ECONOMIST ENTERPRISE

Sponsored by FM

Built for what's next: designing resilience into digital infrastructure

Australia

Country profile

Summary

Artificial intelligence-driven demand and large-scale investment are strengthening Australia's position as a leading data centre market in the Asia-Pacific region.

Australia benefits from strong investment momentum and established hubs in Sydney and Melbourne, but faces growing challenges related to power availability, geographic concentration and pressure on supporting infrastructure.

Resilience efforts are focused on cyber security, energy management and physical infrastructure protection, supported by strong governance and critical-infrastructure requirements.

The next phase of resilience maturity will require greater attention to geographic diversification, community engagement, technology readiness and preparedness for compound disruptions.

Key data

Scale

296
data centres[1]

Capacity

3,530
MW[2]

Capacity growth

15%
annual IT-load growth (estimated 2025–2030)[3]

Geographic hubs

Sydney and Melbourne are Australia's principal data centre hubs. Around half of planned capacity is concentrated in Sydney and about one-quarter in Melbourne. Brisbane, Perth, Canberra and Adelaide are established secondary locations, while operators are also expanding into outer-metropolitan and regional sites with available power, renewable-energy potential and connectivity.[4,5]

About this research

Built for what's next is an Economist Enterprise research programme, sponsored by global property insurer FM. It examines how risks across energy, people and technology often come together to disrupt digital infrastructure, and how organisations can best prepare to meet those shocks.

The research is based on:

- A global survey of 1,800 data centre stakeholders across the digital infrastructure value chain from 21 countries
- Interviews with global industry experts
- An expert panel discussion

Market overview

Growth trends

Growth is being driven by AI, hyperscale cloud demand and upgrades from legacy infrastructure. Amazon alone plans to invest A$20bn (US$14bn) in Australian data centre infrastructure between 2025 and 2029. Supply is struggling to keep pace. Live capacity is expected to rise from about 1.3GW in 2025 to 1.8GW by 2028, leaving a possible shortfall of 0.7-1.7GW. Power availability, grid connections, construction costs and suitable sites are becoming the principal constraints.[6,7,8,9]

Investment trends

Cloud adoption and demand for generative-AI infrastructure are driving investment in Australia's data centres. Industry forecasts suggest that cumulative development could reach A$26bn-150bn (approximately US$18bn-US$106bn) by 2030. Data centre construction is expected to add about six percentage points to growth in real business investment in 2026 and five points in 2027.

Investors are also moving money from offices into digital infrastructure. Real-estate investment trusts, superannuation funds and global private-equity firms are among them. Amazon Web Service (AWS) has committed A$20bn (US$15bn), Microsoft AU$5bn (~US$4bn) and Firmus around AU$5bn (~US$4bn). Goodman Group is allocating 73% of the capital in its active development pipeline to high-density data facilities[10,11,12,13,14]

Key regulatory developments

The National AI Plan, released in December 2025, was followed in March 2026 by national expectations for data centre and AI infrastructure developers covering national interest, the energy transition, water use, skills and local capability. Projects aligned with the expectations may receive priority in regulatory approvals. In July 2026 the government announced forthcoming standards that would require large data centres to underwrite new power supply, pay their connection costs, reduce load when needed and improve water efficiency. Qualifying critical data-storage and processing assets are also subject to the Security of Critical Infrastructure Act 2018, which requires registration, cyber-incident reporting and a critical-infrastructure risk management program.[15,16,17]

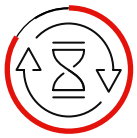
Key risks

Economist Enterprise's survey found that Australian data centre stakeholders perceive the following as the **greatest systemic risks facing the sector**:

87%

Cyber-attacks

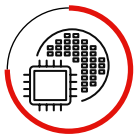
Australia's data centres and cloud infrastructure are attractive targets because they support critical services and hold sensitive data. The Australian Signals Directorate, the government's technical authority on cyber security responded to more than 1,200 cyber incidents in 2024-25, up 11%, while critical infrastructure accounted for 13% of incidents. A successful attack could interrupt hosted services, compromise operational technology and spread disruption across dependent organisations.[18]



