

Trustworthy AI as a value lever



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

EY

Shape the future
with confidence

Ernst & Young LLP (EY US) fielded a study among leading technology executives to better understand how they view trust. The results of the survey were originally published by The Information.



Trustworthy AI as a value lever

Trust is a requirement for the success of AI, an operating condition that helps enable speed, scale and autonomy. As enterprises implement AI technology, they are moving at the speed of trust. Go faster, and unforeseen risks can proliferate; go slower, and you can fall behind your competitors.

Most executives are aware that trust is key to the success of AI, but less than half of companies can effectively support trustworthy AI, reveals a survey of more than 150 readers of The Information.

Seventy-one percent of respondents say that trust in AI is key to achieving business outcomes.

This report outlines the approaches to build trustworthy AI and achieve business value:

Embedding trust in AI: As companies scale deployment of AI, they face constraints related to transparency, liability and compliance. Trust can be embedded into how decisions are made and executed by designing workflows, systems and AI interactions so that policies, thresholds and accountability operate in real time, not after the fact. Respondents describe embedding trust into decisions to help organizations move faster with confidence – making it a way of operating, not an added layer of governance.

Bringing together executives who are split on AI: Executives' mindsets toward AI vary depending on their function. Top management and technology leaders are most likely to be enthusiastic champions; finance and legal functions are cautious evaluators, while risk functions tend to be pragmatic adopters. Executives can find agreement when they trust their AI protocols and understand their responsibilities.

Assigning responsibility for building trust in AI:

Responsibility for building trust in AI is spread across multiple functions. Business and product units often lead, but cross-functional and technology groups all have roles. Survey respondents point toward bringing mindsets together by making all relevant functions cocreators of AI solutions, so that different goals are factored in by design. This approach can help executives work together toward a shared goal.

Designing trustworthy AI

Trust is at the core of decision-making about implementing AI. Seventy-six percent of The Information's survey respondents say that trust in AI significantly influences organizations' decisions to implement it. Trust in AI is treated as table stakes by survey respondents: roughly 65%-75% of respondents agree that "trust in AI is key to outcomes" and "building trust in AI is a top priority." (See chart.)

In other words, trust is a value lever, allowing companies to say "yes" to AI projects more often, leading to business outcomes. Without trust, companies are more cautious with AI, which limits deployment to selected functional areas or data sets. "My organization is currently focused on incorporating AI into our market-facing tool but has not leaned in with the same

enthusiasm in working it into the broader company's workflow," says one of The Information's readers.

Recognition without execution

Please rate your agreement with the following statements about trust in AI: (On a scale of 1 to 5, with 1 being "Do not agree at all" to 5 being "Completely agree"; Percentage of respondents who agree or completely agree)

Trust in AI significantly influences organizations' decisions to implement AI

76%

Trust in AI is key to achieving business outcomes

71%

Building trust in AI is a significant challenge

70%

Building trust in AI is a top priority for our organization

68%

We have effective structures in place to build and support trustworthy AI

44%

There's a gap between recognizing the importance of trust in AI and knowing how to operationalize it. When the question shifts from recognition to execution – "we have effective structures in place to build and support trustworthy AI" – the center of gravity slides downward, with less than half (44%) of the respondents agreeing they have such structures in place. This disparity between awareness and facts on the ground reveals that companies do not have an issue with trust as such but with how to operationalize it.

The Information's survey respondents describe the current state of building trustworthy AI as chaotic and ineffective, "a trial-and-error time, with no single benchmark or guideline." That's why, says another reader, "It's been difficult to create AI governance structures and to scale deployment of AI."

At the same time, many AI-driven decisions are no longer confined to a single function or system – they cut across domains, occur in real time and are increasingly automated. As a result, traditional approaches to governance, which rely on fragmented controls and after-the-fact oversight, struggle to keep pace with how decisions are made and executed in real time.

