uvance Wayfinders

Consulting by Fujitsu

Data sovereignty in the AI era: from risk management to strategic advantage

Fujitsu Data Sovereignty Report

AI has broken traditional data sovereignty. In 2026, sovereignty is no longer a compliance function; it is an architectural, strategic and competitive capability. Only 8% of organizations can control how their AI systems learn and behave post-deployment, exposing them to escalating security, regulatory and reputational risks.

Research from Uvance Wayfinders, consulting by Fujitsu, identifies a new class of “sovereignty frontrunners” who are redesigning their data and AI foundations to unlock growth, collaboration and innovation.

In this report, we explore how organizations are redesigning their outdated sovereignty models and find out what the ones that are evolving faster are doing differently.

Definitions

Data and AI sovereignty

Control over data: where it lives, how it's used and who can access it. Sovereign AI extends this concept to the AI systems that use that data to give organizations visibility and control over how these models are trained, deployed and updated.

Model autonomy

An organization's ability to switch between AI model providers without losing control of the underlying data, workflows or decision-making logic that power AI systems.

Data sovereignty enters the AI era

AI is exposing the limits of traditional models and is forcing a shift from control as compliance to control as architecture

In 2026, data and AI sovereignty has arrived on the agenda. Business leaders can't ignore high-profile AI data leaks, growing legal scrutiny over model-training data and geopolitical tensions that affect cross-border data flows. All of these could cause significant financial and reputational harm.

Our research finds that external tensions are a driving force behind sovereignty redesign:

- 57% of organizations say high-profile incidents have made the reputational impact of getting sovereignty wrong more visible.
- 69% say that recent geopolitical tensions have increased the importance of data and AI sovereignty in their organization.

Increased exposure explains why nearly two-thirds say they lean toward treating data and AI sovereignty as a business responsibility instead of as a technical one. Business decision-makers are right to be involved in setting a strategy that could have such serious consequences, but their caution is slowing AI innovation: 63% say they prioritize governance over speed when it comes to experimentation.

Business leaders' caution is a problem for AI innovation

Q: In practice, when trade-offs arise in decisions involving data use and AI, which way does your organization typically lean in the following situations?

Treating data and AI sovereignty

Technical responsibility ◄——► **Business responsibility**

18% Strongly toward	20% Somewhat toward	26% Somewhat toward	36% Strongly toward

AI experimentation

Prioritizing speed ◄——► **Prioritizing governance**

13% Strongly toward	24% Somewhat toward	23% Somewhat toward	40% Strongly toward

Business leaders might be cautious, but they're also clear that agreeing on a more effective sovereignty strategy is non-negotiable and more urgent than ever. Nearly three-quarters say strong data sovereignty is essential to scaling AI successfully across the organization. And 62% say their strategy is increasingly influencing technology investment and vendor selection decisions.

But they face a deadlock. Inadequate sovereignty strategies can limit an organization's ability to extract value from new technologies and stifle new revenue streams, but more than half of organizations are unable to agree on a balance between innovation and control in AI at an enterprise level.

What this means for CIOs

- Sovereignty has moved onto the board agenda. Business decision-makers must be able to lead the response.
- Treating sovereignty as a risk or compliance issue will slow AI progress. Build it into how platforms and systems are designed.
- Governance frameworks must support experimentation to prevent delays to AI scaling.
- Consider the influence that sovereignty decisions will have on vendor, architecture and ecosystem choices before you commit to ongoing partnerships and investments.

Can organizations operationalize sovereignty?

Business leaders must balance control, collaboration and innovation to accelerate data and AI sovereignty frameworks

Organizations are adopting AI too quickly for governance to keep up. Nearly two-thirds of businesses (62%) say the pace of AI adoption is forcing them to share data more widely across partners and platforms than their current data sovereignty capabilities can comfortably support. Unless leaders find a way forward, they will continue to expose their businesses to unnecessary risk.