84%

Grid capacity constraints

Data centre electricity demand could rise from about 1% of national consumption today to as much as 11% by 2035. Without faster investment in generation, storage and network capacity, connection delays and power shortages could slow construction, raise costs and concentrate development in a limited number of power-ready locations.[19]



75%

Limited critical minerals, semiconductors or cloud vendors

Australian digital infrastructure depends on a small number of global cloud providers and overseas suppliers of semiconductors, servers and specialised cooling equipment. Disruption to a major vendor or upstream supply chain could delay new capacity, increase costs and create common points of failure across businesses using the same platforms.

71%

Extreme weather or climate impact

Heatwaves, bushfires, floods and severe storms can disrupt electricity supply, damage network infrastructure and increase cooling demand. As facilities grow in scale and power density, climate-related failures could affect uptime and reinforce the need for hazard-informed site selection, redundant power and water-efficient cooling.

65%

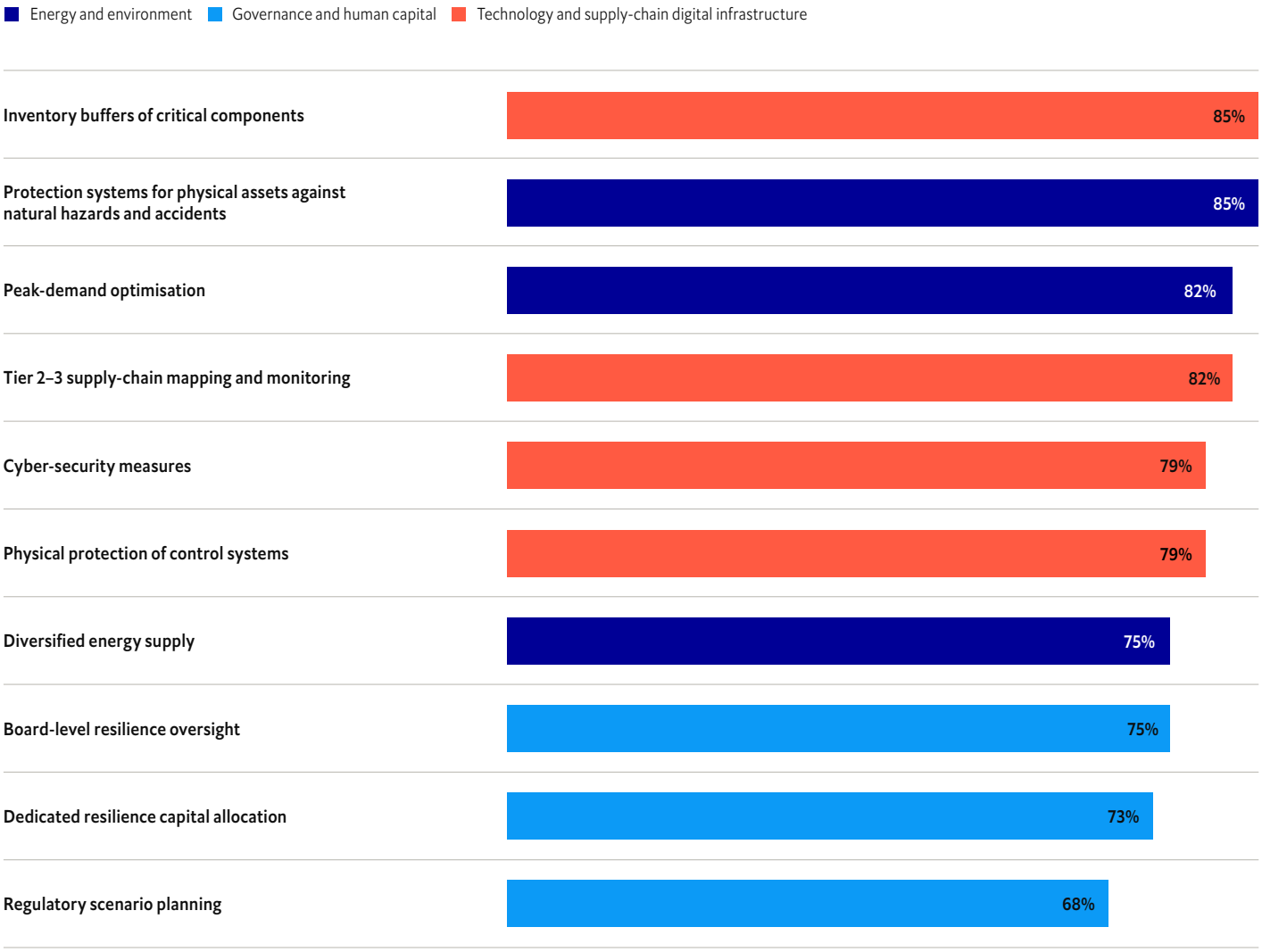
Investment or insurance withdrawal

Rising construction costs, grid delays and exposure to cyber and climate risks can weaken project economics and insurability. If lenders, investors or insurers reassess poorly protected sites, projects may face higher financing costs, reduced coverage or delays, making resilience standards increasingly important to long-term asset value.

Source: Economist Enterprise survey, February-April 2026

Resilience measures

Top 10 resilience measures adopted by data centre stakeholders in Australia



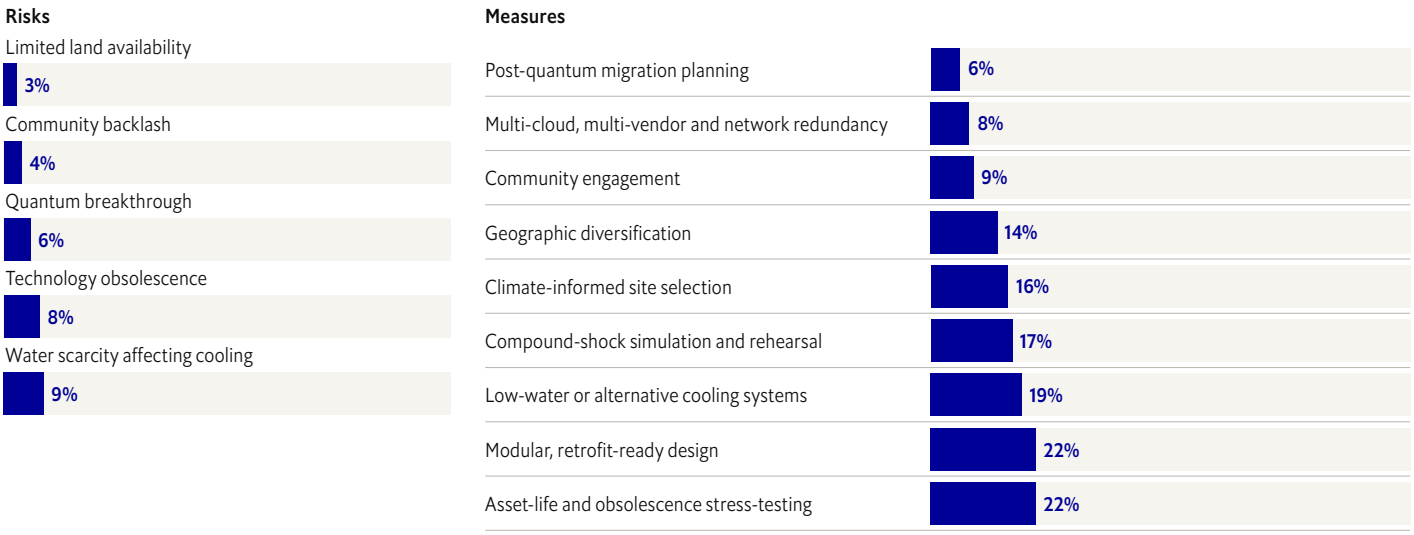
Source: Economist Enterprise survey, February-April 2026

