Insight ON: Digital Sovereignty Trilemma

The Digital Sovereignty Trilemma: Reclaiming Strategic Autonomy in an Era of Geopolitical Turbulence

Digital Sovereignty Trilemma survey report by Insight.

Insight ON: Digital Sovereignty Trilemma

Contents Page

Adrian Gregory
President of Insight EMEA

1. Foreword

As organisations reassess where and how digital value should be created, many are navigating a dual reality: accelerating AI adoption on one hand, while reasserting control over cost, data, and sovereignty on the other—sometimes by rethinking cloud only approaches.

Within this broader recalibration, AI remains a powerful catalyst for change. As we navigate this AI driven paradigm shift, the mandate for leadership has moved beyond mere experimentation toward a fundamental reimagining of the enterprise. To compete in this new era, organisations must anchor their strategy in a simple, relentless question: How do we better serve the client? From streamlining the user journey to delivering net-new value, AI offers a transformative toolkit—but only for those who move beyond "point technology" and "standalone prototypes."

True value realisation requires a comprehensive architectural rewiring. The complexity of the modern AI stack—encompassing everything from model gateways and agent orchestration to authentication and LLM provider interfaces, demands a unified business change programme. Without rigorous attention to cross-cutting fundamentals like MLOps, observability, and compliance, AI initiatives risk becoming poorly crafted extensions rather than core business drivers. At worst, an incorrectly architected solution creates significant security vulnerabilities and spiralling costs; at best, it simply fails to deliver.

At the heart of this transformation lies data—the lifeblood of the modern enterprise. As data becomes more central to value creation, the infrastructure that hosts, processes, and protects it becomes a primary lever for competitive advantage. This brings us to a critical inflection point: the "Digital Sovereignty Trilemma." Our latest research indicates that 67% of organisations already view digital sovereignty as a strategic priority—a figure expected to climb to 82% within three years. Yet, many remain shackled by modernisation debt and a widening skills gap that prevents them from balancing operational resilience with economic efficiency.

At Insight, we believe that organisations that treat digital infrastructure as a strategic asset—rather than a legacy cost—will be the ones best positioned to lead in the decade ahead. True resilience comes from a unified framework that designs for sovereignty from the outset while maintaining the flexibility to adapt as the global landscape shifts.

This report is designed to help you navigate these complexities. By investing strategically in people, partners, and platforms, you can build the confidence needed to reclaim your strategic autonomy and accelerate your digital journey.

2. Executive summary

Organisations today face a defining strategic challenge: how to harness the full potential of digital infrastructure while maintaining control over it. As the geopolitical environment grows more volatile, the regulatory landscape more complex, and AI more central to competitive advantage, the decisions leaders make about their digital architecture have become critical to survival.

At the heart of this challenge lies the Digital Trilemma: the need to balance three interdependent pillars – operational resilience, agility, and economic efficiency. Each is critical in its own right. But the organisations best positioned for the decade ahead will be those that treat all three not as competing priorities, but as a unified strategic framework.

1. Operational resilience

now rests on digital sovereignty. As cyber threats escalate and geopolitical risk grows harder to predict, control over digital assets will become the difference between organisations that can absorb disruption and those that cannot.

- **67%** of organisations already cite digital sovereignty as a critical strategic consideration – rising to **82%** within three years
- **55%** say navigating regulatory complexity is one of their greatest strategic challenges
- **43%** have used strong sovereignty credentials to win or retain business

2. Agility

is being redefined by AI. As organisations move from experimental pilots to production-grade deployments, infrastructure decisions are becoming critical determinants of innovation speed. The hybrid model is fast becoming the new standard – but modernisation debt and skills gaps mean that for many, ambition is running ahead of capability.

- **85%** of European organisations are evaluating or deploying dedicated on-premises infrastructure for AI
- **42%** say their greatest competitive advantage in the next 3–5 years will come from orchestrating a diverse hybrid ecosystem
- **41%** of IT leaders are held back by an inability to move legacy business applications

3. Economic efficiency

is under mounting pressure. The cloud-first era prioritised speed to market to drive digital adoption – a rational strategy that is now being tested by the scale and cost of AI. Building on those foundations for long-term efficiency requires greater architectural discipline and rigorous thinking about total cost of ownership. And this is no longer optional; it is a commercial imperative.

