



TELEHOUSE

Every connection matters

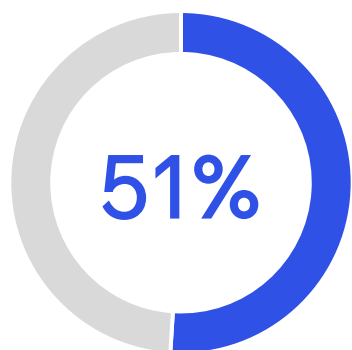
The Readiness Gap

Tomorrow Readiness
Index 2026

Where UK technology ambition is outpacing
infrastructure readiness

Ambition is moving faster than infrastructure

AI adoption is reshaping infrastructure requirements, but operational readiness is uneven. Across AI, cyber security, resilience and sovereignty, the Tomorrow Readiness Index reveals a recurring gap between technology ambition and the infrastructure capabilities needed to support it.



51% of organisations surveyed are either developing or adapting AI applications requiring dedicated infrastructure or have a fully defined AI strategy with all planned use cases operational.



While 32% say their physical infrastructure is mostly or fully ready for sustained high-density AI computing, just 10% report the highest level of capability to scale high-density AI workloads across multiple environments.

The challenge extends beyond AI

Only 23% have tested whether their infrastructure supports cyber security controls across all critical environments. Just 15% have fully integrated business continuity into their technology and infrastructure strategy, while 10% report independently assured, regularly tested sovereignty controls backed by readily available evidence.

These findings expose a wider gap between technological ambition and operational capability. For UK businesses, the challenge is not simply to invest in emerging technologies, but to ensure the infrastructure underpinning them can deliver the capacity, resilience and assurance needed to support long-term growth.

“

The pace of change we're seeing across AI, cyber security and digital services is putting new demands on infrastructure. What this research shows is that being ready for what comes next isn't about one technology or one investment. It requires organisations to think about resilience, connectivity, capacity, data and sustainable growth together - and to plan ahead rather than respond when constraints emerge.

”

Mark PestridgeManaging Director
Telehouse Europe**About the research**

Telehouse commissioned Censuswide to survey 400 UK respondents: 200 from Enterprise organisations and 200 from technology and digital infrastructure service providers. The research assesses infrastructure readiness across five areas, exploring how prepared organisations are for future technology, operational and growth demands.

Fieldwork: September 2026. Further research methodology details on pages 13–14.

Five areas of infrastructure readiness

Tomorrow's business ambitions depend on infrastructure decisions being made today. As organisations accelerate AI adoption, expand digital services and navigate growing regulatory and operational pressures, the demands placed on their infrastructure are changing.

The Tomorrow Readiness Index examines five critical areas that determine whether organisations have the foundations to support future growth.



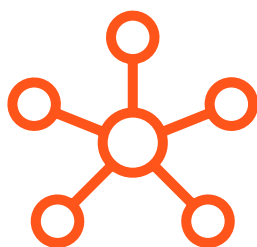
AI INFRASTRUCTURE

The shift from AI experimentation to large-scale deployment is placing new demands on compute capacity, power, cooling and connectivity. Supporting increasingly complex workloads requires infrastructure that can scale across environments without compromising performance or efficiency.



CYBER SECURITY

As digital infrastructure becomes more interconnected, vulnerabilities can extend well beyond an organisation's own systems. Dependencies across networks, suppliers and service providers are increasing the need for stronger security controls, greater visibility and the ability to contain threats before they disrupt critical operations.



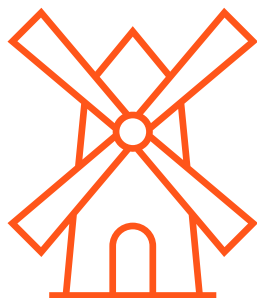
RESILIENCE & BUSINESS CONTINUITY

Disruption can expose weaknesses across even the most established infrastructure environments. Maintaining critical services depends on sufficient redundancy, access to alternative capacity and recovery arrangements that can withstand failures across power, networks, storage and infrastructure providers.



SOVEREIGNTY & COMPLIANCE

The location and movement of data have become increasingly important considerations for infrastructure strategy. Organisations must balance operational flexibility with growing demands for transparency, regulatory compliance and control over where data is stored, processed and accessed.



