

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

Saudi Arabia

Country profile

Summary

Saudi Arabia is rapidly expanding its AI and digital infrastructure under Vision 2030, its strategy to diversify the economy beyond oil and develop new growth sectors, backed by strong government investment and abundant energy.

Cyber security, power availability and climate resilience are becoming the main operational challenges for the Kingdom's data centre sector.

Resilience efforts focus on cyber security, infrastructure protection and energy resilience, supported by dedicated investment.

The next stage of resilience will depend on adapting to climate risks, diversifying infrastructure dependencies and preparing for multiple disruptions.

Key data

Scale

40
data centres¹

Capacity

410
MW²

Capacity growth

20%
annual IT-load growth
(estimated 2025–2030)³

Geographic hubs

Riyadh is Saudi Arabia's largest data centre hub, accounting for about 26% of installed capacity in 2025 and attracting significant hyperscale investment. Jeddah is the country's main western hub, while Dammam and NEOM are emerging as important growth locations.⁴



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

Saudi Arabia's data centre market is expanding rapidly, driven by growing AI investment and cloud adoption. Valued at about 5bn riyals (~US\$1bn) in 2024, the market is projected to reach more than 14bn riyals (about US\$4bn) by 2030.

The country's strategic location, supported by international subsea cables and extensive domestic connectivity, is strengthening its role as a regional digital gateway. Abundant energy resources and a large electricity network provide a competitive advantage for AI infrastructure, while government investment in AI and Arabic large language models is driving long-term demand for digital infrastructure.^{5,6,7}

Investment trends

Vision 2030 and Saudi Arabia's ambition to become a regional AI and technology hub are driving investment in digital infrastructure. At LEAP25, over 56bn riyals (~US\$15bn) of AI-related investments and projects were announced, including commitments to data centres, cloud computing and AI infrastructure.

As part of Vision 2030's broader economic diversification, investment in information and communications technology and the digitalisation of sectors such as healthcare, education, tourism and smart cities are also increasing demand for digital infrastructure and attracting global technology companies.^{8,9}



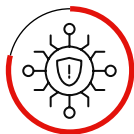
Key regulatory developments

Saudi Arabia's regulatory framework actively supports domestic digital infrastructure. The Saudi Cloud-First Policy prioritises cloud services hosted within the Kingdom and encourages investment in local data centres. The Communications, Space & Technology Commission has introduced regulations to increase competition, improve infrastructure use and attract private investment.

More broadly, Vision 2030 integrates data centre development into national plans for energy, water and digital infrastructure, positioning the sector as a pillar of economic diversification.^{10,11}

Key risks

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

**79%****Cyber-attacks**

The National Cybersecurity Authority (NCA) estimates that Saudi Arabia's cyber security market is expected to reach over 18bn riyals (~US\$45bn) in 2026 to about 29bn riyals (~\$US78bn) by 2031, reflecting growing investment to protect critical digital infrastructure as AI and cloud adoption accelerate. To safeguard critical state resources, the NCA strictly enforces compliance with Essential Cybersecurity Controls, driving a rapid market shift toward zero-trust, automated endpoint security platforms.^{12,13,14}

**73%****Extreme weather or climate impact**

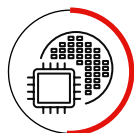
Saudi Arabia's hot, arid climate poses growing operational challenges. Extreme heat increases cooling demand and electricity use, while water scarcity adds pressure to cooling systems. As AI infrastructure expands, operators are investing in liquid cooling, water-efficient technologies and climate-resilient facility designs to maintain reliable operations.^{15,16}

**71%****Grid capacity constraints**

Expanding AI infrastructure is increasing pressure on power networks, particularly around Riyadh and major developments such as NEOM, Saudi Arabia's planned new economic and urban development in the north-west of the country. Sustaining growth will require continued investment in grid capacity, transmission infrastructure and resilient energy systems.^{17,18}

**67%****Investment or insurance withdrawal**

Saudi Arabia continues to attract substantial data centre investment under Vision 2030, supported by government initiatives and commitments from global technology companies. However, the scale of planned AI infrastructure brings significant capital requirements alongside supply-chain, construction, water and regulatory challenges. Managing these constraints will be important to maintaining investor confidence as projects increase in scale.¹⁹

