parametrix

An Introduction to Data Center SLAs: Key Terms, Financial Risk, & Underwriting Implications

JUNE 2026

Service-Level Agreements (SLAs) are part of the contractual arrangements between tenants (customers) and operators (providers) that underpin operational performance requirements. **They define measurable standards such as availability, latency, reliability, and specify financial penalties when these standards are not met.**

Typically structured as an addendum to the lease agreement, SLAs align expectations between providers and customers, enforcing trust and accountability.

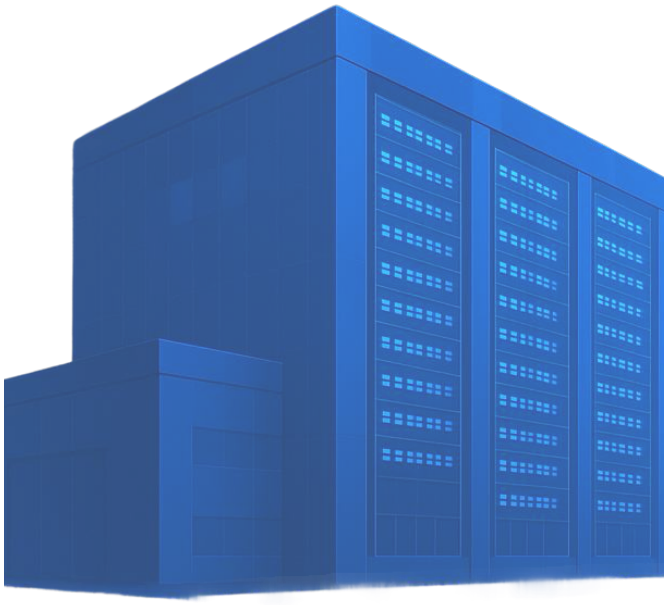
The rapid expansion of the digital infrastructure sector has transformed SLAs from relatively simple uptime guarantees into complex, performance-based frameworks.

As data centers have become mission-critical, high-compute performance assets, even minor performance disruptions and resulting SLA breaches can create significant operational and financial risks.

These breaches can trigger substantial financial penalties, introducing a level of volatility that can deter investors and lenders.

With the continued **growth of AI and cloud computing expected to rely on approximately $3 trillion in data center investment**, developers increasingly depend on institutional capital providers and lenders that prioritize predictable and stable cash flows.

As a result, effectively managing SLA-related exposure has become a critical priority for capital providers.



Capital providers have traditionally underwritten data centers as conventional real estate assets, focusing due diligence on lease structures and tenant creditworthiness, while paying little attention to SLAs.

However, these agreements should be a central component of any risk assessment framework as they have a material impact on a data center's cash flow.

Understanding their structure, implications, and financial impact is essential for capital providers and other stakeholders.

This paper breaks down the core components of these agreements and examines how to effectively evaluate the associated risks and their potential financial consequences.

Core Components of an SLA

Modern SLAs are complex agreements that extend beyond basic uptime guarantees. While structures vary by tenant, most include core standards around availability and performance, measurement and monitoring, as well as remedies and penalties.

1. Availability and Performance Metrics

Availability is the central component of most SLAs and is typically expressed as a percentage (e.g., 99.99% uptime). These metrics define acceptable performance thresholds and often include detailed definitions of what constitutes "downtime", often excluding scheduled maintenance or force majeure events.

These standards apply to **critical infrastructure such as power, cooling and network connectivity, and typically range from 99.9% to 99.999%**, depending on tenant requirements.

This is what aligns data centers with high-compute performance assets rather than passive real estate infrastructure. The required uptime percentages convert into acceptable downtime as seen below:

Required Uptime	With SLA Insurance
99.999%	~ 0.45 minutes/month (~ 5.4 minutes/ year) *Downtime per month (minutes) = (1 - Uptime) x total minutes per month* *Total minutes per month = 31 × 24 × 60 = 44.640* *44.640 × 0.001% = ~ 0.45 minutes per month*
99.99%	~ 4.46 minutes/month (~ 53.6 minutes/year)
99.9%	~ 44.64 minutes/ month (~535.7 minutes/ year)

Interpretation: Per month, the contract specifying 99.999% uptime allows for 0.45 minutes (or 27 seconds) of downtime of power, cooling and/or network connectivity before financial penalties apply.