ENERGY, SUSTAINABILITY & READINESS FOR SCALING

Rising infrastructure demands are intensifying the relationship between power availability, capacity and long-term growth. Expansion decisions must increasingly account for energy reliability, cooling requirements, cost and environmental commitments, particularly as AI workloads place greater pressure on existing infrastructure.

These five areas cannot be considered in isolation. Decisions about AI deployment influence power and capacity requirements. Workload location affects sovereignty and compliance. Connectivity and supplier dependencies shape security and resilience.

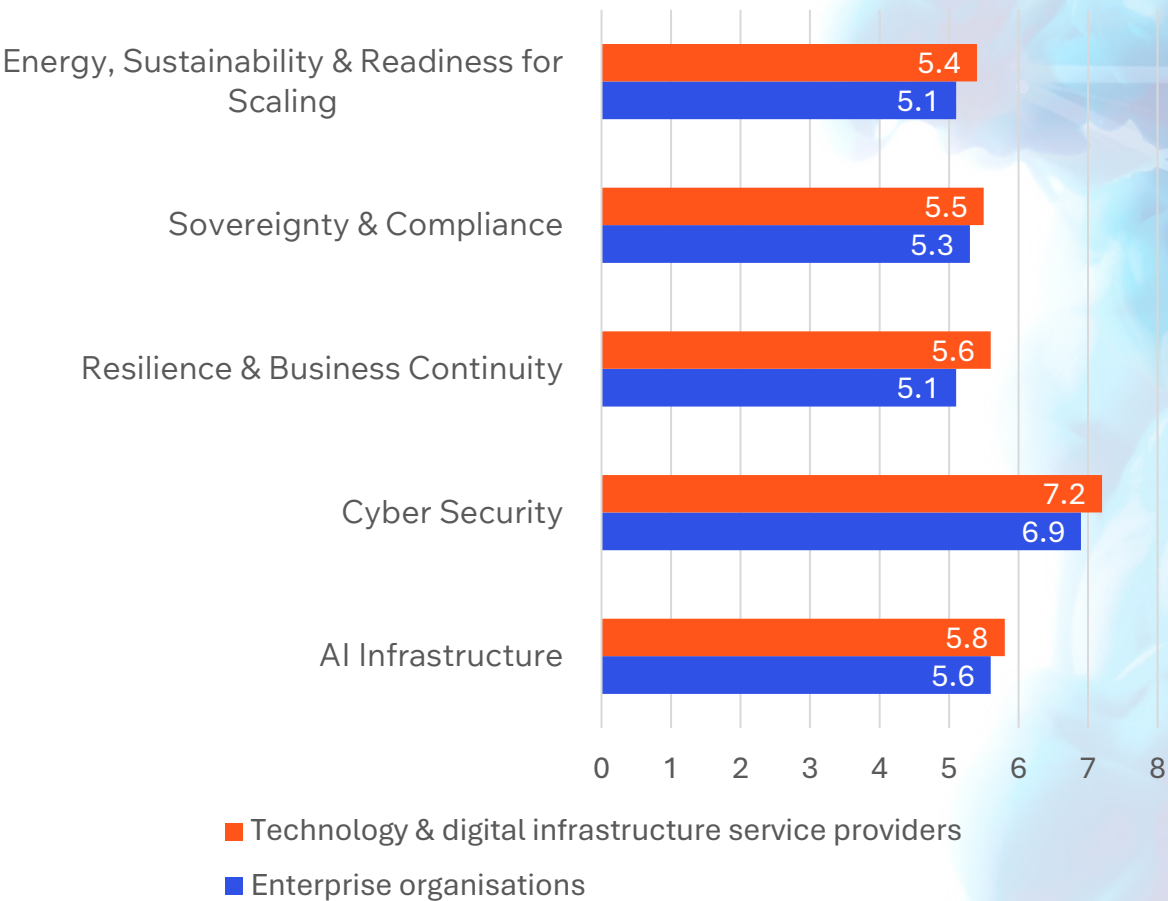
The Readiness Gap examines where UK organisations are building the foundations for growth, and where infrastructure constraints could hold them back.

Where readiness is strongest, and where gaps remain

Cyber Security is the strongest area of readiness for both Enterprise organisations and technology and digital infrastructure service providers. However, four of the five areas score below 6/10 for both audiences.

Digital infrastructure providers score above the Enterprise average across all five areas, with the widest difference in Resilience & Business Continuity.

