pwc

Competing on trust in the Age of AI

Table of contents

At a glance

- **The trust gap widens.** Rapid innovation is outpacing the structures that ensure trust between companies and their customers, suppliers, distributors, and regulators.
- **The past is prologue.** Lessons from previous industrial revolutions demonstrate the necessity of transparency and accountability.
- **Keeping pace with the impossible.** Technologies beyond AI, especially quantum AI, require more than frequent retooling to build trust.

To realise the transformative business potential of AI, it's first necessary to strengthen the foundations of trust underlying the global economy. Economic transactions are enabled by structured markets—and structured markets are built on a robust architecture of trust.

Yet today's rapid transition to a real-time, interconnected, AI-driven network, operating across corporate and national borders, is straining that trust. And with quantum leaps in hardware, software, and data all coming together at once, new vulnerabilities will further undermine it. Unless pioneering firms act, the emerging AI economy will be torn—between the interests of ownership and openness, between central oversight and distributed coordination, between periodic audits and continuous assurance, between national jurisdiction and networked markets, and between technical compliance and demonstrable ethical behaviour.

History offers both comfort and guidance. Many times before, new technology has led to rapid, fundamental changes in the production and exchange of goods and services. From the advent of industrial coal applications to the refining of oil and electricity and, ultimately, the development of silicon and software, each era has spawned technologies that created new markets, new boundaries for industries, and new consumer behaviours and expectations. During each of those transitions, companies reshaped the nature of the trust that allowed commerce to thrive. They can do it again, and those that move quickly will create new sources of competitive advantage, just as trust pioneers have done in the past.

The **outline for success is already** visible. A new trust architecture for the AI era requires interoperable standards, real-time data, and continuous assurance. It demands transparency and accountability. And it relies on fair transactions, secure operations, and responsible deployment of AI.

01

Trust through the ages

Trust has always been the backbone of economic transactions. It's evolved from personal reputation and communal oversight in pre-industrial societies to the complex architectures required by expanding markets. Each industrial era's system of governments, private institutions, standards bodies, and auditors matched the scale, speed, and technical demands of the prevailing market needs. In the process, each successive economy built systems of reliability that made transactions possible.

The First Industrial Revolution (c. 1760–1840)

During the First Industrial Revolution, trust was fundamentally structured around tangible inventions and formalised ownership. Patent protections—embodied in reforms like the US Patent Act of 1836 (and the later British Patent Law Amendment Act of 1852)—lowered uncertainty for inventors and investors and accelerated mechanised productivity. Governments standardised weights and measures, and codified contract, commercial, and bankruptcy law. Trade associations promoted voluntary standards. This architecture facilitated economic transactions while prioritising intellectual property, national standardisation, and new production methods.

The English ceramist Josiah Wedgwood, an innovator in his craft's early industrialisation, thrived during the First Industrial Revolution by pioneering consistent quality, recognisable branding, and reliable distribution in ceramics. In doing so, he created widespread consumer trust in remote, catalogue-driven commerce. His business's standardisation and clear guarantees allowed provincial families in the 1770s to select a full suite of tableware—plates, bowls, and serving dishes—from a pattern book, and trust that any replacements would match, even years later. Trust during this economic age, made tangible through standards and guarantees like Wedgwood's, turned remote commerce into a reliable experience and loyalty into a durable advantage.

The Second Industrial Revolution (c. 1870–1914)

The Second Industrial Revolution saw advances in transportation, communications, production, and distribution that dramatically enhanced productivity and created mass markets. Joint-stock and limited-liability structures pooled capital to fuel the rise of giant enterprises, many of which still exist today. To support this new and growing market, a new architecture of trust emerged. Central banking and later securities regulation brought monetary stability and financial transparency. Public accounting and exchanges formalised disclosure and independent audits. And in a time of labour unrest—the Haymarket Affair, the Pullman Strike, the Seattle General Strike—religious institutions and community-based safety nets helped legitimise labour and corporate responsibility.