“

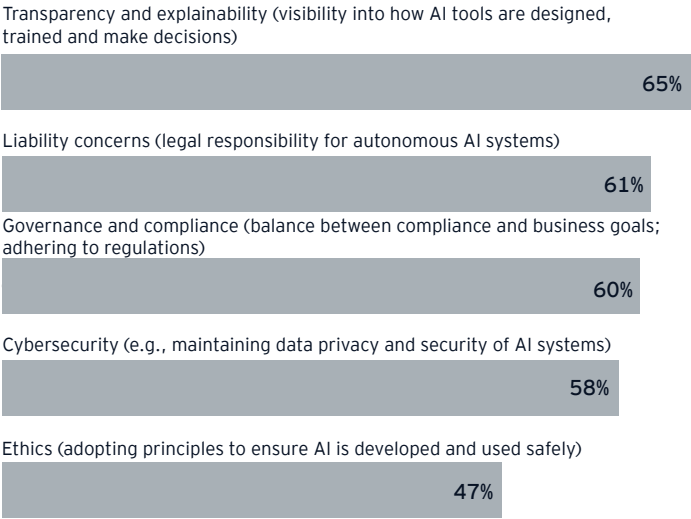
Across industries, leaders are being asked to decide faster, with less certainty and higher stakes. The organizations that move forward with clarity are invested in how decisions get made — driving better visibility and fewer surprises.

- Kapish Vanvaria, EY Americas Deputy Vice Chair - Consulting

Survey respondents link scaled AI deployment to responsible-by-design frameworks that embed crucial requirements into AI processes. These requirements cluster around familiar issues such as transparency and explainability, liability, and governance and compliance. (See chart.)

Design requirements for AI at scale

Which of these are the biggest trust-related barriers or risks preventing your organization from deploying AI more broadly? (On a scale of 1 to 5, with 1 being “Not at all a barrier” to 5 being “A significant barrier”)

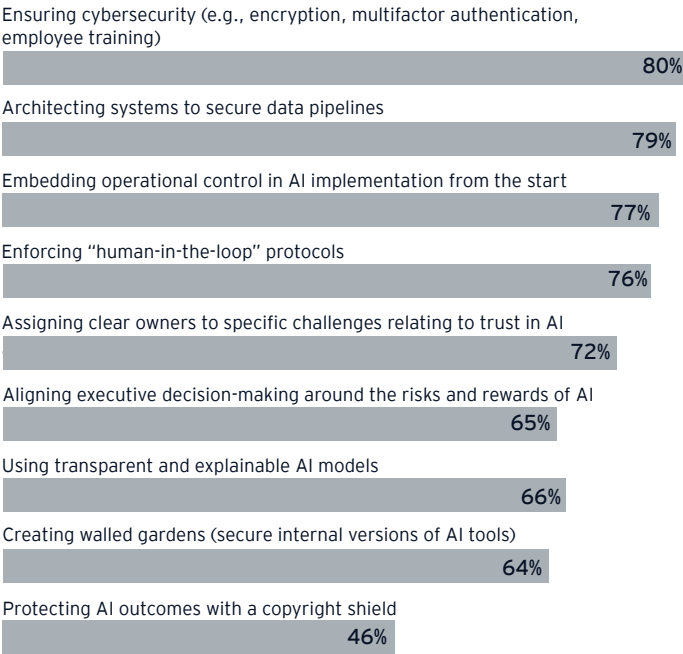


Respondents link responsible scaling of AI to a foundation of trust built on repeatable evaluation and transparency rather than one-time approval. “Treat it like a tool, you get a tool,” notes one reader. In contrast, one company that has baked in most of the trust, compliance and security issues into the protocols is able to focus on content and knowledge fidelity rather than having to constantly address the pain of enforcement.

When building trust in AI, survey respondents prioritize strategies that ensure cybersecurity and secure data pipelines. Such foundational, proactive strategies aimed at maintaining trust in AI come before more defensive strategies, such as creating walls or relying on copyright shields.

Foundational strategies

How important are the following strategies for building trust in AI? (On a scale of 1 to 5, with 1 being “Not at all important” to 5 being “Extremely important”; Percentage of respondents who answered 4 or 5)



“Trust in AI comes down to whether an organization can confidently answer four questions: What did we test? What changed? What risks remain? Why is this safe enough to deploy?” says one of The Information’s readers. To address these questions, respondents point toward building a strong foundation for trust in AI by proactively embedding trust levers within business processes.

