

An aerial photograph of a mangrove forest with a winding river. Overlaid on the image are several glowing blue energy lines that form loops and curves, suggesting a digital or AI theme. The background shows a sunset or sunrise over the ocean with distant islands.

Sovereign AI: Own your AI future

From managing risk to accelerating growth

 **accenture**

Authors

Global



David Wood

Senior Managing Director – Global Technology Consulting Lead, Global Sovereign AI Lead



Bryan Rich

Senior Managing Director – Global AI Lead – Health, Public Services and Defense



Surya Mukherjee

Senior Principal, Sovereign AI Global Research Lead

Europe, Middle East, Africa



Mauro Macchi

CEO – Europe, Middle East and Africa (EMEA)



Mauro Capo

Managing Director – Digital Sovereignty Lead – Europe, Middle East and Africa (EMEA)

Asia Pacific



Kunal Shah

Managing Director – Sovereign AI Lead – Asia Pacific

Artificial intelligence has moved beyond being a technological marvel. It has become the foundation for national competitiveness and business survival. Yet its foundations—models, computing power and data—are concentrated in a few hands. In 2024, nearly 70% of leading AI models originated in the United States and another quarter in China¹. The result is a level of dependence for some countries that raises important questions about resilience, competitiveness and long-term innovation. This path to risk mitigation and resilience also reveals a growth opportunity: **Sovereign AI**.

The good news? Only one-third of an organization's AI workloads need to be sovereign. Working with a mix of global and local providers leads to more opportunities for innovation and growth.

Introduction

Sovereign AI refers to a country's ability to independently develop and deploy AI by relying on its own infrastructure, data, models and talent. This enables a country to foster innovation, drive economic growth and advance strategic goals—while retaining full control over the entire AI lifecycle.



Sovereign AI is not about isolationism or every nation/company building the entire AI stack from scratch—very few can. It's about interoperability on one's own terms. The goal is to make technological choices that are flexible and secure and create a fit-for-purpose AI stack that blends global and local components, each governed by the right level of oversight depending on the use case and national priorities.

Sovereignty allows countries and enterprises to create and participate in new trusted AI ecosystems and build secure ways to share data while hedging against geopolitical risk and strengthening resilience. It fuels local industry growth, fosters self-reliance and accelerates AI-led economic expansion. In essence, sovereign AI turns strategic vulnerability into an engine for innovation, competitiveness and nation-building measured through GDP expansion.



Introduction

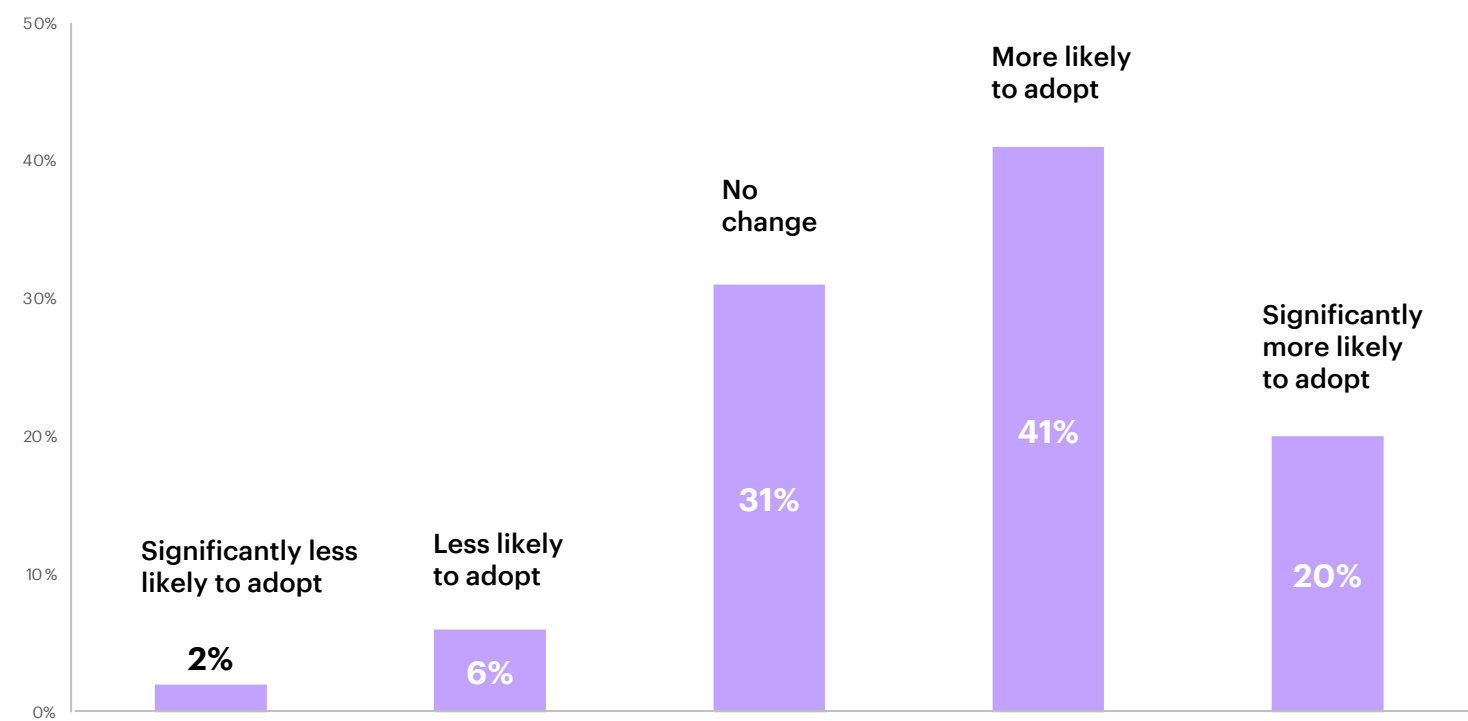
Ongoing geopolitical uncertainties are increasing concerns that relying heavily on a limited number of providers may introduce vulnerabilities into supply chains, potentially affecting innovation and national interests. Proprietary models may embed cultural or regulatory biases misaligned with local norms. Most critically, data and compute sovereignty determine who captures the majority of the value from AI innovation. For nations, it can define economic growth and increase control over public infrastructure; for enterprises, it can accelerate competitive advantage and expand profit pools.

