

WHITE PAPER

Building Resilient Data Centers

Managing contractor and supplier
risk across the entire asset lifecycle

August 2026

www.achilles.com

 **Achilles**
Global Risk Management

Contents

Section One

Introduction

Section Two

The Critical Role of
Supply Chains in Data
Center Resilience

Section Three

Risk Environment One:
Construction

Section Four

Risk Environment Two:
Operational Resilience

Section Five

Managing Dynamic Supply
Chain Risk

Section Six

From Supplier Assurance
to Continuous Supply Chain
Intelligence

Section Seven

Five Questions Every Data
Center Operator Should Be
Able to Answer

Section Eight

The Future of Supply
Chain Resilience



Introduction

The global race to build AI-ready infrastructure has triggered one of the largest waves of data center investment in history. Hyperscale operators, colocation providers and enterprise organizations are expanding capacity at unprecedented speed, often into entirely new geographic regions.

McKinsey estimates that companies will invest almost \$7 trillion in data center infrastructure globally by 2030, with more than 40% of that investment expected to be made in the United States. As capital deployment accelerates, so does the scale and complexity of the contractor and supplier ecosystem required to deliver it.

A modern data center depends on hundreds of specialist organizations throughout its lifecycle. During construction they deliver highly technical infrastructure under intense schedule pressure. Once operational, a different ecosystem of maintenance providers, engineers and specialist contractors

becomes essential to keeping critical infrastructure running.

Historically, contractors were often viewed as external service providers supporting construction and maintenance activities. Today, their role has become integral to the resilience and availability of digital infrastructure. As data centers become increasingly complex, contractor capability, reliability and operational resilience have a direct influence on the continuity of the digital services that modern economies depend upon.

Each phase introduces different risks, but both rely on one common capability: continuous visibility across the supply chain.

The Critical Role of Supply Chains in Data Center Resilience

The rapid growth of artificial intelligence, cloud computing and digital services is driving one of the largest infrastructure expansion programs in recent history. Across North America, Europe and Asia-Pacific, data center owners and operators are investing billions of dollars in new data center capacity to meet unprecedented demand for compute power.

Today's facilities are also becoming significantly larger and more complex. Only a few years ago, facilities requiring around 20–30 MW of power were widely regarded as large-scale developments. Today, hyperscale campuses are increasingly being designed to support 100 MW or more, with several announced projects planned at several hundred megawatts. These projects require extensive civil engineering, specialist electrical infrastructure, advanced cooling systems, high-voltage connections, backup power generation and sophisticated physical and cyber security, all delivered to compressed timescales. This is also a

high-consequence safety environment. US labor data compiled by the Electrical Safety Foundation International shows that construction accounted for 907 of the 2,070 occupational electrical fatalities recorded between 2011 and 2024.

At the same time, the availability of suitable land and power is reshaping where data centers are built. Rather than concentrating solely in established technology hubs, operators are increasingly expanding into secondary and emerging markets where power availability, planning conditions and development costs may be more favorable. JLL reports that 64% of the 35 GW of data center capacity under construction in North America is now located in “frontier markets” outside established hubs. West Texas, Tennessee, Wisconsin and Ohio are among the principal beneficiaries of this geographic shift. At the same time, 92% of North American capacity under construction is already precommitted. JLL identifies this as either binding leased capacity or owner-occupied hyperscale development.



35+ GW of new capacity is under construction across North America, against 39 GW already active.

This expansion is occurring against a backdrop of persistent labor shortages across the construction and engineering sectors. Demand for experienced electricians, commissioning engineers, mechanical specialists and other skilled trades continues to outpace supply, increasing competition for qualified contractors and placing additional pressure on project delivery. As a result, organizations frequently rely on extensive networks of subcontractors and specialist suppliers to meet program deadlines, creating increasingly complex supply chains that can be difficult to oversee effectively.

The challenge extends beyond construction. Once a facility becomes operational, maintaining continuous availability depends on a different but equally critical ecosystem of suppliers. Maintenance contractors, facilities management providers, generator and UPS specialists, cooling engineers, fire protection contractors, security providers

and network infrastructure partners all play an essential role in supporting operational resilience. Many of these organizations operate across multiple sites, with changing personnel, subcontractors, certifications and insurance arrangements throughout the life of the asset.