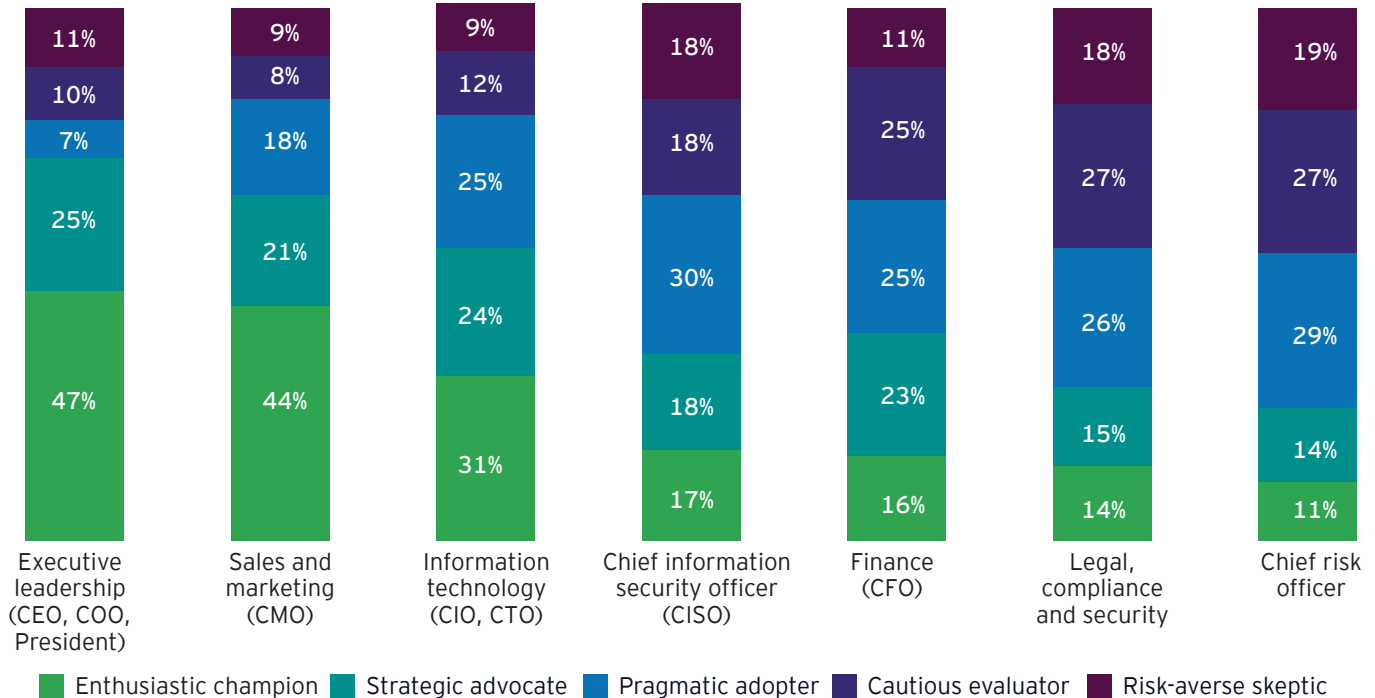
Aligning executive mindsets on AI

Is AI a growth opportunity, an operational tool or a source of risk? It's all three, and which one dominates is heavily

influenced by whom you ask. Leadership is most enthusiastic while risk-related roles are more cautious. (See chart.)

Divergent mindsets

How do different executives and functions in your company approach AI implementation?



"AI challenges human intuition," notes one of The Information's readers. And yet, it is the "human" in the loop that is the ultimate safety valve for AI. How can organizations best harness human intuition to build effective structures for trustworthy AI?

The many divergent human mindsets about how to approach AI, depending on the role of the executive, stem from how they perceive their goals and responsibilities. Leadership seeks growth, technology executives focus on implementation, and risk executives want to limit vulnerabilities and avoid dangers.

The issues surrounding the responsibility for AI follow traditional corporate divisions, such as between business users and technologists. "The issue with AI trust comes down to the business teams being able to have direct access and control over AI agents. The engineers do not know enough about every subject to be able to determine the success criteria for all the AI agents," says one reader.

