

The state of sovereign AI adoption

Achieving a Holistic Strategic Vision for AI Autonomy



Tim Law
Research Director,
AI & Automation, IDC



Shari Lava
Group Vice-President,
AI, Data, and Automation, IDC

Table of contents



Click any title to navigate directly to that page.

In this InfoBrief	3	Data leakage and compliance are top concerns	17
5 top takeaways	4	What drives consideration of sovereign AI?	18
Defining the need for AI autonomy	5	Industry leaders recognize competitive advantage	19
The quest for sovereignty and AI autonomy	6	Building a holistic strategy	20
AI: New technology foundation for the global economy	7	Who’s actually in charge of sovereign AI?	21
The new sovereign AI economy	8	Leadership of sovereign AI varies by country	22
The coming agentic wave: Context	9	Sovereign AI’s value depends on who’s asking	23
Understanding gaps and awareness	10	What hinders sovereign AI readiness?	24
Leaders define sovereign AI as control and autonomy	11	Essential guidance: A strategic vision for AI autonomy	25
Most organizations are flying blind on sovereign AI	12	Appendix: Accessible data tables	26
Across all geos, an awareness gap exists	13	About the IDC analysts	30
Where you are determines what you know	14	Message from the sponsor	31
Inherent risks are not widely understood	15		
Sovereign AI roles and responsibilities remain ill-defined	16		

In this InfoBrief

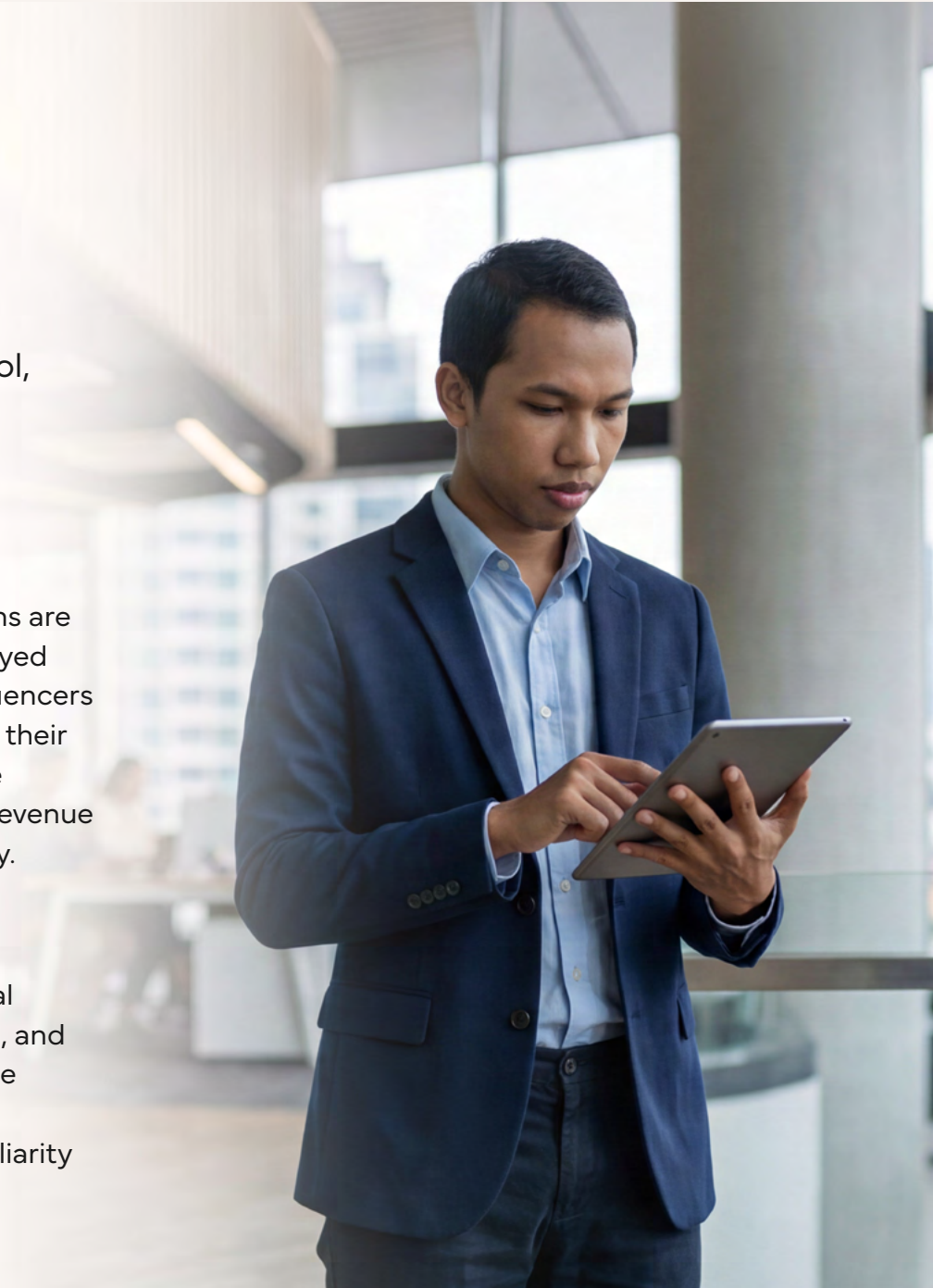
This IDC InfoBrief explores the current state of sovereign AI within enterprises and maps a path toward a more strategic approach to achieving the true benefits of sovereign AI: control, flexibility, and autonomy.

IDC's findings show:

- ➔ While more than half of executive leaders believe sovereign AI is a priority, there is little agreement on the definition, and many cannot define it.
- ➔ The desire for sovereign AI is there, but the plan isn't, and that gap presents an opportunity for enterprise leadership to define and assign ownership for such initiatives.
- ➔ Organizations want sovereign AI but lack the people or the know-how.
- ➔ Most organizations are flying blind on vendor strategy, and regulation is already catching up.

About the research

- ➔ This study was commissioned by Cohere and conducted by IDC to explore how organizations are approaching sovereign AI adoption. IDC surveyed 508 IT and business decision-makers and influencers responsible for AI purchasing decisions within their organizations. Respondents represented large enterprises with over \$1 billion USD in annual revenue across Canada, the U.S., the U.K., and Germany.
- ➔ The sample spanned the industry segments most affected by sovereign AI considerations, including healthcare and life sciences, financial services, public sector, energy, manufacturing, and telecommunications. IDC fielded a quantitative survey in April–May 2026, with respondents screened in advance to ensure a working familiarity with AI.



5 Top Takeaways

1



Healthcare most vulnerable

Healthcare (58%) shows the worst risk awareness, despite being one of the sectors with the highest regulatory exposure and highest consequence of data sovereignty failure.

2



CAIO emerging as sovereign AI lead

The chief AI officer leads in 52% of organizations; given the shift of power toward LOB in AI decision-making, this might signal an organizational realignment around AI initiatives.

3



Data security and privacy drives engagement/competitiveness matters

Data security and privacy is the number 1 driver across all cohorts. These priority risks drive the need for sovereign AI. There is little awareness of other risks addressed by sovereign AI, but there is increasing awareness that sovereign AI can convey competitive advantage.

4



Regional contrasts

There is significant differences in awareness and leadership across regions. Germany leads in concept awareness of sovereign AI. It also views CIO/CTO (not CAIO) as AI led (70%). U.S. respondents show the highest data security urgency (82%).

5



Awareness crisis

Only 13% widely understand sovereign AI concepts; 12% understand its risks. On risk awareness, most organizations are exposed to governance failures they might not recognize.

Source: IDC's Cohere AI Sovereignty Survey, May 2026 (n = 508)

Section 1:

Defining the need for AI autonomy

2

3

The quest for sovereignty and AI autonomy



Across regulated industries and geopolitically sensitive markets, enterprises are re-architecting their digital operating models, shifting from a global-by-default posture to a deliberately sovereign-by-design approach.”

