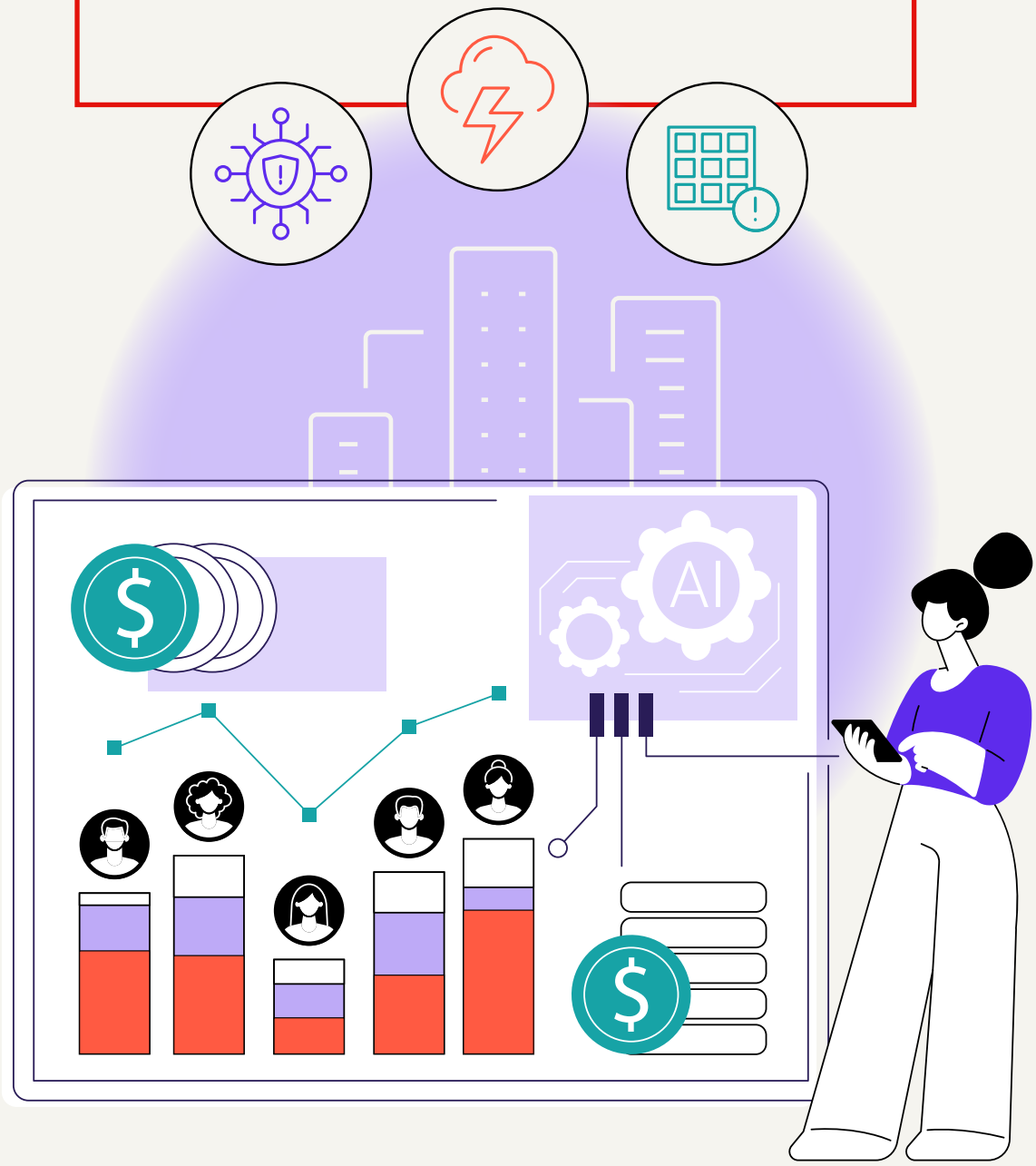
ECONOMIST ENTERPRISE

The tenant guide

Built for what's next: strengthening digital infrastructure resilience



Sponsored by

Sponsor foreword

The Economist Enterprise research presented in this guide highlights an important challenge. While most organisations recognise resilience as a strategic priority and have invested heavily in digital transformation, preparedness is not always keeping pace with the increasing complexity of the digital infrastructure ecosystem. Many organisations remain confident in their ability to manage individual risks, yet disruptions frequently emerge when multiple risks interact across interconnected systems.

For data centre tenants and end users, this matters because resilience cannot be assumed. Power availability, cooling systems, network connectivity, technology dependencies, supply chains and operational processes all play a role in maintaining performance. When vulnerabilities exist across these interconnected systems, disruptions can cascade in ways that are difficult to predict through traditional approaches to risk management.