For data center operators, uptime is the ultimate measure of performance. Every contractor working on critical infrastructure has the potential to influence operational resilience, whether through the quality of installation during construction or the reliability of maintenance activities once the facility is live. As contractor networks expand, maintaining visibility into supplier qualifications, financial resilience, insurance, compliance and subcontractor relationships becomes increasingly difficult using manual processes or periodic reviews alone.

Unlike many infrastructure projects, supplier risk does not end once construction finishes. It simply changes.

Risk Environment One: Construction

Complex projects depend on specialist contractor networks

Building a modern data center requires the coordinated delivery of thousands of activities across a complex network of contractors, suppliers and specialist subcontractors. From groundworks and structural engineering to high-voltage electrical systems, mechanical services, cooling infrastructure, fire protection, security, fiber installation and commissioning, every phase depends on specialist expertise being delivered safely, compliantly and to schedule.

Unlike many large infrastructure projects, data center construction operates under exceptional commercial pressure. Capacity cannot come online quickly enough to satisfy demand, creating compressed delivery schedules and leaving little room for delay. At the same time, shortages of skilled labor often require organizations to engage multiple specialist contractors and subcontractors simultaneously, increasing the complexity of supplier oversight.

Every contractor introduces a new risk profile

Each new contractor introduces its own risk profile. Organizations must ensure appropriate qualifications, certifications, insurance, financial stability and regulatory compliance before work begins, while maintaining confidence that these

requirements remain valid throughout the project. As projects evolve, contractors may appoint additional subcontractors, insurance policies may expire or change, key personnel may be replaced and suppliers may experience financial difficulties. Any of these changes can introduce operational or commercial risk if they go undetected.

Visibility becomes fragmented as projects scale

As contractor ecosystems grow, visibility often becomes fragmented. Information is distributed across procurement teams, project managers, health and safety functions, facilities teams and external delivery partners, with records maintained in spreadsheets, email chains and local systems. While each team may have visibility into part of the picture, few organizations maintain a single, continuously updated view of contractor assurance across the entire program.

Construction risk quickly becomes program risk

The consequences extend far beyond administrative inefficiency. A contractor unable to access site because qualifications have expired, a supplier entering financial distress during a critical phase of construction or an uninsured subcontractor involved in a workplace incident can all disrupt project delivery. The constraint is particularly acute in specialist trades. The

US Bureau of Labor Statistics projects approximately 81,000 electrician openings each year over the 2024–2034 period, including openings created by workforce exits and occupational transfers. Delays to specialist trades frequently have a cascading effect on subsequent activities, increasing program costs, delaying commissioning and extending the time before valuable computing capacity becomes operational.

These pressures are already affecting delivery. JLL reports that more than half of data center projects experienced delays in 2025, reinforcing the need for realistic delivery buffers and stronger oversight of the supply chains behind each build. McKinsey analysis suggests that supply chain shocks can erode almost 45% of one year's EBITDA over a decade, while a single prolonged production disruption may cost 30–50% of a year's EBITDA. In large-scale data center projects, where specialist contractors can be difficult to replace and commissioning activities follow tightly sequenced programs, even relatively small disruptions can have disproportionate commercial consequences.

These risks are becoming more common as contractor networks expand. Achilles' 2025 Risk and Sustainability Survey found that 31% of organizations experienced supplier financial failure or distress affecting their supply chain within the previous 12 months, highlighting the growing importance of continuously monitoring

supplier resilience rather than relying solely on due diligence at the point of onboarding.

For construction leaders, the challenge is no longer simply qualifying contractors before work begins. It is maintaining confidence that every organization working across the project remains compliant, financially resilient and capable of delivering throughout the build. Achieving that level of assurance requires visibility that is continuous rather than periodic, enabling emerging risks to be identified before they affect program delivery.

IN PRACTICE

Supporting hyperscale data center operations

This challenge is already being recognized by leading hyperscale operators. As contractor ecosystems become larger and more geographically dispersed, maintaining continuous visibility into supplier assurance is becoming a strategic capability rather than an administrative exercise. Achilles supports organizations such as Google in managing complex contractor ecosystems across their global data center operations, helping maintain confidence in supplier compliance and operational readiness.

Risk Environment Two: Operational Resilience

Construction ends. Operational risk begins.

Completing construction marks the beginning of a new supply chain challenge rather than the end of one. Once a data center becomes operational, the focus shifts from delivering infrastructure to maintaining continuous availability. While the contractors involved may change, the need for effective supplier oversight becomes even more critical.

