

MARSH

Financing the digital infrastructure buildout: Credit and political risk solutions across the value chain



How Marsh's Credit Specialties strategies can protect and better enable access to capital during the AI and data center investment supercycle

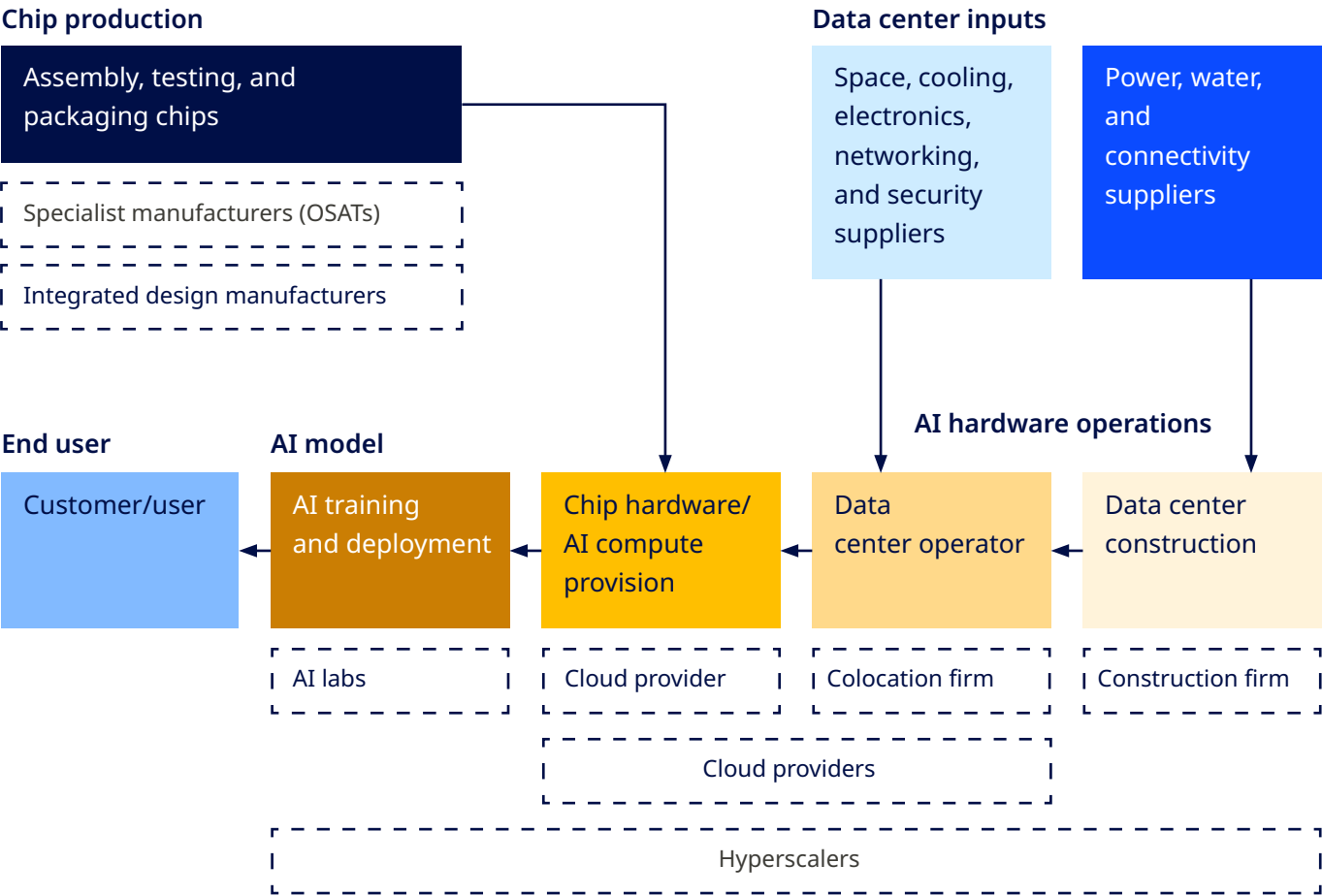
The AI and data center buildout reaches far beyond the companies at its center. Its risks extend across a global ecosystem of manufactures, suppliers, builders and financiers.

This complex ecosystem extends to many other corners and industries of the world:

- In the Netherlands, to the sole global supplier of extreme-ultraviolet lithography systems, whose own output depends on specialist optics, laser, and component manufacturers across Asia and Europe.
- To advanced foundries in Taiwan, whose packaging capacity binds accelerator shipments.
- To memory producers in South Korea, and server assemblers, networking-gear, and power-equipment suppliers with multi-year order books.
- Globally, to the construction and engineering firms building physical campuses and the utilities and independent power producers establishing grid connectivity.

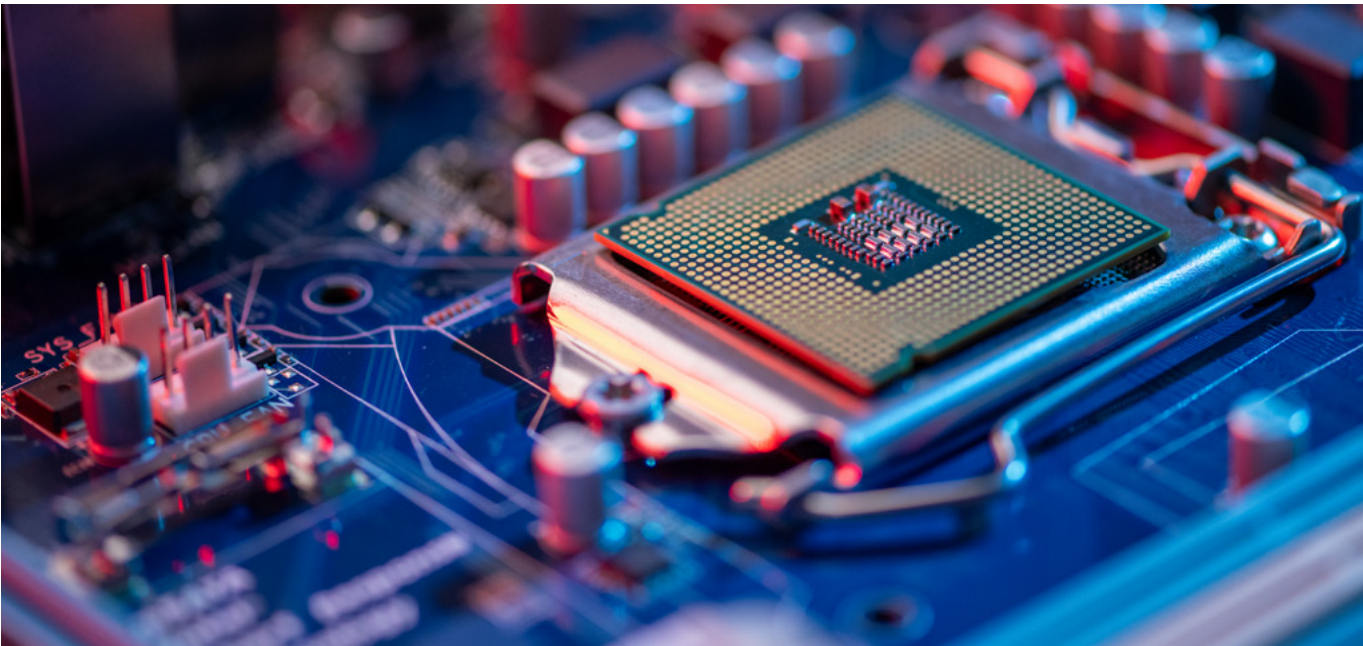


Figure 1: The AI infrastructure supply chain



Source: [OECD](#)

Note: This diagram provides a simplified overview of the key steps in the AI infrastructure supply chain. It does not cover other inputs to AI systems, such as data, algorithms, models, or know-how.