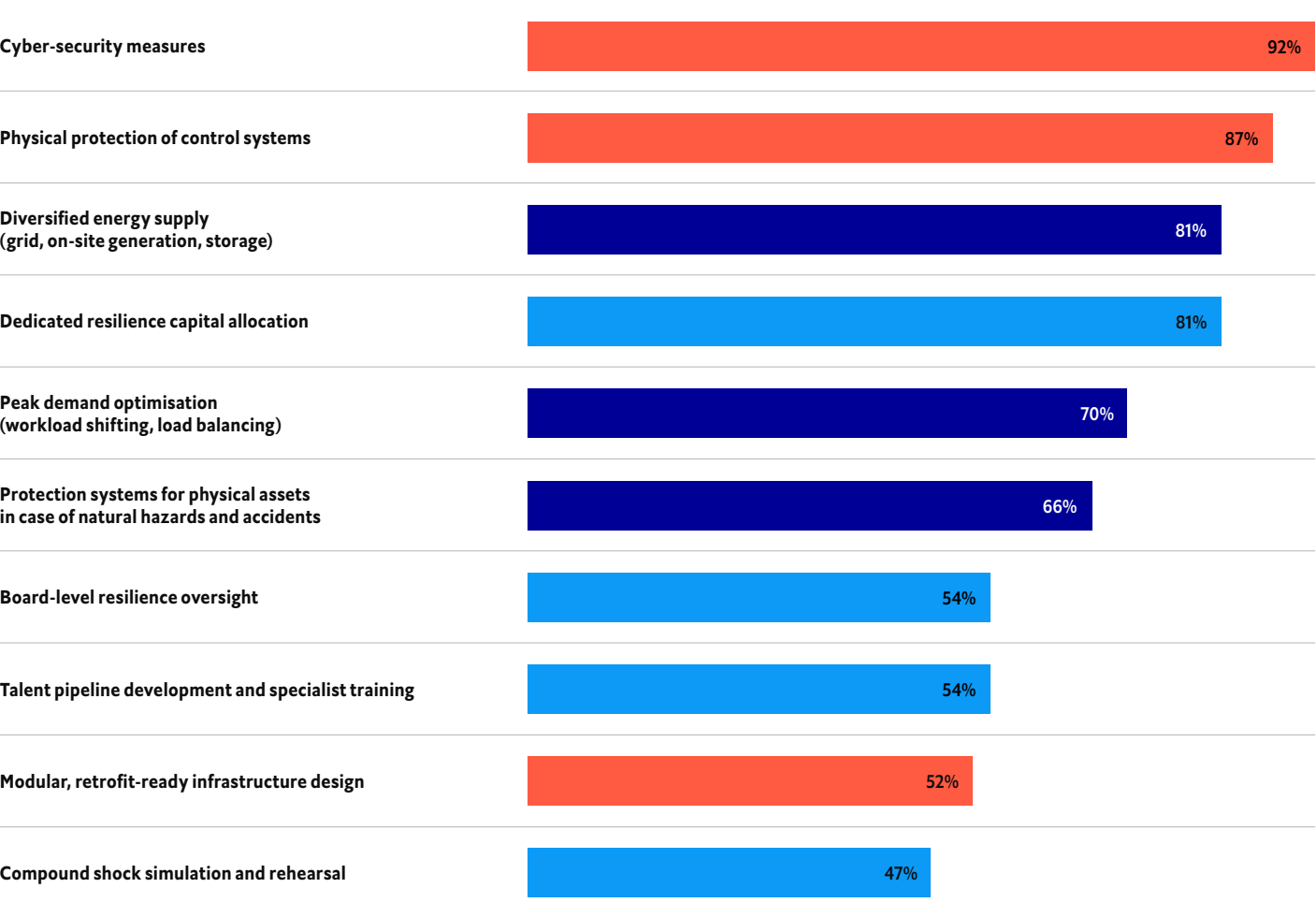
**51%****Limited critical minerals, semiconductors or cloud vendors**

