

Unlocking the digital infrastructure opportunity:

Protecting capital and enabling growth

MARSH

Table of contents

03 **Foreword**

04 **A complex risk ecosystem**

07 **Comprehensive risk insight:** Novel risks demand novel solutions

09 **Capital enablement**: Navigate complexity with clarity

11 **Resilience building strategies:** Unlock capital and build lasting resilience

13 **Protecting capital and enabling growth**

14 **Why work with Marsh?**

Foreword

Digital infrastructure is the backbone of the global economy. Like a utility, it supports everything from contactless payments to next-generation AI models and is increasingly integrated into critical systems like healthcare and energy.



Michael Mathews

Global Digital Infrastructure Practice Leader

While data centers are the core of digital infrastructure, the ecosystem extends far beyond the walls of any single facility: Fiber and wireless networks, enabling technologies, advanced cooling and battery systems, and a rapidly expanding service sector of mission-critical contractors. All of them must work together seamlessly to meet an unprecedented surge in demand.

By 2030, an estimated US$3 trillion will be invested in digital infrastructure worldwide – around one-third in brick-and-mortar data centers and the rest in enabling equipment, infrastructure, and services. Even as the first shovels hit the ground, the ecosystem is innovating in real time. Energy providers are building dedicated plants for data centers and on-site battery backup systems. Contractors are retrofitting older sites to bring 'edge' infrastructure closer to end-users.

This represents a golden opportunity for the whole ecosystem. But the sheer scale of the capital involved and the pace of technological evolution can accelerate the velocity of risk. Contracts may include ever more stringent service-level agreements and severe penalties for downtime; builders risks are changing as construction and operations overlap; the networking of on-site hardware can leave facilities more vulnerable to cyber-attacks. Many operational teams in this vital industry are forced to navigate a labyrinth of overlapping risk exposures.

In this report, we outline our ecosystem-wide approach to digital infrastructure risk management. Our goal is to help you navigate a complex landscape of interconnected and accelerating risks with more clarity, to better protect your capital and work together with the goal of making all the pieces fit.