FM's engineering research and loss prevention experience demonstrate that resilience is rarely determined by a single asset, technology or provider. It depends on understanding how systems perform under stress, how dependencies interact and where hidden vulnerabilities may exist across the broader digital infrastructure ecosystem. As digital infrastructure continues to evolve, organisations must also consider emerging risks and future challenges that may not yet be fully visible today.

This is where resilience intelligence becomes increasingly important. By combining engineering expertise, scientific research and a deeper understanding of interconnected risk, organisations can make more informed decisions about the resilience of the infrastructure on which they depend.

This guide provides a practical framework to help data centre tenants evaluate resilience more effectively. The organisations best positioned for the future will not simply secure capacity. They will develop a clearer understanding of the interconnected systems that support their operations and build resilience into the decisions they make every day.

About this research

Built for what's next is an Economist Enterprise research programme, sponsored by global commercial 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

The resilience you don't own

There are certain things that executives often fail to consider until it's too late. One of them is the physical foundations of the digital economy. The data centres that enable everything, from modern banking services to the training and use of advanced AI, pose a common risk for the organisations that depend on them: what happens when something interrupts the humming of the servers? The many threats include power outages, cyber-attacks, cooling problems and issues with the networks that connect servers and storage systems together.

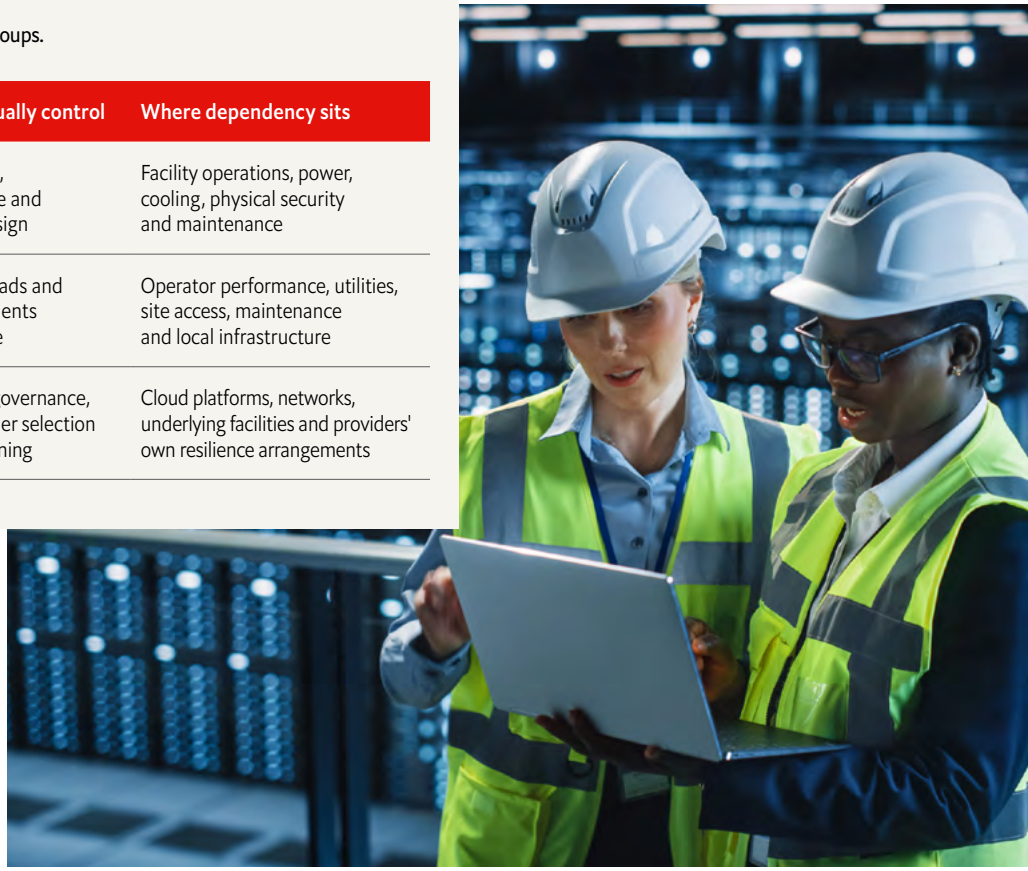
The challenge for data centre tenants and end users—from cloud and AI firms leasing capacity to enterprises using colocation, cloud platforms or software services—is that the resilience of the systems on which they depend is derived from physical infrastructure they do not control. This includes power, cooling, networks, buildings and maintenance crews.

Cloud, AI and technology companies typically control their servers, workloads and service architecture, but rely on facility operators for site-level power, cooling, physical security and maintenance. Direct colocation tenants face similar dependencies, often with fewer options to shift capacity quickly. Enterprises that use cloud infrastructure indirectly have the least visibility into the underlying facilities, so rely even more on provider governance, contracts, portability and business continuity.

Figure 1. Who this guide is for

"Tenant" is a broad word. We use it to cover three main groups.