- AI has driven a **12%** increase in hosting costs in a single year
- European organisations waste an average of **24%** of their annual cloud capacity
- **56%** are not conducting Total Cost of Ownership assessments before significant workload placement decisions as a matter of course

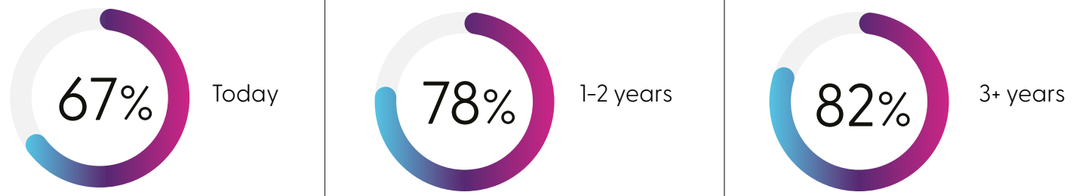
The digital trilemma cannot be solved by addressing each pillar in isolation. It demands an integrated approach – one that treats infrastructure as a strategic asset, designs for sovereignty from the outset, and builds the flexibility to adapt as the landscape continues to shift.

3. Operational Resilience: The Pivot from Privacy to Survival

In today's organisations, operational resilience has become inseparable from digital strategy and data security. As digital infrastructure grows from a back-office storage function to a driver that unlocks value and safeguards business resilience, maintaining digital sovereignty has risen sharply up the executive agenda – while the challenge of doing so has grown increasingly complex.

Today, 67% say maintaining digital sovereignty is a critical consideration when making strategic business decisions, rising to 78% in one to two years and 82% in three or more years. The public sector leads the shift, with 73% viewing digital sovereignty as critical to their strategic decisions, reflecting a heightened focus on national security and jurisdictional safety.

Digital sovereignty is a critical strategic consideration



Until recently, digital sovereignty was often narrowly defined as data residency: the geographic location of "bits and bytes." But in today's geopolitical and commercial environment, the physical location of data is no longer a sufficient safeguard. The business landscape has fundamentally changed.

With organisational resilience now contingent on continuous, secure access to data, any scenario in which an outside entity can effectively pull a "kill switch" to disable enterprise systems represents an existential threat – whether it is through a cyber-attack or the intervention of a foreign jurisdiction with authority over the cloud provider storing or processing the data. Failures of this kind are not merely operational disruptions; they have the potential to be catastrophic to business continuity and survival.

Three quarters of public sector leaders say digital sovereignty is a critical consideration when making strategic decisions.

The solutions are neither simple nor uniform. 39% of respondents cite operational autonomy – the ability to maintain full technical control over operations and encryption keys, and to prevent foreign access – as a top strategic challenge. This is why organisations are increasingly thinking beyond data residency to "serviceability": their capacity to maintain operations even if disconnected from global hyperscale platforms or subjected to foreign jurisdictional interference.

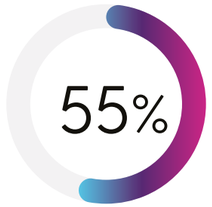
When evaluating their data centre and cloud strategy, 32% of organisations say supply chain resilience and continuity is a top priority – rising to 37% for logistics firms and 36% for pharmaceuticals, where the time-sensitive movement of goods makes serviceability business-critical. A further 3 in 10 cite disaster recovery as a key concern, and the same proportion are focused on the legal jurisdiction of their service provider's parent company. That these issues rank significantly higher than cost control (20%) or speed to market (16%) signals how far operational resilience has moved up the executive agenda.

When evaluating your data centre and cloud strategy, which of the following are your top five priorities?

Regulation Proliferation

Navigating the intersection of technology and geopolitics has become a strategic imperative in its own right. Leaders are moving well beyond GDPR compliance checklists, engaging deeply with current legislation while trying to anticipate new regulatory developments across every jurisdiction in their digital supply chain.