Another fault line lies between enthusiasts and risk managers: "I have adopted the use of AI in all aspects of my business, but the corporate structure is nervous and reluctant to engage until they understand the risks," says one of The Information's readers. The consensus so far is that everybody still has lots

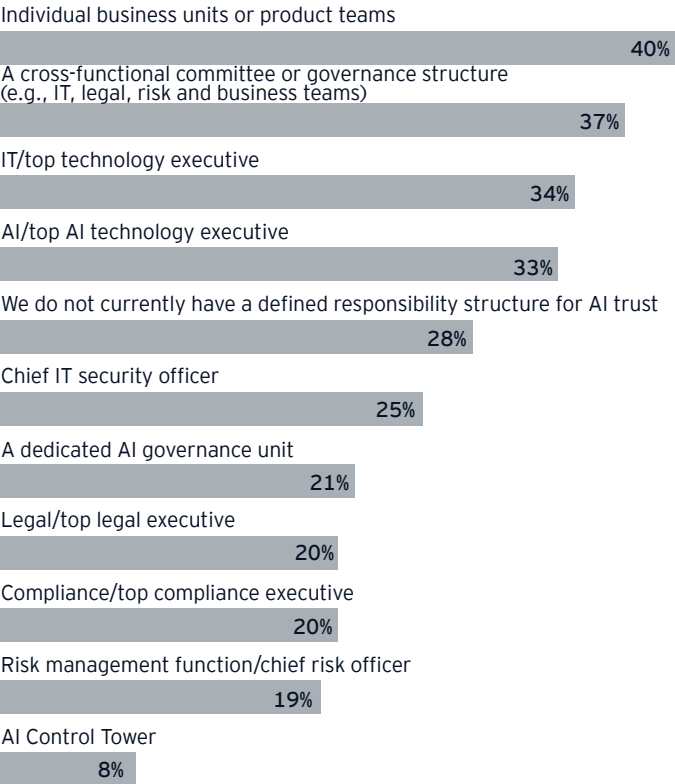
to learn about AI: "Engaging all employees and teams in AI ownership is key. AI is still viewed as a foreign concept, and more education is required."

Key to bringing different executive functions on the same page is "trust [which] is only established when common knowledge is established between parties," notes one reader. That common knowledge boils down to executives knowing that AI-related trust levers are embedded in the processes and workflows and having clarity about their responsibilities and accountability for AI outcomes.

Companies have not yet arrived at a prevalent leading-practice methodology for managing accountability and responsibility for AI. The Information's survey reveals that responsibility for building trust in AI is spread across multiple functions, with no single group dominant. Product or cross-functional teams often lead, but technology, risk or legal all have roles. Such a fragmented landscape reveals that there is no consensus about how best to assign responsibility for building trust in AI. (See chart.)

Diffuse ownership

Which functions, structures or executives in your company have primary responsibility for ensuring trust in AI?



Survey findings support bringing different mindsets together by making all relevant functions cocreators of AI solutions, so that different goals are factored in by design. One of The Information’s readers suggests a broad approach with a governance council responsible for change management and training and composed of technology, legal, cybersecurity and communications executives. “Building trust means that executives need to champion AI, and it should be championed by people in each vertical. Safe space to experiment needs to be provided and encouraged. A secure system is a trusted system,” says the reader.

The governance imperative

Companies are not failing to adopt AI – they are struggling to organize around it. The result may be a system that defaults to cautious, incremental adoption, even when leadership ambitions are higher. The opportunity is not to increase enthusiasm for AI, but to convert existing momentum into structure. Survey findings point to embedding trust levers in AI-driven workflows, establishing clear ownership of AI trust, aligning functions around a shared framework and moving beyond diffuse responsibility toward defined governance.

Survey demographics

Based on a survey of 154 of The Information’s readers, specifically:

- Size: 47% of companies had revenues under US\$10 million, 30% had revenues between US\$10 million and US\$500 million, and 23% had revenues of US\$500 million or more.
- Industry: Respondents came from all major industries, led by technology, media and telecommunications at 40%; professional services at 17%; and healthcare and life sciences at 9%.
- Job function: Respondents represented all functional areas, led by executive leadership at 27%, information technology at 10%, marketing and communications at 8%, and sales at 8%.
- Title: The biggest group of survey respondents were directors at 18%, CEOs and owners at 16%, followed by the C-suite at 17%.

The views reflected in this article are the views of the author and do not necessarily reflect the views of Ernst & Young LLP or other members of the global EY organization.



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.

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

©2026 Ernst & Young LLP.
All Rights Reserved.

US SCORE no.
2606-11079-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