Tenant type	What they can usually control	Where dependency sits
Cloud, AI or technology company leasing third-party capacity	Servers, workloads, service architecture and some resilience design	Facility operations, power, cooling, physical security and maintenance
Direct colocation tenant	Equipment, workloads and resilience requirements within leased space	Operator performance, utilities, site access, maintenance and local infrastructure
Enterprise cloud or software as a service (SaaS) user	Applications, data governance, architecture, provider selection and continuity planning	Cloud platforms, networks, underlying facilities and providers' own resilience arrangements

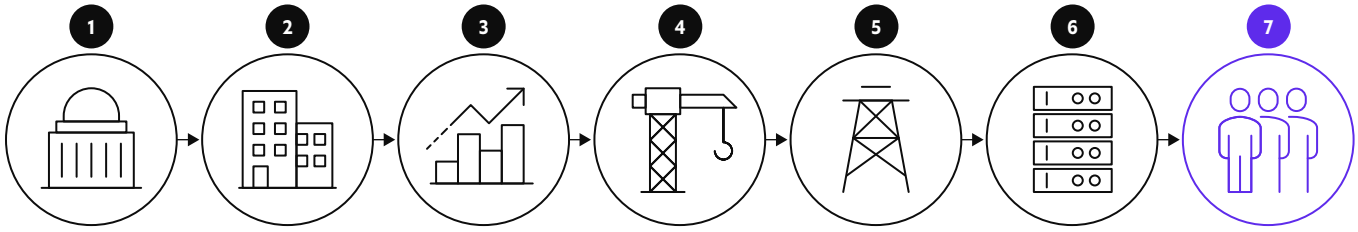


Leverage varies. Colocation tenants can inspect facility specifications and recovery arrangements for themselves. Others must work through architecture, procurement, contracts and whatever governance their providers will disclose. But the strategic challenge is the same for all: to turn dependence on infrastructure they do not own into something they can understand, challenge and test.

How data centre risk arises, how it travels and who ends up carrying it is the subject of *Built for what's next,* an Economist Enterprise research programme, sponsored by FM. It draws on a survey of more than 1,800 senior leaders across the data centre value chain in 21 countries, including more than 720 data centre tenants and end users of cloud computing infrastructure.

One central lesson from our survey is that digital infrastructure risk is largely generated at system level but, in the case of tenants, it is most often managed at contract level. Tenants sit at the end of a long chain of other stakeholders' decisions about where facilities are built, how they are powered and maintained, and how risks are managed. These decisions ultimately shape the availability, performance and cost of AI and cloud services. This guide explores the risks tenants face, how leading organisations are adapting their resilience strategies to those risks, and where resilience practices currently fall short.

Figure 2: The role of tenants in the digital-infrastructure value chain



Source: Economist Enterprise

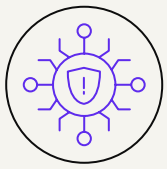
Key takeaway

Tenants are responsible for the demand behind the largest infrastructure boom in modern history, yet they carry the consequences of failures they do not control. Their strongest lever is commercial: what tenants require in contracts, redundancy and disclosure, the market will eventually build.

The risks tenants fear most

Tenants know all too well what can happen when their servers go down. Nearly nine in ten (86%) have experienced a disruption to their digital infrastructure in the past five years, with 12% reporting significant financial and operational impact. That vantage point shapes a distinctive tenant risk hierarchy that is tilted towards threats that arrive suddenly and interrupt operations.

Three risks emerge very clearly from our survey as top of mind for tenants: cyber-attacks, extreme weather and pressure on energy grids. These threats can interrupt operations directly or trigger wider failures across the digital infrastructure ecosystem that ripple through to the tenant and end user.



Cyber-risk doesn't stop at the firewall

No threat looms larger for tenants than a cyber-attack. More than 91% expect cyber-attacks to have a systemic impact, representing the highest share across all surveyed stakeholder groups. This is unsurprising. Tenants' data and applications are the target, whatever building they sit in. Even an attack that does not impact a tenant's data can disrupt by interrupting operations.

Yet tenants are also the stakeholders who feel most confident that cyber-risk can be managed, with 85% agreeing, against 76% of investors. This confidence stems from hard work. Around nine in ten tenants have cyber-security measures in place and physically protect control systems, the two most widely adopted resilience strategies in their toolkit.

One residual danger, however, is that confidence outruns coverage. Cyber-defence, in contrast to domains such as climate-resilience and community opposition, is one area where tenants have decades of institutional muscle memory. But newer failure modes—including an attack on a shared cloud platform, a compromised operator or a vendor concentration that turns one breach into an industry event—sit outside that muscle memory. A tenant's firewalls do not protect it from its provider's weaknesses.