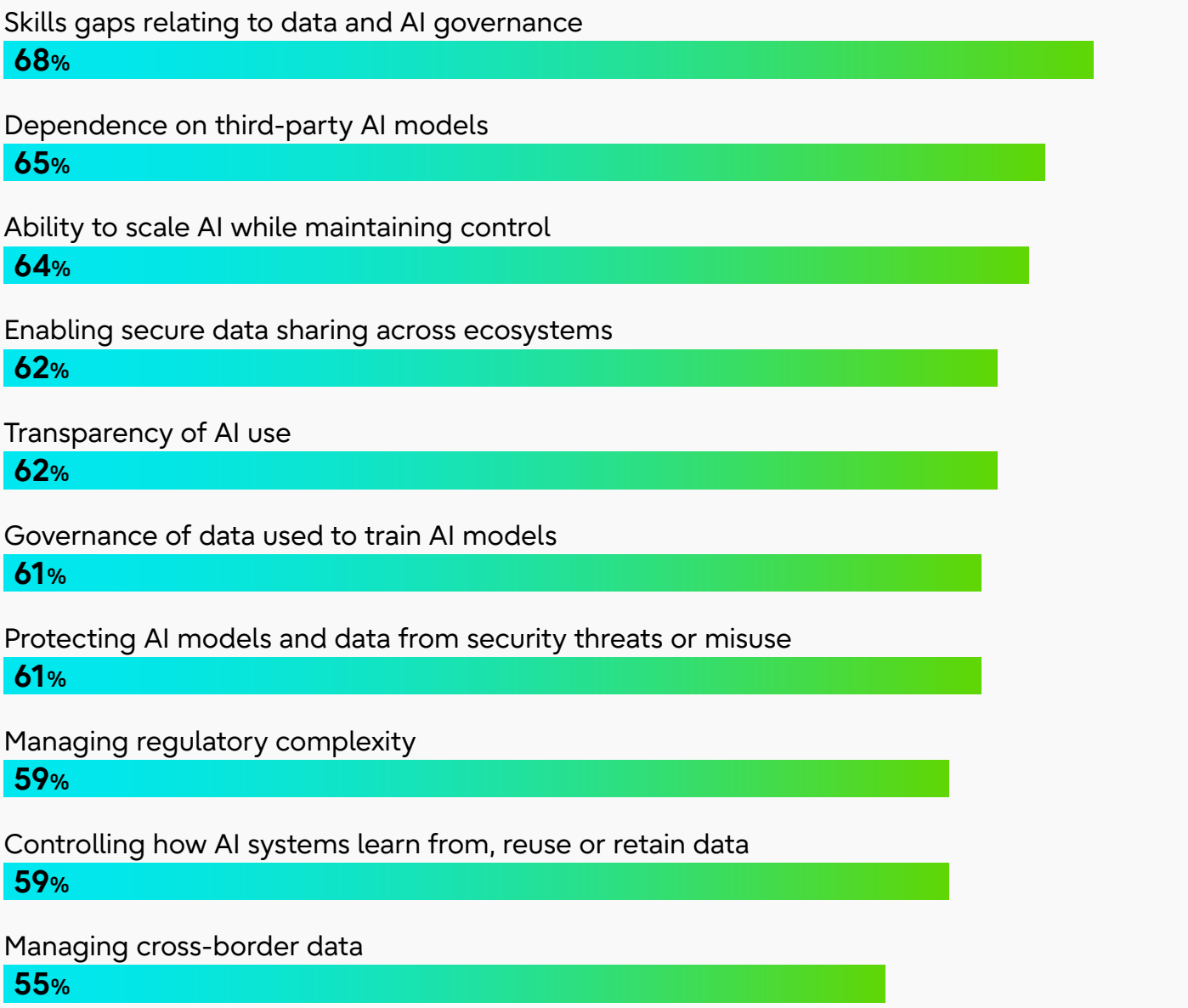
Lack of expertise is hindering progress on other complex issues

Why are organizations struggling to set a strategy that balances risk and control with innovation and collaboration? The mix of challenges is complex, and decision-makers are struggling to identify which are most important.

Skills and expertise are up there. They directly affect knowledge sharing across the enterprise, which slows progress on other serious issues, such as how to share and govern data and how to collaborate with the broader AI ecosystem.

Organizations are struggling to operate within the AI ecosystem

Q: As AI usage increases, how challenging are the following areas? Fairly/very challenging



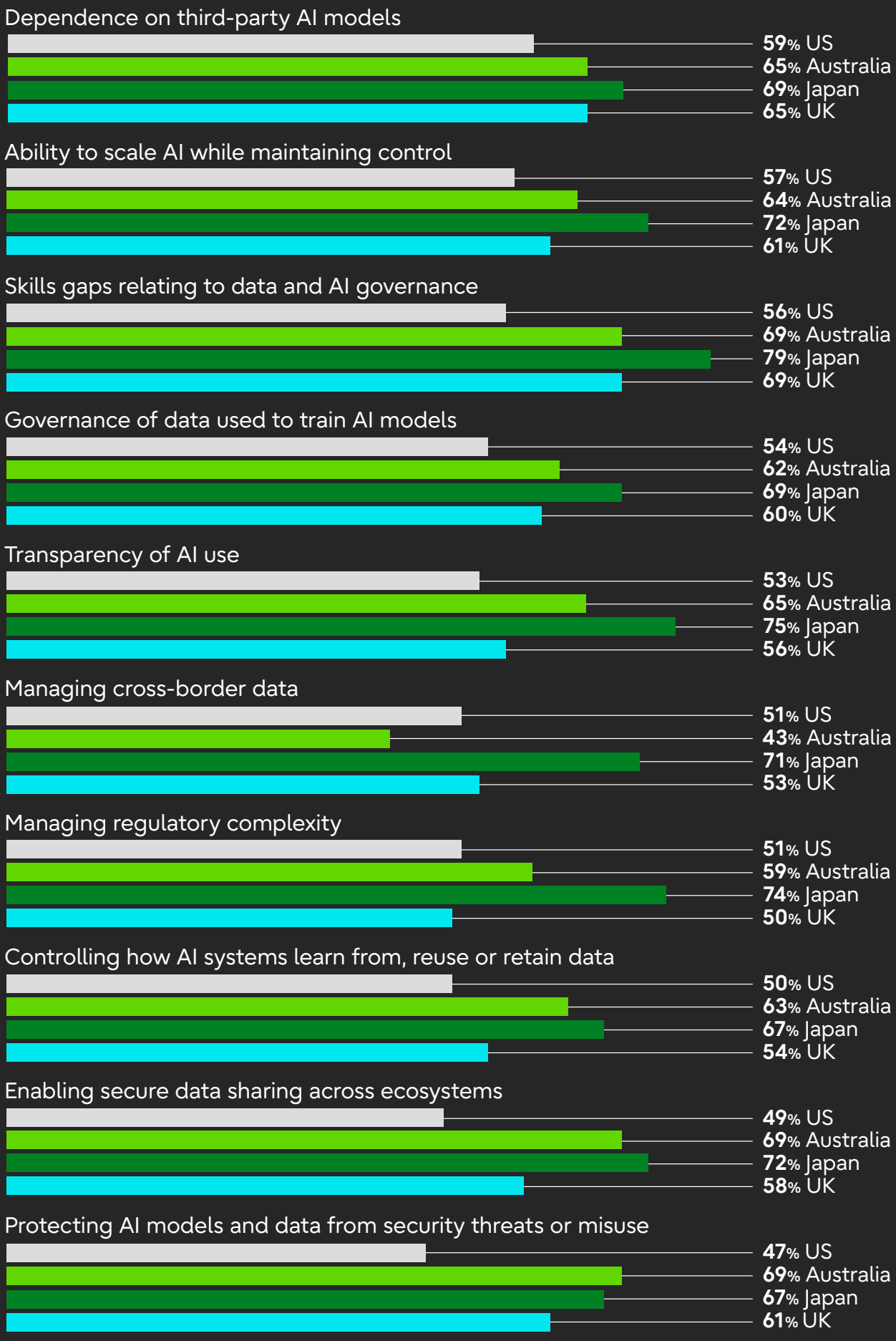
In Japan, organizations are more likely to be struggling; in the US, they're moving to the next stage