Across this complex global AI infrastructure value chain, businesses face two major challenges:

- Global demand is being driven by massive capital expense, which is being driven by high, but uncertain, [future revenue expectations from AI](#). If those expectations are not met, firms across the sector will be exposed to higher financial, performance, and political risks.
- [A growing financing gap](#) exists across parts of the digital infrastructure supply chain — in part because of these risks — where the capital needed to move projects forward is not always available on a desirable scale, timing, or terms.



Businesses contending with both challenges cannot necessarily afford to wait for greater certainty in future demand and the reduced risk that comes with it before committing their own capital. Just like with railroads in the 19th century or the dotcom boom of the early 2000s (see figure 2), companies across today's digital infrastructure supply chain will not want to miss out on the potentially historic growth and revenue opportunity or risk ceding market share to competitors.

However, and especially because most firms in the AI value chain will be less financially stout than the massive technology companies ultimately driving much of the demand, sustainably pursuing the substantial growth opportunities requires careful management of the financial risks involved and the use of available avenues to access capital.

This will be especially true should the capex bets of the largest technology companies disappoint. The resulting consequences may spread beyond the balance sheets of big tech and could include:

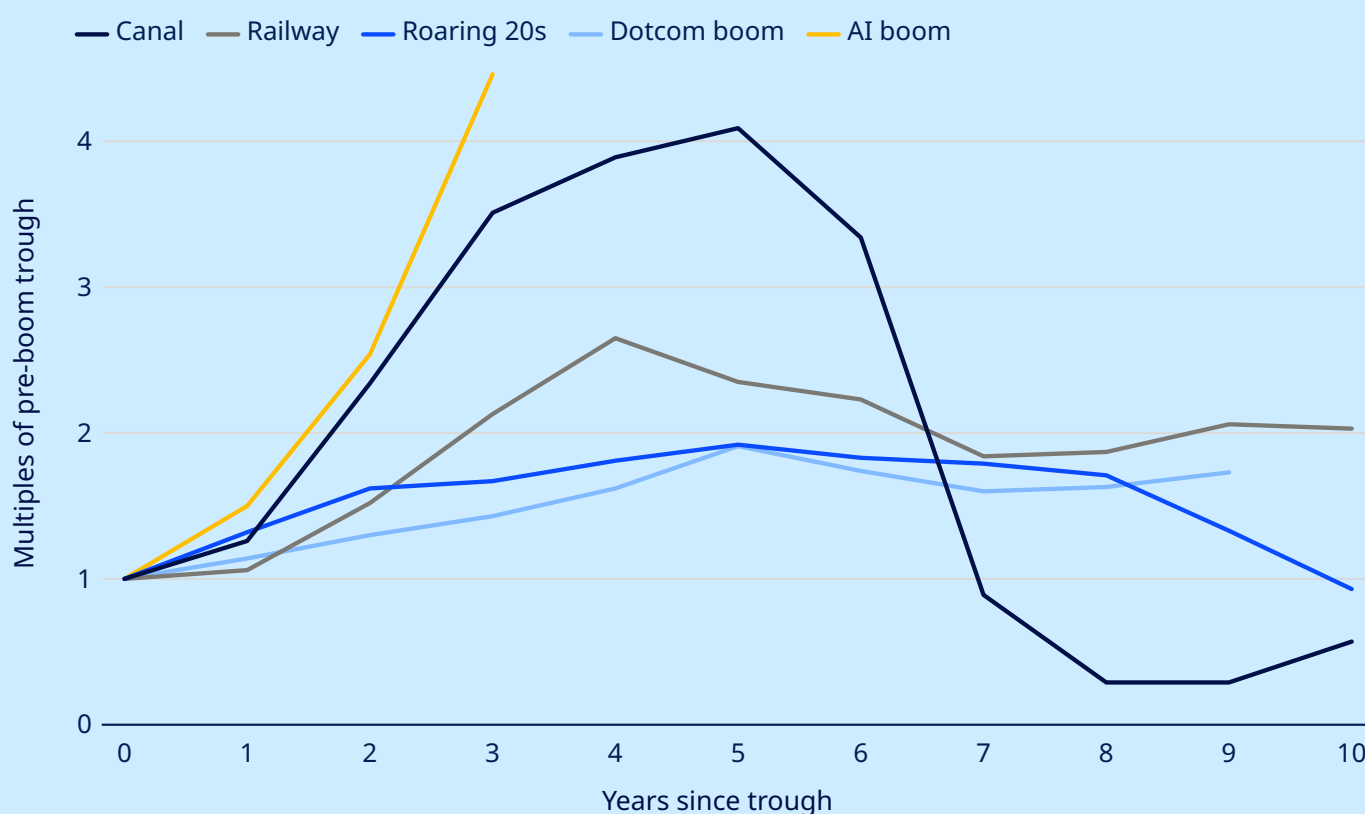
- Contracts across the digital infrastructure supply chain being terminated or renegotiated.
- Payments being delayed or going unmet.
- Anticipated orders failing to materialize.
- Inventory built against forecast demand being stranded.
- Host governments — having pursued investments for jobs, tax base, and strategic capacity — intervening.

The potential exposure for businesses engaged in this sector is financial, performance, and political.

The [Bank for International Settlements](#) (BIS) draws a parallel between the current buildout and other boom-bust cycles, encouraging businesses currently benefiting from growing digital infrastructure investment to consciously manage the downside, financial, counterparty, and political risks.

The BIS data shows the AI boom has already outpaced the canal, railway, 1920s stock market, and dotcom booms. By year two, AI investment had reached 2.54 times its pre-boom investment trough, against 2.34 for canals, 1.52 for railways, 1.62 for the Roaring Twenties, and 1.30 for dotcom. By year three, which in the case of AI was 2025, the multiple hit 4.46 — a rate of capital commitment without precedent. Earlier innovations eventually generated durable returns, but each cycle also produced overinvestment and financial distress among businesses that had committed capital ahead of demand. This is not a prediction that the buildout will fail. It is a reminder that capital is being committed at an unprecedented pace, and that firms across the value chain should plan for volatility.

Figure 2: Boom and bust cycles throughout major innovation periods



Source: [Bank for International Settlements](#)

The AI and digital infrastructure risk landscape

While these risks are detailed separately below, each can amplify the others, with effects that spread across the value chain to counterparties far removed from where the risk originates.