Critical facilities depend on specialist service providers

Operational data centers depend on a broad ecosystem of specialist service providers working across highly sensitive environments. Uptime Institute’s 2025 staffing survey found that 42% of respondents identified hiring new staff as one of their organization’s greatest challenges, based on 864 respondents. These include facilities management providers, electrical and mechanical maintenance contractors, UPS and generator specialists, cooling engineers, fire protection and suppression experts, security providers, network infrastructure partners, fuel suppliers and specialist OEM service engineers. Together, they perform the maintenance, inspections and repairs that protect the resilience of critical infrastructure.

Operational risk changes continuously

Unlike construction projects, where contractor relationships are often temporary, operational supplier relationships may continue for decades. Contractors regularly return to site to undertake planned maintenance, respond to incidents or support infrastructure upgrades. Personnel change, subcontractors are introduced, certifications expire, insurance policies are renewed and financial circumstances evolve. Every change has the potential to affect operational resilience if it is not identified and managed.

The consequences of poor visibility are also fundamentally different. During construction, supplier failures may delay project completion or increase program costs. Once a facility is live, the same failures can directly affect business continuity. An inadequately qualified contractor working on critical electrical infrastructure, an uninsured maintenance provider involved in a workplace incident or a financially distressed supplier unable to fulfill contractual obligations can all introduce operational disruption, increase safety risks and compromise service availability.

These risks are becoming increasingly significant as operators expand

Human error plays some role in approximately two-thirds of data-center outages, based on 25 years of Uptime Institute data.

Approximately **one in ten** respondents said their most recent outage had a serious or severe impact.

In Uptime Institute’s 2026 analysis, 57% of respondents said their most recent major outage cost more than **\$100,000**, while one in five said it cost more than **\$1 million**.

Uptime Institute reports that **external infrastructure failures** are becoming more prominent in publicly reported outages, while outages linked to fiber and connectivity are rising and are more likely to cause **extended disruption**.

geographically and standardize operations across multiple facilities. Contractor populations grow over time, with many suppliers working across several sites, business units and regions. Maintaining confidence that every contractor remains appropriately qualified, insured, financially resilient and compliant becomes progressively more difficult when information is fragmented across different systems, departments and local teams.

Traditional assurance processes were not designed for this level of complexity. Annual reviews provide only a snapshot of supplier compliance at a single point in time, yet operational risk continues to evolve every day. Insurance cover can lapse, financial performance can deteriorate, regulatory status can change and new subcontractors can be introduced long before the next scheduled review takes place. Organizations relying on periodic assessments may therefore remain unaware of emerging risks until they have already affected operations.

For organizations responsible for critical

infrastructure, operational resilience depends not only on the reliability of physical assets but also on the resilience of the organizations responsible for maintaining them. Continuous visibility into contractor qualifications, financial health, insurance, compliance and supply chain relationships enables operators to identify changes as they occur, allowing corrective action to be taken before operational performance is affected.

Business continuity depends on supplier resilience

As data centers continue to support increasingly critical digital services—from AI workloads and cloud platforms to financial systems, healthcare and telecommunications—the resilience of the operational supply chain is becoming a strategic capability. Organizations that can continuously monitor and understand their contractor ecosystem are better positioned to reduce disruption, protect uptime and maintain confidence in the long-term performance of their facilities.

Managing Dynamic Supply Chain Risk

Supplier risk doesn't stand still

Traditional contractor assurance was designed for a very different operating environment. When projects were smaller, contractor networks were relatively stable and supply chains changed gradually, annual qualification reviews and periodic compliance checks provided a reasonable level of assurance.

Today's data center environment is fundamentally different. Organizations are managing larger contractor populations across multiple sites, engaging specialist suppliers for increasingly complex work and operating facilities where uninterrupted availability is business critical. In this environment, supplier risk evolves continuously rather than annually.

Throughout both the construction and operational lifecycle, contractor profiles are constantly changing. New suppliers are appointed, subcontractors are introduced, insurance policies are renewed or allowed to lapse, financial health fluctuates, regulatory requirements evolve and key

personnel move between organizations. Every change has the potential to alter a supplier's risk profile, often long before the next scheduled review.