As a result, signs of a rapidly expanding demand for sovereign AI are everywhere. Our survey of almost 2,000 business and government leaders across 28 countries found that 61% are now more likely to seek sovereign technology solutions as geopolitical risks rise and as the economic value associated with AI is abundantly clear (see Figure 1).

Analysts offer differing estimates of the total opportunity as the market evolves and overlaps with adjacent sectors—but momentum is clearly building. Oppenheimer’s Equity Research firm puts the potential sovereign AI infrastructure opportunity at \$1.5 trillion, including \$120 billion in Europe². According to Gartner®, “by 2027, 35% of countries will be locked into region-specific AI platforms using proprietary contextual data.” Additionally, by 2028, 65% of governments worldwide will add some technological sovereignty rules to improve their independence and protect them from outside regulators³.

Figure 1: Geopolitical turmoil ignites the race for tech sovereignty

Q: In light of the recent geopolitical turmoil—including tariffs, trade tensions, and sovereignty debates—how has your organization’s attitude changed towards technologies with sovereign capabilities?



Source: Accenture Sovereign AI survey, July-August 2025, N=1,928



The race to create sovereign solutions provides opportunities for both global cloud providers and local suppliers to offer cloud-based infrastructure, data, cybersecurity and AI models. For companies, it creates a trusted stack that incentivizes regional industry and cross-industry collaboration and data monetization. For nations, sovereign AI also presents an opportunity to empower people and safeguard their rights, thereby enabling systems that reflect local language, culture and values. It gives citizens recourse if algorithms misstep and allows local institutions to capture more of the value. The reality is that sovereign AI turns AI from something imposed on people into something built *for* them.

No wonder that most nations globally are embedding sovereignty into their AI strategies. From Switzerland's compliant cloud⁴ and the EU's AI Continent Action Plan, India's Sovereign AI plan⁵, to the recent Saudi Arabia's HUMAIN initiative⁶, the shift is unmistakable: Sovereign AI is now a defining pillar of global digital strategy. On the enterprise side, respondents overwhelmingly see governments as a key catalyst: 73% say governments, states or institutions like the EU have a key role to play in increasing digital and AI sovereignty—through regulation, subsidies or investments.

So, what now? Companies that intend to exploit the emerging opportunities created by sovereign AI are moving fast, thinking big and playing both offense and defense. Based on our research and work with leading organizations, four imperatives separate leaders from the rest.

These leaders:

1. Make sovereignty a CEO-led priority to align AI strategy with enterprise resilience, growth and geopolitical realities
2. Reframe sovereignty as a source of value creation, not just risk mitigation or compliance
3. Build hybrid ecosystems that combine local trust with global innovation and scale
4. Architect AI ensuring flexibility across infrastructure, data and models





Imperative

01

CEO Ownership: Make sovereign AI leadership's new power play

When NVIDIA's chief executive Jensen Huang stood beside Denmark's king in Copenhagen last October and switched on the country's first AI supercomputer, the message was unmistakable: The race for AI sovereignty has begun. And it's no longer just a matter for governments—it's a CEO and board-level concern.



Imperative 1 | CEO Ownership: Make sovereign AI leadership’s new power play

Why it matters:

Sovereign AI decides who has oversight over data, who shapes markets and who writes the rules of digital engagement. It influences trust, growth and geopolitics. That’s why the strategy must start at the top. The more regulated the industry, the higher the stakes. In financial services, sovereignty determines who controls transaction data, trading models and customer identities—core assets that define competitive advantage and trust. In healthcare and life sciences, it governs access to patient records, genomic data, and clinical models—areas bound by strict regulation and national oversight. In defense and critical infrastructure, it dictates whether AI systems can safely operate on sovereign compute, free from foreign dependencies or interference. By contrast, sectors such as retail, media and consumer services face fewer sovereignty constraints, though even there, customer profiling data and recommendation models raise growing concerns about control and compliance.

Take action:

Yet today, only 15% of organizations have made AI sovereignty a CEO or board-level concern (Figure 2). This is a critical blind spot. Without executive ownership, sovereignty risks becoming another compliance box to tick—rather than a lever of differentiation and value creation. Governments can lead by example—creating roles such as an AI Sovereignty Officer in the public sector to signal the importance of executive ownership and encourage businesses to follow suit. Our research shows that 20% of governments often have a board level/senior level head for sovereign AI.

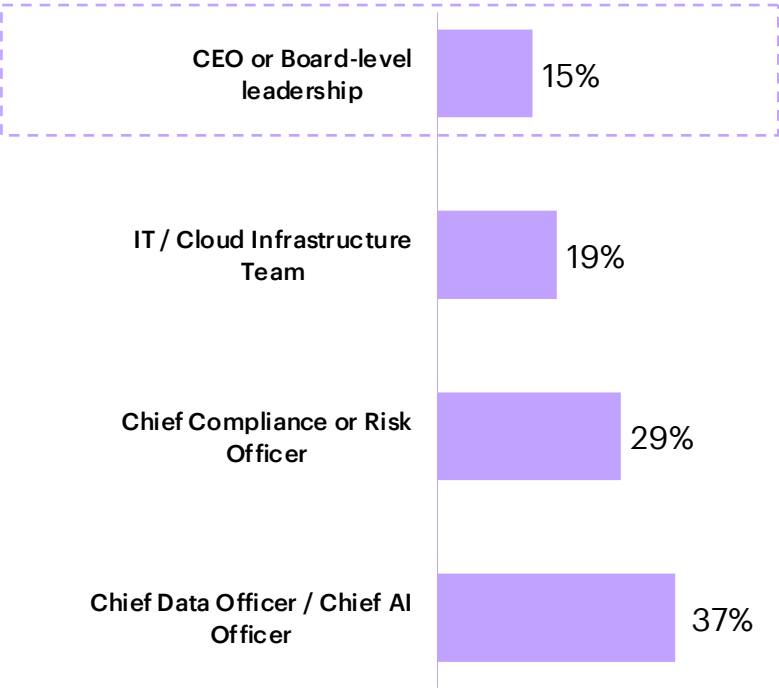
Top-level ownership is non-negotiable. Here are the three decisive actions.