Our research shows that skills shortages are a major challenge in every region but to varying degrees. In Japan, 79% say they lack expertise, compared with 69% in Australia and the UK and 56% in the US. Across nearly every challenge we asked about, Japanese companies are most likely to say they're facing difficulties.

In the US, overdependence on AI models developed by third parties is the biggest challenge (cited by 59% of organizations). But companies there are far more likely to have secure foundations in place: just 47% say that protecting AI and data models from security threats is a challenge. This suggests that companies in the US have a more effective strategic roadmap for AI and data sovereignty redesign.

US companies are strengthening external partnerships

Q: As AI usage increases, how challenging are the following areas? Fairly/very challenging



Organizations are strengthening foundations, but they still have gaps

Only 8% are confident that they have clear governance in place to control how AI systems learn from, reuse or retain data after they're deployed. This is a major risk to businesses, and they need to move faster.

In response to the deadlock, enterprises are focusing on building strong strategic foundations as they prepare to scale AI. About four in 10 (39%) intend to focus on addressing skills gaps and improving data transparency over the next 12 months. Embedding data transparency and ethical principles in AI design also emerge as priorities in response to the most urgent gaps.

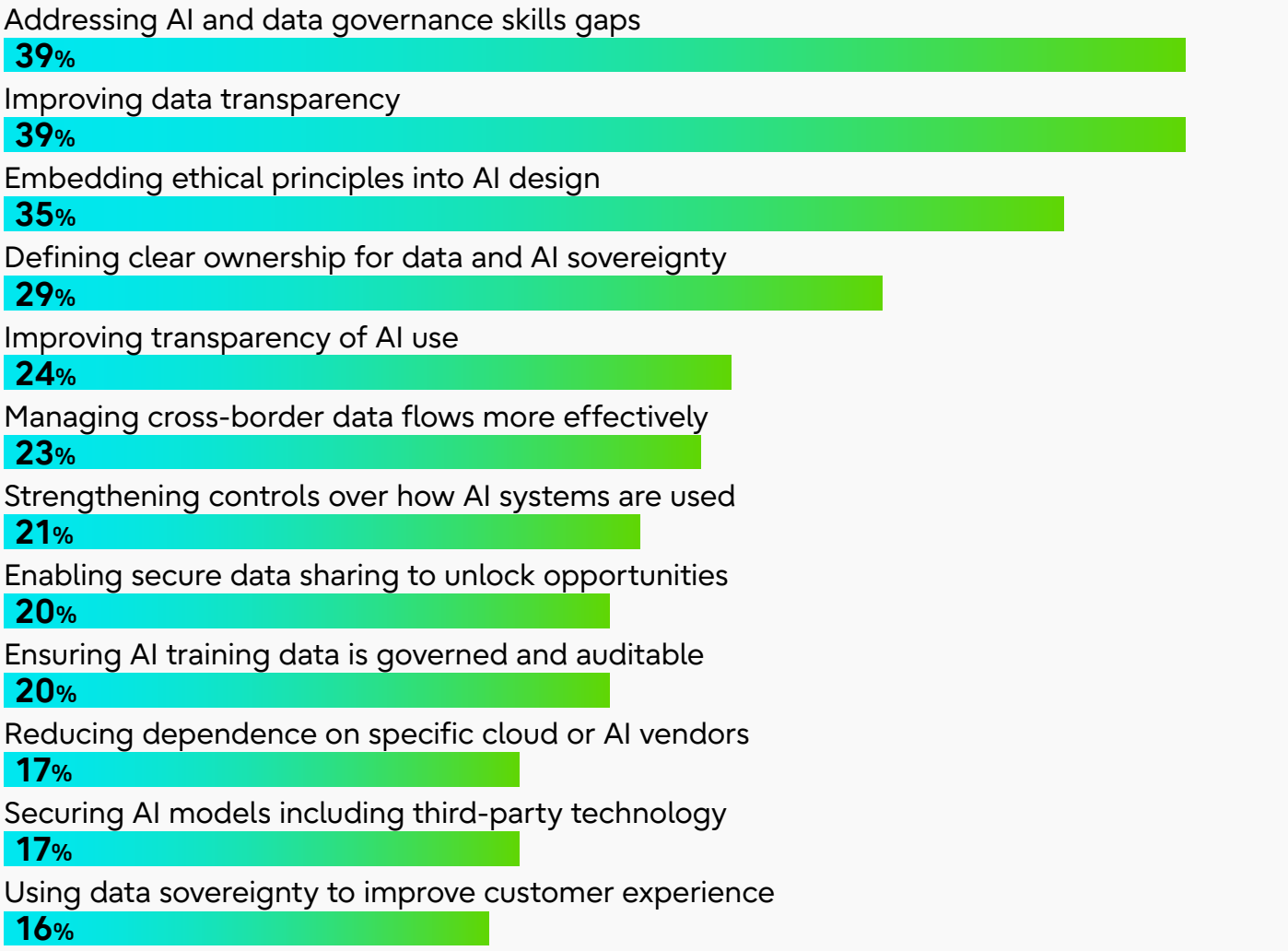
Internal control is prioritized over external trust