Simon Allen, a data centre growth adviser, notes that "the real risk sits at the intersection of grid or power availability and cyber-risk, particularly in operational technology systems such as power management, cooling, energy management, generators, batteries and grid interfaces."

" The real risk sits at the intersection of grid or power availability and cyber-risk, particularly in operational technology systems such as power management, cooling, energy management, generators, batteries and grid interfaces."

Simon Allen,
data centre growth adviser

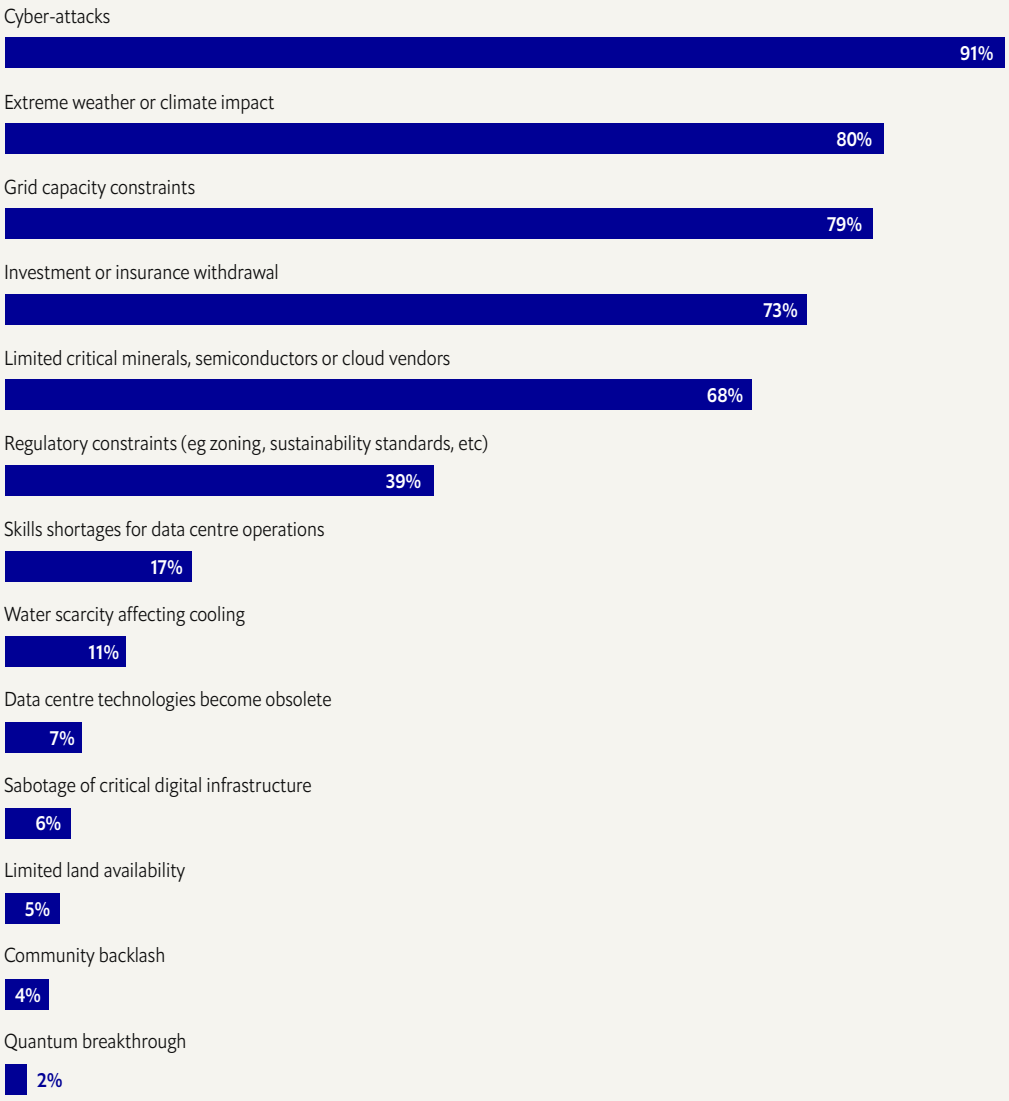
Trouble upstream, costs downstream

The second cluster of tenant anxiety is physical. Eight in ten tenants expect extreme weather or climate impact to cause material disruption—the highest share of any group, and well above the 68% of operators—while 79% point to grid capacity constraints. Monitoring habits reflect these concerns, with electricity price volatility (75%) and grid connection delays (64%) ranking among tenants' most-watched early-warning signals.

The problem is that tenants can neither generate power nor stop a storm. Their exposure to energy and climate risk stems almost entirely from where their providers chose to build, years before the lease was signed. Moreover, issues that begin upstream, such as grid capacity constraints, water scarcity or local opposition to new data centres, translate over time into downstream challenges. These include fewer available connections, workloads concentrated across fewer platforms, higher prices and less flexibility for tenants.

