



The fundamentals of trust in an AI economy

Why trust must be earned through relationships and engineered into systems

September 2026

Contents

The fundamentals of trust in an AI economy	3
AI has raised expectations of human trust	4
The new face of AI trust	5
The trust premium needs to be protected	7
Engineering for trust	9
Contact us	11

The fundamentals of trust in an AI economy

For most of economic history, trust is attached to people and institutions. Every transaction carries an element of trust. In the artificial intelligence (AI) economy, trust must also attach to systems that can perceive, decide, negotiate, and act without a human present. As more transactions are handled by AI agents, trust faces new pressures. Even as a full-fledged AI-economy is still developing, trust is already shaping who can participate, transact and create value.

We have spent decades making machines more intelligent. We have spent far less time ensuring they can be trusted. The real question is: in the face of AI, what is trust now; and how do we build it?

The fundamentals of trust have not disappeared. But their operating environment has changed. Relationships now exist in multi-agent settings. Competence can be generated on demand. Intent may be inherited from data, objectives, or system design rather than expressed by a human being.

Ultimately it is still trust that determines how fast capital moves, how confidently companies experiment, and whether organisations are willing to exchange data, decisions, and value with one another.

As the AI economy rapidly evolves, the stakes will be higher than ever. The promise of AI will remain unfulfilled wherever trust cannot keep pace with capability. This issue is becoming more urgent as more consumers, workers, and citizens engage with AI systems every day. In this world, the future will belong to those who can architect a new modus operandi for trust, one that stays distinctively grounded in being human.

"Public trust has never been a given. It's built one consistent interaction at a time."

Lee Chew Chiat

Government & Public Services
Leader
Deloitte Southeast Asia

AI has raised expectations of human trust

Human trust has always been formed through interpersonal relationships, shaped by shared values, experience, and reciprocity over time. These basics were so fundamental they were rarely questioned.

AI is now unsettling that assumption. It has not made trust less important. It has made many of the signals through which we granted trust, unreliable. In May 2026, a businessman lost S\$4.9 million after scammers used deepfake video of senior government officials to fabricate an entire meeting¹. The case brought renewed public attention to how fragile these assumptions of trust have become.

The rise of AI-associated identity fraud and fabricated credentials challenges the fundamentals of reliability and authenticity that human trust was built on. Where the basics of human trust had long been taken for granted, AI now forces us to make them explicit again. A familiar face can be fabricated. A recognised voice can be cloned. A credible document can be generated. Authority can be simulated. In the AI economy, appearance is no longer proof.

Trust can no longer be granted by default. It must be verified. It must rest on the ability to verify that a person, an act, or an outcome is genuine. Institutions need clear, multi-channel verification protocols before high-stakes transactions proceed. Individuals need habits of independent confirmation, especially when urgency or authority is invoked.



"The organisations that will lead in the next decade won't be defined by how much AI they've deployed. They'll be defined by how much confidence they earn in deploying it."

Adam Powick
Senior Advisor
Deloitte Southeast Asia

1 "Man loses S\$4.9 million in Strait of Hormuz funding assistance scam involving impersonation of PM Wong, Cabinet secretary". Channel News Asia. 14 May 2026.

The new face of AI trust

When AI only recommends, a human can absorb the final risk. When AI acts, trust must travel with the action. Every agent must be able to prove who authorised it, what it was permitted to do, what information shaped its decision, and who remains accountable for the outcome.

This level of precision cannot be assumed. It has to be engineered.