Organizations are right to focus on skills, ethics and security, but many are missing powerful business growth opportunities by prioritizing governance over reputation.

Nearly six in 10 (58%) focus more on preventing internal failures than on preventing external exposure when decisions involve data use and AI. This mindset has led them to deprioritize business value drivers: third-party AI cybersecurity and customer experience are their bottom two goals for the year ahead.

Organizations must consider business reputation as well as technical foundations

Q: Which actions related to data sovereignty will be the highest priority for your organisation in the next 12 months?



There's a gap between compliance-led and business-led approaches

While most organizations are responding to regulatory requirements and incidents, some are starting to move beyond compliance-driven mindsets and approaches. This latter group is embedding data and AI sovereignty into how it designs systems, selects technology and collaborates across ecosystems. These sovereignty frontrunners account for 41% of the organizations we surveyed.

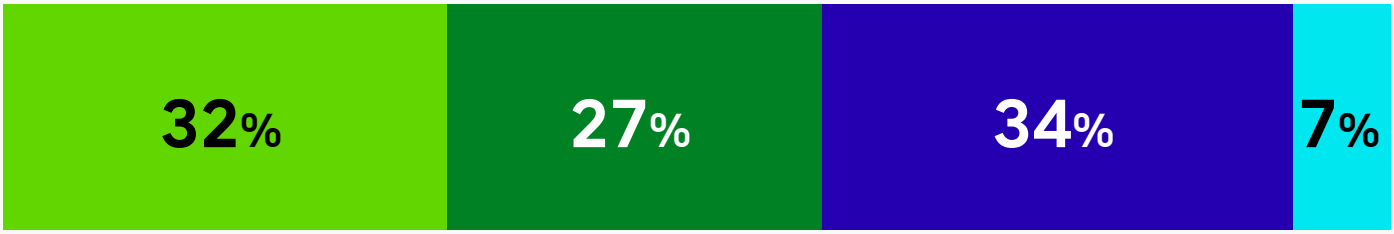
Sovereignty frontrunners are focusing on measures that embed control across the enterprise and on fueling innovation through safer collaboration across the ecosystem. They offer a clear direction to other organizations.

Some organizations are shifting their mindsets from compliance-led to business-focused

Q: Which statement best reflects your organization's current approach to data and AI sovereignty?

- We address data and AI sovereignty in response to regulations, customer requests or incidents
- We have documented policies, but implementation varies across the organization
- We implement organization-wide standards and controls, with clear ownership and monitoring
- Data and AI sovereignty is built into AI lifecycle by design, shaping technology and vendor selection and governing ecosystem collaboration

Immature approach (compliance-led) → **Mature approach (business-value-led)**



What this means for CIOs

Focus on the following to embed a more mature, business-led approach to data and AI sovereignty:

- Build sovereignty into architecture, not policy.
- Design for model autonomy and portability.
- Measure sovereignty outcomes via innovation metrics, not compliance KPIs.