1



Strategic autonomy

Enterprises have growing concern over vendor lock-in and portability to ensure choice.

2



National competitiveness

Enterprises want self-reliance and access to domestic capabilities.

3



Regulatory requirements

Enterprises are subject to data residency requirements (GDPR, AI Act, and other requirements).

4



Security and resilience

Enterprises want the ability to defend against cyber and geopolitical risk. This concern holds for all countries and regions.

5



Transparency

Enterprises need auditable models and data lineage for oversight and responsible AI mandates.

Source: *Sovereignty by Design: How Data Sovereignty Is Reshaping Connectivity and Enterprise Architecture* (IDC #US54566226, July 9, 2026)

Defining the need for AI autonomy

2

3

AI: New technology foundation for the global economy

The multiplier effect:

By 2030, every new \$1.00 USD spent on AI solutions and services will generate \$4.90 USD in the economy.

Source: IDC's Macroeconomic Center of Excellence, 2025

IDC predicts that by 2028, CIOs at multinational organizations will increase investments in modular, sovereign-ready cloud and data localization environments by 65% to future-proof operations against rising sovereignty demands.”

Source: IDC FutureScape: Worldwide CIO Agenda 2026 Predictions (IDC #US53865325, October 2025)

In this environment, enterprises are seeking to ensure AI autonomy to maintain economic competitiveness and strategic control and reduce foreign dependence.



The new sovereign AI economy

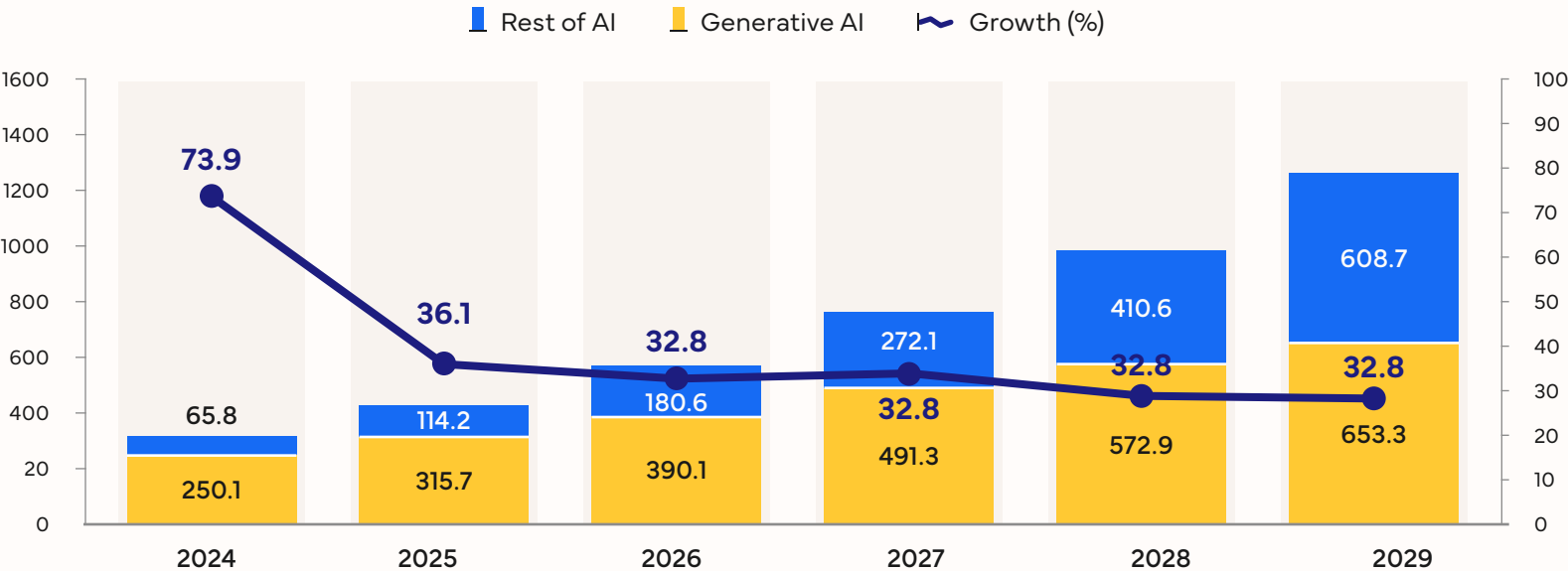
Q: Which of the following AI technologies is your organization currently or planning to use in the next 12 months?

May 2026



Figure 1
Worldwide AI and generative AI spending by AI type, 2024–2029

See the figure data in an [accessible table format](#).



Source: IDC's Worldwide Artificial Intelligence and Generative AI Spending Guide, 2025

Rapid AI adoption in enterprises is happening in the context of rising geopolitical instability. Enterprises view control over AI infrastructure, data, and models as strategic autonomy.

Q: Which of the following AI technologies is your organization currently or planning to use in the next 12 months? Source: IDC's Cohere AI Sovereignty Survey, May 2026 – Total sample: n = 508

The coming agentic wave: Context

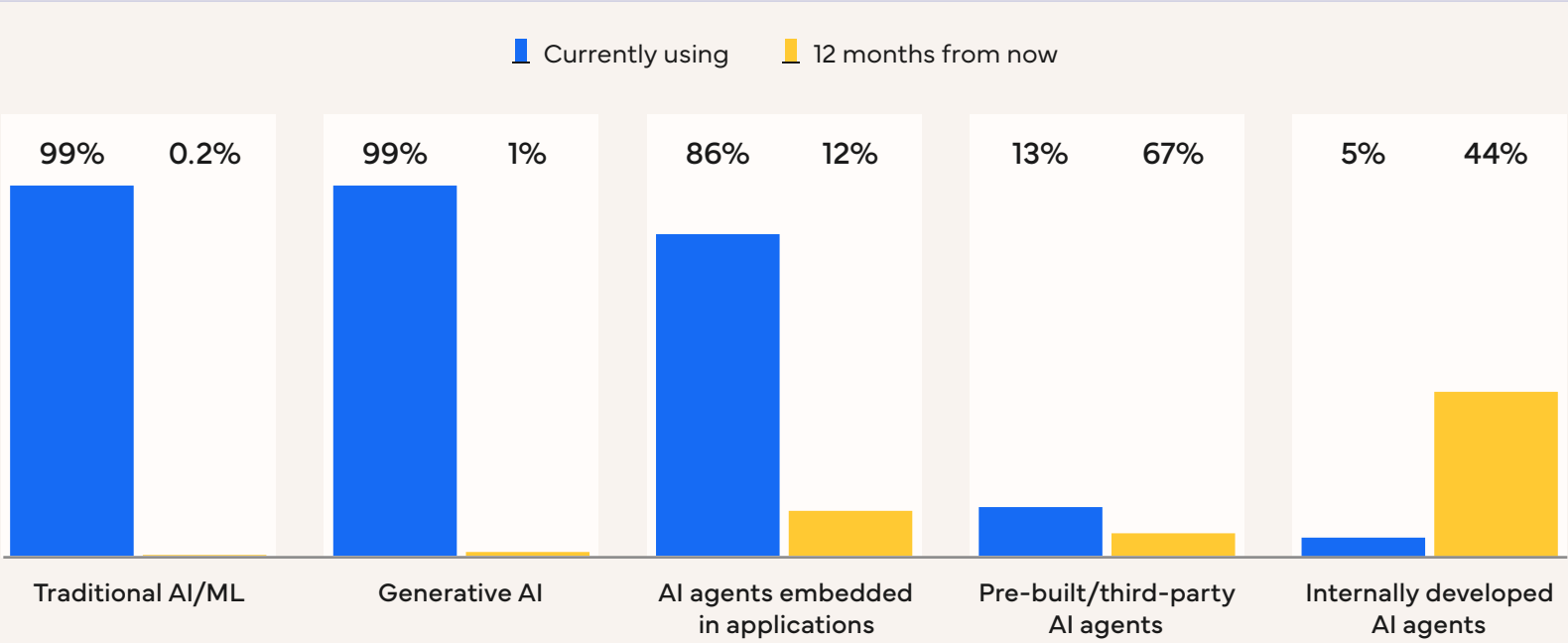
An agentic AI wave will require sovereign AI to be elevated to a strategic enterprise initiative. However, understanding of requirements and readiness lag in most organizations.