Competition for advanced semiconductors and critical infrastructure components could slow AI deployment. Saudi Arabia is responding by strengthening technology partnerships and investing in AI infrastructure to secure long-term access to advanced computing and global supply chains.^{20,21}

Resilience measures

Top 10 resilience measures adopted by data centre stakeholders in Saudi Arabia

■ Energy and environment ■ Governance and human capital ■ Technology and supply-chain digital infrastructure



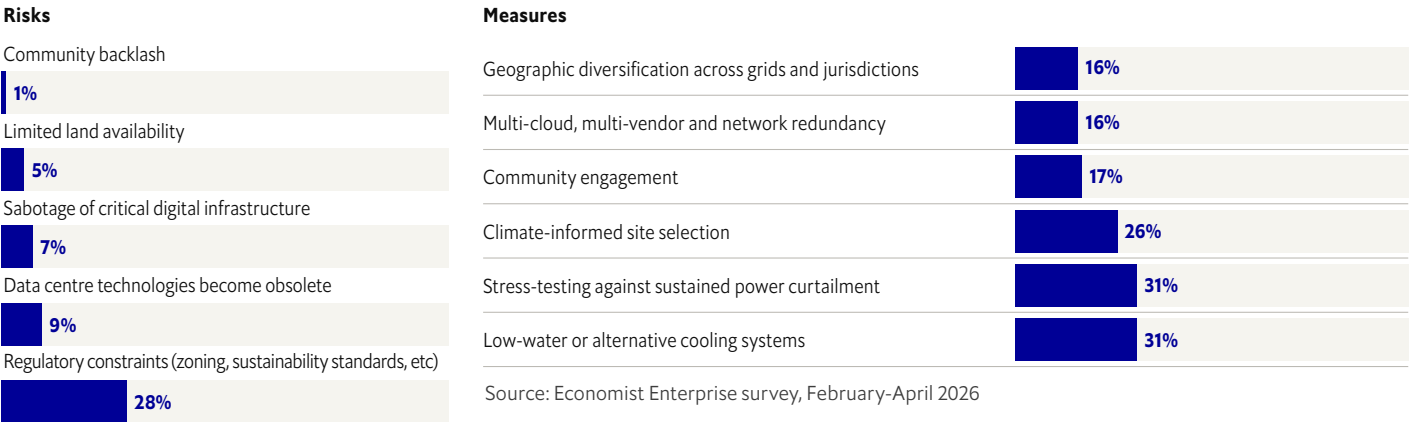
Source: Economist Enterprise survey, February-April 2026

Key takeaway

In Saudi Arabia, resilience efforts focus on cyber security, infrastructure protection and energy resilience as the Kingdom expands its AI and digital infrastructure. Strong investment in cyber security, energy diversification and resilience capital reflects a proactive approach to managing operational risks. Lower adoption of board-level oversight, specialist talent development and compound-shock simulation suggests an opportunity to strengthen long-term resilience.

Priority actions

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



Source: Economist Enterprise survey, February-April 2026

Design for climate

Technological obsolescence (9%) is seen as a relatively minor risk, yet rapid advances in AI computing and extreme desert heat could shorten asset lifecycles. Only 26% of survey respondents use climate-informed site selection and just 31% have adopted low-water or alternative cooling systems. Overcoming these vulnerabilities requires closer collaboration with technology vendors, engineers and enterprise customers to build infrastructure that can adapt to changing cooling and computing requirements.

Key actions:

- 1 Set shared design and engineering assumptions for future rack density, cooling, power and water requirements before capital is committed.
- 2 Use lifecycle stress tests to assess upgrade costs, downtime and residual asset value under changing technology and climate conditions.
- 3 Design modular power and cooling systems that can be maintained, isolated and upgraded without compromising operations.
- 4 Contractually align owners, enterprise tenants, and hardware vendors on upgrade triggers and funding.
- 5 Strengthen the engineering and operational skills needed to manage advanced cooling, power and operational-technology systems.