Static assurance creates operational blind spots

Periodic reviews provide only a snapshot of contractor assurance at a single point in time. They confirm that a supplier met the required standards on the day it was assessed but offer little insight into what may have changed since. Workforce continuity is part of this changing risk picture. Uptime Institute's 2025 staffing research found that junior and mid-level operational roles had the highest reported turnover rates, particularly among colocation providers.

As contractor ecosystems grow, these gaps become increasingly difficult to manage. Information is often distributed across procurement, project delivery, facilities management, health and safety, compliance and finance teams, with each

function maintaining its own records and processes. Without a continuously updated view, organizations may be unaware that a contractor's insurance has expired, a critical certification has lapsed or a key supplier is showing signs of financial distress until those changes begin to affect project delivery or operational performance.

The challenge is compounded by the pace of change within the data center sector. Facilities are expanding, infrastructure is being upgraded more frequently and contractors often work across multiple projects and operational sites simultaneously. The more dynamic the supply chain becomes, the less effective static assurance processes become.

From periodic assurance to continuous supplier intelligence

Leading organizations are recognizing that contractor assurance should no longer be viewed as a point-in-time compliance exercise but as an ongoing risk management capability.

Rather than asking, *"Was this contractor compliant when they joined the project?"*, organizations increasingly need to ask, *"What has changed since then?"*

Continuous visibility enables emerging risks to be identified as they develop rather than after they have disrupted a project or affected operations. It allows organizations to monitor changes in contractor qualifications, insurance, financial resilience, compliance status and subcontractor relationships throughout the supplier lifecycle, providing decision-makers with a current understanding of where risk is increasing and where intervention may be required.

For organizations building and operating critical infrastructure, this represents a fundamental shift in approach. Contractor assurance is no longer simply about verifying documentation; it is about maintaining continuous confidence that the organizations responsible for delivering and supporting critical facilities remain capable, compliant and resilient.

From Supplier Assurance to Continuous Supply Chain Intelligence

The rapid expansion of data center infrastructure is reshaping how organizations think about supplier risk. As facilities become larger, more complex and increasingly critical to the global digital economy, managing contractors and suppliers is no longer simply an operational or compliance activity. It has become a fundamental component of organizational resilience.

Historically, contractor assurance has focused on collecting documentation, verifying suppliers during onboarding and conducting periodic reviews to demonstrate compliance. While these activities remain essential, they were designed for supply chains that were relatively stable and changed slowly. Today's data center environments are fundamentally different.

Throughout the lifecycle of a data center, the supplier ecosystem is continuously evolving. During construction, new contractors, subcontractors and specialist suppliers are introduced as projects progress. Once operational, maintenance providers, engineering partners and critical service contractors continue to change

through personnel movements, contract renewals, organizational restructuring and shifting financial circumstances. At the same time, supplier risk itself is constantly changing. Financial performance fluctuates, insurance policies expire, cyber threats emerge, regulatory requirements evolve, geopolitical events disrupt supply networks and new subcontractors enter the supply chain. Viewed individually, these changes may appear manageable. Viewed collectively, they create a dynamic picture of supplier resilience that can significantly influence operational performance.

This requires organizations to move beyond maintaining approved supplier lists or periodically reviewing contractor documentation. They need confidence that suppliers remain qualified, financially resilient, appropriately insured and operationally capable throughout the duration of their engagement. Achieving that confidence depends upon maintaining continuous visibility across the supplier ecosystem, enabling emerging risks to be identified before they affect project delivery, operational performance or business continuity.

Leading organizations are therefore evolving from traditional supplier assurance towards continuous supply chain intelligence. Rather than viewing financial health, insurance, contractor competence, cyber risk, ESG performance, audits, adverse media and geopolitical exposure as separate compliance activities, they are bringing these signals together to develop a continuously updated understanding of supplier resilience. This enables procurement, operations, facilities management, health and safety and compliance teams to work from a shared understanding of supplier risk, prioritize interventions more effectively and make better-informed operational decisions.

As investment in data centers continues to accelerate, this capability will become an increasingly important source of competitive advantage. The organizations best positioned for long-term success will not simply build facilities more quickly or operate them more efficiently. They will develop supply chains that are transparent, resilient and continuously understood—recognizing that resilient data centers ultimately depend upon resilient supplier ecosystems.



Five Questions Every Data Center Operator Should Be Able to Answer

Building resilient data centers requires more than resilient infrastructure. It requires continuous confidence in the organizations that build, maintain and support it. These five questions provide a simple test of supply chain resilience.