The findings suggest that while organisations are making progress, tested, repeatable and scalable infrastructure capabilities are not yet consistently in place.



Note - Enterprise scores represent the average across Financial Services, Private Healthcare, Retail & Retail Technology, and Media & Entertainment. Digital infrastructure providers include application services, carriers, cloud infrastructure/platform providers, internet service providers, managed service providers and network infrastructure providers.

DIFFERENT AUDIENCES, DIFFERENT PRESSURE POINTS

The overall pattern is shared, but the pressure points are not identical

Although digital infrastructure providers score higher across all five areas, the research reveals different pressures around resilience, scaling and access to information from infrastructure partners.

THE LARGEST DIFFERENCE BETWEEN AUDIENCES

DIGITAL INFRASTRUCTURE
PROVIDERS

5.6/10

ENTERPRISE
ORGANISATIONS

5.1/10

Resilience and Business Continuity – the largest difference between the two audiences

ENERGY & SUSTAINABILITY INFORMATION

DIGITAL INFRASTRUCTURE PROVIDERS



29%

ENTERPRISE ORGANISATIONS



43%

Respondents reporting difficulty obtaining energy and sustainability information from infrastructure partners.

A SHARED CHALLENGE

Energy, Sustainability & Readiness for Scaling is the lowest-scoring pillar for digital infrastructure providers and joint lowest for Enterprise organisations.

DIGITAL INFRASTRUCTURE
PROVIDERS

5.4/10

ENTERPRISE
ORGANISATIONS

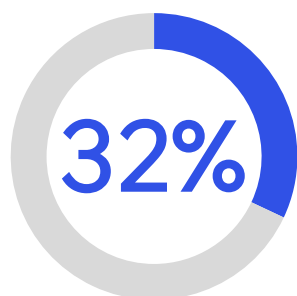
5.1/10

Despite providers scoring higher overall, both audiences face challenges preparing their infrastructure for future capacity, energy and sustainability demands

What sits behind the scores

The Index scores provide an overall measure of readiness. The underlying responses reveal where organisations are making progress and where important gaps remain.

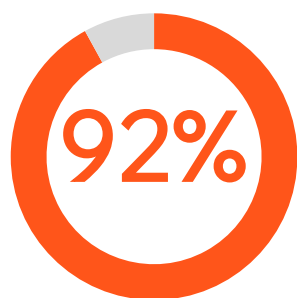
AI INFRASTRUCTURE



Only 32% say their physical infrastructure is mostly or fully ready for sustained high-density AI computing.

Moving AI into production requires more than compute capacity. Power, cooling, connectivity and workload placement all influence whether organisations can support sustained demand. The findings suggest that many are still working towards the infrastructure capability needed for more intensive AI workloads.

CYBER SECURITY



92% ran employee cyber-simulation testing in the past 12 months, but only 23% tested infrastructure cyber controls across all critical environments.

While cyber security testing is widespread, 66% report that gaps identified through employee simulations have not yet been fully addressed. This highlights the difference between conducting security exercises, resolving identified weaknesses and demonstrating that infrastructure controls work across critical environments.

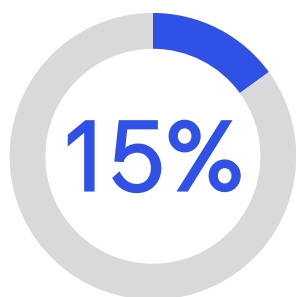
Expert opinion

“AI is evolving quickly, and without frameworks to assess against, it can be difficult for organisations to confidently judge how well they are securing AI workloads. But many of the AI incidents we’ve already seen stem from familiar failures: a lack of isolation, excessive permissions and poorly considered guardrails. The technology may be changing quickly, but the fundamentals are not. The organisations adapting best will be those applying tried-and-tested security principles from the outset, rather than waiting for standards to catch up. **”**

John Fitzpatrick

Founder & Cyber Security Researcher
Lab539

RESILIENCE & BUSINESS CONTINUITY



Only 15% have reached the highest level of business continuity integration.

At this level, business continuity is embedded in technology and infrastructure strategy, supported by regular exercises, alternative operating environments and capacity planning for future AI and digital demand.

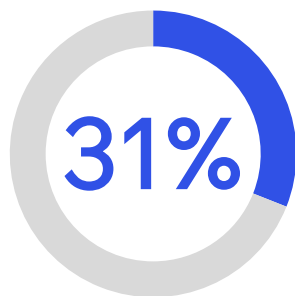
SOVEREIGNTY & COMPLIANCE



Just 1 in 10 can provide independently assured sovereignty evidence.