- 1. Pick suppliers based on complex geopolitics and resilience:** The question is no longer whether to use global players contributing to the AI supply chain. It is where, when and how to best assemble these technologies to capture and retain the most value. These are not IT-level decisions. They involve weighing innovation speed against geopolitical risk, supply chain resilience and long-term costs. Only the CEO and boards have the authority and perspective to make those calls at the enterprise level.
- 2. Coordinate across all business units:** AI sovereignty cuts across legal, financial, technological and reputational boundaries. Without C-suite coordination and board-level oversight, organizations risk fragmented execution. CEOs must ensure governance frameworks align investment, partnerships and compliance with national priorities and corporate and national growth strategies.
- 3. Engage policy and industry leaders:** Sovereign AI is not just being built—it’s being negotiated. As government policies are being developed around the world, it is important for corporate and industry leaders' voices to be part of the process.

Leadership must move swiftly. The companies that treat sovereignty as strategy will shape the terms of the AI era. Those that don’t will inherit the rules written by others.

Figure 2: Sovereign AI responsibility lags at the CEO/Board level

Q: Who in your organization is primarily responsible for AI sovereignty decisions?



Source: Accenture Sovereign AI survey, July-August 2025, N=1,928

Imperative

02

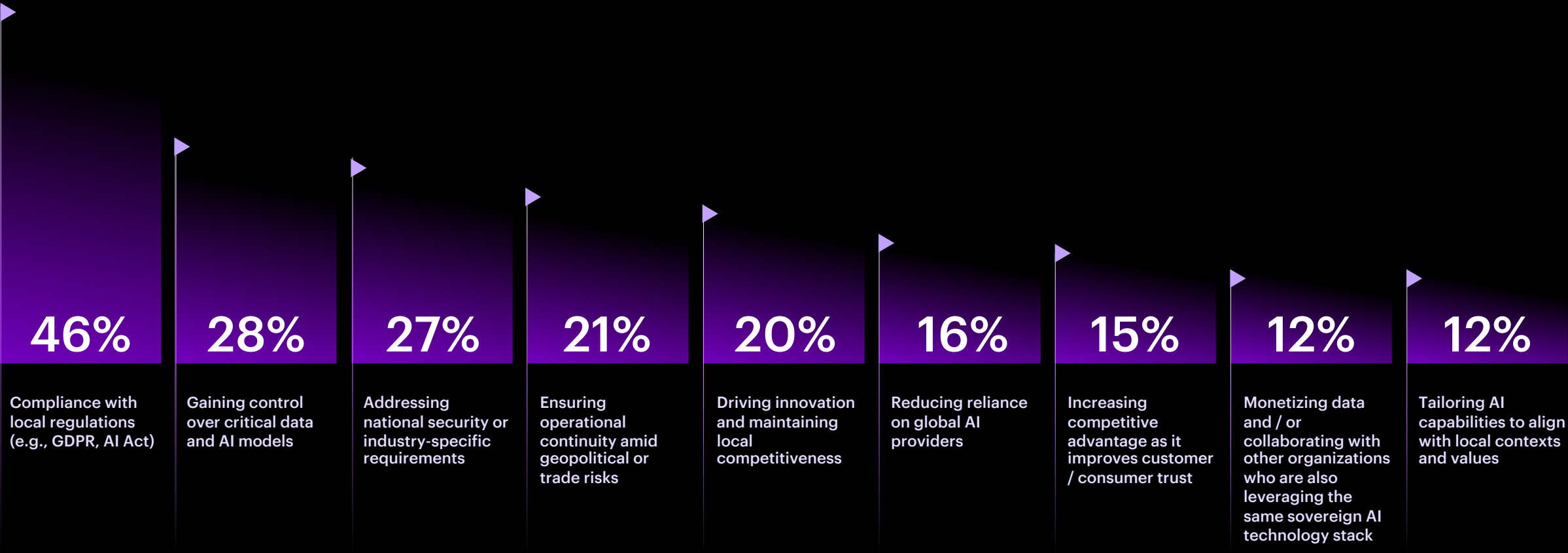
Reframe sovereignty: From risk management to value creation

Most organizations approach sovereign AI with a defensive posture—motivated by compliance requirements (46%), control over critical data (28%) and cybersecurity concerns (27%). Fewer than 13% cite monetization or cultural alignment as strategic motivators (Figure 3). The prevailing view: Sovereignty mitigates risk rather than generates value. Yet treating sovereignty purely as a safeguard leaves vast value untapped.



Figure 3: Sovereign AI drivers are still largely defensive

Q: What were / would be the key motivations for your organization to consider sovereign AI?



Source: Accenture Sovereign AI survey, July-August 2025, N=1,928

Companies should flip the script. Sovereign AI can unlock new value by turning local trust and cultural alignment into competitive advantage.

Why it matters:

When companies build AI that speaks their market's language—literally and figuratively—they capture customer confidence and regulatory approval simultaneously. This trust unlocks collaboration that would otherwise be impossible. Take the OpenBind Consortium⁷—supported by £8 million from the Sovereign AI Unit of the UK Government—which is building a UK-based dataset for AI-driven drug discovery, 20x larger than anything before. This kind of data sharing can only happen with trust at a local level, illustrating how sovereign AI can directly empower national industries and citizens.