Sovereignty frontrunners turn data controls into performance

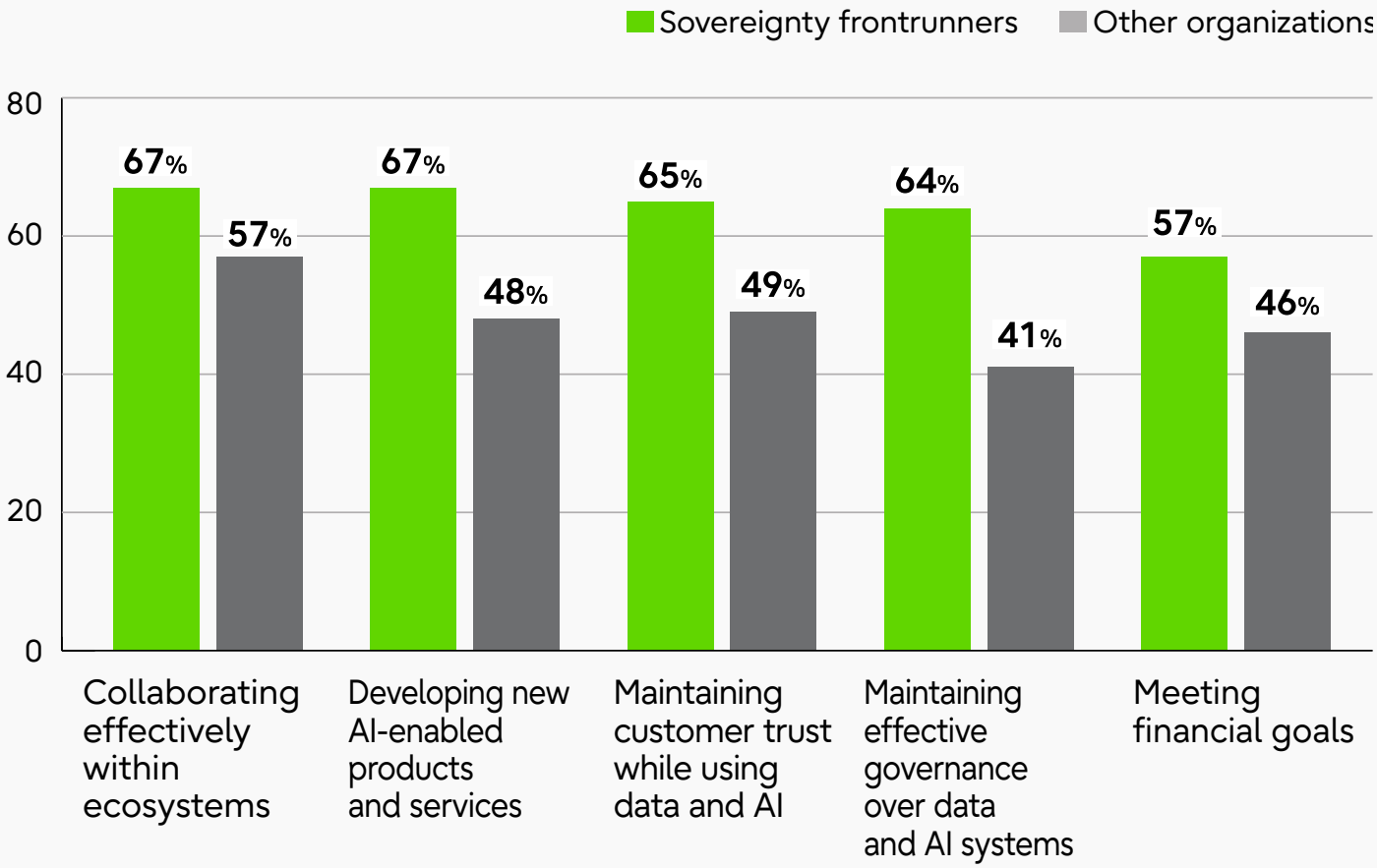
Organizations with mature data and AI sovereignty frameworks prioritize customer trust and ecosystem collaboration to unlock strategic value

While most organizations are struggling, sovereignty frontrunners are operationalizing strategic growth. More than half of these organizations (58%), for instance, treat data and AI sovereignty as a strategic capability that builds customer trust and enables collaboration across ecosystems.

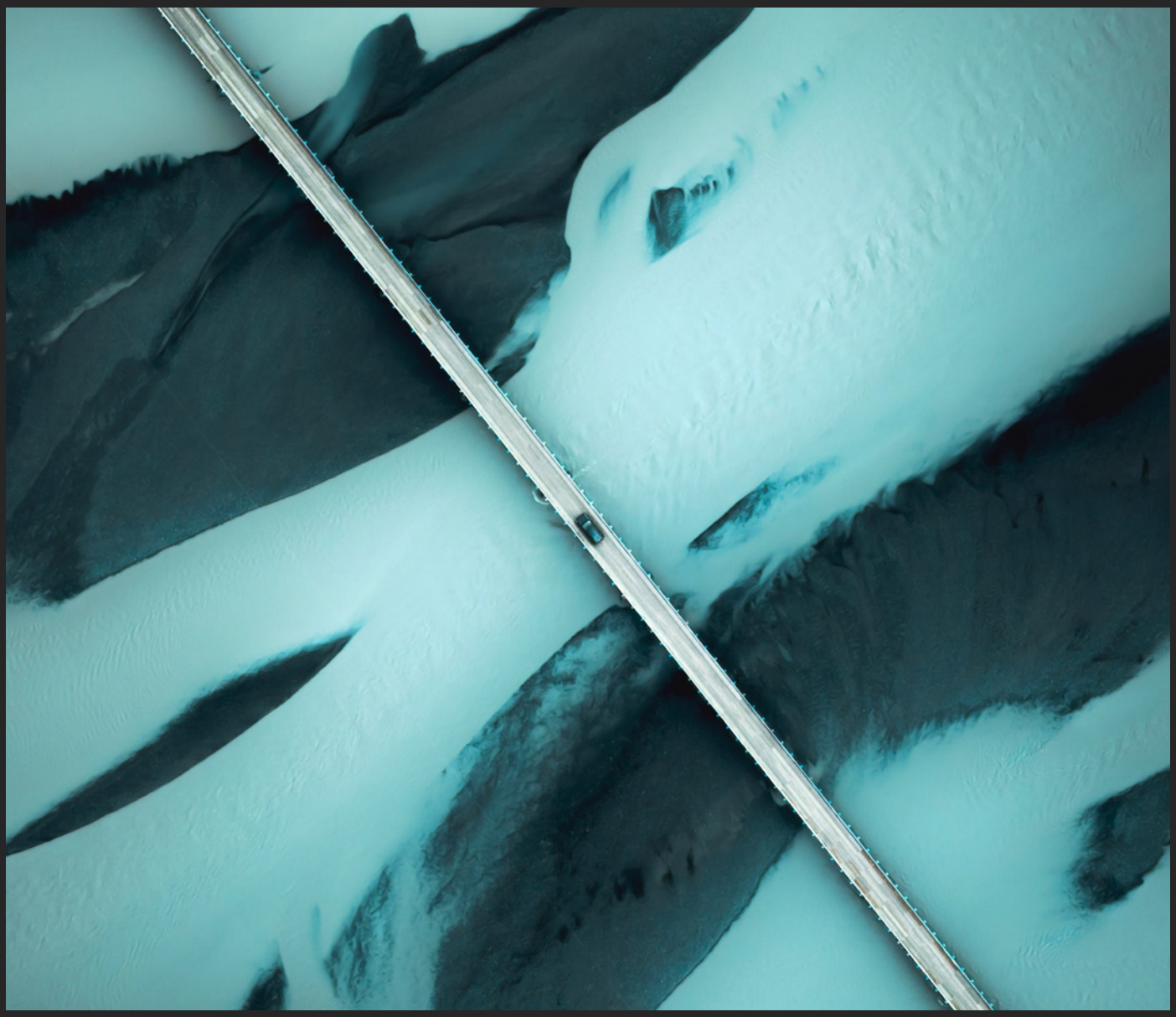
This translates into measurable performance differences: sovereignty frontrunners get better outcomes on security, collaboration, innovation and customer trust. For example, two-thirds say they're well positioned to develop new AI-enabled products and services, compared with just 48% of other organizations. And 64% say they have effective control and governance of AI and data, compared with 41% of other organizations.