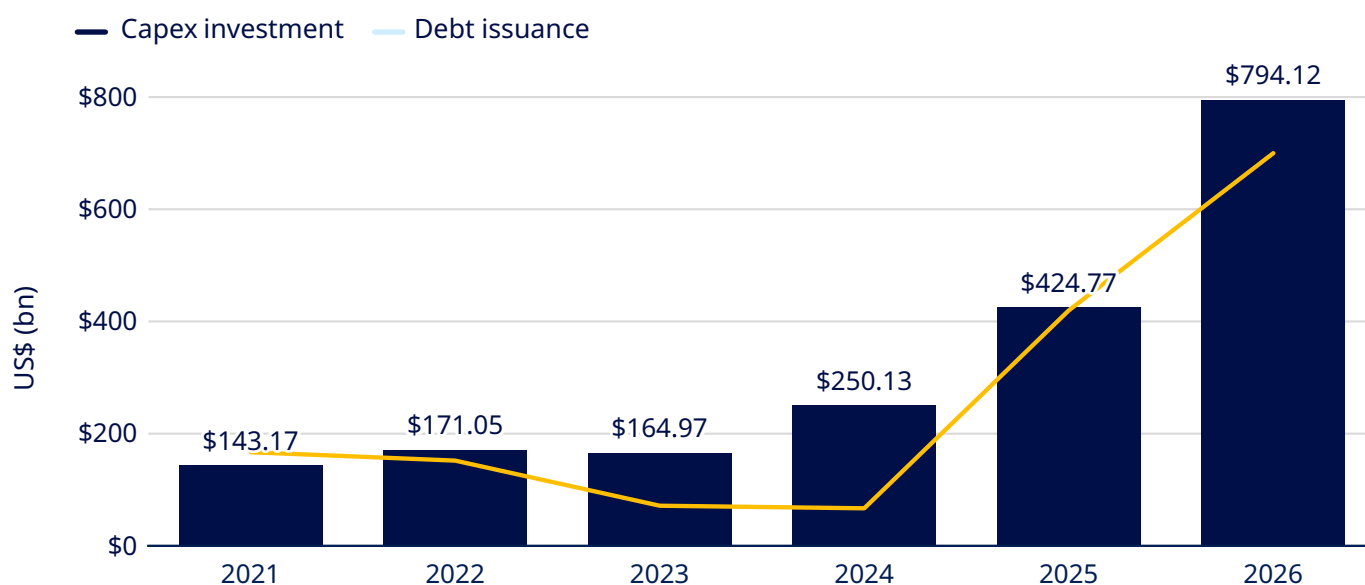


Financial risks

1

The big-tech companies have taken on substantial debt based on future revenue expectations. According to BIS, hyperscale bond issuance jumped fivefold to [US\\$105 billion](#) in 2025 (figure 3), with AI-related borrowers — neoclouds, developers, and the special purpose vehicles (SPVs) financing them — tapping debt markets for at least a further [US\\$200 billion](#) in 2026.

Figure 3: AI capex and debt issuance (FY 2021-2026f, US\$ bn) are on the rise



Source: [Bank for International Settlements](#)

In 2025, the sector generated about [US\\$60 billion in revenue against roughly US\\$400 billion](#) in capital expenditure — spending made well ahead of realized returns, on the expectation that far larger AI revenues will follow. That reliance on future revenues is the source of uncertainty, and it extends beyond borrowers themselves to the wider supply chain. Ultimately, supplier order books depend on those projected revenues being realized.

2

[Complex and opaque financing structures](#) increase contagion risk while SPVs, securitizations, and other off-balance-sheet arrangements can make leverage difficult to assess. As a result, distress at one borrower in the chain can spread before counterparties fully understand their exposure, exacerbating the impact of any failures on immediate counterparties and suppliers deeper in the value chain.

3

Data center operators and colocation companies that are increasingly borrowing against [GPU collateral](#) face a further solvency risk if those assets depreciate much more rapidly than expected. In such a scenario, immediate counterparties would be most exposed, including vendors carrying receivables, lenders providing financing, and landlords relying on lease payments.

Performance-related risks

Supply chain constraints remain a significant operational and, therefore, financial risk: equipment lead times range from [8 to 24 months](#), grid interconnection queues in major hubs [exceed four years](#), and only about [one-third](#) of the roughly 12 GW of US electric power capacity targeted for 2026 is currently under construction.

Material shortages, grid delays, or component delivery failures can delay asset monetization. Where financing is linked to construction milestones, an operational disruption can quickly become a financial event where, for example:

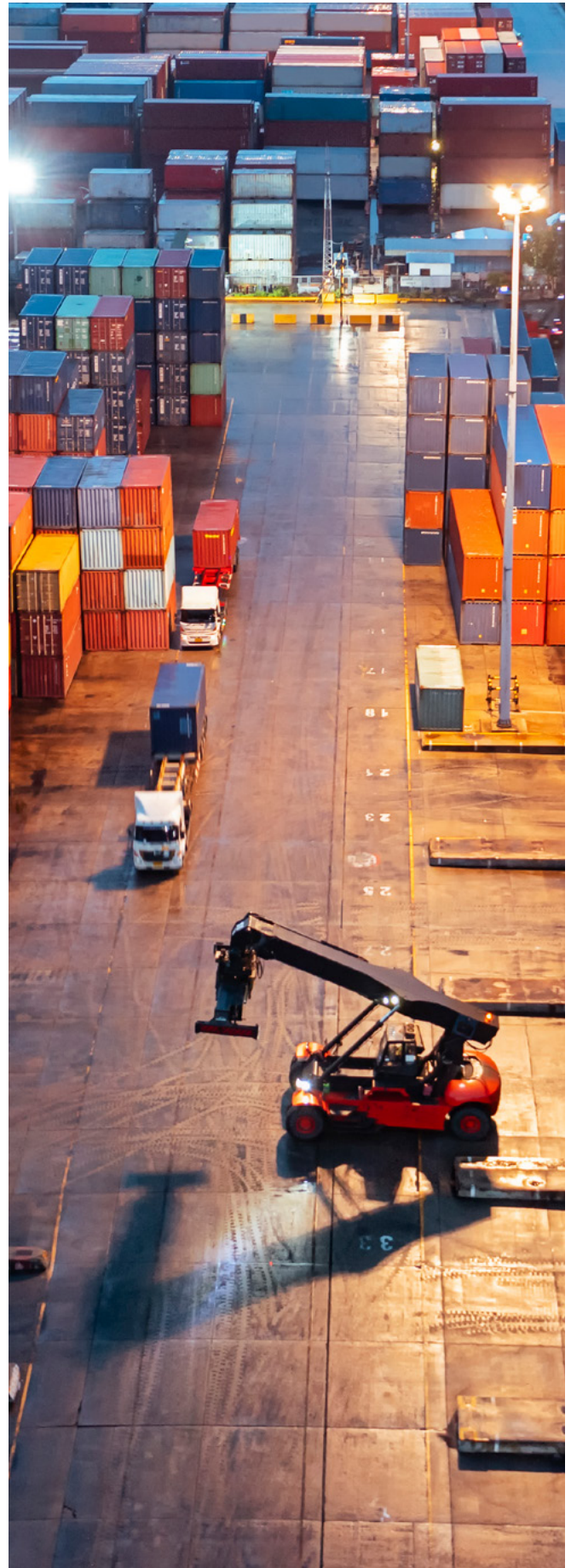
- Debt backstops fail to trigger as anticipated.
- Long-term lease agreements face termination.
- Financial covenants are breached.