Key takeaway

In Australia, resilience efforts prioritise operational continuity through physical protection of critical assets, inventory buffers, peak-demand optimisation and diversified energy supply. Governance measures are also relatively strong, with board oversight, dedicated resilience capital and scenario planning showing a focus on keeping systems running under immediate stress. By contrast, lower adoption of geographic diversification, community engagement and compound-shock exercises points to gaps in longer-term resilience. Overall, while preparedness for individual risks appears relatively mature, measures designed to address interconnected disruptions and concentration risk remain less widely adopted.

Priority actions

Least-adopted resilience measures and underestimated risks among data centre stakeholders



Source: Economist Enterprise survey, February-April 2026

Build future-ready infrastructure

Beyond the ability to scale, future-ready infrastructure needs robust protection systems to prevent disruption and protect critical assets as technology changes. However, only 8% of Australian respondents identify technological obsolescence as a systemic risk, while just 22% use modular infrastructure or conduct obsolescence stress tests. This could underestimate the pace at which AI is changing rack density, cooling and power requirements, and poses a risk to operations. Australia's National AI Plan notes that more than A$100bn (~US$70bn) in potential data centre investment was announced between 2023 and 2025, while government-backed research is already testing more energy-efficient cooling technologies for future facilities. Skills are another constraint. Australia faces a shortage of 141,000 infrastructure workers, potentially rising to 300,000 by 2027, prompting government calls for greater investment in apprenticeships and training. Future readiness will depend on both adaptable assets and the skills to design, operate and upgrade them.[20,21,22,23,24]

Key actions:

1. **Set shared design and engineering assumptions for future rack density, cooling, power and security needs before capital is committed.**
2. **Assess the resilience implications of emerging technologies, including cooling systems, battery storage, electrical infrastructure and high density computing environments, before design specifications are finalised.**
3. **Use asset-life stress tests to compare retrofit costs, downtime and residual value under multiple technology pathways.**
4. **Align owners, tenants, technology vendors, insurers and investors on upgrade triggers and funding responsibilities.**
5. **Build modular power, cooling and data-network pathways into new and refurbished facilities.**
6. **Build the workforce capabilities needed to design, operate, maintain and upgrade increasingly complex digital infrastructure, with expertise spanning engineering, operational technology and cyber resilience.**

Improve preparedness for compound disruptions

Australian resilience measures remain weighted towards individual systems: only 17% of respondents conduct compound-shock simulations, 14% use geographic diversification and 8% use multi-cloud or multi-vendor redundancy. But cyber incidents, power disruptions, equipment failures, extreme weather and supply-chain interruptions can trigger cascading impacts across operations. As digital infrastructure becomes increasingly interconnected, a single failure can result in physical asset damage, operational downtime, reputational impacts and significant business interruption losses. Recent regulatory developments, including enhanced cyber obligations for nationally significant critical assets, reflect a growing recognition that resilience must address interconnected operational, physical and digital risks.[25,26,27]

Key actions:

1. **Map dependencies across power, cooling, cloud, networks, suppliers, insurers and public authorities.**
2. **Identify and address single points of failure across power, cooling, battery storage, networks and operational technology systems.**
3. **Assess critical failure scenarios, including cooling outages, electrical failures, battery incidents and cyber-physical disruptions, to understand operational and financial impacts.**
4. **Conduct joint exercises that combine cyber incidents with power shortages, heat stress or critical-component delays.**
5. **Define cross-functional crisis roles and escalation paths, and use exercise findings to update maintenance and testing schedules, critical spares, contracts, recovery assumptions, staff training and capital plans.**