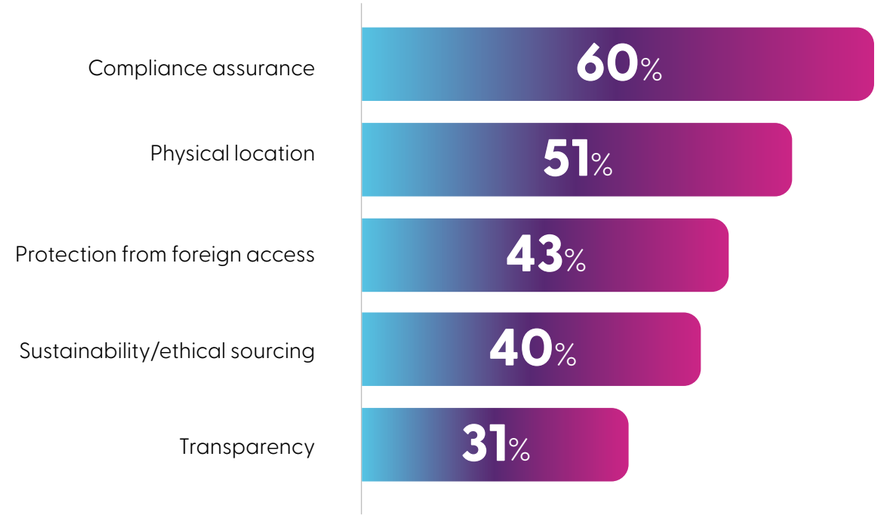
But this is not easy. Regulatory complexity is already the primary hurdle for 55% of organisations, as they navigate overlapping mandates like DORA, NIS2, and the EU AI Act. Designing architecture with the flexibility and control needed to reduce regulatory exposure, protect revenue streams from geopolitical disruption, and shorten recovery times in the event of supply chain or cloud provider instability is becoming a baseline requirement.



of leaders say navigating regulatory complexity is one of their organisation's greatest strategic challenges.

Operational resilience gives organisations the power to survive by protecting internal functionality against shocks, while also mitigating external risks. Designing for safety can come with significant outlay, but it's not only a defensive measure. Data sovereignty credentials are increasingly critical in sales as client interest grows: 60% of organisations say clients demand proof of compliance with legislation such as GDPR and DORA and 43% want assurances of protection from access by foreign governments.

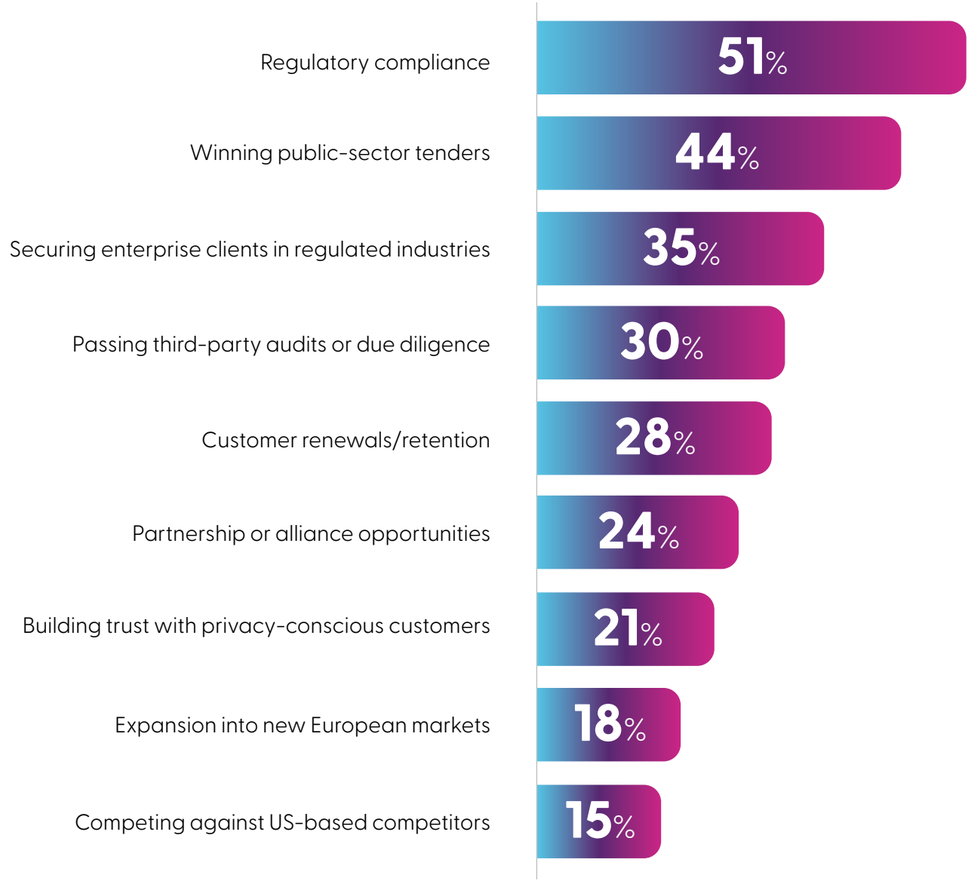
Which aspects of digital sovereignty are most frequently raised by your clients or customers as a prerequisite for doing business with you?