In this era of rapid urbanisation and mass-produced food—when contamination, mislabelling, and opaque packaging were common—the H. J. Heinz Company built trust by making it visible and operational: the company used clear glass bottles so shoppers could see the product, standardised its labels for consistency, reformulated the ketchup itself to avoid chemical preservatives like sodium benzoate, and publicly aligned with the US Pure Food and Drug Act of 1906. Heinz invited consumers and the press into spotless, well-lit model factories to witness sanitary processes firsthand, turning manufacturing transparency into a brand signal. Similarly, The Coca-Cola Company famously built consumer trust by reformulating its recipe to remove cocaine in 1903 and by navigating stricter federal standards. It reinforced that trust through visible consistency, adopting standardised, trademarked packaging. In an era when transparency and compliance were costly for all companies, both Heinz and Coca-Cola used them as hallmarks to differentiate themselves from their rivals. The result? Enduring customer loyalty and a premium in market position.

The Digital Revolution (c. 1960–2000)

The innovations of the Digital Revolution required new ways to cultivate trust, by codifying standards, launching national initiatives, and adapting common codes and networks for rapidly advancing technologies. Multiple independent standards organisations, such as the International Organization for Standardization (ISO), the Institute of Electrical and Electronics Engineers (IEEE), the International Telecommunication Union (ITU), the Internet Engineering Task Force (IETF), and the World Wide Web Consortium (W3C), as well as the China Electronics Standardisation Institute (CESI) and the Institution of Engineers [India] (IEI), authored protocols that made distributed systems interoperable. Governments erected privacy laws and cybersecurity programmes. Public accounting evolved into IT audits and cyber assurance. Trust shifted towards technical proofs and perimeter defences, and the market's enabling infrastructure became software, identity systems, and managed platforms.

Global payments giants Visa and Mastercard made credit card–based commerce ubiquitous during the Digital Revolution by explicitly embedding trust into their networks. They codified network rules and dispute/chargeback procedures, established strong authentication via smart chip technology and network tokenisation, and implemented sophisticated fraud analytics and risk controls. Both Visa and Mastercard emphasised safety, security, and operational resilience in their regulatory filings, reflecting expectations for the reliability of critical payment infrastructure. Trust is core to their brand; it's engineered and codified in the rules, standards, and technology of their networks.

02

The next evolution of trust

Economic progress evolves together with trust—in fact, as we've seen in the industrial ages described above, trust is the prerequisite for sustainable economic progress. The Intelligence Era's open ecosystems and global interoperability demand collaboration beyond the property-centric models and state-led standardisation of preceding eras. Legacy trust mechanisms are **proving inadequate** for today's need for real-time data, accountability, and decentralised risk mitigation. Even digital-era fixes are hitting limits: perimeter security falters, consortium standards lag, and opaque machine learning strains confidence. And looking ahead, technologies beyond AI—quantum computing chief among them—will make the complexities of trusting today's AI models look simple by comparison. The future will demand more than frequent retooling; it'll require a bold commitment to building trust that can keep pace with the impossible.