Sovereign AI platforms enable participants within the same ecosystem—across a nation, a region, an industry or a supply chain—to share and act on data securely. In regulated environments, this means organizations can collaborate on AI models, data and insights without risking compliance breaches or exposing sensitive assets. It's a level of cross-enterprise cooperation that only becomes viable within a trusted sovereign framework.

Leading firms are already proving that sovereignty can extend beyond protection to participation. Some are investing in ecosystem readiness by becoming providers—helping suppliers, customers and governments adopt sovereign solutions. Two-thirds of leaders say their ecosystems need this support. Done right, sovereignty can spark data marketplaces, attract talent, create local models tuned to cultural nuance and nurture local innovation ecosystems—turning compliance into nation building. This is now happening across sectors.

Telecom operators such as Indosat Ooredoo Hutchison in Indonesia are building the country's first sovereign AI cloud with Accenture and NVIDIA⁸—supporting local startups and government clients while ensuring national data stays onshore. In software and platforms, Oracle's EU Sovereign Cloud⁹ and Microsoft's Bleu and Delos partnerships¹⁰ are enabling European organizations to run sensitive workloads fully under EU law. And in healthcare, projects such as the Sovereign AI Factory Frankfurt¹¹ offer compliant environments for hospitals and research institutes to train and deploy models under GDPR and the AI Act.





Take action:

Governments, for their part, play a pivotal role in turning sovereign ambition into economic impact. They can reinforce this momentum by funding local infrastructure, subsidizing trusted providers and opening public datasets in critical sectors to spark innovation by small and medium-sized enterprises (SMEs), startups and research organizations. Partnering with academia is equally vital—building a pipeline of next-generation AI talent, developing new models locally and anchoring innovation at home.

Providers, in turn, should act as ecosystem anchors, enabling smaller players to participate and thrive—covered in greater detail in Imperative 3 below. A clear example is STACKIT, the cloud provider of Schwarz Digits, the IT and digital division of Shwartz Group.

STACKIT began as an internal sovereign cloud to serve the group's own businesses such as Lidl and Kaufland, and has since evolved into a full-fledged provider for external organizations. Today, STACKIT extends its infrastructure and data-sovereign cloud services to both commercial ecosystems and public institutions¹².

To sustain momentum, organizations must participate in sovereignty for long-term relevance and survival, not just security and compliance. What new value will you capture? What new customers or markets will you target because you have sovereign relevance and maturity?

Embedding sovereignty as part of business strategy changes how companies compete. Today, the race for competitiveness is

inseparable from speeding up sovereignty, as organizations seek greater assurance, autonomy and trust in the technologies that underpin their growth. Sovereignty now shapes access to markets, customer trust and revenue performance.

Governments can normalize this shift by embedding sovereignty in national, digital and industrial strategies, setting the tone through policy that requires suppliers to meet sovereignty standards. They can show—through tangible examples—how, if enterprises capture AI's value, it can translate into national advantage.

Similarly, if energy companies apply locally governed AI to grids, it strengthens resilience and lowers national costs. Such proof points can make clear that enterprise value creation and nation-building move in lockstep.



Imperative

03

Expand your ecosystem: Navigate the sovereignty continuum

Sovereignty is not binary—it's a continuum. Companies must determine where sovereignty truly matters, and how to dial it up or down depending on risk and value. The good news is that participating in sovereign markets and benefiting from national sovereign agendas doesn't require changing everything or making every workload sovereign.



Our research shows that companies can meaningfully participate and capture sovereign opportunities by applying sovereignty measures to just one-third of their AI initiatives. Even within that third, the required degree of strict localization needed varies.

Why it matters:

Not everything demands transformational change or heavy investment. Some use cases need only local data residency and oversight of global infrastructure, while others call for full-stack sovereignty—local data and infrastructure, multi-cloud and multi-model access, confidential computing, advanced encryption or even air-gapped systems when necessary.

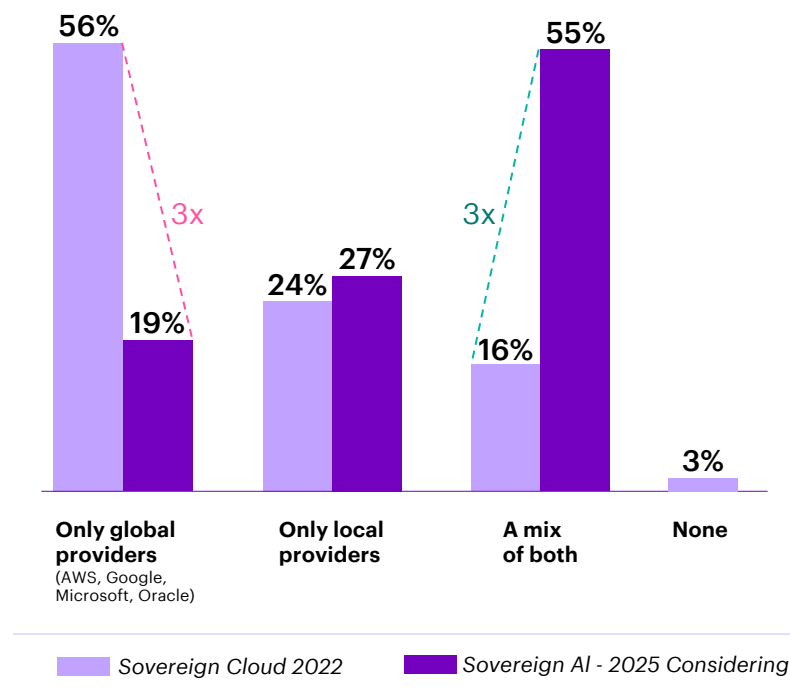
Similarly, the future of AI infrastructure will be a continuum of choices that will allow organizations to fluidly combine global scale with local oversight to create fit-for-purpose solutions.

Consider the rapid growth of small language and industry-aligned models. While many of the larger language models will come from global providers, small language models or industry models may increasingly originate from local vendors developing domain-specific and culturally tuned capabilities. Enterprises need the ability to adapt quickly, selecting and fine-tuning the models that deliver the highest relevance, performance and cost efficiency for their context.