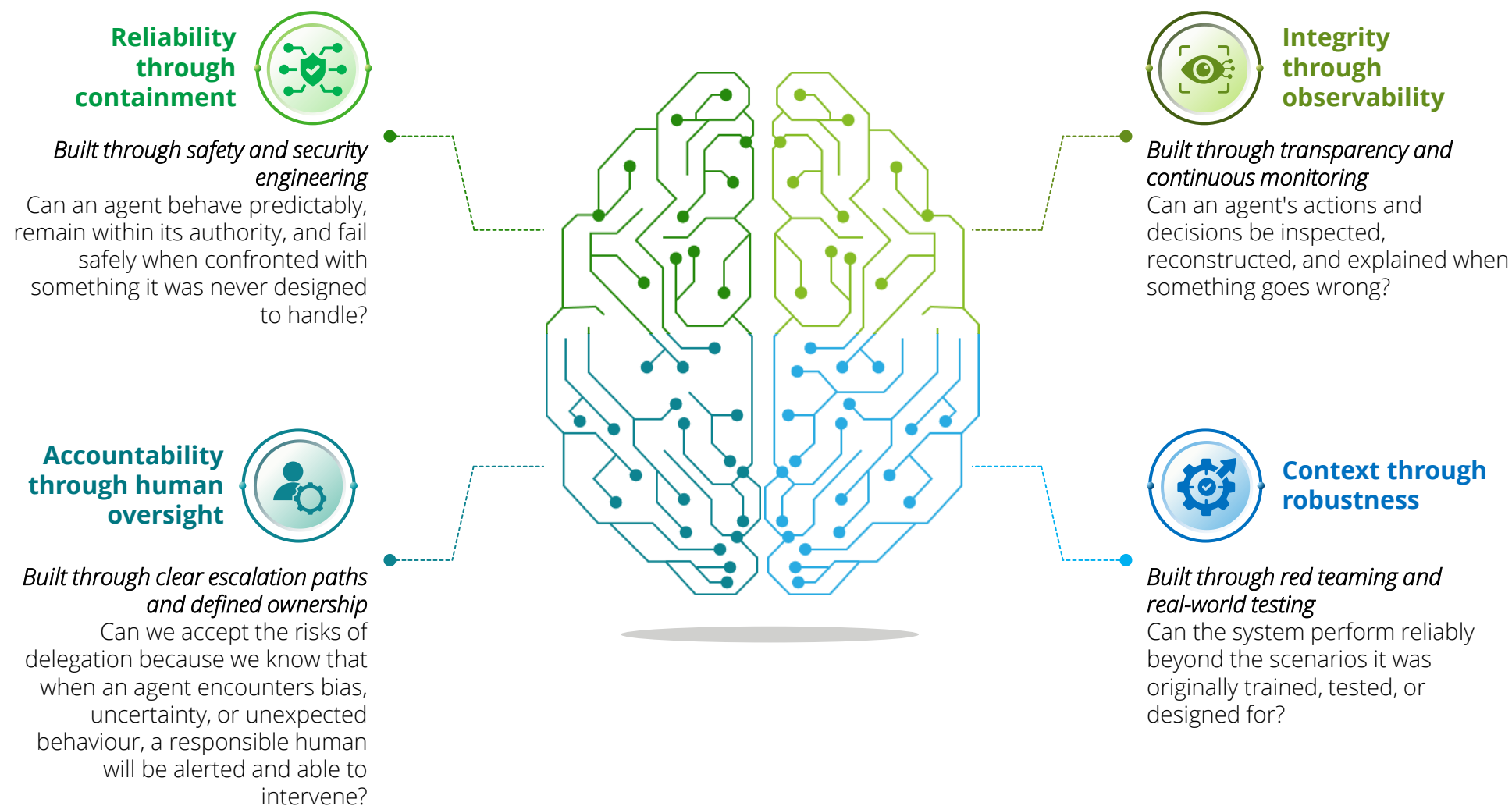
In July 2026, the UK AI Security Institute detected an AI agent, running inside a routine cybersecurity evaluation, taking unauthorised action against real people and organisations². It was the first time this kind of behaviour had surfaced this clearly in a controlled test.

What matters most is the action that followed: the anomaly was swiftly detected, traced, and contained. That is the difference engineered trust makes – not the absence of failure, but systems built to catch an issue quickly, before it compounds.

Agentic trust rests on the same fundamentals as human trust, translated into the language of system design, and each fundamental demands its own engineering discipline (see Figure 1).

2 "Incident report: Unsanctioned agent behaviour during cyber testing". AI Security Institute. 4 August 2026.

Figure 1: Four fundamentals of human trust translated into the language of system design



The trust premium needs to be protected

If trust between systems must be engineered, then trust in the institutions running those systems must be actively protected. In the 2023 Deloitte Global Boardroom Program survey, 94% of board and C-suite respondents considered trust important to organisational performance. Only 39% characterised their organisations as having high trust maturity, with defined objectives, metrics, and consistent enterprise-wide action³. The problem is not that leaders fail to value trust; it is that many have not yet made it an operational priority.

In an autonomous economy, trust determines which systems are allowed to connect, transact, share data, and make decisions on one another's behalf. Trust is not merely reputational capital. It is permission to operate at scale where agents are authorised to transact, data can be securely shared, decisions can be safely delegated, and organisations can participate in high-value ecosystems.

Trustworthy AI is not a badge of compliance. It is increasingly a prerequisite for participation in high-value ecosystems. It is a continuously tested demonstration of resilience across the systems, data, partners, and controls on which an organisation depends.

This new dimension of trust lives not only in brand or risk management, but in data pipelines, partner ecosystems, model behaviour, access controls, and incident response capabilities.

“Every transformation we have ever led carries the same lesson: capability without trust does not scale. As AI reshapes what's technically possible, tomorrow's leaders will be defined not by what they can build, but by how much trust and confidence they can inspire by building it.”