Improve preparedness for compound disruptions

Even as Saudi Arabia develops larger, more concentrated digital infrastructure hubs, resilience efforts remain focused on individual facilities. Only 31% of stakeholders stress-test prolonged power shortages, while geographic diversification and multi-cloud or multi-vendor redundancy are each adopted by just 16%. As hyperscale AI infrastructure expands under Vision 2030, operators will need to strengthen resilience across interconnected power, cloud and telecommunications systems.

Key actions:

- 1** Map dependencies across grid supply, cooling, water, telecommunications and critical equipment.
- 2** Conduct joint exercises combining cyber or sabotage incidents with grid failure, cooling loss and critical-component delays.
- 3** Define crisis roles and escalation paths across operators, tenants, utilities, infrastructure providers and public authorities.
- 4** Use exercises to update maintenance schedules, critical spares, recovery assumptions, staff training and capital plans.
- 5** Apply consistent engineering and operating standards across sites so geographic expansion does not create uneven levels of protection or recovery capability.

Diversify critical infrastructure and service dependencies

Grid constraints are among the most significant risks identified by stakeholders (73%), yet only 16% have diversified across grids or regions, while the same proportion use multi-cloud, multi-vendor or network redundancy. Reducing concentration risk across power systems, cloud services, connectivity and critical technology providers is a shared ecosystem challenge. Building resilience will require co-ordinated planning to diversify critical dependencies while supporting long-term infrastructure growth.

Key actions:

- 1** Co-ordinate capacity planning across emerging digital hubs, power networks and renewable energy systems.
- 2** Build redundancy across cloud platforms, network providers and critical technology vendors to strengthen cyber resilience and reduce single points of failure.
- 3** Balance power availability, climate exposure and connectivity when planning new infrastructure.
- 4** Test how disruptions affecting a single grid, cloud provider or critical supplier could cascade across operations, and use the findings to strengthen continuity planning.

Conclusion

Saudi Arabia's data centre sector has built strong foundations in cyber security, energy resilience and operational preparedness. As Vision 2030 drives a major hyperscale and AI infrastructure build-out, the next stage of resilience will depend on climate-ready infrastructure, more diversified infrastructure dependencies and closer co-ordination across the digital infrastructure ecosystem.