2. Penalties and Remedies

When SLA thresholds are breached, predefined penalties apply. These typically include:

- Service credits: refunds based on monthly contractual rent amount known as Monthly Base Rent (MBR) or Monthly Recurring Charge (MRC)
- Termination rights: allowing customers to exit their leasing contract after repeated or severe breaches

The structure of these penalties, particularly whether liabilities are capped or uncapped, has significant financial implications for operators.

In some cases typical hyperscaler/ colocation credit structures can look as seen in the table below. **A 45-minute breach can trigger service credits between 100% and 200% of monthly rent, eroding nearly half of the data center's annual cash flow.**

Downtime Duration per Month	Credit (Monthly Rent)
27 seconds - 5 minutes	25% - 50%
> 5 minutes < 45 minutes	70% - 100%
> 45 minutes	100% - 200%

For example, if we applied this penalty structure to a 100 MW data center with $144M in annual rent and $57.6M annual cash flow, a 45-minute breach would trigger a penalty of 200% of monthly rent, resulting in $24M in losses. That reduces overall annual cash flow by 42%.

Even more **concerning for institutional capital providers and lenders who evaluate the asset's long-term risk profile is the lease termination clause.** These provisions usually include early lease termination rights as well as potential relocation costs of the tenant to a new facility.

A possible clause could state that if there are three SLA breaches in 12 months, or one outage exceeding a defined threshold, the tenant has the right to terminate their lease.

Hyperscaler and colocation tenants typically negotiate termination rights if reliability repeatedly fails. With the rapid growth of AI and the dominance of hyperscalers, bargaining power lies in favor of tenants.

If a tenant decides to terminate their lease, the data center no longer receives rent and is therefore left without revenue, which can be detrimental to service a large debt burden. This is especially prevalent in hyperscale facilities that typically have one or two tenants that provide 70% - 100% of their overall revenue, thus eliminating a majority of the revenue stream.

The Financial Risk of SLAs

SLAs can have a direct and often underestimated impact on the financial performance of data center assets by transforming minor operational disruptions into significant financial losses. This volatility can materially impair asset value, making SLA exposure a critical concern for capital providers.

1. Impact on cash flow

The severe financial impact of service credits, and especially the presence of termination rights, can create substantial cash flow volatility. **This volatility can impair debt serviceability, threaten collateral value and negatively impact credit ratings and financing spreads**, especially as stabilized data centers are increasingly used as collateral for the development of new projects.

The impact this has on a data center's risk profile can narrow the pool of potential capital providers and ultimately reduce the asset value.

2. Due diligence gaps

Due diligence processes have traditionally focused on lease structures and tenant creditworthiness, as data centers have historically been underwritten as conventional real estate assets. This approach, however, fails to account for their evolution from passive real estate into active, high-performance, mission-critical infrastructure.

As such, risk assessment frameworks have not sufficiently adapted to consider the growing importance of operational performance, nor the potentially significant financial consequences of SLA breaches and service disruptions.

This creates a major blind spot as **understanding the sensitivity of SLAs is crucial in forecasting revenue and cautiously underwriting the asset class.**

Data Center Disruptions In The Headlines

As businesses and critical services become increasingly reliant on continuous data center uptime, especially as AI becomes more prominent in every-day use, even localized infrastructure failures can cause widespread operational and financial disruption. The recent incidents below highlight how **failures in power, cooling and backup systems can impact thousands of organizations and create significant SLA-driven exposure** for data center operators.

Amazon Data Center | Virginia | May 2026[1]

A cooling failure led to rising temperatures that resulted in the preventative automatic shutdown of servers in a single data center within the AWS us-east-1 cloud region. The incident took 21.5 hours to fully recover and caused cascading disruptions across major platforms such as Coinbase, where users were left unable to access the exchange for buying, selling or managing digital assets during a critical window.

Keppel REIT Data Center | Netherlands | May 2026[2]

A fire at a data center owned by DC Keppel REIT and operated by NorthC led to downtime of operations. Among the companies impacted were IBM Cloud and Vonage, whose global SMS services were affected for over 36 hours.