Figure 3. Risks to business continuity

Top risks tenants expect to have the greatest systemic impact on digital infrastructure over the next five years



Source: Economist Enterprise survey, February–April 2026

Resilience is funded but rarely tested

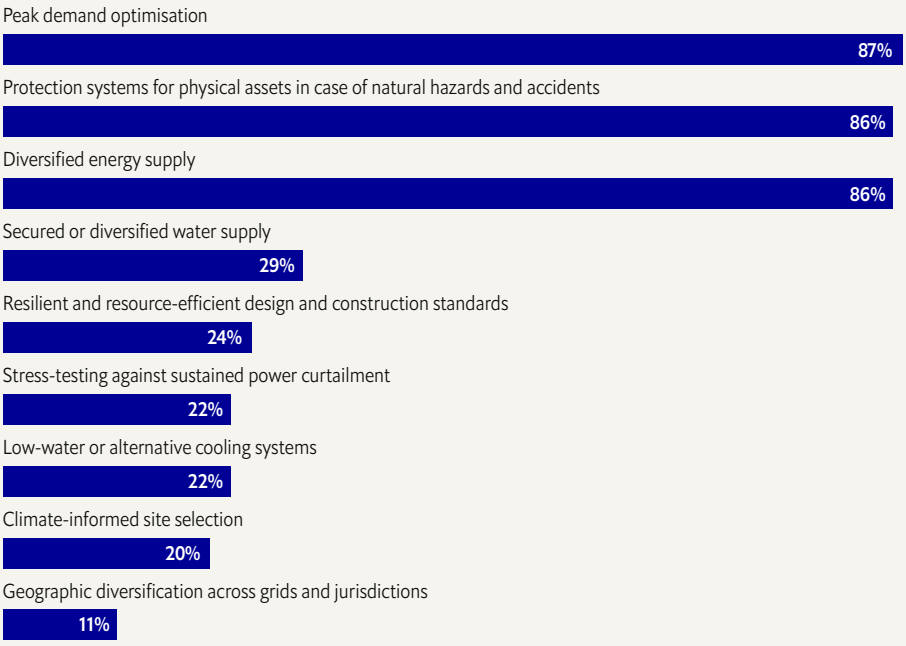
It is easy for tenants to assume that data centre resilience is the landlord's job. But this would be misguided. Because tenants supply the demand that finances the data centre boom, what they insist on—in procurement, in contracts and in the signals they monitor—shapes what gets built.

Our survey finds that they are starting to wield their influence.

Operational defences are strong

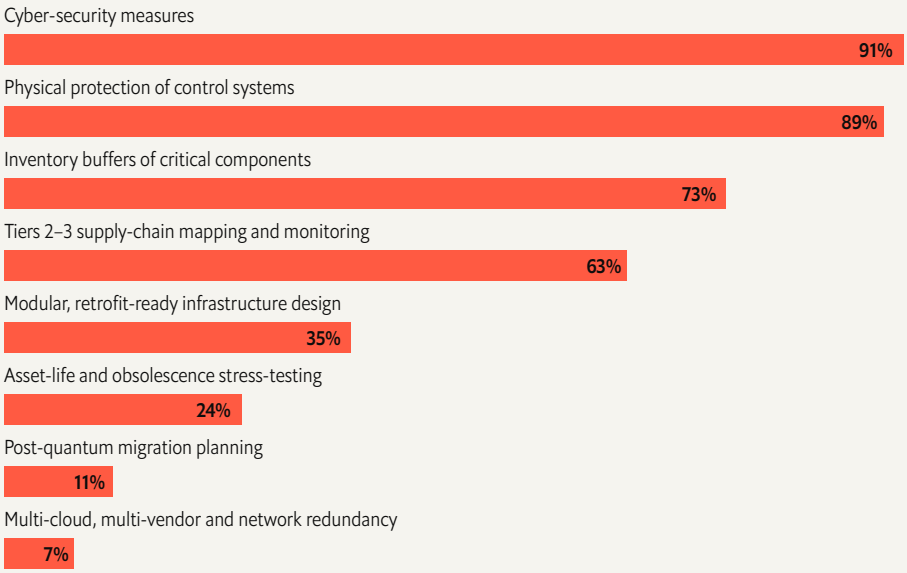
Cyber-security remains the leading area of investment, with nine out of ten (91%) tenants reporting measures in place. Physical protection of control systems (89%) and inventory buffers of critical components (73%) also rank highly, showing that many organisations are investing in the practical measures needed to keep services running. These measures matter differently across the tenant group. For cloud and AI companies, they help protect high-density infrastructure and service commitments. For direct colocation tenants, they reinforce the equipment and workloads managed inside a facility. For enterprises relying on cloud services, strong internal cyber controls reduce one part of the risk, although provider and platform dependencies remain.