Diversify critical infrastructure and service dependencies

Australia's operational data centres remain concentrated primarily in Sydney and Melbourne, increasing exposure to regional grid, planning and infrastructure constraints. The data centre electricity use in the National Electricity Market is expected to rise from about 2% of grid demand in 2025 to around 6% by 2030. New geographically separated inter-capital cable routes are improving connectivity options, but operators and tenants must ensure that expansion does not reproduce concentration in power, networks or service architecture. As AI workloads, cloud services and interconnected digital systems become more complex, the risk is no longer just where infrastructure is located, but how it fails. Understanding how these systems interact, and where single points of failure may exist, will be critical to maintaining service continuity and protecting long-term asset performance.[28,29]

Key actions:

1. **Compare regional sites using grid availability, subsea/fibre connectivity, water exposure and planning readiness.**
2. **Identify and address single points of failure across power, cooling, network, battery storage and operational technology systems to improve long-term resilience.**
3. **Co-ordinate early with local authorities, operators, investors and tenants on connection timelines.**
4. **Use other regional hubs to diversify latency, cable and energy dependencies.**
5. **Evaluate resilience trade-offs alongside rental, land and power-cost advantages.**
6. **Apply consistent engineering and operating standards across sites and assess resilience benefits alongside land, power, construction and latency costs.**

Secure a social licence to operate

Community opposition is viewed as a minor risk by Australian respondents (4%), but recent developments suggest it is becoming more consequential. In 2026 a proposed A$1.1bn data centre near Perth was withdrawn following concerns about noise, environmental impacts and inadequate community engagement. Australia's new national expectations also make community benefit, responsible water use and support for the energy transition central to developers' social licence to operate.[30,31]

Key actions:

1. **Establish joint planning forums between operators, utilities, local authorities, investors, tenants and communities.**
2. **Publish transparent data on projected energy, water, land-use, noise and local economic impacts.**
3. **Conduct community-impact assessments alongside site selection and expansion decisions.**
4. **Include community opposition and permitting delays in resilience and scenario-testing exercises.**

Conclusion

Australian data centre stakeholders have established strong foundations in cyber security, energy resilience and infrastructure protection. However, the primary challenge is no longer recognising individual risks but understanding how these risks interact and amplify disruption across increasingly interconnected systems. Reaching the next stage of resilience will require more adaptable facilities, stronger community trust and targeted preparation for compound shocks as AI demand places increasing pressure on power systems and concentrated infrastructure.

References

1 Data Center Map. Australian Data Centers. Aug, 20. Available from: https://www.datacentermap.com/australia/

2 Mordor Intelligence. Australia Data Center Market Size & Share Analysis - Growth Trends and Forecast (2026 - 2031). January 2026. Available from: https://www.mordorintelligence.com/industry-reports/australia-data-center-market

3 Mordor Intelligence. Australia Data Center Market Size & Share Analysis - Growth Trends and Forecast (2026 - 2031). January 2026. Available from: https://www.mordorintelligence.com/industry-reports/australia-data-center-market

4 CEFC. Data centre boom to reshape Australia's energy future: CEFC – Baringa report. December 2025. Available from: https://www.cefc.com.au/media/media-release/data-centre-boom-to-reshape-australia-s-energy-future-cefc-baringa-report/

5 Data Center Map. Australian Data Centers. August, 20. Available from: https://www.datacentermap.com/australia/

6 Mordor Intelligence. Australia Data Center Market Size & Share Analysis - Growth Trends and Forecast (2026 - 2031). January 2026. Available from: https://www.mordorintelligence.com/industry-reports/australia-data-center-market

7 Amazon News. Amazon investing AU$20 billion to expand data center infrastructure in Australia and strengthen the nation's AI future. June 2025. Available from: https://www.aboutamazon.com/news/aws/amazon-data-center-investment-in-australia

8 CBRE. Why Australia For Data Centres. August 2025. Available from: https://www.cbre.com/insights/reports/why-australia-for-data-centres

9 US dollar figures have been converted into Australian dollars using the exchange rate as at 2 August 2026 (US$1 = A$1.4139). Converted figures are rounded.