Oracle Data Center | Virginia | January 2026[3]

A winter storm caused a power outage in the Oracle data center, which resulted in network and storage issues affecting tens of thousands of servers supporting TikTok in the US. This incident lasted several days and customers experienced connection timeouts, errors, lags and failures when trying to post content.

CyrusOne Data Center | Illinois | November 2025[4]

A mechanical cooling failure caused servers to overheat and shut down, impacting the CME Group's trading operations. The outage raised investor concerns about reliability and operational risk, pausing a $1.3 billion commercial mortgage-backed bond sale issuance from Goldman Sachs tied to CyrusOne data centers.

1. Tech AWS data center outage hits trading on FanDuel, Coinbase — recovery to take hours | CNBC
2. NorthC data center outside Amsterdam suffers fire | Data Centre Dynamics
3. TikTok attributes recent glitches to a power outage at a US data center | TechCrunch
4. CyrusOne Halts Bond Sale After Data-Center Failure Cripples CME | Bloomberg

Guidance for Capital Providers

As data centers evolve into performance-driven infrastructure assets, it is crucial for capital providers to incorporate SLA analysis into their evaluation frameworks. When reviewing SLAs, key risk considerations include:

Service credit structures and performance/uptime definitions

Understand how credits are calculated, whether they are capped, and what specifically constitutes a breach- including applicable exclusions, measurement methodologies and permitted downtime- to accurately assess the operator's exposure. These penalties effectively function as variable operating expenses that reduce net operating income, thus analyzing them is critical to forecast revenue downside, assess asset value, and evaluate debt serviceability.

Maintenance windows and infrastructure capability alignment

Review how planned maintenance is treated within SLA frameworks to ensure that routine facility upkeep does not trigger penalties. Properly managed maintenance is also essential to support the infrastructure's reliability and enable the data center to meet its committed uptime obligations. It is also critical to verify that the underlying data center design and resilience standards, such as the facility's tier certification, actually support the committed SLA requirements.

Operational due diligence

Understand historical downtime performance and operational practices because past performance can help predict future risk by understanding management expertise, their weaknesses and ability to remedy breaches. It is also necessary to determine the level of the operator's dependence on third-party utilities to better assess their control over breaches.

Underwriting integration and solution implementation

Incorporating SLA risk into credit models and financing decisions - and recognizing its direct impact on asset stability and income predictability - should be a key component of underwriting processes. Potential mitigation strategies, including insurance solutions designed to cover earnings volatility and enhance financial stability for the capital providers, should also be evaluated.

SLAs as a Central Underwriting Component

The digital infrastructure sector demands near perfect operational performance from data centers and requires an unprecedented level of new investment in the sector. This evolution has transformed data centers into active, high-performance, mission-critical assets that require substantial institutional capital to support their continued growth.

These stringent operational requirements are embedded within SLAs, where brief disruptions can trigger substantial financial penalties. This resulting exposure introduces material cash flow volatility that can deter investors and lenders from deploying capital into the sector.

To unlock the scale of investment required for the continued expansion of digital infrastructure, risk assessment methodologies must evolve accordingly. Capital providers require greater visibility into these operational exposures in order to accurately assess risk, structure financing and deploy capital with confidence.

SLAs should become a central component of underwriting and due diligence processes, enabling stakeholders to better assess exposure, structure mitigation solutions and build resilient investment strategies.

parametrix

About Parametrix

Parametrix, the leading provider of digital business interruption solutions, specializes in parametric insurance that protects against the financial cost of technology and digital infrastructure downtime. Leveraging a proprietary network of monitoring systems, we collect and analyze real-time, granular data on the performance and availability of critical infrastructure — including data centers, SaaS providers, and cloud services — to accurately assess risk and deliver fast, transparent claims payments. Our solutions enable businesses, data center stakeholders, and (re)insurers to quantify, manage, and transfer the financial risks of downtime with unmatched precision. Parametrix is a Managing General Agent and Lloyd's Coverholder, with policies backed by major A-rated global insurers, and is headquartered in New York.

www.parametrixinsurance.com
parametrix-insurance
info@parametrixinsurance.com