Sovereignty frontrunners report better performance outcomes

Q: How well is your organization currently performing against the following objectives? Top two on a five-point scale



Footnote: sovereignty frontrunners n = 163, other organizations n = 237



Characteristics of sovereignty frontrunners

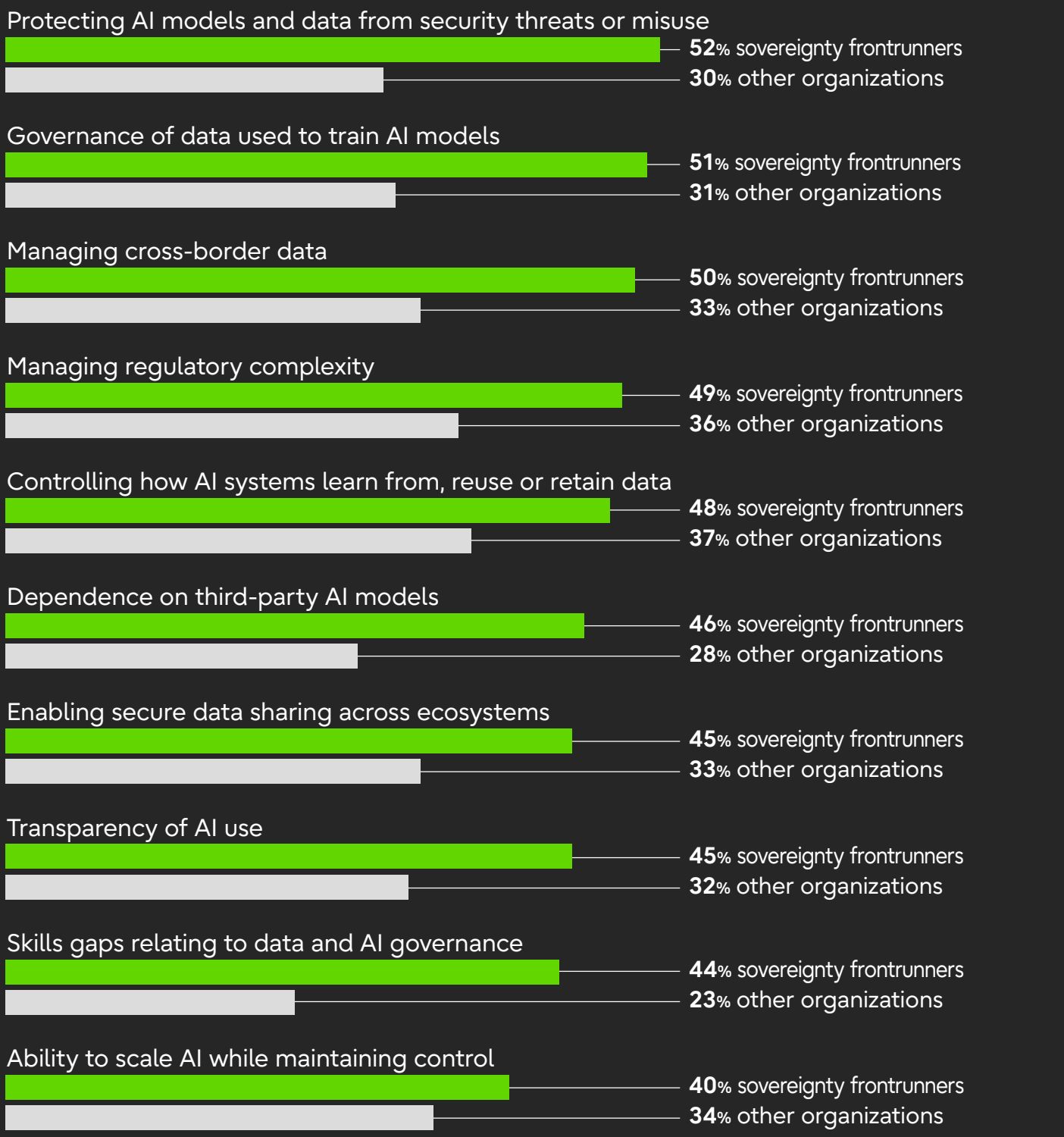
Sovereignty frontrunners are most likely to be in highly regulated industries. The top sectors are healthcare (17%), financial services (15%) and retail (15%). Legislation probably gave them a roadmap for redesign and helped them identify how to address their foundational challenges.