References

- 1 Research and Markets. Saudi Arabia Data Center Market - Investment Analysis & Growth Opportunities 2026-2031. March 2026. Available from: <https://www.researchandmarkets.com/report/saudi-arabia-data-centers-market>
- 2 Mordor Intelligence. Saudi Arabia Data Center Market Size & Share Analysis - Growth Trends and Forecast (2026 - 2031). January 2026. Available from: <https://www.mordorintelligence.com/industry-reports/saudi-arabia-data-center-market>
- 3 Mordor Intelligence. Saudi Arabia Data Center Market Size & Share Analysis - Growth Trends and Forecast (2026 - 2031). January 2026. Available from: <https://www.mordorintelligence.com/industry-reports/saudi-arabia-data-center-market>
- 4 Mordor Intelligence. Saudi Arabia Data Center Market Size & Share Analysis - Growth Trends and Forecast (2026 - 2031). January 2026. Available from: <https://www.mordorintelligence.com/industry-reports/saudi-arabia-data-center-construction-market>
- 5 Global News Wire. Saudi Arabia Data Center Market Investment Analysis & Growth Opportunities 2025-2030: Saudi Arabia Emerges as a Digital Hub as Data Center Market Set to Hit \$3.9 Billion by 2030. March 2025. Available from: <https://www.globenewswire.com/fr/news-release/2025/03/12/3041661/0/en/Saudi-Arabia-Data-Center-Market-Investment-Analysis-Growth-Opportunities-2025-2030-Saudi-Arabia-Emerges-as-a-Digital-Hub-as-Data-Center-Market-Set-to-Hit-3-9-Billion-by-2030.html>
- 6 S&P Global. The Saudi Arabia data center market: A catalyst for economic innovation. December 2025. Available from: <https://www.spglobal.com/en/research-insights/special-reports/look-forward/data-center-frontiers/saudi-arabia-data-center-market>
- 7 US-dollar figures have been converted into Saudi Arabian riyals at an exchange rate of US\$1 = SAR3.75, as at August 2nd 2026. Converted figures are rounded.
- 8 Saudi Press Agency. Saudi Arabia Solidifies Its Position as a Regional and Global Hub for AI with \$14.9B in Investment at LEAP25. February 2025. Available from: <https://www.spa.gov.sa/en/N2258405>
- 9 S&P Global. The Saudi Arabia data center market: A catalyst for economic innovation. December 2025. Available from: <https://www.spglobal.com/en/research-insights/special-reports/look-forward/data-center-frontiers/saudi-arabia-data-center-market>
- 10 Imarc. Saudi Arabia Data Center Market Size, Share, Trends and Forecast by Data Center Size, Tier Type, Absorption, and Region, 2026-2034. March 2026. Available from: <https://www.imarcgroup.com/saudi-arabia-data-center-market>
- 11 Greenberg Traurig. Saudi Arabia's Data Centre Expansion: Regulatory Framework and Strategic Considerations. January 2026. Available from: <https://www.gtlaw.com/en/insights/2026/1/saudi-arabias-data-centre-expansion-regulatory-framework-and-strategic-considerations>
- 12 Markets and Markets. Kingdom of Saudi Arabia Cybersecurity Market. March 2026. Available from: <https://www.marketsandmarkets.com/Market-Reports/kingdom-of-saudi-arabia-cyber-security-market-3336684.html>
- 13 Trellix. National Cybersecurity Authority (NCA) Cybersecurity Controls of Saudi Arabia. February 2025. Available from: <https://www.trellix.com/assets/solution-briefs/leveraging-trellix-nca-controls-solution-brief.pdf>
- 14 Alpin. Saudi Arabia's Data Center Boom: Powering the Digital Future with Sustainability. January 2026. Available from: <https://www.alpinme.com/saudi-arabias-data-center-boom-powering-the-digital-future-with-sustainability/>
- 15 Rayyan Secutech. Mastering Precision: Optimizing Data Center Cooling in Saudi Arabia. June 2026. Available from: <https://www.rayyansecutech.com/mastering-precision-optimizing-data-center-cooling-saudi-arabia>
- 16 Ken Research. KSA data center liquid immersion cooling market report Size, Share, Growth Drivers, Trends, Opportunities & Forecast 2025–2030. February 2026. Available from: <https://www.kenresearch.com/saudi-arabia-data-center-liquid-immersion-cooling-market>
- 17 Kapsarc. AI and Energy: The Future of Data Centers in Saudi Arabia. December 2025. Available from: <https://www.kapsarc.org/media/ip0dt4i1/dp00503-v1.pdf>
- 18 Neom. DataVolt signs agreement with NEOM to design and develop the region's first truly sustainable, net-zero AI factory campus in Oxagon. February 2025. Available from: <https://www.neom.com/en-us/newsroom/datavolt-signs-agreement-with-neom>
- 19 S&P Global. The Saudi Arabia data center market: A catalyst for economic innovation. December 2025. Available from: <https://www.spglobal.com/en/research-insights/special-reports/look-forward/data-center-frontiers/saudi-arabia-data-center-market>
- 20 Middle East AI News. Oracle commits \$14 billion to Saudi Arabia's tech future. May 2025. Available from: <https://www.middleeastnews.com/p/oracle-commits-14-billion-to-saudi>
- 21 Reuters. US tech firms Nvidia, AMD secure AI deals as Trump tours Gulf states. May 2025. Available from: <https://www.reuters.com/world/middle-east/saudi-arabia-partners-with-nvidia-spur-ai-goals-trump-visits-2025-05-13/>

About FM

This research programme is sponsored by FM, one of the world's largest commercial property insurers, and is dedicated to helping organisations build resilience and protect long-term business value. Drawing on nearly two centuries of engineering expertise, scientific research and loss-prevention experience, FM helps clients better understand and manage the risks that affect critical operations and infrastructure.

FM Intellium brings together research, engineering insight and resilience intelligence to help organisations evaluate, strengthen and benchmark resilience across the digital infrastructure ecosystem. By providing a clearer view of resilience vulnerabilities, system interdependencies and emerging risks, FM Intellium supports better business, investment and policy decisions in an increasingly complex digital environment.