Q: Which of the following AI technologies is your organization currently or planning to use in the next 12 months?

AI technology in use now and in the future

- Third-party agents **5× leap**
- Internally developed AI agents nearly a **10× increase**
- Current sovereign AI approaches and lack of readiness put enterprises at risk

Figure 2
See the figure data in an [accessible table format](#).



Source: IDC's Cohere AI Sovereignty Survey, May 2026 (n = 508)

1

Section 2:

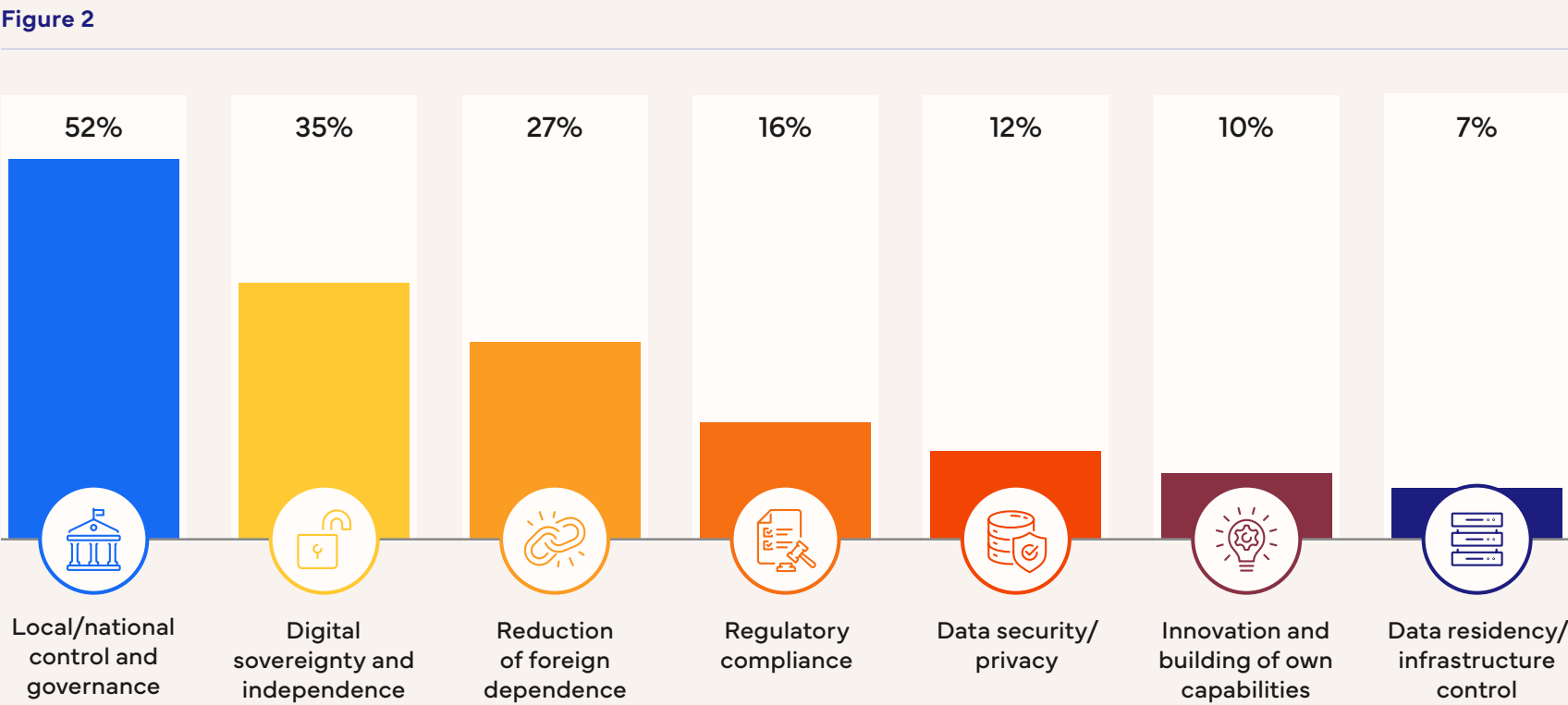
Understanding gaps and awareness

3

Leaders define sovereign AI as control and autonomy

In your own words (without looking it up), how would you describe the concept of Sovereign AI to a colleague who was unaware of it?

- **52%** of respondents explicitly describe sovereign AI in terms of local/national control.
- **35%** invoke digital autonomy as a concept.
- **But one in three** had difficulty describing it in their own words.



Source: IDC's Cohere AI Sovereignty Survey, May 2026 (n = 508)

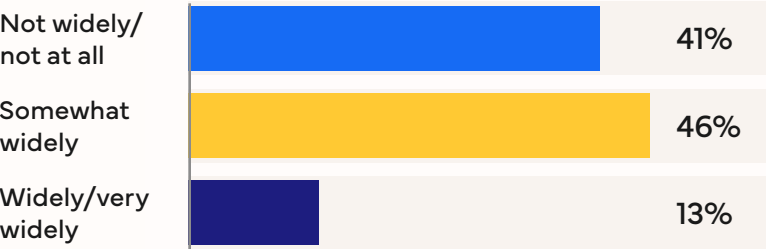
Most organizations are flying blind on sovereign AI

Conceptual understanding is low and varies widely across the organization

IDC defines sovereign AI as the ability to have free choice and control over the design, development, deployment, accessibility, operation, maintenance, and governance of AI systems and applications, as well as the underlying technology foundations they depend on.

Q: How widely are concepts associated with sovereign AI understood across your organization?

Figure 3
Even AI leaders have widely varying levels of understanding of sovereign AI.



Source: IDC's Cohere AI Sovereignty Survey, May 2026 (n = 508)

- ➔ Sovereign AI awareness remains critically low; only 13% report it is widely understood.
- ➔ "Not widely aware" and "somewhat widely aware" are only separated by five percentage points.
- ➔ A lack of clear understanding hampers organizational alignment and adoption.



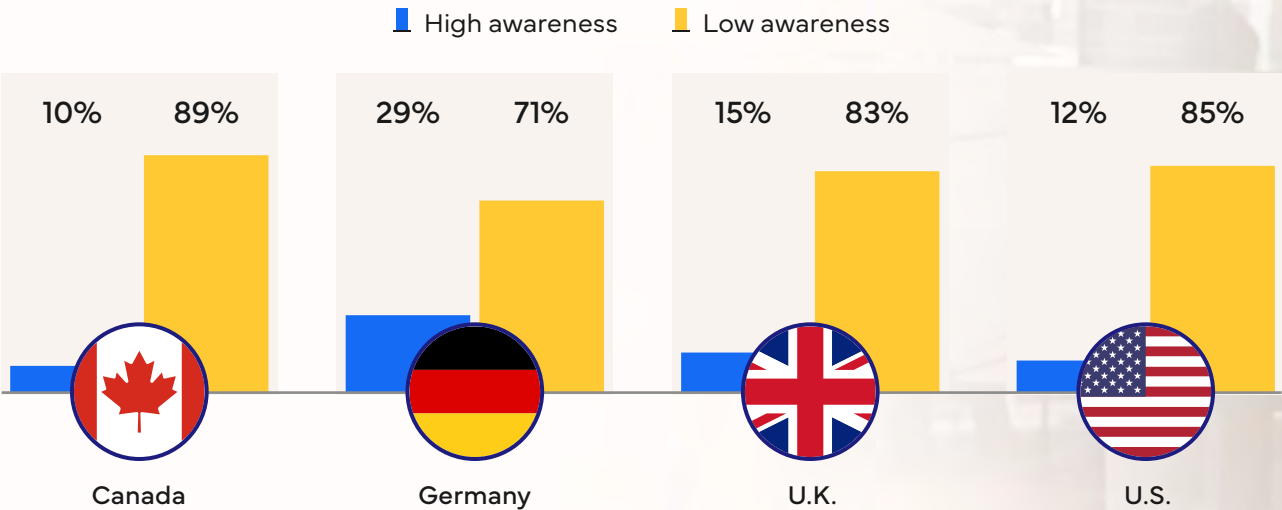
Across all geos, an awareness gap exists

To implement an effective sovereign AI strategy, enterprises across the world must first raise awareness and create a common understanding at all levels of the organization.