Similarly, while cloud compute infrastructure at a global level will still be best served by a global cloud provider, regional providers can augment them seamlessly for workloads that need high-intensity AI training without moving data, or edge processing and low-latency inferencing.

Figure 4: The move toward a greater provider mix fuels flexibility

Q: Which of the following sovereign solution providers are you considering?



Sources: Accenture Sovereign Cloud Survey in Europe, October 2022; N=300 | Accenture Sovereign AI survey, July-August 2025, N=1,928

This evolution points to an ecosystem that is far more adaptive and distributed than before. The competitive advantage lies not in uniformity, but in the ability to orchestrate the right combination of providers, architectures and models/services—continuously evolving as technology, regulation and market needs change.

Local providers are essential to sustaining choice across this continuum. Yet in many regions, they remain limited or absent, creating structural dependencies on global players. Without viable local options, sovereignty becomes constrained by external capacity and priorities. Governments are actively helping local providers become more resilient, competitive and trustworthy.

For example, European countries appear keen to create an AI Gigafactory by pooling resources, with strong interest from 16 Member States across 60 different sites submitted in response to the Call for Expression of Interest in AI Gigafactories in June 2025. Such models will expand as governments intervene to strengthen domestic supply.

Take action:

Organizations have many choices today when it comes to AI solution providers. They include:

Global cloud providers offer unmatched scale, service breadth and pace of innovation. They also provide strong legal, operational and technical sovereign capabilities: e.g., AWS's European Sovereign Cloud, Microsoft's EU Data Boundary and Google's sovereign offerings with EU partners.

Frontliners are country-endorsed national champions (often local incumbents such as telcos or high-tech companies) with local brand recognition that can meet public sector trust requirements and run government-endorsed industry or cross-industry solutions (data and application spaces for AI).

Neoclouds are AI-native providers built for the new era of compute. They deliver high-performance infrastructure tailored to AI workloads, combining local capacity built on a modern stack created for AI workloads. Players such as Nebius, Nscale, CoreWeave and Lambda exemplify this model—offering rapid deployment, modern architectures and trusted operations that let enterprises scale AI securely and at speed.

Federated consortia are alliances of governments, industries and technology providers that co-develop shared sovereign infrastructure solutions and governance frameworks. Earlier initiatives such as Catena-X demonstrated the value of trusted data collaboration across organizations. The next wave—exemplified by AI Gigafactory-style consortia emerging across Europe, and national programs such as Saudi Arabia's HUMAIN initiative and Indonesia's Sovereign AI TechCo—moves from federated governance to federated capability. They operate above the infrastructure layer as well—turning trust, interoperability and compliance into shared capability and new market opportunities.

Each brings distinct, complementary strengths—cloud providers with global scale and innovation cadence, frontliners with policy-grade assurance and sector convening power, neoclouds with nimble, locally governed AI buildouts, and consortiums with the power of pooled resources and collaboration. The most resilient strategies combine all four as needed, orchestrated by data residency and multi-cloud design.

Sovereignty in action	<p>Nebius is an AI cloud platform engineered to support the full lifecycle of artificial intelligence workloads, from model training to inferencing to agent deployment. Nebius integrates custom hardware, proprietary software and energy-efficient data centers located across the US, Europe and Middle East, giving organizations the flexibility to meet local data residency requirements and build sovereign AI factories in different regions. Through its partnership with Accenture, Nebius combines its robust AI infrastructure with Accenture’s transformation expertise and industry capabilities, helping enterprises and public-sector organizations accelerate local AI adoption. Together, we’re providing industry-tailored, secure solutions that operationalize and scale AI while ensuring both compliance and business impact.</p>	<p>Cassava Technologies (Africa)</p> <p>Partnering with Accenture to launch a full stack of secure GPU offerings and industry solutions in local data centers to drive access, adoption and new value across the continent.</p>
		<p>Telus (Canada)</p> <p>Opened the country’s first fully sovereign AI factory, enabling Canadian organizations to harness global AI innovation while keeping data within national borders. Accenture is developing and deploying industry-specific solutions on this sovereign platform to accelerate AI adoption across Canada.</p>
		<p>Telia Cygate (Sweden)</p> <p>Collaborating with Accenture to create the sovereign AI infrastructure for Sweden based on their fixed and mobile networks and security-classified data centers.</p>
		<p>Indosat Ooredoo Hutchison (Indonesia)</p> <p>Through its subsidiary Lintasarta, partnering with Accenture to accelerate its sovereign AI cloud platform, aimed at propelling AI-driven digital transformation in Indonesia.</p>

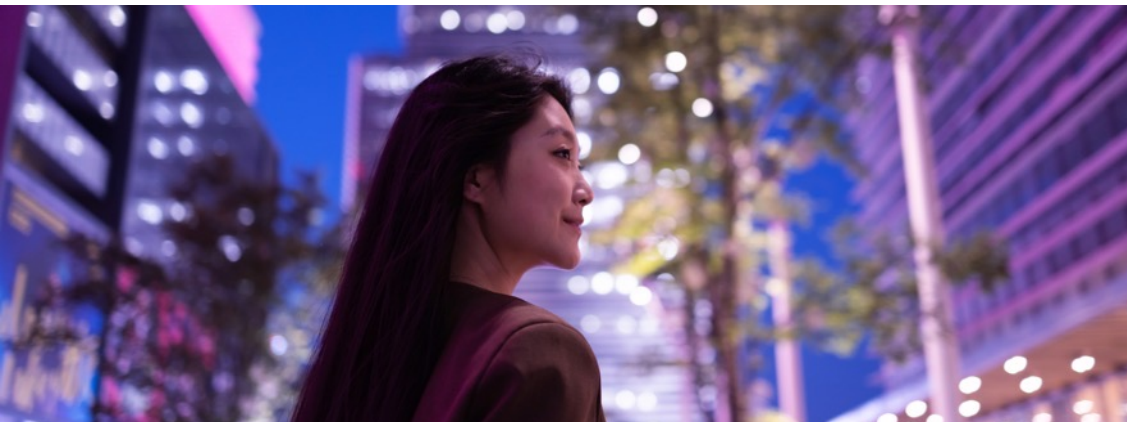
Imperative

04

Redefine architecture: Sovereignty for intelligence, not just infrastructure

With business commitments and operating models in place, organizations should next assess their digital foundations against sovereignty requirements. This means aggressively evaluating hardware, data, cloud readiness, compute needs, cybersecurity and AI model selection for each critical use case.