A complex risk ecosystem

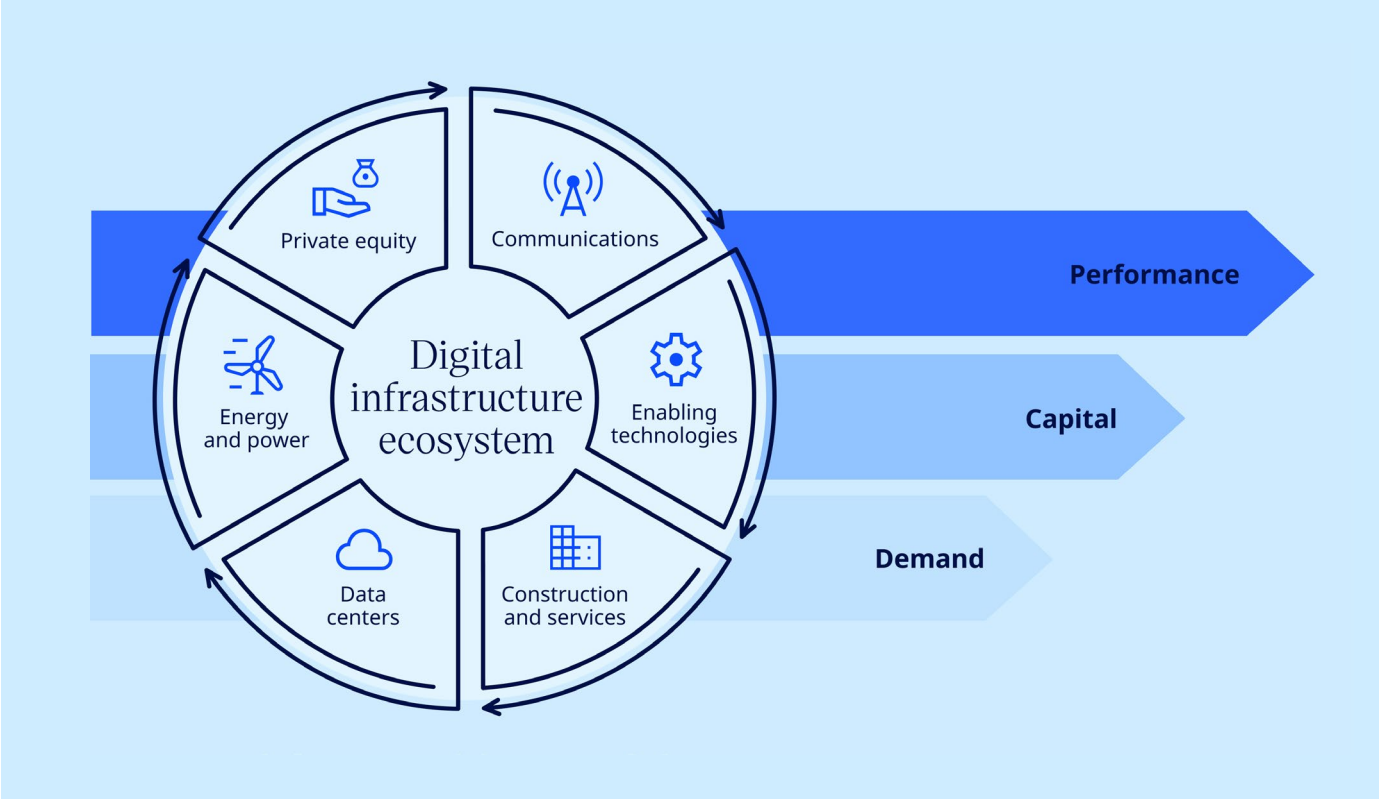
Global data consumption is surging. The world is in the midst of a boom in AI, machine learning and cloud computing. All of this is fueling an unprecedented demand for the digital infrastructure that underpins these technological leaps. Trillions of dollars will be invested globally to build and sustain what is emerging as a critical backbone of the exponentially expanding digital and data economies.

Competition is fierce and growing. In the US alone, overall digital infrastructure transaction volumes nearly doubled year-on-year between 2024 and 2025. This is opening up countless opportunities, but can also accelerate the velocity of risk.

The digital infrastructure ecosystem

Digital infrastructure is far broader than the data centers that dominate headlines. It is an interconnected web of enabling technology manufacturers (chips, racks, servers, cooling systems), telecommunications networks (wireless, fiber, subsea cables), power and energy providers, construction and mission-critical contractors, cloud and hosting platforms, as well as the investors and lenders who fund them.

All of these stakeholders are scaling and innovating in parallel to support high-performance AI and cloud workloads. At the same time, all depend on one another to deliver the near-instant, always-on services that many businesses and consumers now expect.





This is why Marsh considers digital infrastructure a "new utility": It increasingly underpins how we live and work, so customers can expect levels of reliability that are on par with electricity and water.

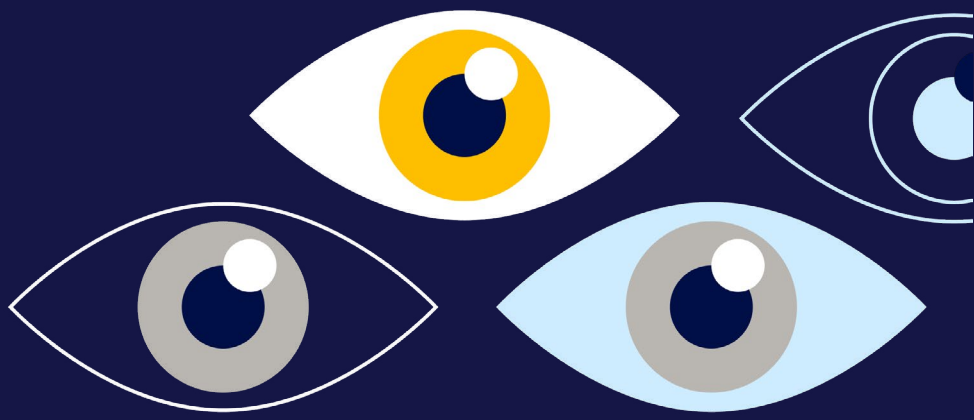
Investors, developers and operators are scrambling to meet insurance requirements and manage increasingly challenging and novel exposures, including stricter indemnifications obligations, severe delay in startup or downtime penalties, and more stringent lender requirements. How can stakeholders future-proof their investment and capitalize on the opportunities ahead, while minimizing their risks?