Among organisations with sovereignty requirements, 46% rely mainly on supplier assurances or visibility of the contracted hosting region. This contrasts with the small proportion able to demonstrate regularly tested location and access controls, with evidence available promptly when needed.

ENERGY, SUSTAINABILITY & READINESS FOR SCALING



31% say infrastructure constraints regularly impede innovation.

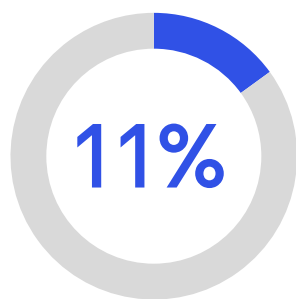
Only 9% report the highest level of preparedness for AI-related energy demands, while 36% find it difficult to obtain the energy and sustainability information they need from infrastructure partners

What readiness means in practice



AI INFRASTRUCTURE

Plan infrastructure alongside AI strategy



11% of organisations report having a repeatable architecture for placing and moving AI workloads across on-premises, colocation, cloud and edge environments.

WHAT THIS TELLS US

Many organisations are advancing their AI ambitions but the ability to deploy and move workloads consistently across environments remains limited. Infrastructure planning needs to start earlier, before use cases are ready to scale



RESILIENCE & BUSINESS CONTINUITY

Test resilience across the full dependency chain

Resilience depends on more than individual controls or availability targets. Organisations need to understand the sites, connectivity, suppliers, data and infrastructure that services depend on.



Sites



Connectivity



Suppliers



Data



Infrastructure

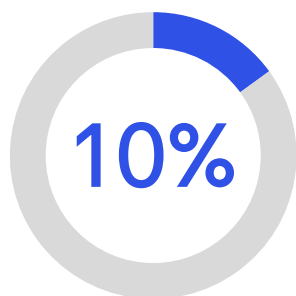
WHAT THIS TELLS US

Resilience needs to be tested across the full infrastructure environment, not just individual systems. Organisations should understand the dependencies their critical services rely on and ensure recovery arrangements can support operations when disruption occurs.



SOVEREIGNTY & COMPLIANCE

Demonstrate sovereignty and compliance through evidence



10% of organisations with sovereignty requirements have independently assured, regularly tested controls backed by readily available evidence

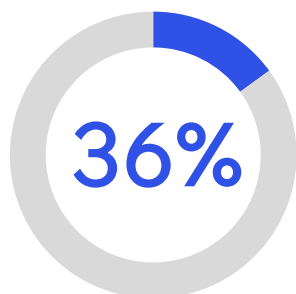
WHAT THIS TELLS US

Sovereignty is about demonstrating control, not simply knowing where data is hosted. Organisations need clear, independently verifiable evidence of how sensitive data is managed and protected, particularly when responding to customers, auditors and regulators.



ENERGY, SUSTAINABILITY & SCALING READINESS

Plan capacity, energy and sustainability together



36% of organisations find it difficult to obtain the energy and sustainability information they need from infrastructure partners..

WHAT THIS TELLS US

Preparing for future growth requires organisations to consider infrastructure capacity, energy availability and sustainability together. Power and cooling requirements need to be factored into infrastructure planning early, particularly as AI workloads increase demand. Organisations also need reliable information from infrastructure partners to understand potential constraints and make informed investment decisions.

The wider implication

Whether organisations are scaling AI, managing critical infrastructure or responding to regulatory requirements, readiness needs to be demonstrated rather than assumed. This means connecting technology plans with capacity, security, resilience, compliance and sustainability requirements.

Your readiness action plan

The Tomorrow Readiness Index highlights five areas that infrastructure leaders should be reviewing now. Use these questions to identify where further investigation or planning may be needed.



AI INFRASTRUCTURE



Can our infrastructure support AI as use cases move from experimentation into production and scale?

Review whether future demand could change requirements for compute density, power, cooling, storage, connectivity and workload placement.

Consider whether infrastructure that supports today's pilots can also support production workloads across the environments where they need to run.



CYBER SECURITY



Have we tested cyber controls across every environment and supplier our critical services depend on?

Check whether testing covers infrastructure as well as users and policies.