Why it matters:

Recent developments in generative and agentic AI have made it possible—and necessary—to rethink traditional architectural methods more broadly. Sovereignty now means more than just choosing where data is stored or managed and where the infrastructure is. It also includes the intelligence itself—how models, agents and platforms talk, learn and make choices within set limits.

This evolution demands a new class of architectures built for multi-cloud, multi-model and now multi-agent collaboration, where technologies share memory, exchange context and coordinate to solve complex workflows. What makes sovereignty particularly challenging for these scenarios is that a single workload might be drawing from multiple services and models from different providers with varying levels of sovereignty.

These distributed, agentic systems also introduce new design imperatives and risks. They require error handling for probabilistic outcomes, compliance and guardrails embedded within every model and agent and governance that allows autonomy while preserving accountability, trust and resilience.

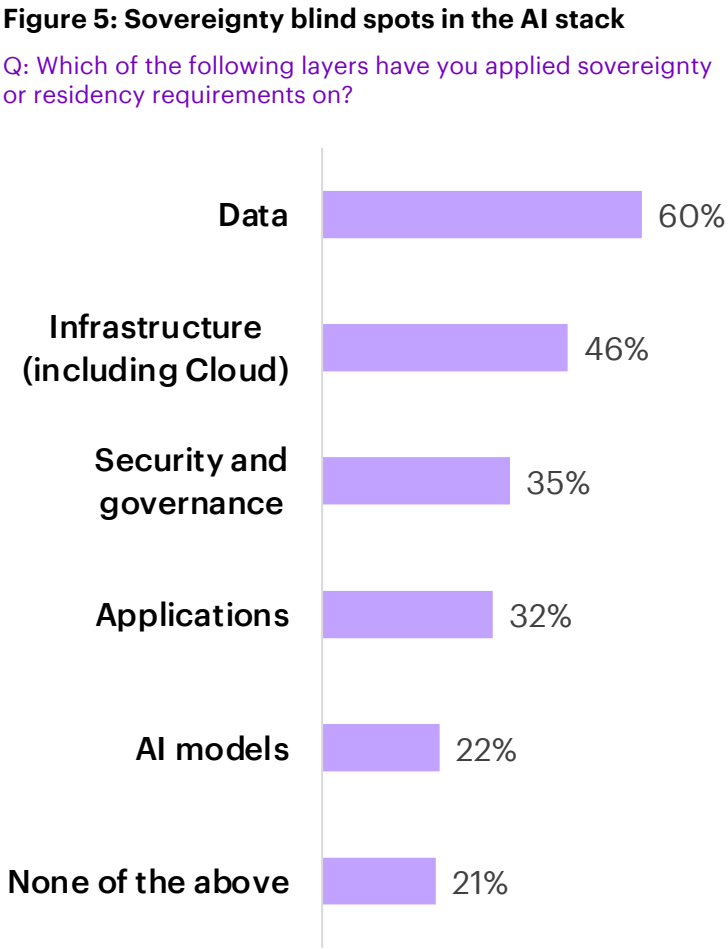
Take action:

The first step is to conduct a sovereignty audit for each use case, considering factors such as country risk, industry regulation and business or use-case criticality. Based on this assessment, companies can determine the appropriate level of sovereignty required and apply technology accordingly.

Then, they should benchmark their current infrastructure, data residency and provider dependencies to establish a clear baseline. This benchmarking helps identify gaps and prioritize remediation efforts across the organization. As part of this process, firms must also detect systemic, interconnected threats woven into their digital core—issues that often span across applications, platforms and providers.

Finally, organizations should establish dynamic controls and governance across the entire AI stack, enabling them to anticipate emerging risks and maintain systems that are resilient, trusted and defensible. This approach shifts sovereignty from a static compliance exercise to a living capability that evolves with regulation, technology and business needs.

Our research shows that 60% of organizations apply sovereignty oversight to data and 46% to infrastructure. Yet only 22% extend sovereignty oversight to AI models and just 32% apply them to applications. The blind spot is enormous and leaves AI’s most strategic layers exposed (Figure 5).



Source: Accenture Sovereign AI survey, July-August 2025, N=1,928

Auditing and measuring in real-time across layers—hardware, data, cloud, compute and AI models—helps firms detect dependencies before they become liabilities. It also clarifies where dynamic control is required. Static compliance no longer suffices. AI systems must anticipate and adapt to emerging regulations and threats. Sovereignty must become predictive, not reactive.

The point is to deliver the most innovation at the lowest risk profile. That means enabling access to millions of open-source models, while putting in place mechanisms to ensure safety—checking for prompt injection, tracing nefarious behavior and guarding against hidden backdoors. These safeguards must operate across layers: at the data level, the model level and even at the chip/runtime level. With such oversight embedded, enterprises and governments can unlock innovation at scale while ensuring sovereignty and security are never compromised.

Globalization, rewired for sovereignty

Sovereign AI marks the next phase of globalization—a world where nations and firms share technology but retain agency. As sovereign ecosystems mature, new markets emerge. Local AI developers build models attuned to domestic culture and regulation, while industries monetize intelligence tailored to national contexts. Sovereignty ceases to be a constraint; it becomes the driver of digital competitiveness.

The organizations that act now—making sovereign AI a CEO priority, reframing sovereignty from risk management to value creation, expanding their ecosystems across the sovereignty continuum and redefining their architecture for the future—will shape the contours of the next technological era.