Derisking growth through risk management and insurance

In today's competitive environment, success can be defined by speed to market, resiliency, and capital efficiency. The digital infrastructure opportunity awaits investors and operators that can derisk innovation and unlock growth. Insurance can be a key enabler.

Those that can demonstrate strong risk and capital management tend to be more likely to secure better financing terms and lower borrowing costs. Tools like surety guarantees, for example, can free up cash for growth rather than locking it in collateral, which may free capital that can be reinvested to support faster expansion. But considering the diversity of players and breadth of risks throughout acquisition, development and operation, the sector needs broader and more technically complex insurance than ever before.

End-to-end visibility across the digital infrastructure ecosystem may be essential to better future-proof investments and optimize performance. Understanding interconnected risks can enable owners and developers to *better anticipate* vulnerabilities and implement integrated mitigation strategies that can support overall resiliency and sustainable growth.



Comprehensive risk insight:

Navigate complexity with clarity

Digital infrastructure is delivered by an interdependent web of entities. Challenges for any one participant or stakeholder can affect the delivery and long-term profitability of the entire project. In this high-stakes interconnected risk landscape, end-to-end visibility and expertise across the entire ecosystem is pivotal.

The risk lifecycle

The lifecycle of a digital infrastructure project typically breaks down into three key phases: Acquisition and agreement, development, and ongoing operations. Each comes with its own set of risks that may materialize further down the line. At acquisition, for example, construction, power purchase agreements (PPAs), and financing agreements often lock in dates for commercial operation and uptime commitments, with penalties for delay in start-up or downtime. If agreements for factors like equipment supply, cloud hosting and, above all, utility and interconnection do not impose the same obligations, each party can leave themselves exposed. The global technology supply chain, for instance, is extremely competitive, and can be vulnerable to periodic geopolitical disruptions, shock events, and raw material shortages.

Any hiccups could have dramatic impacts. Businesses across the digital infrastructure ecosystem could potentially face liquidated damages and reputational hits when delays or outages occur, with limited recourse to counterparties.

At least 2000 new facilities are planned to be built in the next five years and many more will need retrofitting to meet modern demands. 'Mission-critical' contractors are pulled into work on highly specialized sites with cutting-edge equipment on tight timelines, and increasingly taking responsibility for processes like power interconnections and the installation

Digital infrastructure project lifecycle

Key areas of risk



Acquisition and agreement

• Contract review • Surety agreements • Due diligence • Liability management • Project design • Capital • Land, power, development partners • Tenants • Talent acquisition



Development

• Builders risk • Project management • Transition to operational • Contractor governance/controlled risk • Power development and interconnect • Equipment protection and logistics management



Operations

• Property management • Resiliency • Governance • Business interruption prevention • Service-level agreements • Liability and mission critical contractors • Talent growth and retention

of coolant systems and batteries. Supply chain bottlenecks or specification changes can cause delays or force them into compromises that may lead to disruptions later on, shifting risk further down the asset lifecycle. As a result, operators and owners are increasingly taking out insurance policies intending to mitigate these cascading risks as breaches in service-level agreements (SLAs) could incur claims from tenants later on.

Indeed, risks remain prevalent once facilities are up and running. Aside from a host of property risks and exposures to material damages, owners/operators and tenants must remain vigilant to contractual complications. For instance, a cyber incident or failure in digital control systems can cascade quickly across interconnected assets, and may take down multiple sites or customers at once. The resulting outages or data breaches can link back to service agreements and investor expectations negotiated at acquisition, so a technical failure can influence asset valuations, refinancing and customer relations. Predicting and building resilience to these interlocking risks can be essential for digital infrastructure players, wherever they are in the ecosystem, to keep projects on track.