Q: How widely are concepts associated with sovereign AI understood across your organization?

Figure 4
The awareness gap: How familiar are you with the concept of sovereign AI?

See the figure data in an [accessible table format](#).



Source: IDC's Cohere AI Sovereignty Survey, May 2026 (n = 508)

Where you are determines what you know

Understanding of sovereign AI varies by role, industry, and geography

Q: How widely are concepts associated with sovereign AI understood across your organization?

Understanding of sovereign AI varies across various roles, industries, and geographies. Highly regulated industries in geographies with structured regulatory regimes for data security and privacy tend to have the highest awareness levels. Moreover, IT is much more aware of the requirements than most business leaders.

Who leads in awareness?



IT professionals (21%) show **2×** the awareness of LOB leaders (10%).



Financial services (18%) and telecom (16%) top the industry rankings.



German enterprise AI leaders have the greatest awareness at 26%.



Source: IDC's Cohere AI Sovereignty Survey, May 2026 (n = 508)

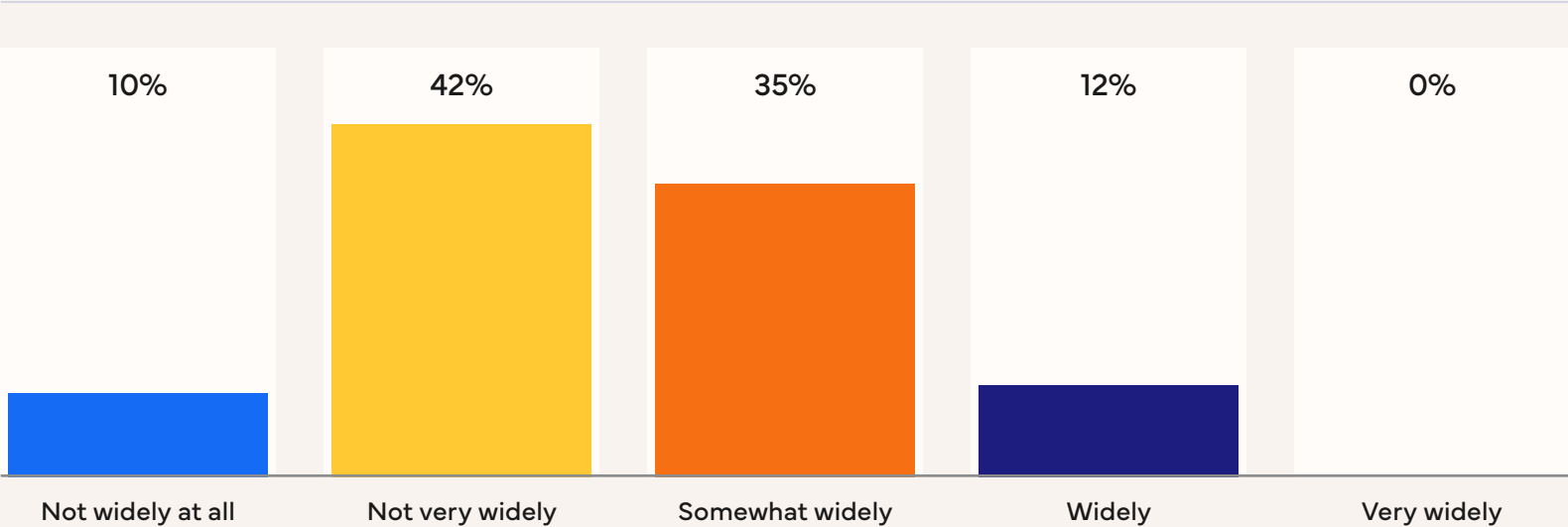
Inherent risks are not widely understood

Enterprises are failing to broadly understand the inherent risks that sovereign AI addresses

Q. How widely are the inherent risks that sovereign AI addresses understood across your organization?

- ➔ The largest enterprises with \$20B USD in revenue are much more risk-aware than small firms.
- ➔ Most enterprises (78%) report risks are not very widely or only somewhat widely understood.
- ➔ Only 12% of respondents say that the risks sovereign AI mitigates are widely understood in their organizations. 0% reported the risks being very widely understood.

Figure 5



The lack of understanding of inherent risks holds across geographies, roles, and industries. While low across all cohorts, Europe (17%) is almost **2x** more widely aware of the inherent risks than North America (9%).

Source: IDC's Cohere AI Sovereignty Survey, May 2026 (n = 508)

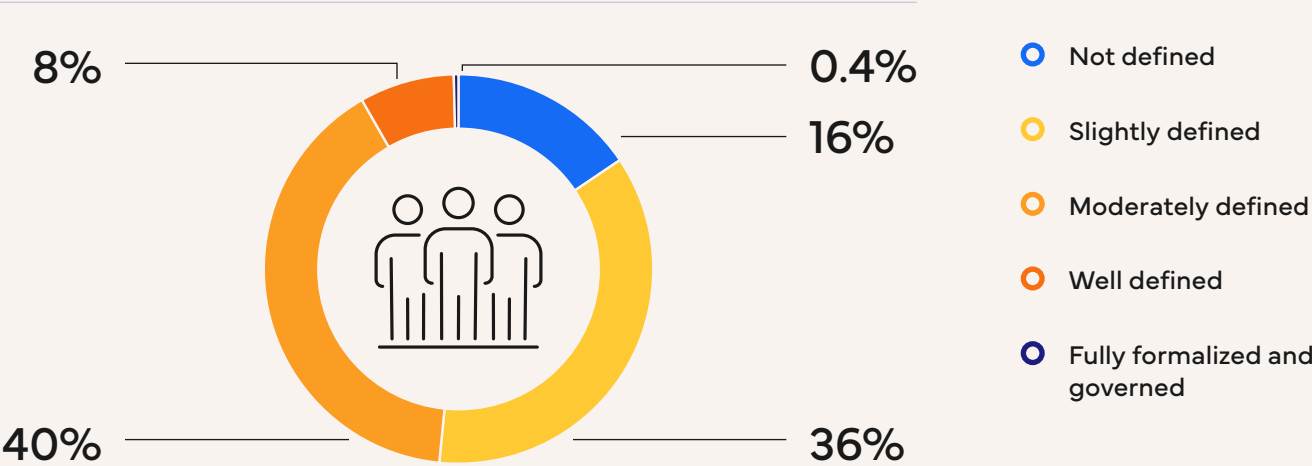
Sovereign AI roles and responsibilities remain ill-defined

Given that roles are ill-defined, it reinforces the finding that there is also low awareness across all cohorts. It would be the role of a sovereign AI leader to ensure awareness of goals and objectives across the enterprise.