Figure 4(A): Energy and environmental resilience measures adopted by tenants



Source: Economist Enterprise survey, February–April 2026

Figure 4(B): Technology and supply-chain resilience measures adopted by tenants



Source: Economist Enterprise survey, February–April 2026

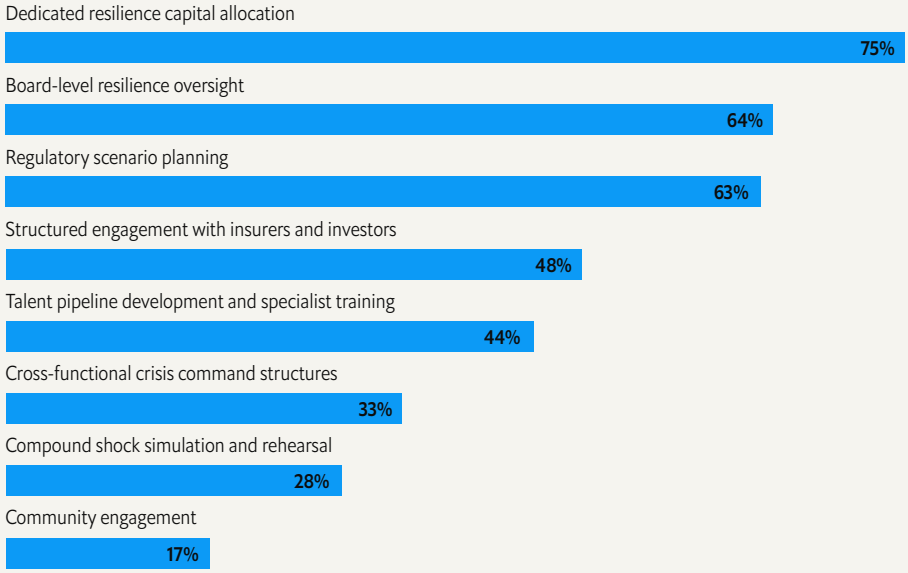
Energy resilience is another priority. Nearly nine in ten tenants have measures to manage peak electricity demand, protect physical assets and diversify energy supplies, providing a solid foundation for day-to-day operations. Direct colocation tenants may be able to specify power density, redundancy and recovery requirements. But enterprises that rely on cloud services have less influence over facility design so are more reliant on provider due diligence and workload portability.

Operational resilience outpaces crisis readiness

Tenants are fairly confident in their ability to manage operational risks. For example, 85% feel confident they can manage cyber threats, while more than 60% say they can manage grid capacity constraints and extreme weather. But confidence is not the same thing as preparedness for systemic disruption.

The unresolved question is whether these safeguards would withstand systemic stress. That requires tenants to clarify accountability, test assumptions and escalate risks through procurement, risk and business-continuity processes. That, in turn, demands expanding their approach to governance. More than 60% of tenants report board oversight on resilience measures and regulatory scenario-planning, but only a third (33%) have cross-functional crisis command structures to manage response when situations arise. Even fewer (28%) run simulations to test what happens when multiple threats occur at once or in quick succession.

Figure 4(C): Technology and supply-chain resilience measures adopted by tenants



Source: Economist Enterprise survey, February–April 2026

The lease is a lever few tenants pull

Tenants hold more contractual power than they seem to exercise. Fewer than half (48%) report structured engagement with insurers and investors. And only 17% say they have formal crisis co-ordination across all critical internal and external stakeholders, the machinery through which a tenant would learn, mid-crisis, what its provider is doing.

The renewal of every data centre contract is an opportunity to change this. Tenants can demand disclosure of grid-connection status, water sourcing, insurance coverage and concentration among a provider's other customers. They can also write service credits, portability rights and crisis-communication protocols into agreements.

Where tenants remain exposed

Tenants may have measures in place to address the risks at the top of the register: cyber-attacks, grid constraints, extreme weather, cloud outages and skills shortages. But the dependencies that allow one failure to spread across all of them are harder to see. It's through understanding these dependencies that the biggest resilience gains can be made.

Gap 1:

Diversification can mask concentration

When too many services depend on the same infrastructure, a single fault can disrupt whole sectors. For example, a single-cloud-region outage in 2025 lasted more than 15 hours, taking down applications, office tools and consumer platforms across multiple organisations.[1]

Tenants are attuned to this risk, but as Leonard Schliesser, senior researcher at the Centre for Security Studies at ETH Zurich, notes, multi-cloud and multi-vendor redundancy is often treated as a "nice to have" due to the additional costs, especially when the priority for working capital is growth.

Our survey highlights the tension. Only 7% of tenants report having multi-cloud, multi-vendor and network redundancy in place. When asked what the biggest barriers to further investment in resilience are, short-term financial growth targets top the list, cited by more than two-thirds of tenants.