10 https://mandalapartners.com/reports/empowering-australia-s-digital-future

11 https://www.commbank.com.au/articles/newsroom/2026/08/australias-data-centre-boom

12 https://www.imarcgroup.com/australia-data-center-construction-market

13 https://www.goodman.com/en/investor-centre/announcements-media/2026/goodman-group-reports-operating-profit-while-strengthening-the-data-centre-pipeline-in-1h26

14 Australian dollar figures have been converted into US dollars using the exchange rate as at 2 August 2026 (A$1 = US$0.70). Converted figures are rounded.

15 Department of Industry, Science and Resources. Expectations of data centres and AI infrastructure developers. March 2026. Available from: https://www.industry.gov.au/publications/expectations-data-centres-and-ai-infrastructure-developers

16 Ministers for the Department of Industry, Science and Resources. AI in Australia's Interests. July 2026. Available from: https://www.minister.industry.gov.au/t-ayres/media/ai-australias-interests

17 Critical Infrastructure Security Centre. SOCI Act 2018 for data storage and processing. December 2023. Available from: https://www.cisc.gov.au/information-for-your-industry/data-storage-and-processing/legislation-regulation-and-compliance/soci-act-2018

18 Australian Signals Directorate. Annual Cyber Threat Report 2024-2025. October 2025. Available from: https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/annual-cyber-threat-report-2024-2025

19 CEFC. Data centre boom to reshape Australia's energy future: CEFC – Baringa report". December 2025. Available from: https://www.cefc.com.au/media/media-release/data-centre-boom-to-reshape-australia-s-energy-future-cefc-baringa-report/

20 Department of Industry, Science and Resources. Capture the Opportunities. 2025. Available from: https://www.industry.gov.au/publications/national-ai-plan/capture-opportunities

21 Ministers for the Department of Industry, Science and Resources. $12.7 million to support life-changing quantum technology projects. February 2026. Available from: https://www.minister.industry.gov.au/t-ayres/media/127-million-support-life-changing-quantum-technology-projects

22 Australian Signals Directorate. The Commonwealth Cyber Security Posture in 2025. February 2026. Available from: https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/the-commonwealth-cyber-security-posture-in-2025

23 Infrastructure Australia. 2025 Infrastructure Market Capacity Report. November 2025. Available from: https://www.infrastructureaustralia.gov.au/reports/2025-infrastructure-market-capacity-report

24 Department of Industry, Science and Resources. Expectations of data centres and AI infrastructure developers. March 2026. Available from: https://www.industry.gov.au/publications/expectations-data-centres-and-ai-infrastructure-developers

25 Critical Infrastructure Security Centre. Critical Infrastructure Security Month 2025. 2025. Available from: https://www.cisc.gov.au/how-we-support-industry/events-and-outreach/critical-infrastructure-security-month-2025

26 Home Affairs. Safeguarding Australia's most critical infrastructure. March 2025. Available from: https://minister.homeaffairs.gov.au/TonyBurke/Pages/safeguarding-australias-most-critical-infrastructure.aspx

27 Home Affairs. Critical Infrastructure Security Conference 2026: Program. 2026. Available from: https://www.cisc.gov.au/how-we-support-industry/events-and-outreach/critical-infrastructure-security-conference-2026/cis-conference-resilient-connections/program

28 AEMO. Digital demand surge: Preparing Australia's power systems for the rise of data centres. June 2026. Available from: https://www.aemo.com.au/newsroom/news-updates/digital-demand-surge

29 AEMO. AEMO's updated forecasting methodology targets rapidly growing electricity loads, following industry consultation. August 2026. Available from: https://www.aemo.com.au/newsroom/news-updates/aemos-updated-forecasting-methodology-targets-rapidly-growing-electricity-loads

30 The Guardian. Developer withdraws plans for Perth data centre after fierce community opposition. 2026. Available from: https://www.theguardian.com/technology/2026/may/15/developer-withdraws-plans-for-perth-datacentre-after-fierce-community-opposition

31 Department of Industry, Science and Resources. March 2026. Available from: https://www.industry.gov.au/publications/expectations-data-centres-and-ai-infrastructure-developers