The resulting economic losses may not be isolated, with direct impacts on counterparties, including contractors, suppliers, and lenders.

Political risks

Political intervention, meanwhile, including license revocation, permit reversal, restrictions on power or water access, forced localization, and capital-transfer controls can impair an asset's operations or revenues.

In the [first quarter of 2026](#) alone, 75 US data center projects representing roughly US\$130 billion were blocked or delayed, while the number of active opposition groups more than doubled to 833. Sovereign and sub-sovereign action is now a first-order delivery risk, not a tail scenario. These actions can have similar financial and counterparty impacts as a performance failure: delayed or lost revenues, pressure on financing structures, and exposure passed through to suppliers and lenders.



Insurance as a key enabling and mitigating tool

Insurance can play a key role in addressing the interconnected risks and enabling of digital infrastructure investments (figure 4).

The solutions described below can help support the financing of infrastructure projects by providing capital that supplements lender involvement.

Insurance solutions can support financial institutions managing country and counterparty concentration, seeking to mitigate transaction risks, or wanting to access institutional investors with debt rating restrictions.

They can also promote manufacturers extending credit, contractors to meeting obligations, suppliers to making receivables financeable, and operators to providing long-dated power security.

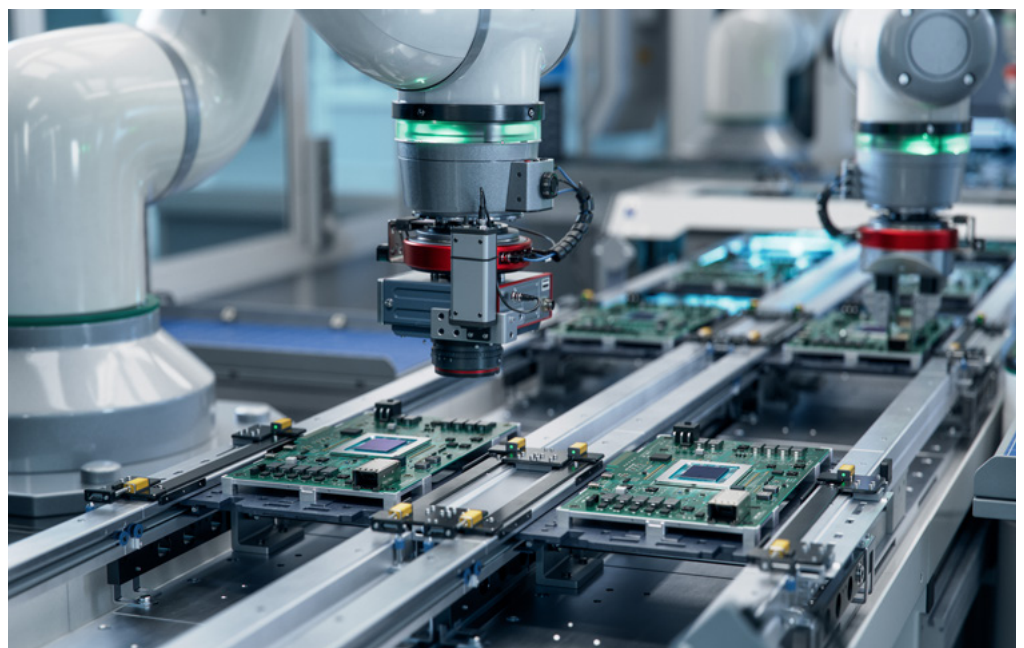
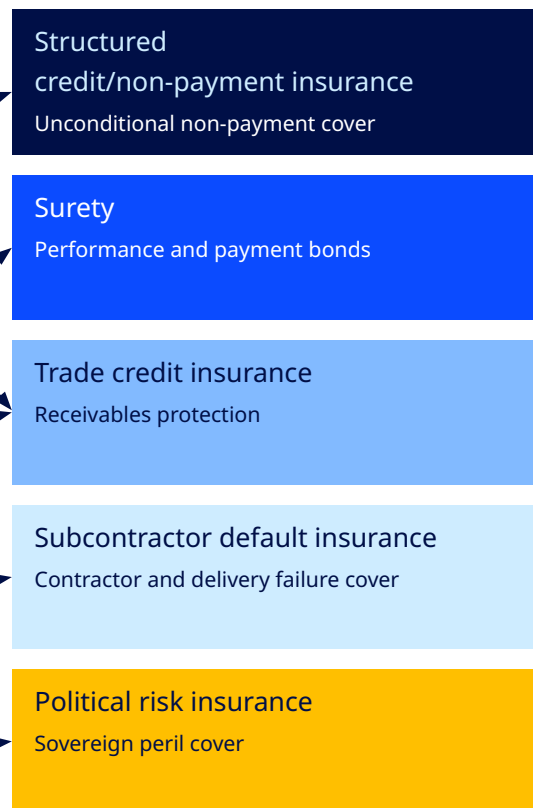


Figure 4: Credit and political risk (CPRI) solutions that help address risks and enable digital infrastructure investment

