, which concentrate exclusively on individual machine learning models, system cards provide a holistic overview of the entire AI system. This thorough approach, embraced by KPMG LLP, assesses the wide-ranging integration and impact of various system components.

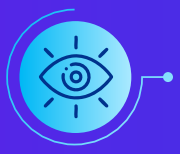


Overcoming AI pain points

Building and maintaining system cards addresses key challenges to AI system signoff. System cards can:

Make AI systems easier to understand

Although system cards won't crack open the "black box" of the language models behind GenAI, they can help stakeholders get more comfortable with some of a large language model's nuances. With a clear, concise description of an AI system's purpose, data considerations, and performance metrics, stakeholders can better understand how a model's inputs translate to its outputs.



Clarify system confusion

With system cards, stakeholders can make informed decisions on the suitability and readiness of AI tools for different jobs with simple, yet detailed descriptions of what makes up the system. Each AI system is comprehensively evaluated through a robust series of independent assessments that provide a full picture of the tool.

Demonstrate responsible AI principles

System cards ground design choices and performance in organizational values. By disclosing system performance against key measures of ethical use and trust, system cards build credibility for your AI systems. The evaluation process helps ensure that the technology aligns with and reinforces the standards and principles guiding the business. And, they are a valuable resource for tracking compliance and reporting efforts back to regulators.

© 2025 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

How the life-cycle view benefits stakeholders

With this full-lifecycle view across critical domains, system cards operationalize transparency, helping to build trust and confidence. How? By benefiting various stakeholders in different ways:

Responsible AI leaders

Can evaluate how the system performs against acceptable thresholds, allowing them to make informed decisions on deployment and risk mitigation.

Risk and compliance leaders

Can leverage this information for internal and external reporting to key stakeholders.

AI developers and engineers

Can gain insights into the technical approach and interdependencies of the system's components, using this knowledge to drive future technology improvements.

System end users

Can understand how to interact with an AI system, explore its key capabilities, and determine if it's suitable for their specific use case.

© 2025 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG recommended approach to system cards

A robust system card incorporates three primary inputs, all of which can be created in parallel with the system card process:

1. A set of responsible AI principles that reflect an organization's values and align with leading frameworks
2. An AI asset inventory that categorizes systems by risk tiers
3. A defined set of AI risks, controls, and measurable attributes

Establish responsible AI principles aligned to leading frameworks:

While most users are aware of the major risks posed by AI, these risks can vary among adopters depending on use cases, region, and application of the technology. An organization's responsible and ethical principles should address its specific risks, reflect its core values, and align with the leading frameworks and standards set by regulators and agencies in its markets.

Implement an AI asset inventory with risk-tiers:

Centralizing AI systems within an asset inventory to effectively trace and manage risk levels (e.g., Unacceptable, High, Medium, Low) aligns with emerging standards and regulations, enabling companies to make informed risk and compliance decisions. Assets with the highest risk levels demand greater oversight and risk mitigation strategies.

Define AI risks, controls, and measurable attributes:

KPMG recommends aligning risks, controls, and measurable attributes systematically by risk levels. Prior to launching into production, thorough testing is essential—this includes deploying a "purple team" to rigorously conduct offensive testing and defensive evaluation in concert against the organization's responsible AI framework. Automated tooling for these evaluations is critical for speed and throughput. In addition, supplementary attestations from system owners may be required to augment tests. By calculating a trust score derived from these evaluations, organizations can accurately gauge the system's readiness and performance relative to their principles.

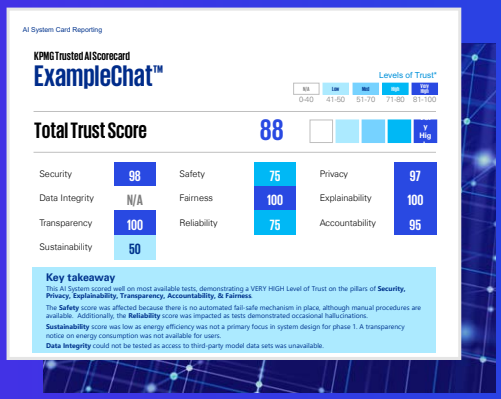
Operationalize and start implementing today:

Effectively operationalizing system cards requires a blend of established frameworks, automation tools, and human expertise. Additionally, a publishing strategy is necessary to ensure system cards are accessible, transparent, and continuously refreshed.