This means a robust approach is not just an additional cost which protects the organisation's serviceability, it's also a commercial advantage. 43% of firms have used this strength to win or retain business and another 33% are developing it as a brand strength.

Digital sovereignty credentials are particularly valuable in high-stakes procurement contexts. Organisations that leverage digital sovereignty as a competitive strength say it is particularly beneficial when responding to RFPs with strict compliance requirements (51%), winning public sector tenders (44%), and securing clients in regulated industries (35%).

You mentioned that your data protection or sovereignty approach has helped you win or retain business. Where has it been most valuable?



When data sovereignty sits at the heart of architecture decisions, operational resilience becomes embedded rather than reactive. In a world of escalating cyber threats, geopolitical instability, and foreign jurisdictional risk that can shift without warning, control over digital assets is increasingly the difference between organisations that can absorb disruption and those that cannot. The organisations that recognise this shift earliest, and design their architecture accordingly, will be best placed to turn an increasingly complex operating environment into a source of lasting advantage.

Autonomous AI

could help many organisations cut through digital regulatory complexity and keep pace with cycles of innovation. But **trust in the technology is holding leaders back**.

To learn more, read our report

'Navigating the Autonomous AI Trust Barrier'

4. Agility: AI as the Catalyst for the “Hybrid Normal”

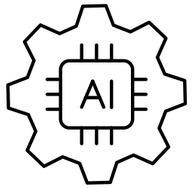
Artificial Intelligence is acting as the ultimate catalyst for an infrastructure rethink. Innovation is no longer synonymous with public cloud alone; instead, organisational agility is increasingly defined by a sovereignty-aware architecture that places workloads based on performance, IP protection, and compliance.

As organisations move rapidly from experimental AI pilots to production-grade deployments, a new infrastructure logic is taking hold: rather than moving massive datasets to the cloud, it is often more efficient, secure, and cost-effective to bring compute power to the data. This shift is giving rise to a “Hybrid Renaissance”: a more deliberate model of innovation in which workloads are placed where they perform best, sensitive data and proprietary models are kept under closer control, and infrastructure decisions are driven by strategy rather than convention.

The scale of this shift is already visible. 84% of European organisations are already evaluating or deploying dedicated on-premises infrastructure specifically for AI and machine learning.

As AI moves to the centre of enterprise strategy, infrastructure decisions are becoming critical determinants of competitive advantage – not just operational efficiency. They define how quickly new ideas can become operational capabilities, and how effectively organisations can translate AI ambition into sustained innovation.

Leaders are acutely aware of this. 42% say their greatest competitive advantage in the next 3–5 years will come from orchestrating a diverse ecosystem of hyperscalers, regional sovereign providers, and on-premises infrastructure – reflecting a recognition that no single model will be sufficient.