Key risks



Potential solutions



— Primary response
- - - Supporting response

Source: Marsh analysis

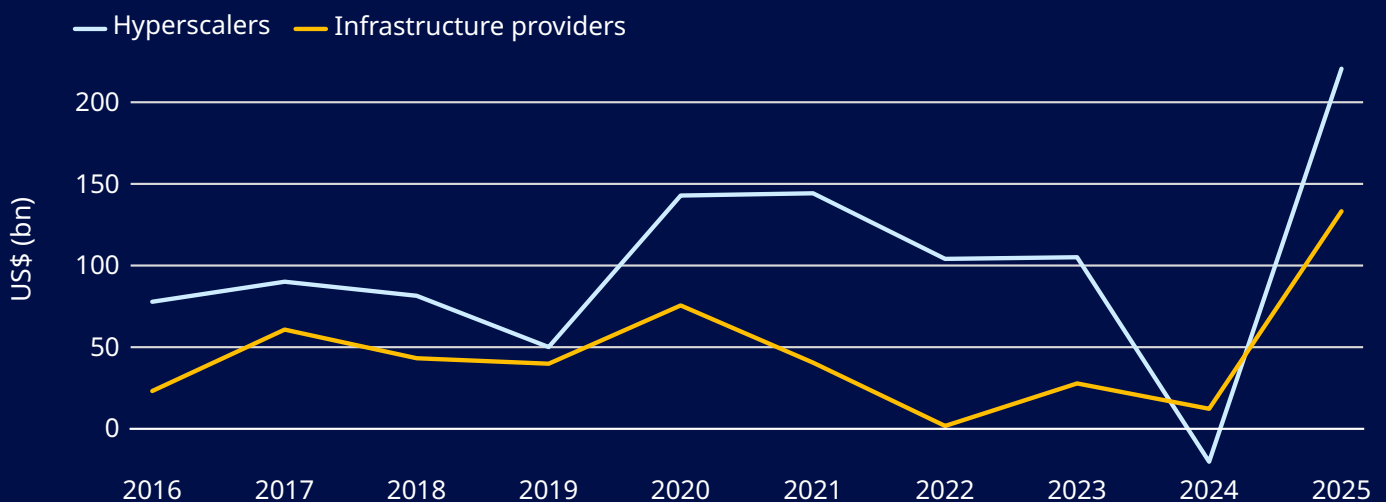


Structured credit solutions

Structured credit and non-payment insurance tend to be key in large, complex financings — data center campuses, grid and power projects, and the layered structures funding them — where lenders face exposure to borrowers whose repayment hinges on realization of an AI revenue bet. That exposure is growing broader. As figure 5 shows, long-term debt has risen sharply since 2016 not only among hyperscalers, but also among infrastructure providers as leverage accumulates beyond just the technology companies at the center of the buildout.



Figure 5: Long-term debt change for AI investments has sharply increased over the past decade



Source: [Bank for International Settlements](#)

The complex financing structures being used for large digital infrastructure projects illustrate why these tools are valuable. A hyperscaler may fund a campus through SPVs, [a private credit manager](#), and a bond issuance. Or a developer may raise high-yield notes to build capacity leased to a neocloud, supported by a backstop from a [larger technology company](#) — conditional on construction completion and capable of lapsing if the project is delayed.

The common feature of these arrangements is that the credit support is conditional: it depends on events that may not occur, and it is most likely to fail in circumstances that would trigger a claim. Non-payment insurance addresses that contingency with an unconditional, pre-agreed commitment. For digital infrastructure project finance, non-payment insurance can support lenders and SPV funding.

This is not a theoretical concern. Major [rating agencies have warned](#) that hyperscaler disclosures may understate the scale of lease-related obligations, which are heightening credit risks for firms, and credit markets are responding. Figure 6 shows spreads on AI-related corporate debt widening against a broad investment-grade benchmark since early 2025, signaling that the market increasingly considers this exposure as riskier than comparable credit.

Figure 6: AI firms' credit risk is up (spread change since January 2025)



Source: [Bank for International Settlements](#)

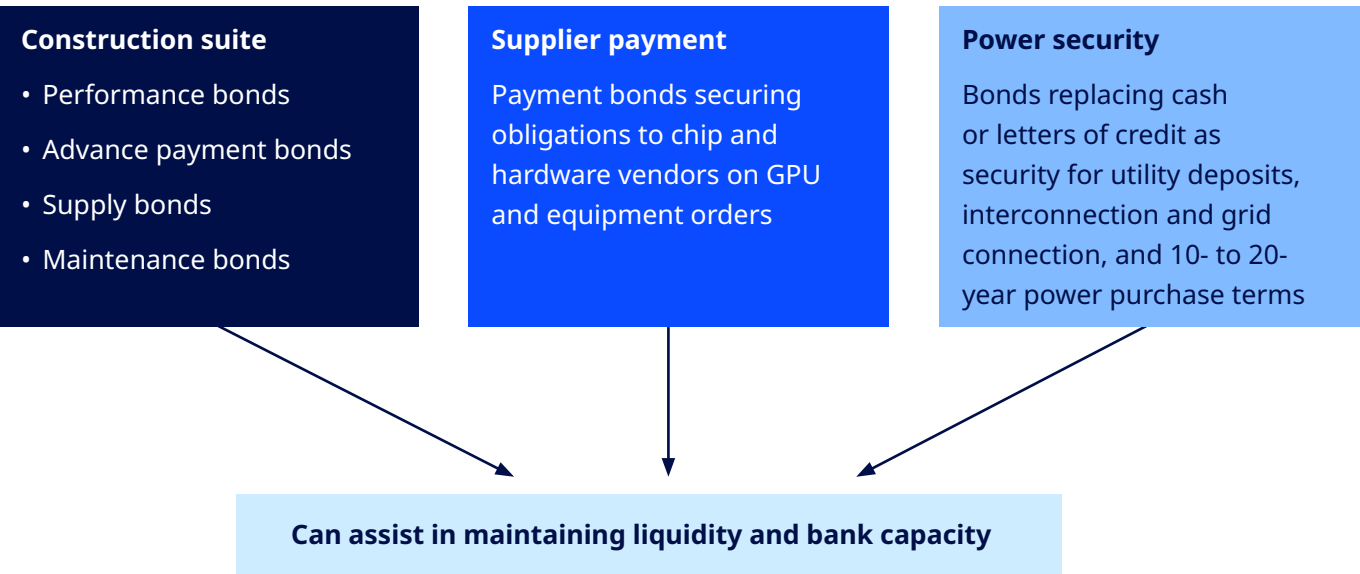
Surety bonds

Construction and delivery risk in digital infrastructure is [rising](#): US data center construction spending more than doubled in 2025 to exceed [US\\$50 billion](#). Hyperscale campuses depend on multiple contractors, network-equipment suppliers, and performance obligations delivered on aggressive timelines, often while facing skilled labor shortages, equipment lead times of [8 to 24 months](#), and [utility connection delays](#) that can stretch to five years.

Because financing is often tied to construction milestones, delays can do more than raise costs — they can disrupt the broader financing structure.

Surety bonds support the sector in three main ways.