End-to-end visibility

Successfully managing these interconnected risks calls for comprehensive visibility across the ecosystem. By identifying and anticipating risks over the various phases of the asset lifecycle, owners, operators and investors may be able to set themselves up for success. Investors, for example, must manage capital allocation and tenant relationships, as well as conduct thorough due diligence – including warranty and indemnity protections. Going through these steps at the acquisition phase may help reduce risk early.

Silent demand

While new mega-campus projects dominate the headlines, there is a simultaneous surge in demand for smaller, localized facilities. The ‘edge’ data center market was already generating US$51 billion in 2025 – and that number is due to more than double by 2030.

This ‘silent demand’ represents a massive opportunity, but also a potentially risky one. Operators often have to work in live environments without disrupting ongoing operations, while integrating modern systems into aging infrastructure and navigating phased construction alongside active tenants. With such a high concentration of expensive, interconnected and sensitive assets all within a single site – from graphic processing units (GPUs) and servers to bespoke power and cooling systems – these data centers are stretching risk to builders in unprecedented ways. That level of complexity can require tailored risk management and insurance strategies.





Capital enablement:

Novel risks demand novel solutions

"SLA contractual risk is one of the top areas that digital infrastructure companies are discussing, as there is no standardized solution for it. Everything is being custom-created."

Tom Srail, Cyber Analytics and Digital Infrastructure Leader, Marsh

Ecosystem visibility and integrated expertise are the basis for building resilience in digital infrastructure. But how can businesses convert that into a comprehensive risk management strategy that addresses risk interdependencies, manages contractual complexities, and bolsters operational vulnerabilities with clarity and confidence? A range of insurance solutions have traditionally been available in the digital infrastructure space, but these are being stretched to breaking point.

Traditional insurance solutions – builders risk insurance, property and casualty coverage, contractor-controlled and owner-controlled insurance programs (CCIPs and OCIPs) – can be integral to protecting physical assets and liabilities during construction and operation. Yet mega-campuses go far beyond the risk profile of past digital infrastructure projects that may have been covered by operator property capacity insurance (OPCI). With GPUs, power supply, battery backup, cooling equipment and other assets all under one roof – and increasingly owned by a single entity – multiple losses can aggregate and hit owners/operators in one blow.

Similarly, data center owners/operators, cloud hosting providers, and telecommunications companies have historically purchased technology errors and omissions (tech E&O) insurance. But the digital infrastructure space is being shaped in real time by rapid innovation. And, currently, none of these 'off the shelf' solutions are broad enough to cover the multitude of novel risks investors, developers, owners and operators are now exposed to.



Cyber risk is often misunderstood in the digital infrastructure ecosystem. In almost every other industry, it primarily concerns data protection and privacy. But in digital infrastructure, it means resiliency: Keeping systems running securely and efficiently.

In this context, cyber insurance's main function is to mitigate the risk of system breaches and outages, whether caused by malicious actors, software failures, or compromised operational technology (OT). This includes threats to critical components and controls: Power distribution units (PDUs), cooling systems, building management systems, biometric access, and battery backup systems – all of which are networked and vulnerable to cyber incidents.

Essentially, that means even when they do not handle data directly, providers could potentially be held liable for contractual risks with tenants if a cyber-attack interferes with SLA obligations. For example, a cyber-attack that takes over ambient temperature controls or power management can trigger the same catastrophic outages and multi-million-dollar SLA penalties as a physical equipment failure.

As digital infrastructure owners increasingly hire third-party mission-critical contractors to manage operations, cyber risk can ripple through the value chain to parties that may not have traditionally been exposed to it.

Take SLA risk as an example. Data center tenants expect 24/7, year-round service, with only minutes of downtime – whether due to power outages, cooling system failures or software bugs – allowed per year. Many SLAs include stricter conditions with harsher penalties for downtime or delayed start-up, leaving contractors with far greater and more diverse risk exposures than ever before. Digital infrastructure companies are, in turn, trying to build resiliency against these mounting risks but finding a lack of insurance options available.