AI is driving a “Hybrid Renaissance”

with **85%** of organisations now considering or investing in dedicated on-premises infrastructure for AI and machine learning.

This transition is a significant undertaking; for many organisations, the primary focus is now on evolving established infrastructure to meet new AI demands. 41% of IT leaders are held back by an inability to move legacy business applications, while 32% are hindered by the sheer complexity of modernisation projects.

And technical complexity isn't the only blocker. One third of organisations are being prevented from modernising their on-prem infrastructure by an internal skills gap, showing that many leaders' aspirations for keeping pace with AI innovation aren't matched by current capabilities. Despite these challenges, investment in hybrid infrastructure is accelerating – driven in particular by the growing strategic importance of AI models and the data that trains them.

The public sector is particularly struggling with the complexity of moving legacy business applications: this is preventing 55% from modernising on-prem infrastructure.

What are the main barriers preventing your organisation from modernising its on-premises infrastructure?

The Hybrid Renaissance in Action

As AI models develop into an increasingly important asset, data sovereignty becomes critical for protecting them. One quarter of all European organisations say ensuring that their proprietary AI models and training data aren't visible to public cloud providers is one of their top strategic challenges.

These concerns are prompting diversification of compute provision into hybrid architectural choices, in particular on-prem investment for AI, with leaders saying their primary drivers for placing AI on-prem are sovereignty over sensitive data on-prem (46%) and intellectual property protection (40%). As more organisations invest in creating bespoke AI models, these challenges will intensify, transforming model sovereignty from a technical consideration into a core issue of intellectual property protection and long-term competitive advantage.

Organisations are already considering and using a wide range of models to ensure data sovereignty, including private cloud with dedicated, air-gapped hardware (59%), partner-led sovereign cloud from trusted regional suppliers (53%), and bringing hyperscalers onto their private infrastructure or data centre (44%).

Manufacturing is particularly driven by security and IP protection: 52% say it is one of their key drivers for keeping AI on-prem. High profile security breaches in the industry may be driving higher levels of caution, although other industries are not necessarily at less risk of future attacks.

Regional and local cloud providers are emerging as a meaningful component of hybrid architectures, offering a middle ground between hyperscale capability and jurisdictional control. European organisations identify control over data jurisdiction as the primary benefit of working with regional providers (43%), while the more limited ecosystem of third-party services remains the most commonly cited challenge (46%). As sovereign and regional cloud offerings mature, however, this constraint is likely to diminish – making regional providers an increasingly compelling part of a diversified infrastructure strategy.

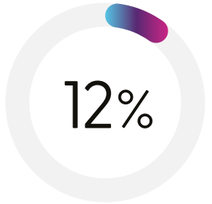
The organisations best positioned for the AI decade ahead will be those that treat infrastructure not as a legacy cost to be managed, but as a strategic asset to be designed. A well-architected hybrid environment – one that balances hyperscale capability with sovereign control and regional flexibility – can accelerate time-to-value for AI initiatives, protect intellectual property as it becomes a core enterprise asset, and reduce the drag of legacy dependency. The window to make these decisions well is narrowing. Those that act now will compound the advantage; those that delay will find the gap increasingly difficult to close.

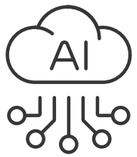
5. Economic Efficiency: Optimising Infrastructure for a New Era

The bottom line underpins the smooth running of all organisations, and it can feel in tension with other priorities. But in the context of the digital trilemma, economic efficiency is not about cutting costs indiscriminately – it is about avoiding the vendor lock-in and price volatility that prevents reinvestment and constrains long-term growth. During the initial cloud-first wave, speed to market was the primary strategic driver, often taking precedence over long-term economic analysis. Now leaders face ballooning costs from non-European cloud providers, with 28% of organisations describing unpredictable price hikes as a major strategic challenge.