Figure 7: Surety bonds solutions across the data center buildout



Source: Marsh analysis

1

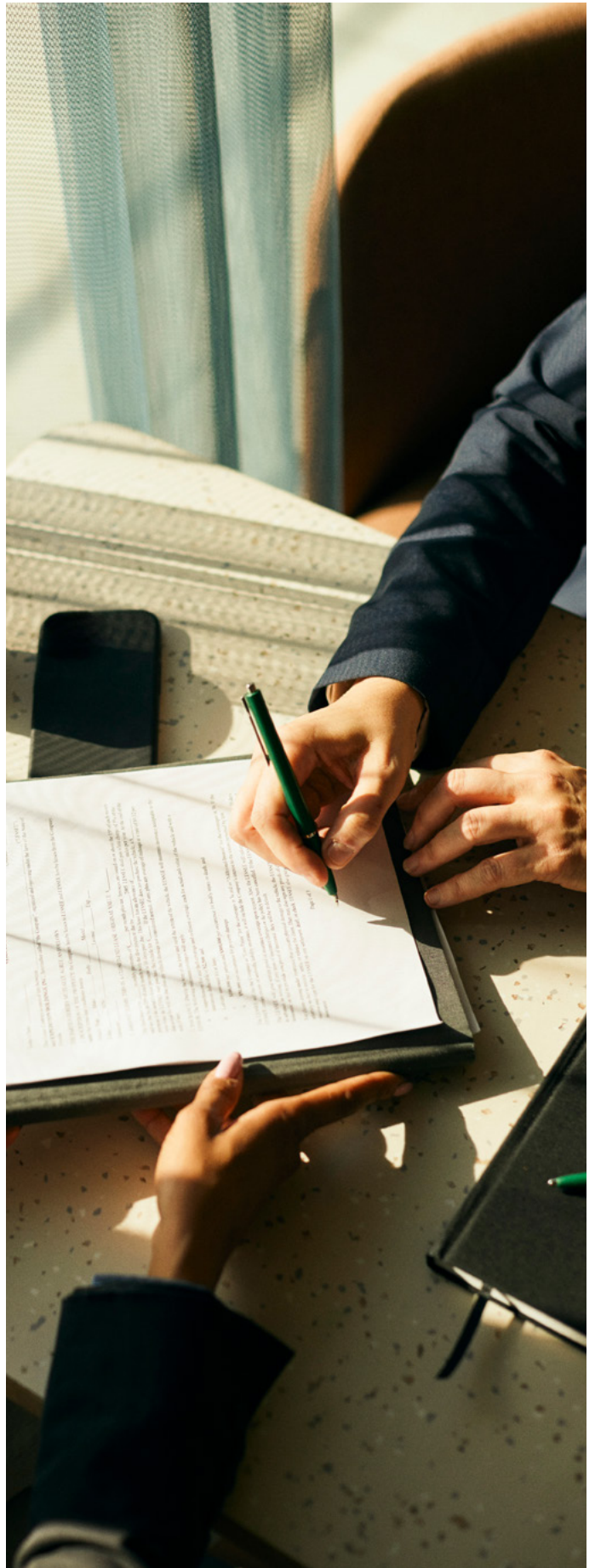
Performance bonds (covering subcontractors and suppliers), advance payment bonds, and maintenance bonds help contractors and developers during construction, with bond requirements for individual campuses running from tens to hundreds of millions of dollars. While many general contractors may not be required to post a suite of surety bonds covering the construction of the data center, it may be appropriate for critical subcontractors and suppliers to be bonded.

2

Payment bonds and supplier guarantees can support purchases of GPUs, servers, and long-lead electrical equipment, thereby reducing the need for buyers to post cash or use bank lines.

3

Surety can support [power procurement security](#). Data center operators face growing credit-support requirements from utilities and power suppliers at every stage of securing power. Utilities increasingly require deposits and interconnection or grid connection security before committing to network upgrades, and operators must also secure long-term power purchase agreements (PPAs) and [Transmission Security Agreements](#) (TSAs). TSAs can require collateral or parental guarantees for 10 to 20 years, sometimes before grid infrastructure is built and regardless of actual usage. Surety is well suited to provide this long-dated credit support, meeting utility security requirements while preserving cash, bank capacity, and balance sheet flexibility.



Subcontractor default insurance (SDI)

Subcontractor default insurance (SDI) is an insurance solution available largely in the US and serves as a first-party risk management tool that replaces traditional surety bonds. It typically covers direct and indirect financial losses when specialized trade partners fail to perform, go insolvent, or delay critical-path installations.

Data center builds rely heavily on synchronized, high-tech installations by specialized mechanical, electrical, and plumbing (MEP) and IT infrastructure trades. Surety bonds are an effective tool for covering construction risk, yet the claims validation process can take time. SDI aims to shorten that process and is designed to enable general contractors to promptly tap funds to fix or reassign work.

SDI can offer large aggregate limits (sometimes hundreds of millions of dollars via project-specific programs) tailored to multi-phase mega-builds. SDI can address complex causes of financial loss, including equipment repositioning, corrective rework, extended overhead, job acceleration, and liquidated damages, which standard surety default frameworks frequently exclude.

SDI can have important impacts for various stakeholders:

- **General contractors/construction managers:** Typically maintain direct operational control during a default, allowing the general contractor to choose replacement subs and dictate the recovery timeline without waiting for third-party approval.
- **Project owners and developers:** Adds to confidence in project completion and mitigates timeline slippage, with lesser risk of missing revenue generation targets once the facility goes operational.
- **Lenders and financial backers:** Can address completion risk requirements by providing protection in the event of localized trade defaults.
- **Subcontractors:** Encourages prequalification and safer financial tracking, and promotes stable, high-performing job sites.



Trade credit insurance (TCI)

Trade credit exposure sits primarily with chip and hardware suppliers. Leading GPU manufacturers, along with server, networking, and power equipment vendors, extend large receivables to a concentrated group of buyers, including hyperscalers, neoclouds, developers, and SPVs. The exposure extends to utility and power providers as well, which can obtain cover on a data center developer against failure to pay contracted amounts.



Two factors can make that exposure material.

1

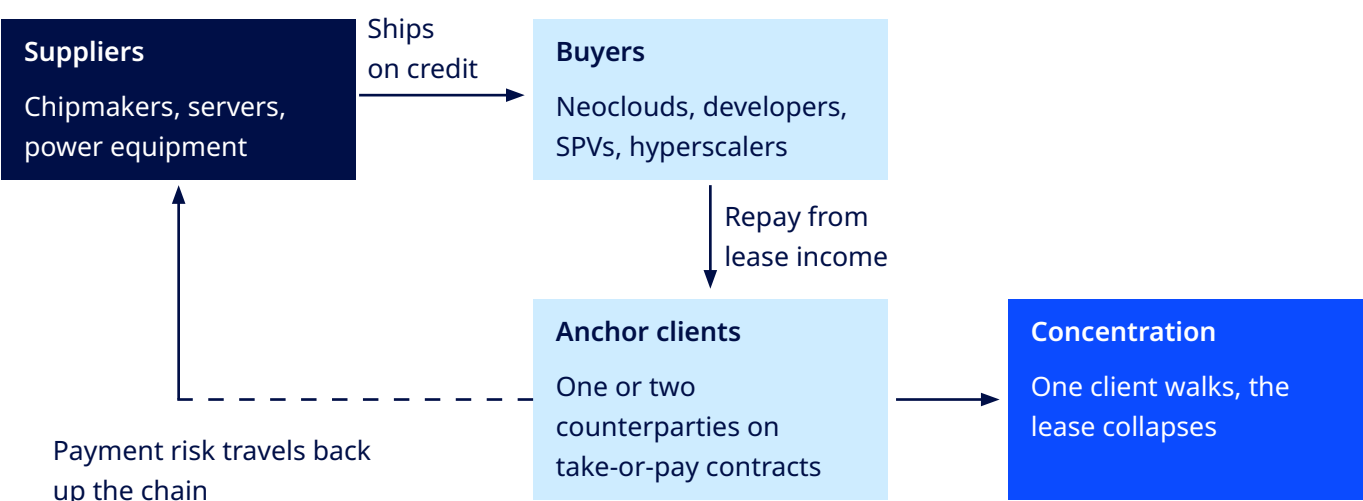
Counterparty quality can be uneven. Several prominent neocloud operators are rated below investment grade at the corporate level, even where individual financings benefit from contracted customer cash flows. A supplier shipping hundreds of millions of dollars of equipment to such a buyer is effectively extending unsecured credit to a leveraged counterparty whose revenues may [depend on one or two anchor customers](#). Those customers, in turn, may be relying on the same assumptions about future AI revenues.