Keep in mind that AI and the regulatory environment will continue to rapidly evolve—striving for perfection should not hinder progress. Establishing system cards is an iterative process that demands organizations remain adaptive and agile. The EU AI Act, for example, mandates ongoing system and risk monitoring as well as documentation of regular updates. As new laws and frameworks emerge, waiting to act is not an option.

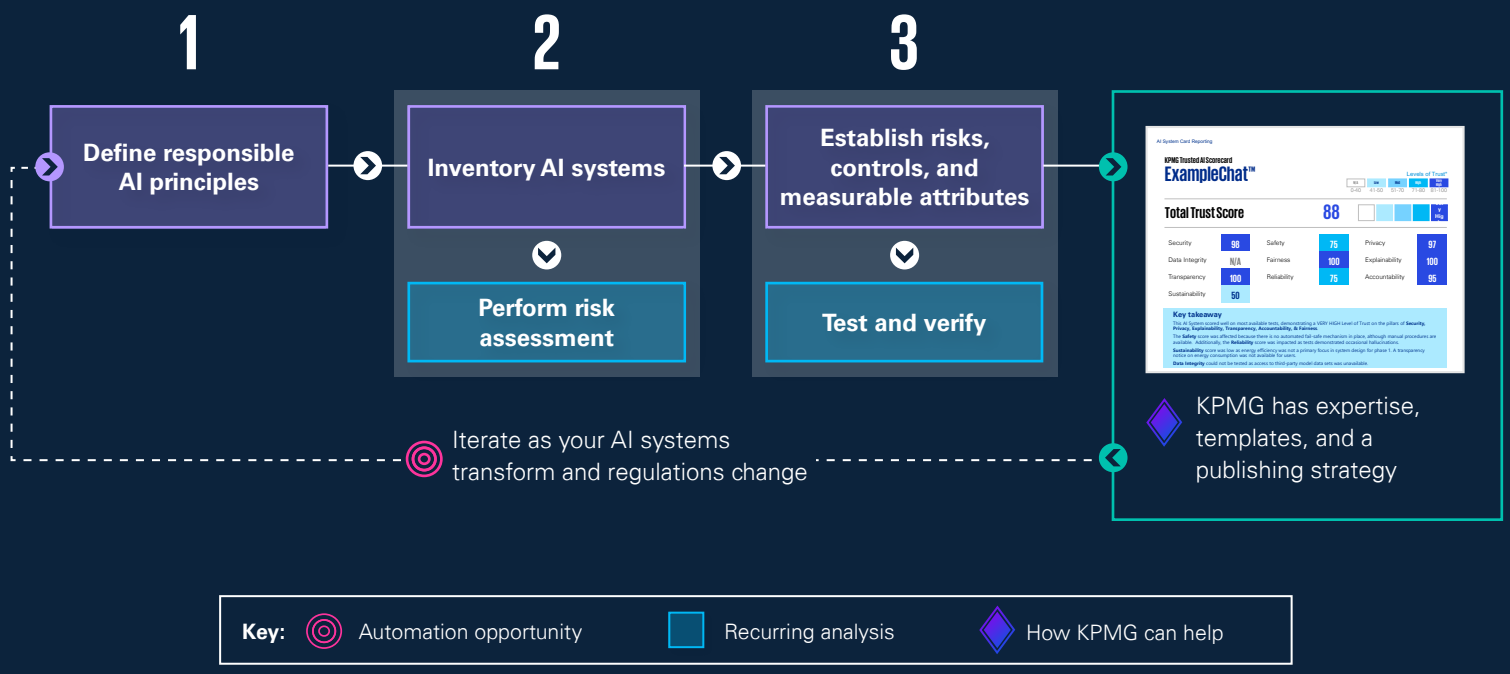
Key system card success factors:

- Alignment of stakeholders on approach, timeline, objectives, and ongoing governance
- Automated testing of AI systems across several categories including security and privacy
- Publishing system cards, helping ensure they are accessible and easy to understand



© 2025 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

KPMG has a defined process to create system cards

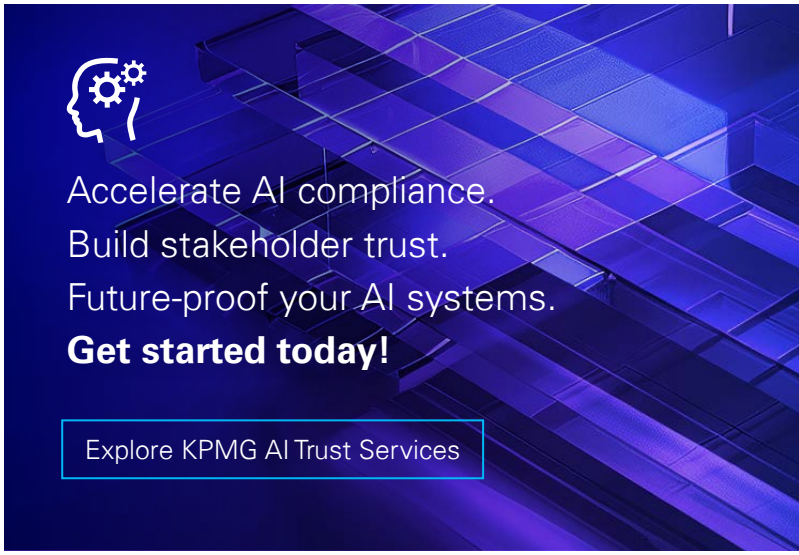


The KPMG advantage

The KPMG System Card (patent-pending) is an advanced extension of the KPMG Trusted AI framework, designed to provide a transparent, structured, and thorough evaluation of AI systems in their entirety—whether they are classic AI models, knowledge assistants, or agentic systems.

The KPMG System Card enhances traditional evaluations by assessing AI against key pillars like reliability, safety, fairness, and accountability. With a holistic aggregated trust score aligned to ethical principles, the system card enables stakeholders and end users to confidently assess, govern, and monitor AI at scale.

We combine our deep industry experience and modern technical skills to help businesses harness the power of AI to accelerate value in a trusted manner—from strategy and design to implementation and ongoing operations. Whether you're deploying AI-powered assistants, agentic systems, or enterprise AI solutions, our industry-leading Trusted AI framework and patent-pending AI system cards can help you accelerate value with confidence.



© 2025 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Authors

Bryan McGowan
Principal,
Global and US Trusted AI Leader

Caleb Hargesheimer
Director,
Advisory,
US Trusted AI

Aisha Tahirkheli
Managing Director,
Advisory,
US Trusted AI

Leigh Harton
Manager,
D&A Modeler,
US Trusted AI

For more information, please contact:

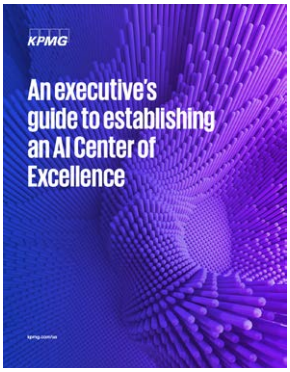
Bryan McGowan
Principal,
Global and US Trusted AI Leader
bmcgowan@kpmg.com

The authors would like to thank:
Michael Bender, Lisa Bigelow, Taylor Campbell, Christopher Jambor, Elizabeth Kalooky, and Lara Volpe.

Related thought leadership:

An Illustrative AI Risk and Controls Guide

KPMG AI Quarterly Pulse Survey: 2025 is the year of agentic AI



An executive's guide to establishing an AI Center of Excellence

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

Please visit us: **kpmg.com** **Subscribe**

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.

© 2025 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

DASD-2025-17065