Historically, contractual obligations – especially liquidated damages clauses – have been explicitly excluded from insurance policies such as tech E&O or CCIP, because insurers do not want to provide coverage for risks which an SLA stipulates are voluntarily assumed by two private parties. Yet the scale of SLA exposure is so great that Marsh is actively creating and shaping a new market for SLA-specific coverage in an effort to meet the demand. That entails working with underwriters to define coverage terms, quantifying exposures, and piloting innovative products intending to address risks insurers have traditionally declined.

Resilience building strategies:

Unlock capital and build lasting resilience



Long-term success in this dynamic industry may depend on the ability of owners, operators and investors to identify rapidly evolving risks and build resilient organizations capable of withstanding them.

Resiliency efforts should span all asset phases – from planning and construction to operations and ongoing management. They should also be broad enough and backed by sufficient expertise, enabling them to cover everything from revenue lifecycles to cash flow to contractual risk transfer. This is what could sustain competitive advantage over the full project lifecycle.

ARC lifecycle management: Marsh's integrated approach

Marsh's ARC (asset, revenue, contract) lifecycle management approach seeks to address the complex interplay between asset lifecycles, revenue streams, and contractual obligations in the digital infrastructure industry.

The asset lifecycle tracks physical infrastructure: Data halls, power systems, cooling equipment, and network connectivity. Each has defined technical lifecycles, maintenance schedules, and end-of-life planning requirements. Major technology providers, for example, produce GPU and server equipment with five to six-year lifespans, creating a continuous cycle of planning, procurement, deployment, refresh, and decommissioning that must be coordinated across portfolios.

Once sites are up and running, focus shifts from builders risk to property risk. Operators must maintain strict temperature and humidity conditions, shift from buried to above-ground cable connections with varying weather exposure, and enforce physical security aligned with the site's threat profile. Fire prevention also remains complex, with many large facilities still relying on water-based suppression, which poses a risk to sensitive electronic equipment. Even noise pollution can be problematic, especially for AI facilities that are significantly noisier than most data centers, and can be built right next to residential areas.



The revenue lifecycle is governed by tenant lease agreements, hyperscaler contracts, colocation arrangements and, increasingly, AI-driven workload commitments. Revenue timing, ramp schedules, renewal options, and expansion rights must align with physical infrastructure readiness and contractual service-level obligations to avoid costly mismatches.

The contract lifecycle adds further timing, performance, and penalty structures across both asset and revenue cycles. That includes SLAs with tenants, power purchase agreements with utilities, construction contracts with mission-critical contractors, equipment supply agreements, and financing covenants with lenders. Any misalignment – for example, failing to pass down delay penalties from tenants to contractors – can create unhedged risk that cascades through all three lifecycles.

ARC lifecycle management provides dynamic, coordinated oversight of these interdependencies, enabling owners and operators to maintain resilience as conditions change. This approach can be critical for large, multi-site portfolios where equipment refresh cycles, tenant churn, contract renewals, and refinancing events occur continuously and must be managed in tandem rather than as isolated events.

Traditionally, digital infrastructure owners and operators have needed bank letters of credit to sign performance security bonds for power purchase, equipment orders and other long-term agreements. But this can lock up millions of dollars at the exact moment they are needed for the rapid construction and expansion demanded in this fast-moving space.

Surety guarantees may offer a useful alternative. They can provide counterparties (utilities, landlords, suppliers, or public authorities) with the same assurance that performance obligations will be met, but without forcing developers to sequester cash or consume scarce credit lines. In effect, this can mean:

- Cost savings, since surety guarantees have no collateral requirements.
- Enhanced liquidity and cash flow, freeing up cash for developers to use for other projects.
- Reduced financial exposure, since surety guarantees may provide a clear, enforceable guarantee backed by highly rated insurers, which can be critical when dealing with large, complex projects involving billions of dollars in infrastructure investments.