Make sure identified weaknesses are being addressed and that recovery processes have been tested against defined targets.



RESILIENCE & BUSINESS CONTINUITY



Could our critical services continue and recover if a site, network route, power source or infrastructure supplier failed?

Map the dependencies behind critical services and understand where redundancy, alternative capacity or supplier options exist. Test recovery under realistic conditions rather than relying only on documented plans or availability commitments.





SOVEREIGNTY & COMPLIANCE



Could we demonstrate where regulated data is stored, processed, backed up and accessed if asked today?



Look beyond the primary hosting location.
Review visibility over backups, support access, subcontractors and third-party providers, and make sure evidence can be supplied when customers, auditors or regulators require it.



ENERGY, SUSTAINABILITY & READINESS FOR SCALING



Do we know where capacity, power, cost or sustainability could constrain future growth?



Review expected infrastructure demand over the next three to five years and where additional capacity may be required.
Make sure infrastructure partners provide the energy, sustainability and capacity information needed to support planning and reporting.

Be Tomorrow Ready

Readiness is not about predicting every future requirement. It is about understanding where constraints could emerge and making informed infrastructure decisions before they become urgent.

How ready is your infrastructure?

The Tomorrow Readiness Index shows the wider picture. The next step is to understand where your own organisation is strongest, where gaps may exist and what should be prioritised next.

Take the Tomorrow Readiness Assessment

Answer **15 questions** across



TAKE THE ASSESSMENT



AI Infrastructure



Cyber Security



Resilience & Business Continuity



Sovereignty & Compliance



Energy, Sustainability & Readiness for Scaling

In approximately 3 minutes, you'll receive your Tomorrow Readiness Score, a breakdown across all five areas, and an indication of where further attention may be needed.

Your results include:



Your overall Tomorrow Readiness Score



Your score across all five readiness areas



Your strongest area and biggest opportunity

There is no single infrastructure roadmap for tomorrow readiness.

The starting point is understanding what your organisation needs next — and planning early enough to keep future options open.

Continue the conversation

[Take the assessment](#) | [Speak to an expert](#) | [Visit our London Docklands campus](#)

About this research

The **Tomorrow Readiness Index 2026** research was commissioned by Telehouse and conducted by Censuswide, surveying **400 UK respondents** across Enterprise organisations and technology and digital infrastructure service providers.



Total of
400 UK respondents

Half of respondents (200) were from Enterprise organisations across **Financial Services, Private Healthcare, Retail & Retail Technology, and Media & Entertainment**, with 50 respondents from each sector.

The remaining **200 respondents** were from technology and digital infrastructure service providers, including **application services, carriers, cloud infrastructure/platform providers, internet service providers, managed service providers and network infrastructure providers**.

Enterprise organisations

200 respondents across four sector
(50 in each sector)

 Financial Services	50
 Private Healthcare	50
 Retail & Retail Technology	50
 Media & Entertainment	50

Technology and digital infrastructure service providers

200 respondents across six provider categories

 Application services
 Carriers
 Cloud infrastructure/platform providers
 Internet service providers
 Managed service providers
 Network infrastructure providers

Respondents came from organisations of a range of sizes. The largest group, 45%, worked in organisations with 100–249 employees, followed by 28% with 250–500 employees. A further 15% worked in organisations with 50–99 employees and 10% in organisations with more than 500 employees. The remaining respondents were from organisations with fewer than 50 employees.

What the Index measures

The Tomorrow Readiness Index assesses readiness across five areas:

- AI Infrastructure
- Cyber Security
- Resilience & Business Continuity
- Sovereignty & Compliance
- Energy, Sustainability & Readiness for Scaling



Each area was assessed through a series of questions covering strategy, infrastructure, testing, operational capability, evidence and future planning. Index scores are presented out of 10, with higher scores indicating greater readiness. The findings also draw on individual survey responses to highlight differences between audiences and identify specific areas of progress and concern.

About Telehouse

Telehouse is a leading global data centre service provider that brings together a diverse range of business partners, including carriers, mobile and content providers, enterprises, cloud providers and financial services companies.

Established in 1989 by Fortune 500 telecommunications company KDDI, Telehouse operates more than 45 data centres worldwide and provides reliable, secure and flexible colocation solutions, enabling organisations to accelerate speed to market and create business opportunities through fast, efficient and secure interconnections.

For more information, visit [telehouse.net](https://www.telehouse.net).