Q: Currently, how clearly do you feel the roles and responsibilities related to sovereign AI are defined in your organization?

- ➔ Only **8%** said that sovereign AI roles are well-defined or formalized/governed.
- ➔ **51%** said roles are slightly or not at all defined.
- ➔ **40%** said they are moderately defined.

Figure 6



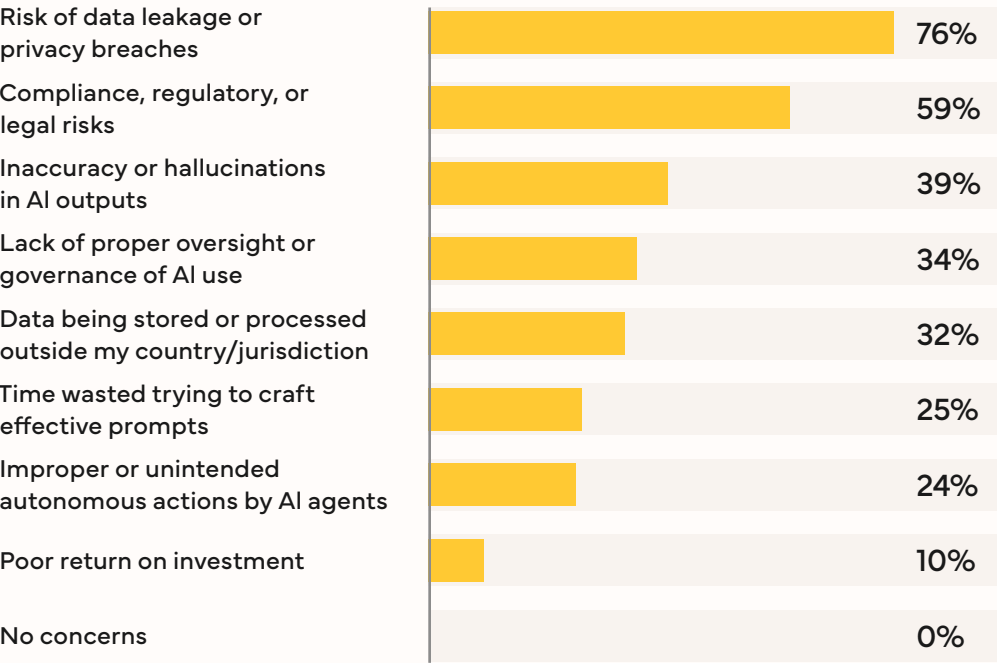
Source: IDC's Cohere AI Sovereignty Survey, May 2026 (n = 508)

Data leakage and compliance are top concerns

Enterprises note a wide number of concerns beyond data leakage and compliance

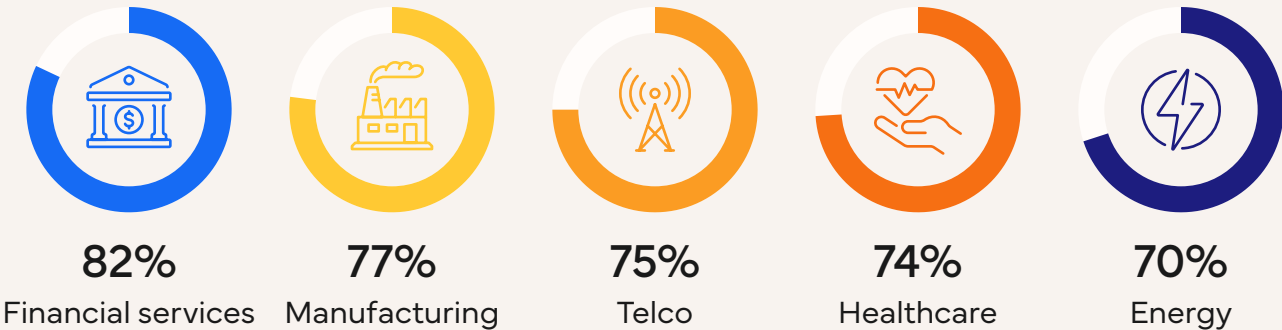
Q: Top concern: Rank the top 3 concerns you have about using generative and agentic AI tools.

Figure 7
Top concerns driving the need for sovereign AI



Source: IDC's Cohere AI Sovereignty Survey, May 2026 (n = 508)

Concerns about data leakage and privacy are high across all industries:



A majority see compliance and regulatory risk as the second-greatest concern across industries.

Enterprises see data leakage/privacy, compliance, and regulatory concerns as top concerns around the use of AI that can be addressed with sovereign AI initiatives.



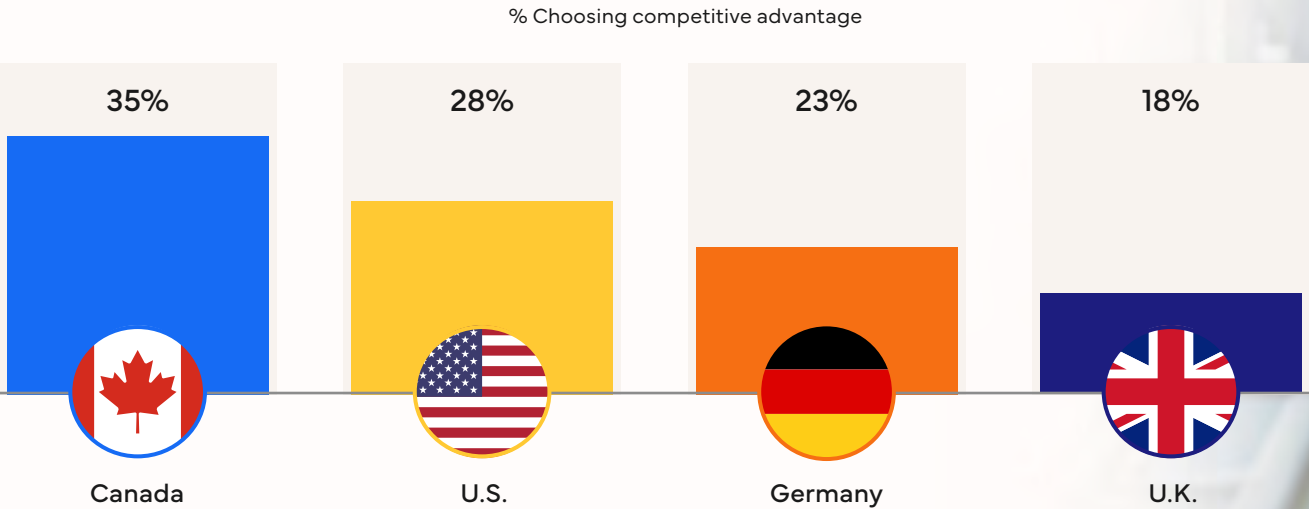
What drives consideration of sovereign AI?

Q. What are the primary drivers that should make your organization interested in sovereign AI?

Data security/privacy and risk management were top drivers, but competitive advantage was also a driver across geographies.