They also tend to be smaller organizations: 67% are companies with fewer than 10,000 employees. This could indicate that it's easier at smaller companies to design systems and processes from the ground up, whereas larger companies have to manage more complex structures, legacy technologies and partnerships.

As a result, sovereignty frontrunners have stronger data and AI sovereignty frameworks in place. More than half say security and governance of AI is, at most, only slightly challenging, compared with fewer than one-third of other organizations that say the same.

Sovereignty frontrunners are far more confident that they're managing data and AI challenges

Q: As AI usage increases, how challenging are the following areas? Not/slightly challenging



Footnote: sovereignty frontrunners n = 163, other organizations n = 237

Customer trust is a strategic priority, not a compliance outcome

Sovereignty frontrunners place more emphasis on customer trust than on regulatory risk. This reflects growing concern about AI-generated misinformation, misuse of customer data and lack of transparency in automated decision-making – all of which can quickly erode trust.

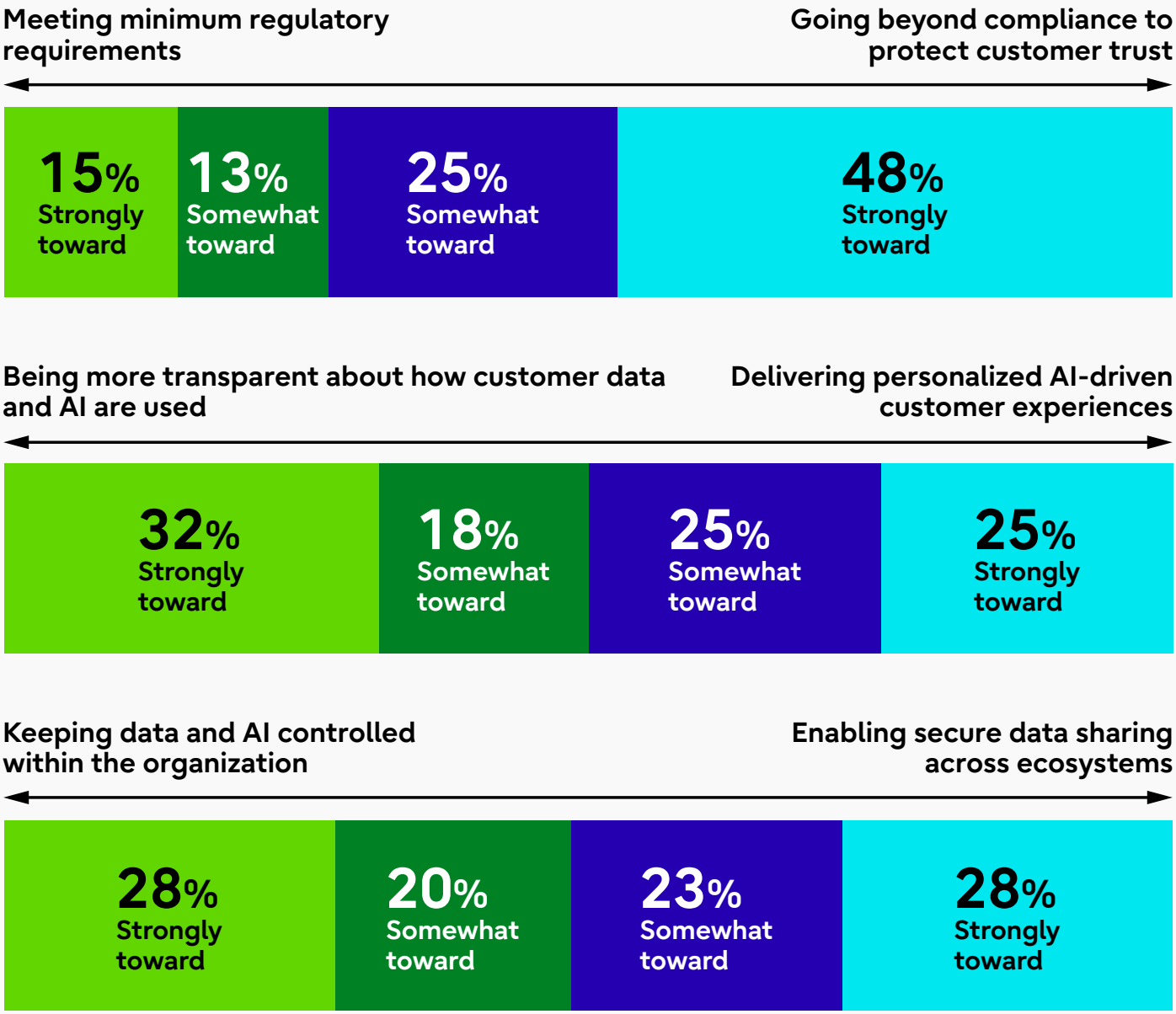
More than six in 10 (61%) say they're more worried that weak data governance could damage customer trust than they are about it triggering regulatory consequences. And 58% actively measure the impact of data governance on customer trust.