Cloud-first strategies made commercial sense when speed to market was the primary competitive lever. But the geopolitical, regulatory, and cost landscape has shifted significantly – and for many, architectures made during periods of rapid growth now have structural inefficiencies, where teams are managing the symptoms of yesterday's decisions rather than the demands of today. FinOps has been a valuable discipline for managing capacity and costs – but a tipping point has been reached. Organisations can no longer rely on FinOps alone to compensate for workload placement decisions that were reasonable when made, but have become misaligned with today's sovereignty, cost, and resilience requirements. The function is being asked to do too much, and is much more effective when paired with a strategic re-evaluation of where workloads are placed.

European organisations waste **24%** of their annual cloud capacity





AI drove a 12% increase in hosting costs in the last year.

The cost of inefficiency is stark: on average, European organisations estimate they waste 24% of their annual cloud capacity. Some unused capacity reflects deliberate overprovisioning to support resilience: 62% of IT firms say this is a key reason they keep a buffer. But the majority of wasted capacity is driven by operational failures, including inactive and orphaned resources (47%), poor visibility across cloud environments (44%) and a lack of effective governance and cost accountability (41%).

AI is the catalyst that makes the status quo untenable. As well as unlocking new organisational capabilities, AI has led to a 12% increase in hosting costs in the last year alone. Rising AI and ML costs have brought increased scrutiny from finance and procurement for 59% of organisations, and the financial pressure is already forcing damaging trade-offs: 44% are reprioritising budgets away from other IT projects to cover rising infrastructure costs.

Looking ahead, leaders must ensure that naïve adoption of AI models does not create a new generation of locked-in costs – the same trap that many firms still face from workload placement decisions in the cloud-first era. The token economics of large language models carry precisely this risk. Without careful financial analysis as AI capabilities are built, organisations risk architecting themselves into token-based models that offer rapid early value but become increasingly expensive and restrictive as products and services scale.

Organisations already understand that the cheapest option is not always the most economical: 67% have chosen higher-cost infrastructure to support digital sovereignty or meet regulatory requirements. Applying that same long-term discipline to architectural decisions more broadly will be critical. Yet currently, 56% of organisations are neglecting to conduct Total Cost of Ownership assessments before making significant workload placement decisions – a gap that risks compounding inefficiencies that become harder and more expensive to unwind over time.

The path to sustainable economic efficiency runs through architectural discipline, not reactive cost management. By prioritising strategic workload placement, rigorous Total Cost of Ownership analysis, and portability by design, organisations can limit exposure to price volatility and prevent the lock-in that restricts long-term financial flexibility. Addressing inefficiency at a structural level – rather than relying on FinOps controls to patch over poor decisions – is what will allow organisations to stabilise costs, protect innovation budgets, and reinvest with confidence.

Which of the following best describes the main causes of unused or wasted cloud capacity?

“As organisations reassess where and how digital value should be created, many are navigating a dual reality: accelerating AI adoption on one hand, while reasserting control over cost, data, and sovereignty on the other—sometimes by rethinking cloud only approaches.”

Adrian Gregory

President of Insight EMEA

Gernot Hofstetter
Co-CEO, Yorizon

6. Client Perspective

Europe is in the middle of a historic shift – one that will shape not only how our organisations operate, but how our societies function in an increasingly digital world. The Digital Sovereignty Trilemma captures this reality well. But for many European business leaders, the challenge runs even deeper: Europe has relied for too long on digital infrastructure it does not fully own, control, or influence.

My perspective comes from leading a young European CLOUD Infrastructure company, Yorizon, which was created to help address part of this gap. We focus on building the sovereign cloud infrastructure that runs within European data centres, and through our work – and the collaboration required to make that work meaningful – I've seen first-hand how much of Europe's digital foundation has been shaped elsewhere. This isn't inherently negative; global platforms have enabled remarkable innovation. But dependence on them has consequences for how confidently Europe can pursue its own strategic priorities.