- 35% in Canada and 28% in the U.S.
- 23% in Germany and 18% in the U.K., reflecting the higher focus on regulatory frameworks

Figure 8

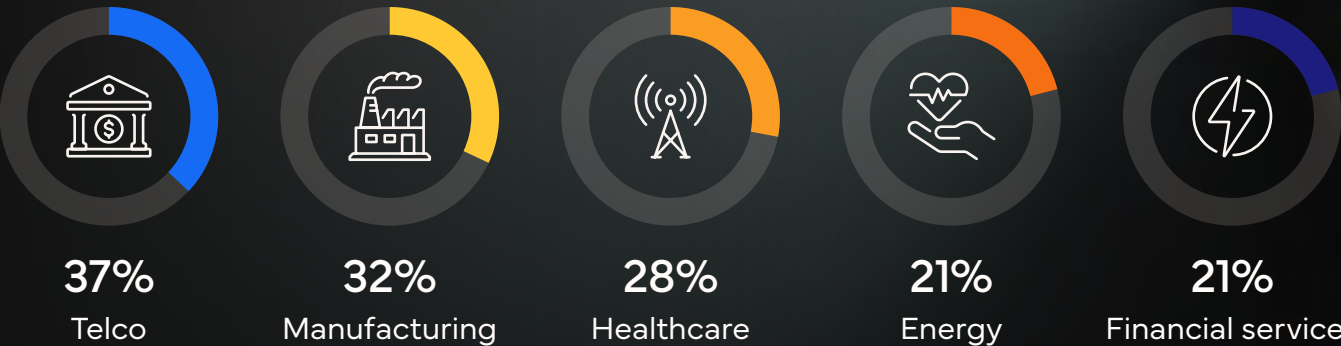


Source: IDC's Cohere AI Sovereignty Survey, May 2026 (n = 508)

Industry leaders recognize competitive advantage

- ➔ Across industries leaders, recognize that sovereign AI can be a competitive advantage.
- ➔ Telco leads with **37%**, recognizing the benefits of sovereign AI beyond regulatory compliance, privacy, and data security, along with manufacturing **(32%)**.
- ➔ Even industries that are highly regulated around data privacy, such as healthcare **(28%)** and financial services **(21%)**, see benefits.

Competitive advantage as a driver



1

2

Section 3:

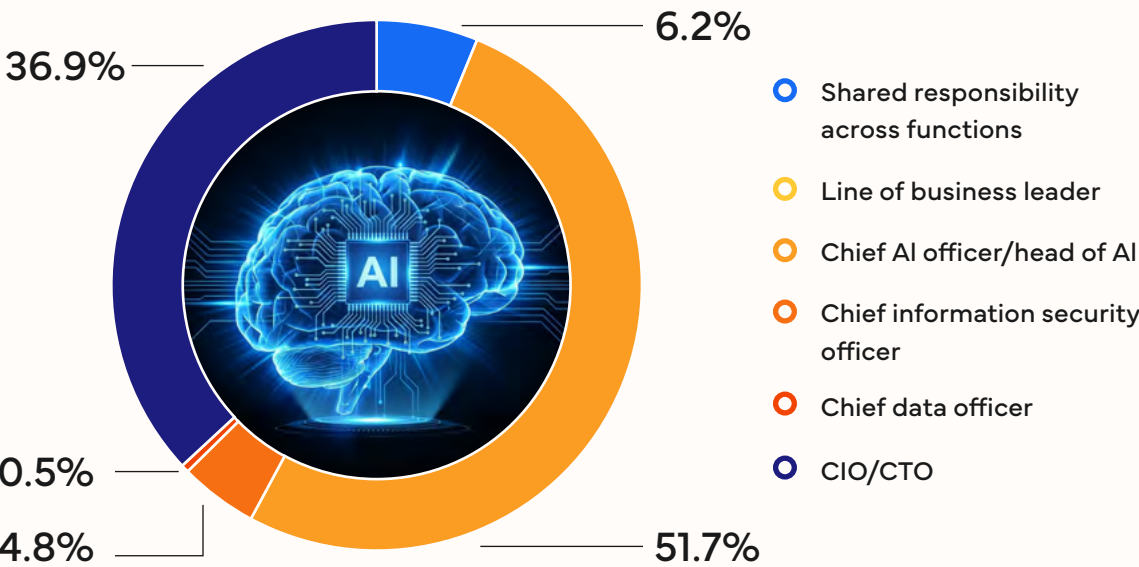
Building a holistic strategy

Who’s actually in charge of sovereign AI?

Clearly defined roles and responsibilities are critical to the success of AI autonomy initiatives, but roles vary significantly across organizations and geographies

Q: What role or position takes the lead in the management of sovereign AI?

Figure 9
Who manages sovereign AI?



There is no established industry standard for how sovereign AI initiatives are managed. Sometimes (40%), it is managed by IT; a slight majority (52%) consider it an AI initiative. But management of sovereign AI varies widely by region. This has clear implications for trying to execute a cohesive global AI autonomy strategy.

- ➔ Chief AI officer/head of AI leads in 52% of organizations, but its dominance is **highly uneven** by country.
- ➔ The CIO/CTO (37%) often takes the lead.
- ➔ The responsibility is rarely shared.
- ➔ There are significant country variations.
- ➔ Across most countries, except for Germany, the chief AI officer takes the lead for sovereign AI initiatives.

Source: IDC’s Cohere AI Sovereignty Survey, May 2026 (n = 420 organizations with dedicated sovereign AI responsibility)

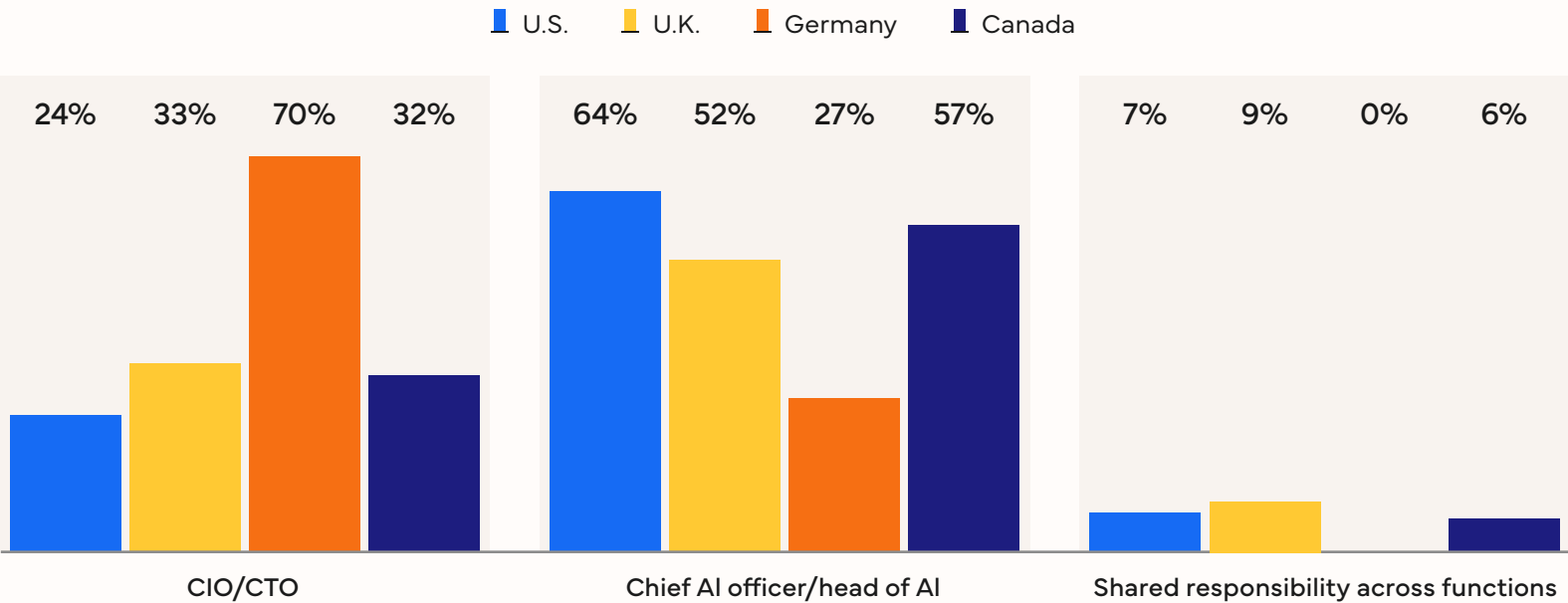
Leadership of sovereign AI varies by country

Sovereign AI lead role distribution by country

Q: What role or position takes the lead in the management of sovereign AI?