Standing still is the only real risk. Geopolitical uncertainty will persist, regulations will tighten and AI's strategic value will soar.

The future belongs to those who build it—and in the age of artificial intelligence, that means those who build it sovereign.

Who's leading the charge?
Global and industry
front-runners in AI sovereignty

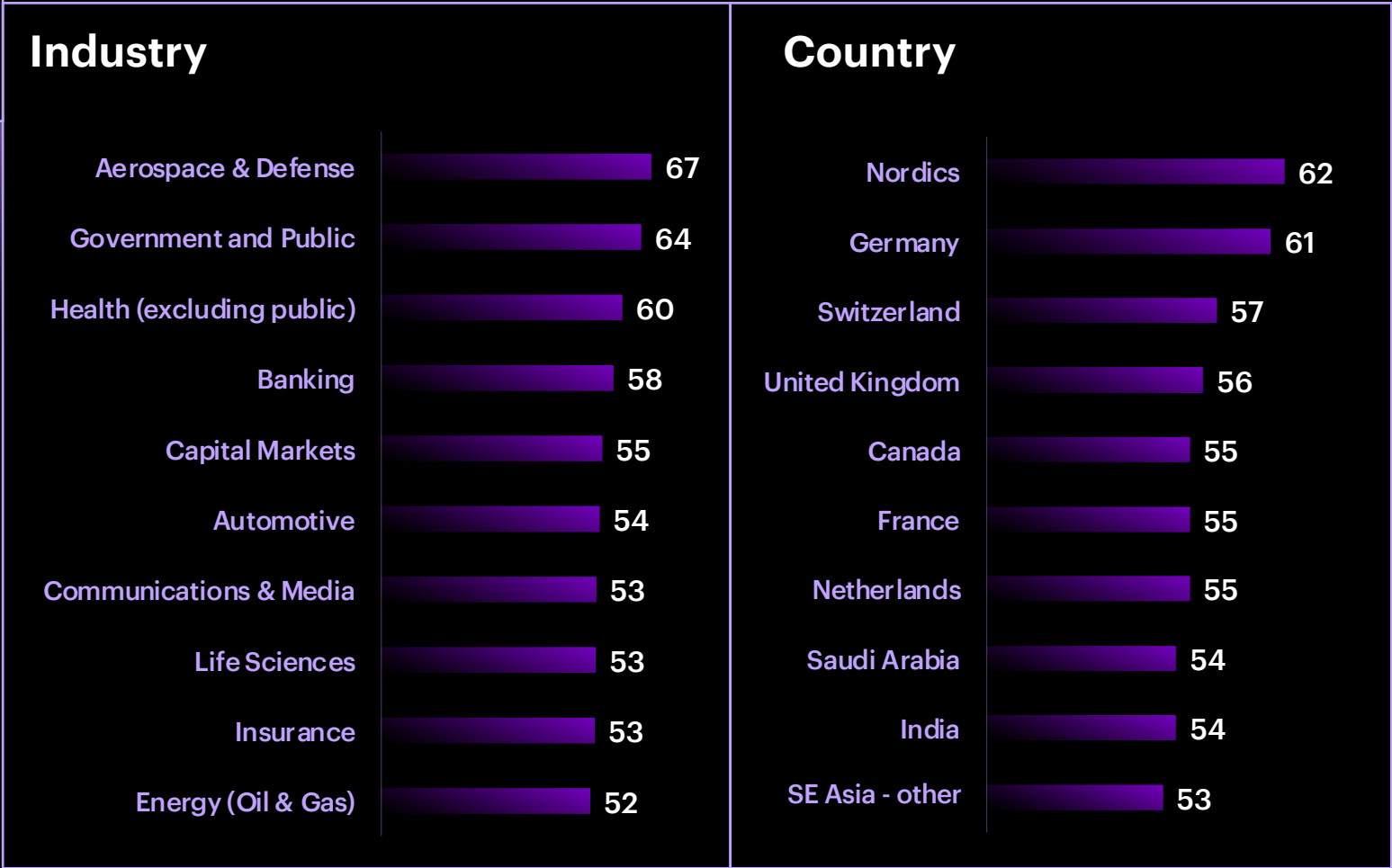
To explore which industries and countries have the highest digital and AI sovereignty, we created a Sovereignty Maturity Index that measures the sovereignty of respondents on a 0–100 scale (Figure 6). The index weighs an organization's current and target maturity, technology stack-level sovereignty, investments and data oversight. The numbers represent average scores for respondents across companies and national governments.

As our chart shows, regulated sectors lead in sovereign maturity—the ability to apply sovereign controls across hardware, data, compute, cloud, cybersecurity and AI models. Not surprising, Aerospace and Defense tops the list, followed closely by the Government and Public Sector, then Health.

Europe is the epicenter of sovereign action. The Nordics, Germany, Switzerland, the UK and France all score above average in our Sovereignty Maturity Index. Canada is the only non-European country to match that performance. Saudi Arabia leads in the Middle East.

Figure 6: Sovereignty Maturity Index

Q: Which of the following layers have you applied sovereignty or residency requirements on?



Source: Accenture Research analysis of 1,928 respondents; Full list of included countries and industries in About the Research section. “- other” indicates groupings of countries that did not have large enough sample sizes in our survey to be statistically significant alone. SE Asia - other includes Vietnam, Thailand, Malaysia, Philippines.

About the Research

This study combines quantitative, qualitative and policy research to examine how governments and enterprises are advancing Sovereign AI and Sovereign Cloud.

A global survey of **1,928 organizations** across **28 countries** and **18 industries** conducted during Jul–Aug 2025 provides the quantitative foundation. Respondents were senior technology and policy leaders—CIOs, CTOs, Chief Data, AI and Risk Officers—from both public and private sectors. All represented organizations that consider sovereignty highly or critically important to their technology stack.