1



Do we know every organization working across our critical infrastructure?

Visibility should extend beyond primary contractors to include subcontractors, specialist suppliers and service providers across construction and operations.

2



Can we be confident they remain qualified, insured and compliant today?

Supplier assurance is not a one-time activity. Certifications, insurance, financial health and regulatory compliance all change over time.

3



Do we understand which suppliers represent our greatest operational risk?

Not every supplier is equally critical. Organizations should understand where dependency exists and where supplier failure would have the greatest operational impact.

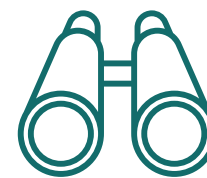
4



How quickly can we respond when our supplier landscape changes?

New contractors, changing regulations, financial distress and workforce shortages require organizations to adapt without compromising governance or delivery.

5



Can we identify emerging supplier risks before they become operational disruptions?

The most resilient organizations don't simply respond to disruption—they recognize changing risk profiles early enough to act before projects or operations are affected.

If any of these questions cannot be answered confidently, there may be hidden risks within your supply chain that are difficult to identify through periodic assurance alone.

The Future of Supply Chain Resilience

The infrastructure supporting this growth—from power generation and transmission to cooling systems, construction and specialist suppliers—is becoming increasingly critical and interconnected. The International Energy Agency expects global data center electricity demand to exceed 945 TWh by 2030. In the United States, data centers are projected to account for almost half of electricity-demand growth over the same period.

The next generation of data centers will require more than technical capability and investment to deliver successfully. As projects become larger, timelines become more compressed and supplier ecosystems become more complex, effective management of contractors and suppliers will become an increasingly important factor in successful delivery and ongoing operations.

As AI drives demand for larger campuses, geographic expansion and greater operational complexity, supply chain resilience is becoming an important consideration alongside power availability, physical security and network connectivity.

Organizations that have greater visibility into supplier capability, risk and performance will

be better positioned to manage disruption, maintain uptime and support sustainable growth.

The resilience of future data centers will depend not only on the reliability of their physical infrastructure, but also on the strength and resilience of the supply chains that support them.

See how Achilles helps data center operators strengthen supply chain resilience

Achilles enables this approach by bringing together multiple sources of supplier intelligence, including financial health, insurance, compliance, contractor competence, ESG, cyber risk, audits, adverse media and geopolitical exposure, to provide organizations with a continuously updated understanding of supplier risk across the entire data center lifecycle.



Sources

1. McKinsey & Company, *The Data Center Balance: How US States Can Navigate the Opportunities and Challenges*, 8 August 2025. [View source \[mckinsey.com\]](#)
2. McKinsey & Company, *Scaling Bigger, Faster, Cheaper Data Centers with Smarter Designs*, 1 August 2025. [View source \[mckinsey.com\]](#)
3. JLL, *North America Data Center Report: Year-end 2025*, 17 February 2026. [View source \[jll.com\]](#)
4. JLL, *2026 Global Data Center Market Outlook*, 5 January 2026. [View source \[jll.com\]](#)
5. Uptime Institute, *Annual Outage Analysis 2026: The Causes and Impacts of IT and Data Center Outages*, May 2026. [View report \[datacenter.uptimeinstitute.com\]](#)
6. Uptime Institute, *Outages: Understanding the Human Factor*, 8 June 2022. [View source \[journal.uptimeinstitute.com\]](#)
7. Uptime Institute, *Data Center Staffing and Recruitment Survey 2025: Staffing Crisis Persists as Colos Struggle to Retain Junior Operators*, October 2025. [View report \[intelligence.uptimeinstitute.com\]](#)
8. International Energy Agency, *Energy and AI: AI Is Set to Drive Surging Electricity Demand from Data Centers*, 10 April 2025. [View source \[iea.org\]](#)
9. Electrical Safety Foundation International, *Workplace Injury and Fatality Statistics: 2011–2024*, published 5 March 2026, using data from the US Bureau of Labor Statistics and Occupational Safety and Health Administration. [View source \[esfi.org\]](#)
10. Achilles, 2025 Risk and Sustainability Survey.



Address

Achilles Information, LLC.,
5271 California Ave, Suite 290
Irvine, CA 92617



Email

enquiries@achilles.com



California

+1 949 899 6850



Texas

+1 281 809 4400



Web

www.achilles.com