What encourages me is that the conversation is now shifting from whether Europe needs greater digital autonomy to how it can practically achieve it. Across public institutions and private enterprises, I hear a common message: organisations want infrastructure they can rely on, built on principles that match European regulatory expectations, societal values, and longterm risk considerations. They want transparency in how systems operate and where data resides. And they increasingly see sustainability not as an optional aspiration but as a core requirement.

This is where the trilemma becomes real. It is difficult to achieve sovereignty without sacrificing resilience, or resilience without adding cost – yet it is possible when infrastructure is deliberately designed around decentralisation, accountability, and openness. Smaller, regionally distributed facilities, for example, reduce dependency on single large sites and can strengthen local resilience. But architecture on its own isn't enough: it must be accessible and usable through established ecosystems of partners and integrators who can help organisations adopt sovereign options without friction.

Europe now has a meaningful opportunity to shape its own digital backbone for the next decade. The growth of AI, the digitalisation of critical services, and the increasing complexity of compliance all point to the need for a stronger European capability. If we choose to build this capability now, Europe can define an approach that reflects its values: sustainability, openness, and resilience. If we leave the moment to pass, we risk locking ourselves into another cycle of dependency at exactly the time digital infrastructure becomes inseparable from economic and societal stability.

For me, digital sovereignty is not about retreating from global innovation or isolating Europe from the world. It is about building the capacity to participate on equal footing. It is about ensuring that organisations – whether public or private – have genuine choice and confidence in the systems they rely on. And it is about recognising that the ability to shape our digital future begins with the foundations we decide to build today.

The Digital Sovereignty Trilemma is undoubtedly a challenge. But it is also a catalyst. It forces us to look closely at where our data lives, how our systems operate, and who ultimately has influence over the digital engines of Europe. If we approach it with ambition rather than hesitation, Europe can emerge stronger, more innovative, and more self determined than at any point in the digital era.

7. Recommendations: Navigating the Digital Sovereignty Trilemma

1. Redefine sovereignty as operational serviceability, not data residency

Digital sovereignty can no longer be treated as a geographic checkbox. Organisations need to assess their capacity to maintain operations even if disconnected from global hyperscale platforms or subjected to foreign jurisdictional interference and design their architecture accordingly.

- Evaluate the case for sovereign landing zones or air-gapped environments for highly sensitive data.
- Establish clear measures of operational autonomy, including the ability to maintain technical control over data and encryption keys.

2. Adopt a sovereignty-aware hybrid architecture

The hybrid model is fast becoming the infrastructure standard for the AI era. Bringing compute to the data – rather than moving sensitive datasets to the cloud – can protect intellectual property, safeguard against shifting jurisdictional requirements, and unlock the agility needed to scale AI effectively.

- Develop a workload placement strategy that balances hyperscalers with regional sovereign providers and private cloud.
- Invest in dedicated on-premises infrastructure for AI and ML where sovereignty and IP protection are priorities.

3. Address modernisation debt to unlock AI ambition

Without resolving legacy complexity, AI ambitions will remain constrained by the infrastructure of the past. Modernisation is not a technical project, it is a strategic enabler.

- Prioritise migration of legacy business applications that block the transition to agile, sovereign-ready infrastructure.
- Invest in closing the internal skills gap through targeted hiring or external partnerships: the capabilities needed to manage a modern hybrid ecosystem are as important as the infrastructure itself.

4. Embed Total Cost of Ownership thinking into architectural decisions

With AI driving a 12% increase in hosting costs in a single year, rigorous economic analysis can no longer be an afterthought. While FinOps is a critical discipline, its impact is maximised when architectural choices are aligned with the organisation's long-term sovereignty and cost goals.

- Mandate TCO assessments before significant workload or AI infrastructure decisions.
- Design for portability from the start to limit exposure to price volatility and prevent locked-in costs from cloud providers and AI models.

5. Build sovereignty credentials as a commercial asset

Strong digital sovereignty is not only a defensive investment – it is increasingly a source of competitive advantage. 43% of organisations have already used sovereignty credentials to win or retain business, and client demand for proof of compliance is growing.

- Formalise data protection and jurisdictional safety protocols to provide demonstrable proof of compliance with GDPR, DORA, and equivalent frameworks.
- Track the impact of sovereignty credentials on RFP success rates, particularly in public sector and regulated industry procurement.