Figure 10
Sovereign AI lead role distribution by country, %

See the figure data in an [accessible table format](#).



Source: IDC's Cohere AI Automation Survey, May 2026 (n = 420 organizations with dedicated sovereign AI responsibility)

- ➔ **Germany** is the outlier, with CIO/CTO ownership dominant (70% vs. 24–33% elsewhere). Sovereign AI is seen as an IT/infrastructure initiative. Regardless of where ownership rests, alignment with business initiatives is critical.
- ➔ **The U.S. and Canada** lead in dedicated ownership, with a Chief AI Officer/head of AI role in most organizations (64% and 57.0%, respectively), signaling sovereign AI has achieved C-suite priority independent of IT.

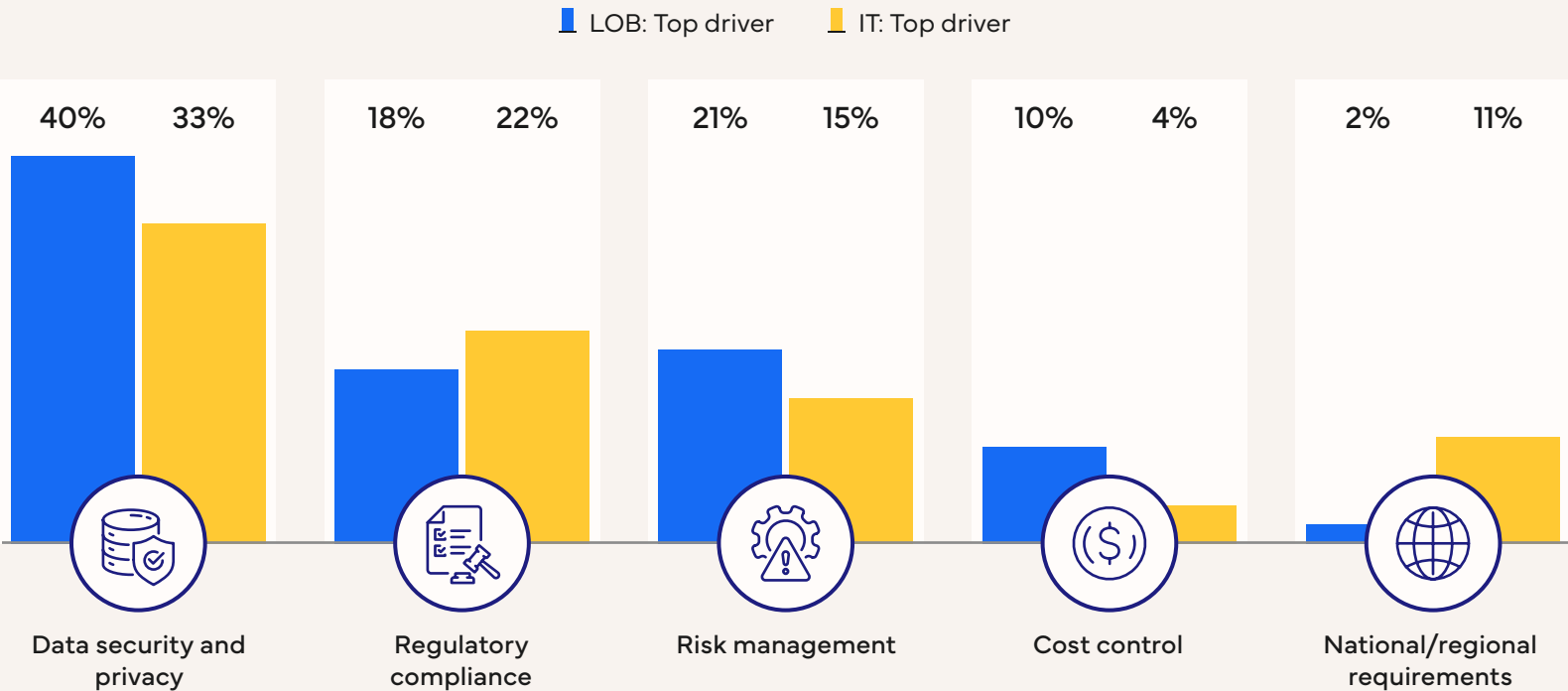
Sovereign AI’s value depends on who’s asking

Q: Given what you now understand about the concepts of sovereign AI, what are the primary drivers that should make your organization interested in sovereign AI? (Top 5 primary)

- LOB leaders largely view sovereign AI as a means to **managing business risk**, including data security and privacy and cost controls.
- IT leaders view sovereign AI as **regulatory compliance** and the ability to meet national/regional requirements.

Figure 11
Top 5 drivers of sovereign AI

See the figure data in an [accessible table format](#).



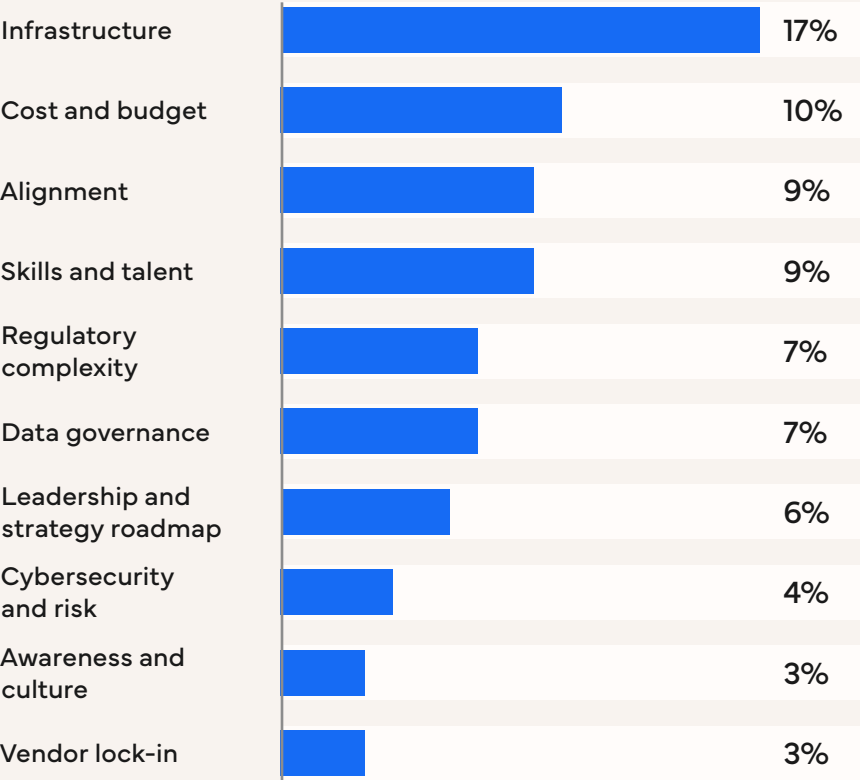
Source: IDC’s Cohere AI Sovereignty Survey, May 2026 (n = 508)

What hinders sovereign AI readiness?

Q: What is the biggest barrier preventing your organization from achieving sovereign AI readiness?

- ➔ When asked to describe barriers to AI readiness, there was little consensus but many perceived barriers.
- ➔ Infrastructure outpaced the responses at **17%**, but many barriers were cited, including cost.
- ➔ The lack of consensus among AI decision-makers is consequential and reflects the need for leadership on sovereign AI strategy.

Figure 12



Source: IDC's Cohere AI Sovereignty Survey, May 2026 (n = 508)

“

We need stronger infrastructure before handling sovereign AI confidently internally”

“

The total cost of implementing sovereign AI systems [is] higher than originally expected”

“

Limited internal expertise continues to slow progress...”