By measuring data and AI sovereignty performance, sovereignty frontrunners gain insight into how to design customer-centric frameworks that balance trade-offs relating to data control, customer trust and ecosystem collaboration. Three-quarters say they go beyond compliance to protect customer trust, and they say innovating to deliver personalized customer experiences is as important as being cautious and transparent with customer data (50:50).

Sovereignty frontrunners are embedding a strategy that's both built on secure foundations and designed to give them long-term growth.

Customer trust and collaboration are central to sovereignty frontrunners' data and AI strategies

Q: Which way does your organization typically lean in the following situations?



What this means for CIOs

- Prioritize customer trust as a measurable outcome, and build it into how AI systems are designed and deployed.
- Enable secure collaboration across ecosystems by embedding sovereignty into platforms, data flows and partner integrations.

How to become a sovereignty frontrunner

To turn data and AI sovereignty into a strategic advantage, organizations must act on four priorities:

1. **Make data and AI sovereignty a business priority, not a compliance function**
   Change the way you think about data and AI sovereignty. Embed it into decision-making so that it actively shapes technology investment, partnerships and long-term growth.

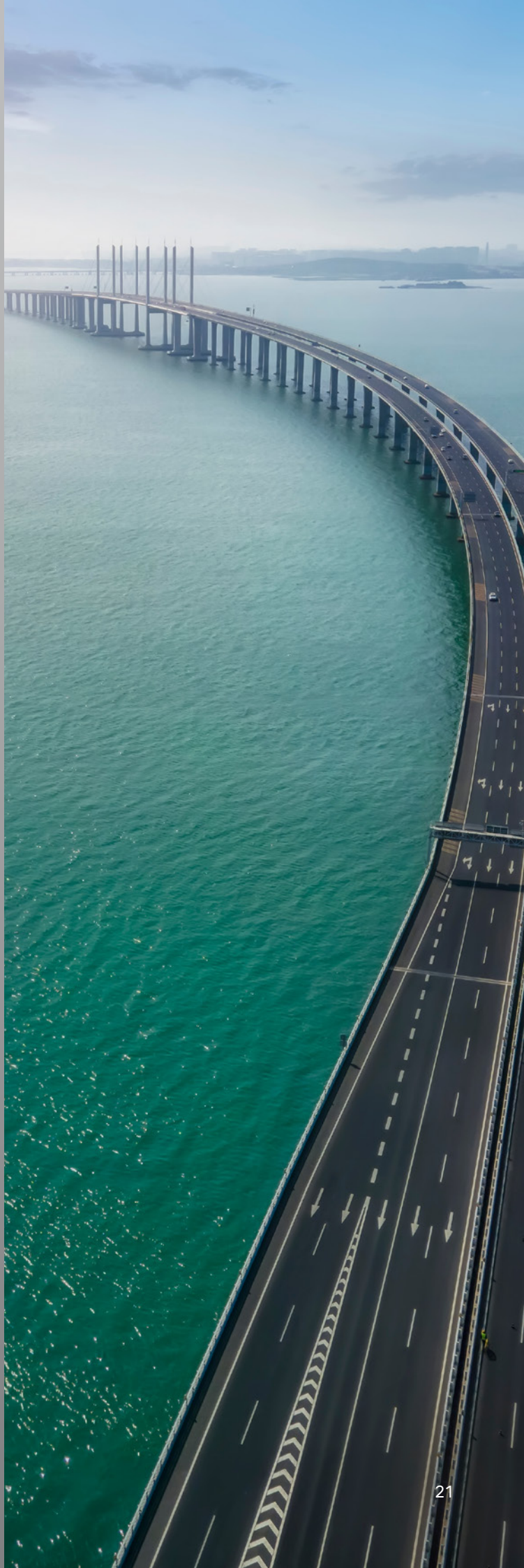
2. **Build sovereignty into platforms and AI systems at the outset**
   Design governance into architectures and lifecycles upfront, rather than relying on policies and controls after deployment.

3. **Design for secure data sharing across ecosystems**
   Develop architectures and operating models that allow you to collaborate with partners and platforms while retaining visibility and authority over data and AI.

4. **Measure the impact of sovereignty on customer trust and business performance**
   Track how data governance and AI use influence trust, adoption and outcomes, and use this insight to adapt decision-making and demonstrate value.

About the research

In February 2026, Uvance Wayfinders surveyed 400 senior business leaders based in Australia, Japan, the UK and the US. They represented technology and IT, finance, strategy and operations equally and were from companies across the following sectors: financial services; manufacturing; energy, resources and utilities; logistics and supply chain; retail and consumer goods; healthcare and life sciences; the public sector, government and defense; technology and telecommunications; and professional services. About half (53%) of companies had between 1,000 and 4,999 employees, 20% had between 5,000 and 9,999 employees and 28% had more than 10,000 employees. Percentages throughout this report may not sum precisely due to rounding.



uvance
Wayfinders

Consulting by Fujitsu

FUJITSU