2

This type of digital infrastructure demand can be partly circular. Where a component manufacturer invests directly in an AI model developer and simultaneously holds equity in several of its largest customers, the financial relationships between supplier and buyer become intertwined — and underlying demand becomes correspondingly harder to assess from outside. The pattern echoes vendor financing in telecom equipment in the [late 1990s, when customer defaults](#) undermined both the loans extended and the revenues those loans had generated.

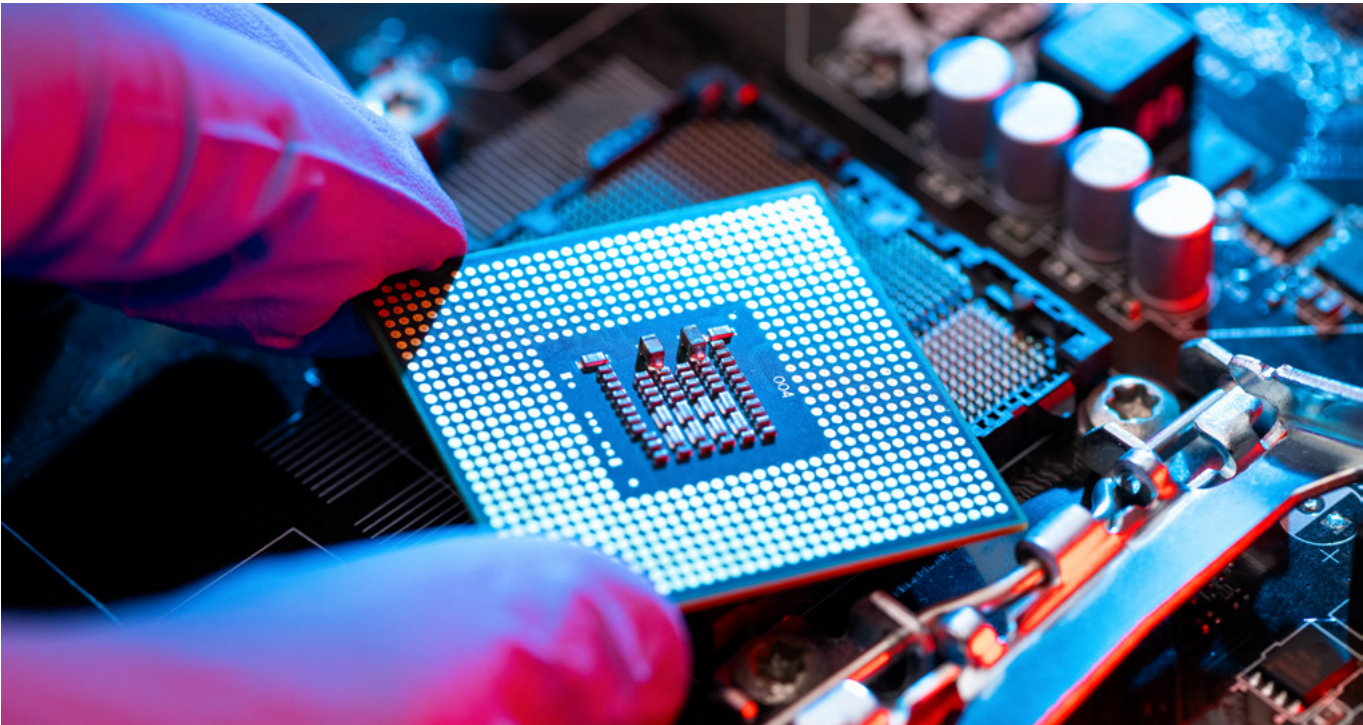
TCI helps suppliers manage concentrated buyer risk by supporting larger credit lines without breaching internal limits, tending to increase the ability to finance receivables, and improving portfolio management across the value chain. (figure 8).

Figure 8: TCI solutions across the data center buildout



Trade credit insurance covers the supplier receivable

Source: Marsh analysis



Political risk insurance (PRI)

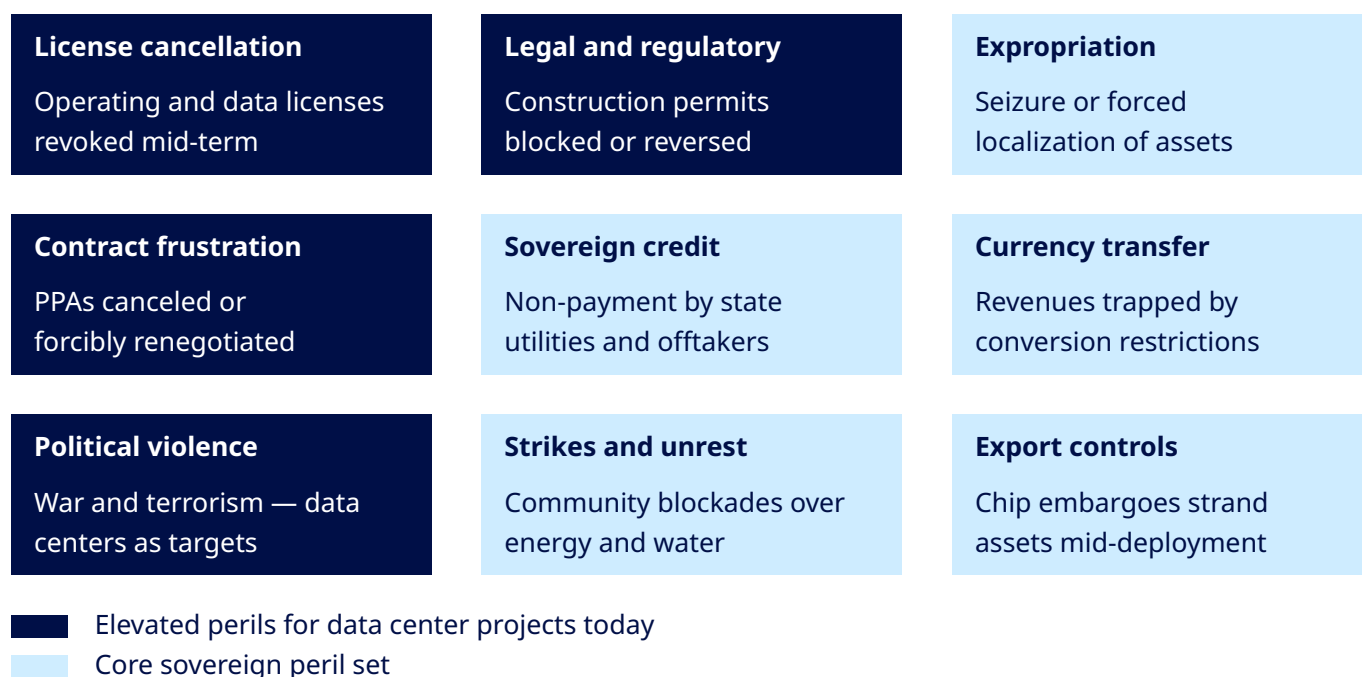
Digital infrastructure assets pass through three core phases — financing, construction, and operation — and the political risk profile can change at each stage.