Essential guidance: A strategic vision for AI autonomy

Defining • Understanding • Building

- 1** Create a **strategic vision** and plan to achieve AI independence, with measurable goals, objectives, and responsibilities. Ensure responsibility rests with either the chief AI officer or CIO/CTO. The majority of organizations place responsibility with the CAIO.
- 2** **Adopt AI sovereignty** as a strategic enterprise objective that is shared throughout the organization. Assign clear goals and objectives at every level of the organization.
- 3** **Align the organization**, including technical and line-of-business leaders, around an enterprise strategy for AI independence.
- 4** **Bridge the awareness gap** and create a **common understanding** throughout the organization that aligns IT and LOB goals and objectives.
- 5** **Invest** in sovereign AI platforms to create a technical foundation for success and close the infrastructure gap.
- 6** Acquire **sovereign AI skills** by both acquiring skills externally and building skills internally for sustainable initiatives.



Achieving AI independence

- ➔ Define the strategy.
- ➔ Align the organization.
- ➔ Create common understanding.
- ➔ Invest in platforms and skills.

Appendix: Accessible data tables

Page 8 figure 1
WW AI and generative AI spending by AI type (2024–2029)

	Rest of AI	Generative AI	Growth (%)
2024	250.1	65.8	73.9
2025	315.7	114.2	36.1
2026	390.1	180.6	32.8
2027	491.3	272.1	33.8
2028	572.9	410.6	28.8
2029	653.3	608.7	28.3

Source: IDC's Worldwide Artificial Intelligence and Generative AI Spending Guide, 2025
[Return to figure](#)

Page 9 figure 2

	Currently using	12 months from now
Traditional AI/ML	99%	0.2%
Generative AI	99%	1%
AI agents embedded in applications	86%	12%
Pre-built/third-party AI agents	13%	67%
Internally developed AI agents	5%	44%

Source: IDC's Cohere AI Sovereignty Survey, May 2026 (n = 508)
[Return to figure](#)

Page 13 figure 4
The awareness gap: How familiar are you with the concept of sovereign AI?

	High awareness	Low awareness
Canada	10%	89%
Germany	29%	71%
United Kingdom	15%	83%
United States	12%	85%

Source: IDC's Cohere AI Sovereignty Survey, May 2026 (n = 508)
[Return to figure](#)

Appendix: Accessible data tables (continued)

Page 22 figure 10
Sovereign AI lead role distribution by country, %

	U.S.	U.K.	Germany	Canada
CIO/CTO	24%	33%	70%	32%
Chief AI officer/head of AI	64%	52%	27%	57%
Shared responsibility across functions	7%	9%	0%	6%

Source: IDC’s *Cohere AI Sovereignty Survey*, May 2026 (n = 420 organizations with dedicated sovereign AI responsibility)

[Return to figure](#)

Page 23 figure 11
Top 5 drivers of sovereign AI

	LOB: Top driver	IT: Top driver
Data security and privacy	40%	33%
Regulatory compliance	18%	22%
Risk management	21%	15%
Cost control	10%	4%
National/regional requirements	2%	11%

Source: IDC’s *Cohere AI Sovereignty Survey*, May 2026 (n = 508)

[Return to figure](#)

Appendix: Accessible data tables (continued)

U.K.

Question	Recommended stat
QA04. (OVERALL) Rank the top 3 concerns you have about using generative and agentic AI Tools.	78% of UK respondents cite data leakage/privacy breaches as a top concern about using generative and agentic AI tools; 61% cite compliance, regulatory or legal risks.
QA01. Which of the following AI technologies is your organization currently or planning to use in the next 12 months?	In the UK, use of internally developed AI agents is expected to rise from 7% currently to 47% within 12 months.
QVE01. How well aligned is your vendor strategy with Sovereign AI objectives?	Only 7% of UK respondents say their vendor strategy is strongly or fully aligned with sovereign AI objectives; 51% say it is not aligned or only slightly aligned.
QVE03. (OVERALL) What are the three most important capabilities and services that vendors supporting Sovereign AI need to provide?	68% of UK respondents cite strong security controls, 55% cite auditability and compliance support, and 46% cite transparent model governance as top vendor capabilities.
QA05. In which IT environments has your organization deployed generative or agentic AI tools for processes subject to external regulations (e.g., finance, healthcare, data privacy, or industry-specific rules	Among UK IT respondents deploying generative or agentic AI for externally regulated processes, 82.4% use private cloud/VPC, 80% use public cloud, 38% use hybrid environments and 3% use on-premises.

Appendix: Accessible data tables (continued)

Germany

Question	Recommended stat
QSA17. Over the next 2-3 years, how do you expect the focus on the concepts of Sovereign AI to change in your organization?	75% of German respondents expect their organization’s focus on Sovereign AI to increase over the next two to three years: 56% expect a slight increase, 17% a significant increase and 2% a dramatic increase.
QF04. In the next year, what changes in your current IT infrastructure do you plan to implement in order to address Sovereign AI concerns?	62% of German respondents say they plan to bring sensitive AI workloads or data under direct control within the next year.
QVE03. (OVERALL) What are the three most important capabilities and services that vendors supporting Sovereign AI need to provide?	63% (transparent model governance), 57% (clear data ownership) and 42% (regional data hosting guarantees) are the combined top-three selections for vendor capabilities, rather than the percentage naming each item as their single most important requirement.
QSA07. What benefits would or does your organization expect from adopting the concepts associated with Sovereign AI capabilities?	Germany recorded the highest figure across the four surveyed markets (32%) for economic competitiveness and innovation.

NOTE: All are based on the full German sample. For QSA17, the 75% figure combines “increase slightly”, “increase significantly” and “increase dramatically”; for QSA16, the 57% figure is the Bottom-2-Box result. Important detail: Specify QVE03 (OVERALL). The 63%, 57% and 42% figures combine respondents’ first-, second- and third-ranked choices. They are not the results from the separate “Top Capability” table.

About the IDC analysts



Tim Law
Research Director, AI & Automation, IDC

Timothy Law is a Research Director for AI & Automation, responsible for the generative AI lifecycle tools and technologies research practice. Mr. Law’s core research coverage includes the evolution of generative AI infrastructure and platforms, foundation models, developer tools, observability solutions, agentic systems, and generative AI services. This research analyzes the trends and developments in the AI software markets, including the costs, benefits, and impact of generative AI technologies.

[More about Tim Law →](#)



Shari Lava
GVP Research, AI, IDC

Shari Lava is Group Vice-President, AI, Data, and Automation. Ms. Lava’s core research coverage includes the fast-evolving AI software market, as well as the Automation and Data foundations essential for deploying AI at enterprise scale. This includes deep analysis of market dynamics, adoption trends, and how these technologies converge to deliver superior business outcomes. She is based remotely in Toronto, Canada.

[More about Shari Lava →](#)

Message from the sponsor



Your data. Your infrastructure. Cohere keeps it that way.

Cohere is the world's leading sovereign AI company. We build foundation models and end-to-end AI products to solve real-world business problems. We partner with organizations to deliver seamless integration, deep customization, and user-friendly solutions. Our all-in-one platform provides maximum security, privacy, and deployment flexibility across public clouds, private on-premises environments, and fully air-gapped settings. Headquartered globally in Toronto and San Francisco, Cohere also operates offices in London, New York, Montreal, Paris, and Seoul, serving customers worldwide.

See how you can own your AI with Cohere

IDC Custom Solutions

IDC Custom Solutions produced this publication.

The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis that IDC independently conducted and published, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies.

This IDC material is licensed for external use and in no way does the use or publication of IDC research indicate IDC's endorsement of the sponsor's or licensee's products or strategies.



[IDC.com](#)

[IDC on LinkedIn](#)

[IDC Blog](#)

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives.

©2026 IDC. Reproduction is forbidden unless authorized. All rights reserved. [CCPA](#)