Master the digital sovereignty trilemma by scheduling a Strategy Assessment with Insight to audit your infrastructure and secure your IT foundation today.

Contact us

uk.insight.com
0344 846 3333

8. Client Stories

Surplus prepares for digitalisation and AI with Insight

Industry: Healthcare

Challenge
Deploying AI to support their modernisation plans.

Outcomes
- Elevated security and data management
- Enhanced compliance
- Developed a more efficient process through automation

"Digitalisation is crucial for safeguarding the human dimension but should not be at the expense of privacy. The workshops with Insight provided valuable insights into data usage and protection of patient data."

Information Security Coordinator, Surplus

Auroflex defines digital transformation path with Insight to harness the value of AI in the creation of luxury labels

Industy: Luxury label printing

Challenge
Transform its business processes by introducing automation, digitalisation, and artificial intelligence.

Outcomes
- 20% reduction in order processing times
- 80% reduction in defects
- 80% reduction in quotation times
- 4x increase in the graphic possibilities offered

"I appreciated Insight's great professionalism and the ability to have multiple solutions available, not just for the cloud. We found professionalism, availability of solutions and alternatives, and expertise."

Fabio Butera, CEO, Auroflex

Echo Datacenter GmbH get their competitive edge strengthened with AI and Insight

Industy: Managed hosting provider

Challenge
Looking for ways to integrate AI services into their operations to achieve efficiencies, cost optimisation and improved performance.

Outcomes
- Operational processes were automated and optimised, resulting in a significant increase in efficiency.
- Minimised unplanned downtime and thus reduce costs.

"The introduction of AI services strengthens the competitiveness of Echo Datacenter GmbH through innovative and powerful solutions. That makes this project very important for us and that's why it was so important for us to work with a service provider who could provide us with optimal support and carry out the integration seamlessly."

Christoph van Lück, CEO ECHO eG

Belgian pharmaceutical company optimises cloud spend with Insight

Industy: Pharma

Challenge
The main challenge was cost optimisation. This could be achieved by resizing workloads, cleaning up old resources and applying cloud cost models. The company was also interested in governance and security benefits.

Outcomes
- Potential to reduce occupational therapy lead times by 8 weeks.
- Improved employee experience and helps attract new care givers to the profession.
- Significantly reduce costs related to cloud operations
- Gain security and governance benefits by eliminating end-of-life tools and disabling redundant users through better access control.

"With the help of Insight, we have regained control of our cloud operations and costs. We have appointed an internal consultant to look at processes in a more recurring way. The cost of Insight's workshop paid for itself through all the savings we've made so far. We knew there were things to optimise, but didn't know where the problems were located. Insight's efforts go far beyond a standard report."

Belgian Pharmaceutical Company Professional

9. About the Research

This research was conducted by Coleman Parkes between December 2025 and January 2026 and targeted 900 senior decision makers in digital sovereignty strategy, investment or risk management.

All survey respondents work for organisations with 500 employees or more, and they work across a range of industries: financial services, healthcare and pharma, manufacturing, retail, IT and tech, travel and tourism, logistics, and the public sector.

Their job titles include Chief Operating Officer, Head of Enterprise Architecture, Director of IT and Digital Transformation, and Head of Data Governance. Respondents are based across Europe in Austria, Belgium, France, Germany, Italy, the Netherlands, Spain, Sweden, and the UK.

About Insight

Insight is a Fortune 500 Solutions Integrator helping organisations accelerate their digital journey to modernise their business and maximise the value of technology. Insight's technical expertise spans cloud and edge-based transformation solutions, with global scale and optimisation built on 35+ years of deep partnerships with the world's leading and emerging technology providers.

About Coleman Parkes

Coleman Parkes is a full-service B2B market research agency specialising in IT/technology studies, targeting senior decision makers in SMB to large enterprises across multiple sectors globally. For more information, contact Stephen@coleman-parkes.co.uk.

uk.insight.com