[Government actions](#) pose a high risk to digital infrastructure investments as they can directly impair asset financing and valuation through the revocation of operating permits, discriminatory restrictions on grid and connectivity access, mandatory localization or ownership requirements, exclusion from public procurement, and capital-transfer controls that restrict the repatriation of interest, principal, dividends, or sale proceeds. (figure 9 for further reference).

These interventions may not operate in isolation: they can compound, simultaneously compromising equity valuations, collateral integrity, debt-servicing capacity, and exit assumptions.



Figure 9: Political and sovereign risks for data centers



Source: Marsh analysis

In some cases, investors expect to rely on investment treaty protections rather than purchase PRI.

Treaty claims can be slow to advance, complex, and heavily dependent on how the investment was structured before any dispute became foreseeable — investor-state arbitrations, whether under ICSID or UNCITRAL rules, average [three to four years](#) from filing of a claim to a final award. A US\$2.7 billion claim by a nation illustrates possible limitations on claims under a free trade agreement: alleged government [interference with a toll concession](#) led to the asset being deconsolidated and placed into liquidation before the claim was resolved. While data centers differ structurally from traditional assets like toll roads, government overreach can severely disrupt operationally complex, multi-tiered investments — a risk that continues to grow and evolve.

Sub-sovereign risk is not limited to emerging markets. In Oregon, [advocacy groups and local residents have sued](#) seeking to overturn enterprise zone tax exemption agreements covering 17 data center applications, approved shortly before a statewide pause on the program took effect. The claim is not that the authorities breached those agreements, but that they exceeded their authority and approved the applications without sufficient evidence of the economic benefit state law requires. Whether such a loss is insurable turns on the instrument and the trigger — PRI responds to breach of a specific obligation owed to the insured, not to the withdrawal of a generally available statutory incentive.

The pattern is also present internationally. In [Kenya](#), a flagship billion-dollar partnership stalled when the sponsor's request for guaranteed government payments could not be met, given power constraints on national supply — showing how sovereign fiscal capacity alone can halt a project despite genuine political commitment.

Building AI's digital infrastructure with greater capital confidence

The AI buildout is one of the largest and fastest capital deployment cycles in history, but its success will depend not only on demand for AI services, but on the resilience of the financing and delivery systems behind it. Across the digital infrastructure value chain, businesses engaged in meeting the demand face a combination of financial, performance, and political risks that can delay projects, weaken counterparties, and constrain access to capital at vital times.

In that environment, insurance is more than a protection tool. It can also be a strategic enabler of growth. By helping businesses manage downside risk, strengthen credit profiles, and contribute to greater lender and supplier confidence, risk transfer solutions play an important role in keeping capital flowing through a period of uncertainty.

For firms seeking to participate in the AI investment supercycle, the ability to manage risk effectively may prove as important as the opportunity itself.



Figure 10: Mitigating digital infrastructure risks through PRI, SCI, TCI, Surety bonds, and SDI

Risk	Potential exposure	Political risk insurance (PRI)	Structured credit insurance (SCI/NPI)	Trade credit insurance (TCI)	Surety bonds and subcontractor default insurance (SDI)
Construction and delay risk	Cost overruns, milestone misses, and project delivery slippage impact credit backstops, triggering lease terminations	Not applicable	Not applicable	Not applicable	Performance, advance payment, supply, and maintenance bonds on behalf of prime contractors or key/critical subcontractors or suppliers, supporting project completion; SDI arranged by the prime contractor covering the risk of default by key subcontractors
Buyer non-payment (chips, hardware, equipment)	Suppliers extend payment terms to leveraged neoclouds, SPVs, and data center developers whose existing capital base requires third-party security	Not applicable	Not applicable	Protects against insolvency, protracted default, or unwillingness to pay by private obligors; supports financing of receivables	Payment bonds provide an alternative form of supplier payment security, helping maintain cash and letter of credit lines
Failure to secure required power from a utility or other provider	Utilities and other third-party power providers expend significant capital when creating interconnections to the power grid, and ultimately the power required by the data center	Not applicable	Not applicable	Utility or other power provider can obtain protection in the event of failure of a developer to pay amounts as contracted	Surety bonds arranged by the data center covers payment obligations for interconnection obligations and under long-term PPAs
Non-payment to lenders (SPVs, project loans, GPU-backed facilities)	Borrower defaults on data center SPV debt, construction loans, or GPU-collateralized facilities; conditional backstops fail to trigger; collateral depreciates faster than amortization	Can be written to protect lenders' interest where non-payment stems from a political act	Lender can obtain a commitment to pay in the event of borrower default	Not applicable	Not applicable

Risk	Potential exposure	Political risk insurance (PRI)	Structured credit insurance (SCI/NPI)	Trade credit insurance (TCI)	Surety bonds and subcontractor default insurance (SDI)
Expropriation and license cancellation	Government seizure of data center assets; revocation of operating licenses	Indemnifies equity value upon outright or creeping expropriation; responds to license cancellation subject to proof of wrongful sovereign action	Not applicable	Not applicable	Not applicable
Currency inconvertibility and transfer risk	Capital controls trap data center revenues; conversion or repatriation of dividends, debt service, or exit proceeds is blocked	Pays investors in hard currency when government action blocks conversion or transfer	Non-payment under a loan agreement indemnified, including government intervention, but typically without foreign exchange impact	Not applicable	Not applicable
Breach of contract (PPAs, concessions, incentive agreements)	Government cancels or forcibly renegotiates PPAs, grid access, licenses, or contracted incentive agreements, undermining project cash flows	Protects against unlawful cancellation or failure to honor awards; regulatory action may qualify if expropriatory or in breach of contract	Where payment is affected, responds to non-honoring of contractual payment obligations regardless of cause	Not applicable	Unfair-calling cover (written in the PRI market) protects against wrongful drawing of bonds by government obligors
Political violence and physical damage	Damage, project delays, forced abandonment, or business interruption from war, terrorism, riots, or community blockades	Compensation for property damage, forced abandonment, and business interruption caused by violence	Not applicable	Not applicable	Not applicable

Disclaimer: This table describes common PRI, SCI, TCI, surety bonds, and SDI features and the risks they often address. The terms and conditions of the issued policy or bond will describe the extent of coverage for a particular risk. Potential policy benefits can vary by product and should be the subject of each purchaser's own assessment and risk appetite, among other factors.

Source: Marsh analysis

Contact us

For more information about how we can support your organisation, please contact a member of our team:

Philip Neighorn

Global Industry Leader
Digital Infrastructure
Credit Specialties, Marsh Risk
Dallas | Madrid
+1 214 208 6587
philip.neighorn@marsh.com

Michael Mathews

Digital Infrastructure Leader
Marsh Risk
United States
+1 (617) 9975209
Michael.Mathews@marsh.com

About Marsh

Marsh (NYSE: MRSH) is 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, 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