Protecting capital and enabling growth

Ultimately, we all need to get this right. And while every deal is different, and we are moving at lightning speed, there are some core risk management tools we should be thinking through and/or consistently leveraging throughout the digital infrastructure lifecycle:



Acquisition and agreement phase – While core property, casualty, and executive risk programs are standard, digging deep into SLAs, surety and credit alternatives, risk-informed site and design analysis, and conducting rigorous due diligence enables more effective risk mitigation.

Development phase – Builders risk and owner-controlled programs are considered standard. However, with rising penalties for delays, and overlapping builds across many campuses, it is prudent to also:

- ☐ Secure adequate delay in startup coverage.
- ☐ Ensure that builders risk programs transition seamlessly to provide coverage for operational exposures.
- ☐ Include sufficient protection for supply chain risks.

This additional diligence can be the difference between uncovered roadblocks and resilient development.

Operational phase – Operational success often pivots on a deep understanding of the contract, revenue, and contract lifecycle. Predictability and resilience across physical, digital, performance, contracts, and stakeholder expectations demands that every part of the ongoing cycle is protected against off-strategy risks.

As the unprecedented demand for digital infrastructure continues to grow at a fast clip, managing interdependent risks requires an ecosystem-wide approach that spans the lifecycle of digital infrastructure assets, addressing revenue and contract-related challenges. Successful risk mitigation strategies will often depend on end-to-end visibility, robust risk management strategies, and tailored insurance solutions that effectively address risks as they arise and enable owners/operators to focus on capitalizing on opportunities.

Why work with Marsh?

Marsh currently works with 75% of the top 25 companies engaged in data centers and are a partner to 10 of the largest global technology companies by revenue.
Our dedicated digital infrastructure integrates our extensive experience with energy providers — including grid, nuclear, and renewables — and deep relationships with contractors, private equity investors, and technology suppliers into one seamless practice.

We support clients throughout their lifecycle with proven supply chain and cyber resilience strategies, as well as innovative capital solutions that have unlocked hundreds of millions of dollars in capital. Let us help you in your quest to navigate complexity, protect your capital, and accelerate growth — every step of the way.

Marsh currently works with

75%

of the top 25 companies engaged in data centers and are a partner to 10 of the largest global technology companies by revenue



MARSH

About Marsh Risk

Marsh Risk is a business of Marsh (NYSE: MRSH), a global leader in risk, reinsurance and capital, people and investments, and management consulting, advising clients in 130 countries. With annual revenue of $27 billion and more than 95,000 colleagues, Marsh helps build the confidence to thrive through the power of perspective. For more information about Marsh Risk, visit marsh.com, or follow us on LinkedIn and X.

This document and any recommendations, analysis, or advice provided by Marsh (collectively, the "Marsh Analysis") are not intended to be taken as advice regarding any individual situation and should not be relied upon as such. The information contained herein is based on sources we believe reliable, but we make no representation or warranty as to its accuracy. Marsh shall have no obligation to update the Marsh Analysis and shall have no liability to you or any other party arising out of this publication or any matter contained herein. Any statements concerning actuarial, tax, accounting, or legal matters are based solely on our experience as insurance brokers and risk consultants and are not to be relied upon as actuarial, tax, accounting, or legal advice, for which you should consult your own professional advisors. Any modeling, analytics, or projections are subject to inherent uncertainty, and the Marsh Analysis could be materially affected if any underlying assumptions, conditions, information, or factors are inaccurate or incomplete or should change. Marsh makes no representation or warranty concerning the application of policy wording or the financial condition or solvency of insurers or reinsurers. Marsh makes no assurances regarding the availability, cost, or terms of insurance coverage. Although Marsh may provide advice and recommendations, all decisions regarding the amount, type or terms of coverage are the ultimate responsibility of the insurance purchaser, who must decide on the specific coverage that is appropriate to its particular circumstances and financial position.

1166 Avenue of the Americas, New York 10036.

Copyright © 2026 Marsh. All rights reserved.