Tenants must also remember that what appears as smart diversification could be masking concentration at a deeper level. As Piers Wilson, cybersecurity and data privacy expert (now at International Schools Partnership) notes, "tenants may use multiple SaaS tools, vendors or cloud environments, yet still depend on the same underlying provider."

Recommended actions:

Map dependencies and build resilience into procurement

Tenants should test whether workloads can move, whether back-up sites are genuinely independent and whether apparently separate applications ultimately depend on the same provider, region or network.

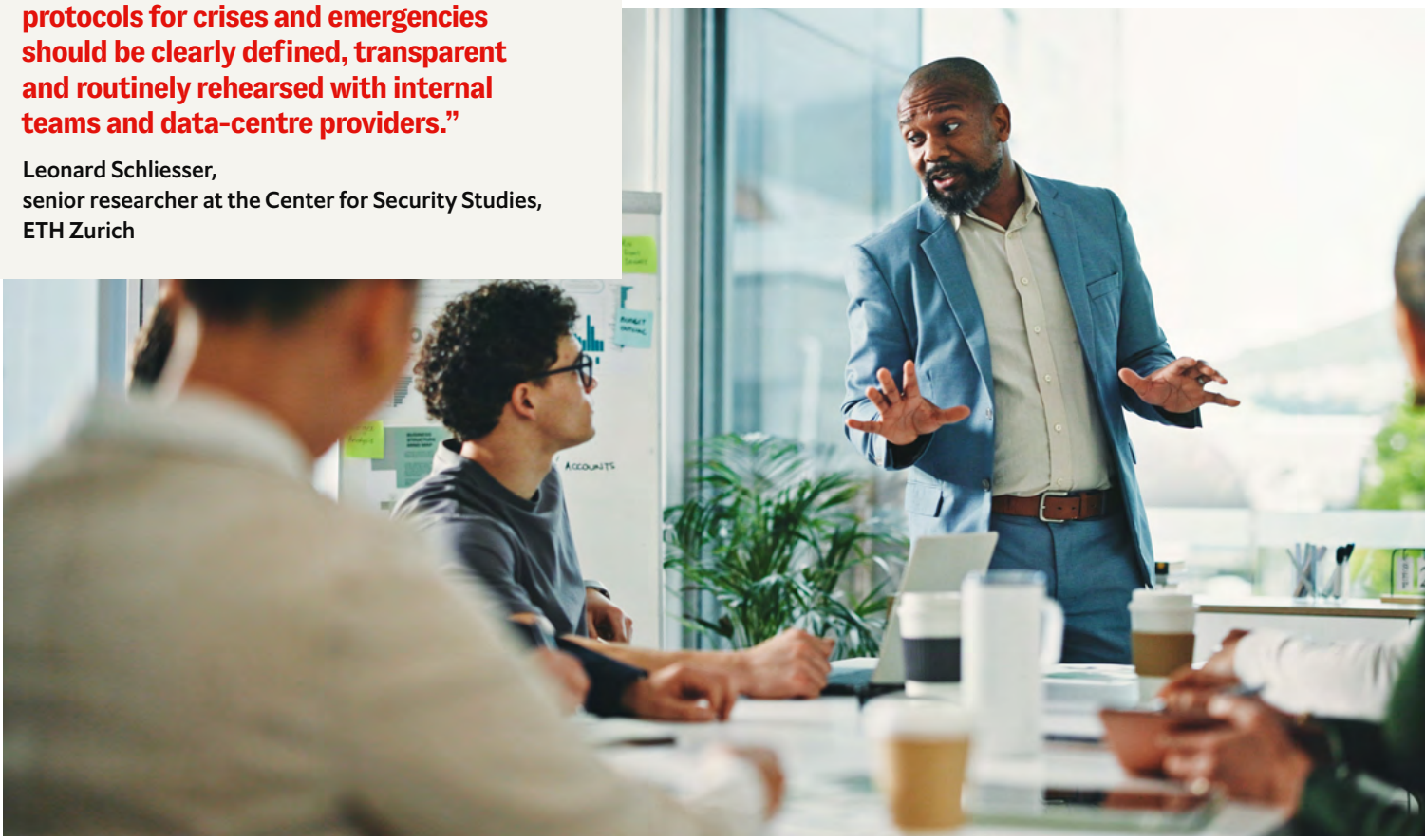
Standard service-level agreements rarely cover compound failure scenarios. But if tenants start to require this level of preparedness at procurement, the market will respond.