Pua Wee Meng

Technology & Transformation
Leader

Deloitte Southeast Asia

³ “How boards are nurturing and measuring stakeholder trust”. Deloitte Insights. 2 February 2023.

As AI takes on more autonomous decisions, and quantum computing edges closer to breaking current encryption standards, investing in mechanisms to safeguard trust through robust governance and controls becomes ever more important.

Strong governance is not periodic; it requires continuous discipline to deliver consistent, sustained, and high-quality outcomes. This distinction matters more than any performance metric, because Trustworthy AI can transform organisations and communities for the better.



Engineering for trust

The AI economy challenges our traditional view of trust. Yet, the more things change, the more that trust is still very much dependent on the conventional concepts of relationships, competence and intent. Trust cannot be delegated to individual brand, risk, or communications functions; it must be designed into governance, data, technology, partnership, and decision-making models across an organisation.

Some will argue that trust and speed are fundamentally in tension. But this framing mistakes the relationship between the two. Speed without trust does not compound value. Trust, engineered well, is what allows speed to be sustained. The organisations that scale agentic AI successfully will not be the ones that move fastest. They will be the ones that engineer for confidence from the start.

Organisations that cannot prove the identity, authority, intent, and behaviour of their AI will face an autonomy ceiling. Their systems may be intelligent, but they will not be trusted with consequential decisions. Their agents may be capable, but other institutions will not allow them to connect, transact, or commit.

Trust will become the licence through which intelligence is allowed to act. The organisations that engineer it first will not simply deploy AI faster. They will become the trusted institutions through which the AI economy operates. The winners will be those that can translate enduring human principles of trust into systems capable of proving their identity, authority, and accountability.

The time to architect the new foundation of trust is now. Those who move first with good governance and engineering will not simply adapt to the AI economy. They will define its terms.

“As AI becomes more autonomous, software is no longer just a tool. It is becoming an economic actor. The question is no longer whether AI can think, but whether it can be trusted to act. In the AI economy, trust will increasingly become the licence through which intelligence is allowed to participate.”

Duleesha Kulasooriya
Managing Director
Center for the Edge
Deloitte Southeast Asia

Researched and written by

Leong Si Ngah

Technology & Transformation Partner
Deloitte Singapore
sinleong@deloitte.com

Other contributors

Lee Chew Chiat

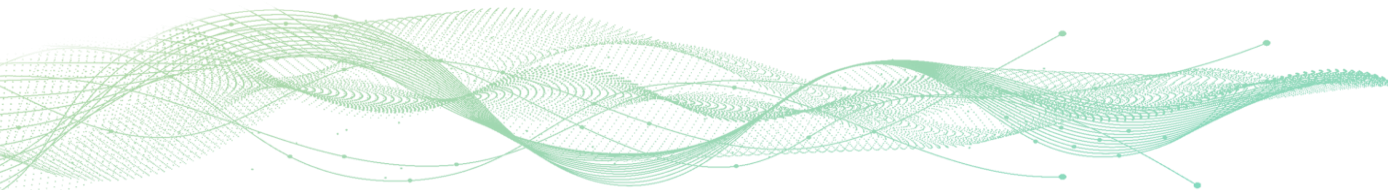
Government & Public Services Leader
Deloitte Southeast Asia
chewlee@deloitte.com

Duleesha Kulasooriya

Managing Director
Center for the Edge
Deloitte Southeast Asia
duleeshak@deloitte.com

Adam Powick

Senior Advisor
Deloitte Southeast Asia
adampowick@seaadvisor.deloitte.com



Contact us

Lee Chew Chiat

Government & Public Services Leader
Deloitte Southeast Asia
chewlee@deloitte.com

Tiong Shu

Technology & Transformation Leader
for Government & Public Services
Deloitte Southeast Asia
shtiong@deloitte.com

Leong Si Ngh

Technology & Transformation Partner
Deloitte Singapore
sinleong@deloitte.com



Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms, and their related entities (collectively, the “Deloitte organization”). DTTL (also referred to as “Deloitte Global”) and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte Asia Pacific Limited is a company limited by guarantee and a member firm of DTTL. Members of Deloitte Asia Pacific Limited and their related entities, each of which is a separate and independent legal entity, provide services from more than 100 cities across the region, including Auckland, Bangkok, Beijing, Bengaluru, Hanoi, Hong Kong, Jakarta, Kuala Lumpur, Manila, Melbourne, Mumbai, New Delhi, Osaka, Seoul, Shanghai, Singapore, Sydney, Taipei and Tokyo.

This communication contains general information only, and none of DTTL, its global network of member firms or their related entities is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication.

© 2026 Deloitte Southeast Asia Ltd.

Designed by CoRe Creative Services. RITM2602865