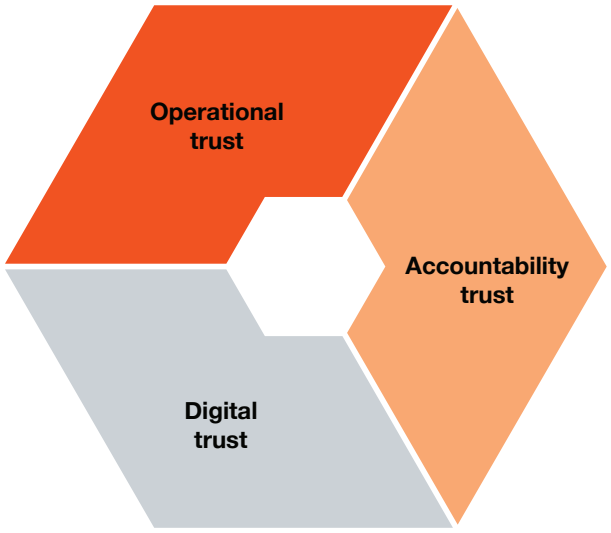
In the meantime, governments are taking divergent approaches to how AI is built and used—and the rules they're establishing vary widely. The EU is adopting strict, risk-based requirements on transparency and user rights. The US favours a lighter, sector-led approach, with few federal mandates. China is pushing for rapid adoption under tight state control of data and algorithms. This patchwork of oversight leaves companies juggling overlapping, sometimes conflicting rules. The speed of rule-making shows the urgency in how governments see AI's societal risks. But with such potent technology, concerted action and strong leadership are essential to ensure that AI benefits society while minimising harm. In this fluid moment, engaging with all stakeholders and harmonising standards across borders will be key to gaining lasting competitive advantage in the AI era.

It's time for a new trust architecture that is fit for today's decentralised technologies, advanced analytics, globalised markets, and complex systems. This new architecture

centres on operational trust, accountability trust, and digital trust, all grounded in enduring principles of interoperability, transparency, and reliability. In the AI era, trust isn't something verified after the fact; it's designed into systems, decisions, and data flows from the start.

Trust for a new era

CEOs can make trust a durable, strategic asset by focusing on three imperatives. The building blocks are data, processes, and controls.



Operational trust

- Interoperable standards
- Accurate, real-time data
- Continuous assurance

Accountability trust

- High-quality reporting
- Confident communications
- A shared fact base

Digital trust

- Secure digital assets and operations
- Transparent governance
- Proportionate exchange of value

Source: PwC

Operational trust

Operational systems and processes within today's companies are complex. These systems range from enterprise and supply chain technology to compliance and risk management. Literally every activity in the value chain is undergoing reinvention today through data and AI.

Operational trust depends on common standards, high-quality real-time data, and continuous assurance. The goal is reliable execution with rapid, safe adaptation—so leaders can sense shocks, model scenarios, and make confident decisions. In practice, that means modernising core systems and data platforms, reshaping operations for observability, and creating clear guard rails for AI-powered automation.

Standardisation is key. The harmonisation of international standards for AI systems and data flows is essential to align regulatory regimes and promote reliability on all sides of a transaction. The form changes—legal codification, monetary stability, disclosure mandates, or algorithmic accountability—but the function endures. Standardisation creates predictable frameworks that lower transaction costs and make complex markets accessible.

Consider, for example, how having an established trust architecture in place enabled one company to navigate the US policy shifts in 2024 that raised tariff and enforcement risk on imported solar components. A US-based manufacturer had built an integrated domestic supply chain supported by a single audited presentation of information, enabling developers, lenders, and tax advisors to make confident decisions. This included consistent origin proofs, bills of materials (BOM) for domestic-content claims, and attestations aligned to customs and treasury rules. The company also set clear expectations for capacity and pricing, avoided opaque surcharges, and shared the same documentation with customers and authorities. This level of transparency, supported by trust mechanisms that were deliberately integrated into the supply chain, resulted in a lasting competitive edge.

Accountability trust

Accountability trust supports high-quality reporting and confident communications by meeting regulatory requirements and stakeholder expectations with precision and integrity. It rests on the data, processes, and controls that produce information reliably and repeatably.

Accountability trust has many dimensions. It means evolving the controls environment from periodic, manual checks to continuous assurance. It means automating financial and operational controls as well as the collection and storage of logs, approvals, and system outputs to demonstrate that the controls have operated as intended. And it means instrumenting systems for observability to create timely, auditable trails and reduce error rates.