Requests for proposals should require:

- Recovery times, failover arrangements, redundancy levels and incident reporting standards
- Demonstration of response to compound shocks: simultaneous power failure, cooling failure, cyber-attack and cloud-region outage
- Visibility into workload, data and connectivity concentration across providers, regions, grids and jurisdictions
- Operational capability, including maintenance practices, incident-response arrangements and staffing resilience

> **"Tenants may use multiple SaaS tools, vendors or cloud environments, yet still depend on the same underlying provider."**
>
> **Piers Wilson,**
> **cyber-security and data privacy expert,**
> **International Schools Partnership**

> **"Communication flows and response protocols for crises and emergencies should be clearly defined, transparent and routinely rehearsed with internal teams and data-centre providers."**
>
> **Leonard Schliesser,**
> **senior researcher at the Center for Security Studies, ETH Zurich**



Gap 2:

Crisis plans remain fragmented

Most business-continuity plans assume a disruption that can be handled within existing structures. Systemic failures rarely oblige. A cloud outage may coincide with a cyber incident. A power failure may disable both a facility and the networks needed for recovery. A regional disruption may affect both the tenant and its designated back-up suppliers.

Preparing for these eventualities requires "clear accountability, cross-functional co-ordination and open lines" with external partners, says data centre growth adviser Mr Allen. This is because when "multiple things go wrong at once", speed determines outcomes.

Our survey finds that tenants could do more here to strengthen their preparedness. Only a third have cross-functional crisis command structures in place to manage situational responses and fewer than one in five formally co-ordinate with all critical internal and external partners during a crisis.

Recommended actions:

Test plans with the partners who must deliver them

Tenants should rehearse compound shocks with the partners on whom they depend, including facility operators, utilities, network providers and vendors. They should also test for site loss, restricted access, cooling failure, cloud-region outages, data-recovery constraints and manual workarounds.

"Communication flows and response protocols for crises and emergencies should be clearly defined, transparent and routinely rehearsed with internal teams and data-centre providers," argues Dr Schliesser, so that response protocols are agreed before a crisis.

Organisations that practise their response together are more likely to respond effectively when several failures occur at once.

Gap 3:

Tenants underestimate skills shortages

When it comes to resilience, systems and infrastructure receive most attention. But recovery depends on the people who monitor, maintain, escalate and recover those systems when they fail.

Skilled staff maintain equipment, read alarms, manage escalation, restore systems and exercise judgement when the standard procedure runs out. Stretching those teams and incidents could last longer and small errors could have material consequences.

Nearly 60% of data centre operators struggle to fill roles with qualified staff, according to research from the World Economic Forum.[2] Yet fewer than one in five tenants identifies skills shortages as a systemic risk. This mismatch should worry tenants.

Experts point to the importance of embedding resilience into organisational culture. This means training teams to challenge assumptions, build in buffers and escalate risks before they become continuity failures.

Due diligence should also extend beyond technical specifications... Tenants should assess providers' staffing levels, training, fatigue management, escalation capacity and incident-response readiness, not just the infrastructure they operate.

Recommended actions:

Build in-house skills and test providers' readiness

Outsourcing infrastructure does not remove the need for technical judgement. It changes where that judgement has to be applied.

Cloud and AI companies need expertise at the seam between IT, operational technology and facility engineering. Colocation tenants need enough in-house capability to stress-test a provider's assumptions about redundancy, maintenance and recovery. Enterprises need strong cloud governance, architecture, procurement and continuity skills, even if they never touch a rack.

Due diligence should also extend beyond technical specifications. Mr Allen notes that data centre workers are under "immense stress", increasing the risk of burnout, mistakes and staff turnover. Tenants should assess providers' staffing levels, training, fatigue management, escalation capacity and incident-response readiness, not just the infrastructure they operate.

From buying capacity to governing resilience

Data centres have become central to business continuity, AI deployment and digital growth. Yet many tenant-provider relationships still turn mainly on capacity, performance and cost.

As digital infrastructure grows more concentrated, more power-constrained and more operationally complex, tenants need to know not only what service is promised, but how resilience is built, tested and governed. That doesn't mean becoming an infrastructure expert. It means planning with all critical partners, agreeing on communication protocols and defining responsibilities before disruption occurs. It also requires contracts that set clear expectations for how providers will respond to complex failures, not just routine outages.

In a market where capacity is scarce and dependencies run deep, resilience will depend less on what is promised in normal times and more on how quickly the whole ecosystem can act together under stress. Tenants who invest now in the contracts, relationships and skills to make that possible will be better placed to protect their operations and be credible partners to the operators and providers they rely on.

Five actions for data centre tenants:

1. **Test resilience against systemic stress.**
2. **Map hidden dependencies.**
3. **Write resilience requirements into contracts.**
4. **Build the skills to challenge providers .**
5. **Rehearse compound failures with critical partners.**

References

1. AWS Outage Analysis: October 20, 2025. ThousandEyes. October 20th (updated October 24th 2025). Available at: https://www.thousandeyes.com/blog/aws-outage-analysis-october-20-2025

2. The data centre boom needs a resilient workforce - here's how to build one. World Economic Forum. September 24th 2025. Available at: https://www.weforum.org/stories/2025/09/data centre-resilient-workforce/

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.