Countries included: Australia, Canada, China, France, Germany, India, Indonesia, Italy, Japan, Singapore, South Africa, Spain, United Kingdom, Saudi Arabia, United Arab Emirates, Ireland, Netherlands, Switzerland, United States, Philippines, Denmark, Malaysia, Sweden, Thailand, Vietnam, Qatar, Kuwait, and Oman.

Industries included: Automotive, Energy (Oil & Gas), Software & Platforms, Government and Public Sector, High Tech, Consumer Goods & Services and Retail, Communications & Media, Insurance, Banking, Metals & Mining, Aerospace & Defense, Life Sciences, Industrial Equipment, Utilities, Capital Markets, Chemicals, Travel, and Health (excluding public healthcare).

The survey included **29 core questions** on awareness, adoption, motivations, challenges and maturity across the digital core—data, cloud, AI, integration and governance. Results were analyzed by region, sector and industry to identify patterns in awareness, ambition and achieved sovereignty. We also compare results with Accenture’s Europe-based Sovereign Cloud Survey from October 2022 with N=300.

The **Sovereignty Index** measures the degree of digital and AI sovereignty within organizations by consolidating four components:

1. **Current and target sovereignty levels**, reflecting both the organization’s present state and ambition (weight = 0.5).
2. **Sovereignty achieved across five layers** of the digital and AI stack—Applications, Data, AI Models, Infrastructure, and Security & Governance (weight = 0.3).
3. **Investment in sovereignty initiatives** (weight = 0.1).
4. **Control over data** (weight = 0.1).

Each component was normalized and combined to produce a composite score on a **0–100 scale**, where 0 indicates no sovereignty and 100 represents full sovereignty across all dimensions.

Quantitative findings were complemented by a **desk study of national AI policy documents and strategy papers** across major economies, mapping how sovereignty principles—data control, model autonomy, ethical governance and infrastructure localization—are being embedded into national AI strategies.

Together, these approaches provide a layered view of how nations and industries are building Sovereign AI capabilities to drive public value, resilience and competitiveness.

References

1. [The AI Index 2025 Annual Report](#), AI Index Steering Committee, Institute for Human-Centered AI, Stanford University, April, 2025.

2. [Why Oppenheimer Is Excited About Nvidia's Potential Gains from Sovereign AI Demand](#), Investopedia, June 16, 2025.

3. [How Sovereign AI Impacts Enterprise Opportunity and Creates Nonobvious Threat](#), Gartner, September 2025.

4. [About Us](#), Swisscom Trust Services.

5. [Cabinet Approves Ambitious IndiaAI Mission to Strengthen the AI Innovation Ecosystem](#), PMIndia, March 7, 2024.

6. [HRH Crown Prince launches HUMAIN as global AI powerhouse](#), Public Investment Fund (PIF), May 12, 2025.

7. [UK to become world leader in drug discovery as Technology Secretary heads for London Tech Week](#), gov.uk, June 9, 2025.

8. [Indosat Ooredoo Hutchison Group and Accenture accelerate sovereign AI cloud to power Indonesia's digital future](#), Accenture News Release, September 17, 2024.

9. [Oracle EU Sovereign Cloud helps organizations across Germany securely manage critical business data](#), Oracle, May 14, 2025.

10. [Announcing comprehensive sovereign solutions empowering European organizations](#), Microsoft, June 16, 2025.

11. [Sovereign AI Factory Frankfurt](#), Polarise.

12. [Our goal: Satisfied STACKIT customers](#), STACKIT.

Acknowledgements

The authors would like to thank the following people for their contributions to the report:

Research Team: Garg D. Ajay, Krishna Kanth Sutraye, Amal Sebastian, Jakub Wiatrak, Ana Ruiz Hernanz, Addis Chiara, Emily Thornton, Gargi Chakrabarty
M+C Team: Salena Gallo, Kristin Barger, Janine Stankus, Micaela Soto Acebal, Luis Diego Rojas, Sanjay Ramanujam, Mark Kiernan, Karen Wolf, Bradley Nixon, Rachel Crowley, Joanna Duff

Special thanks to Laurence Morvan, Valerio Romano, Andrew Levy and Junius Lie for your insights and recommendations.

About Accenture

Accenture is a leading solutions and global professional services company that helps the world's leading enterprises reinvent by building their digital core and unleashing the power of AI to create value at speed across the enterprise, bringing together the talent of our approximately 779,000 people, our proprietary assets and platforms, and deep ecosystem relationships. Our strategy is to be the reinvention partner of choice for our clients and to be the most AI-enabled, client-focused, great place to work in the world. Through our Reinvention Services we bring together our capabilities across strategy, consulting, technology, operations, Song and Industry X with our deep industry expertise to create and deliver solutions and services for our clients. Our purpose is to deliver on the promise of technology and human ingenuity, and we measure our success by the 360° value we create for all our stakeholders. Visit us at [accenture.com](https://www.accenture.com).

About Accenture Research

Accenture Research creates thought leadership about the most pressing business issues organizations face. Combining innovative research techniques, such as data-science-led analysis, with a deep understanding of industry and technology, our team of 300 researchers in 20 countries publish hundreds of reports, articles and points of view every year. Our thought-provoking research developed with world leading organizations helps our clients embrace change, create value and deliver on the power of technology and human ingenuity. For more information, visit Accenture Research on www.accenture.com/research.

Disclaimer: The material in this document reflects information available at the point in time at which this document was prepared as indicated by the date provided on the front page, however the global situation is rapidly evolving and the position may change. This content is provided for general information purposes only, does not take into account the reader's specific circumstances, and is not intended to be used in place of consultation with our professional advisors. Accenture disclaims, to the fullest extent permitted by applicable law, any and all liability for the accuracy and completeness of the information in this document and for any acts or omissions made based on such information. Accenture does not provide legal, regulatory, audit, or tax advice. Readers are responsible for obtaining such advice from their own legal counsel or other licensed professionals. This document refers to marks owned by third parties. All such third-party marks are the property of their respective owners. No sponsorship, endorsement or approval of this content by the owners of such marks is intended, expressed or implied.