Consider what that might mean for **AI-enabled taxation**, for example. Governments are increasingly able to directly access financial data and automatically calculate tax due, often in real time. That means companies have to be able to trust that their data is correct and consistent from the moment it's recorded in their systems (since it may be automatically fed into tax calculations). Continuous monitoring, change management gates, and exception handling make it possible to shorten reporting cycles without sacrificing accuracy. The goal is not maximal openness but credible, consistent, and stakeholder-appropriate disclosures that allow others to rely on a company's statements and decisions.

Digital trust

Digital trust allows companies to maximise the potential of AI and other technologies by demonstrating how they protect sensitive data, maintain secure operations, and use digital capabilities responsibly and ethically. Consumers rank protection of their data as a top driver of trust, often above product quality, so cybersecurity cannot be an afterthought. Yet, as digital footprints expand across remote work, cloud platforms, and value chains, the **potential for cyberattack** grows. Nearly nine in ten investors (88%) agree that companies should **increase their capital allocation** to cybersecurity. And AI raises the stakes further: it lowers barriers for attackers but can also strengthen defences through intelligent detection and automated response.

88%

of investors agree that companies should increase their capital allocation to cybersecurity.

Source: PwC's Global Investor Survey 2025

To protect themselves, their suppliers, and their customers, companies must keep their digital tools secure and govern them transparently. Furthermore, they need to automate checks for low-risk uses to move fast while maintaining deeper review and human oversight for high-impact decisions.

At the same time, tools must be fair. Trust holds when stakeholders see risk and value shared transparently and proportionately. Customers, suppliers, and business partners are increasingly aware that AI can amplify information asymmetry and allow a business to take unfair advantage. Even legal business practices, when poorly implemented, can erode trust. For example, using advanced AI modelling to estimate a customer's willingness to pay, and adjusting prices or offers in real time, may be legal in some jurisdictions but may also be perceived as unfair.

Collaboration across the ecosystem is key. In a global, networked economy, harmonised standards and regulatory cooperation are essential to oversee AI systems, data flows, and algorithmic decision-making across borders. This is an area where rule-making and private implementation are rapidly evolving. Privacy laws (e.g. the EU's General Data Protection Regulation [GDPR] or China's Personal Information Protection Law [PIPL]) and emerging AI governance frameworks (e.g. the EU AI Act, the National Institute of Standards and Technology [NIST] Artificial Intelligence Risk Management Framework [AI RMF], and the International

Organization for Standardization/International Electrotechnical Commission [ISO/IEC] standards 23894 and 42001) are converging on security, transparency, and accountability.

To take advantage of AI capabilities, one global retailer launched a generative AI shopping assistant. The assistant bases its recommendations on live catalogue data—pricing, promotions, and store-level availability—to reduce hallucinations, and it runs within company policy guard rails for sensitive categories. It personalises recommendations consistent with customer account settings under strict privacy controls and offers clear explanations and clarifying questions, so choices are transparent. High-impact transactions (such as age-restricted items or purchases related to sensitive health topics) follow stricter rules and, where appropriate, human review, even as everyday features iterate quickly under automated checks. The result: **the retailer can roll out AI features** while respecting privacy controls and safety policies and keeping the experience understandable—turning responsible AI, security, and transparency into a competitive edge.

As institutions reconfigure trust for an Intelligence Era economy, they can take inspiration from past eras. The formula for building trust is changing, but the principles of transparency, reliability, accountability, and shared responsibility are timeless. Our historical survey of trust shows that no one wins alone—so join a collaborative ecosystem to help close AI-era vulnerabilities. Engage with standards-setting bodies, share signals, and protect the commons. And move now—design trust into data, decisions, and products, and publish interoperable proofs. Early movers will set the rules and turn trust into a durable competitive edge.

Authors

Dallas Dolen
Technology, Media, & Telecommunications
Industry Leader, PwC United States

Kazi Islam
Global Assurance Strategy and Growth Leader,
PwC United States

Competing on trust in the Age of AI

www.pwc.com/gx/en/issues/trust/competing-trust-age-of-ai.html

© 2025 PwC. All rights reserved. PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.