BSP
Technical Advisors

Data Center Technical Due Diligence:
What We've Seen and Wished We Hadn't

April 2026

This piece highlights the red and yellow flags discovered by BSP during technical due diligence engagements across a diverse range of data center assets. It reflects patterns observed in the field—conditions that, if unaddressed, can materially impact uptime, safety, and long-term scalability. While each facility is unique, the themes outlined below represent potential failure points that investors and operators should take into account as part of an M&A process.

A. Planning and Architectural Deficiencies

In several cases, early-stage design and planning decisions constrained operational performance and resilience. These foundational issues are often the most difficult and costly to remediate.

- **High-Risk Site Selection.** Facilities located in flood-prone or environmentally exposed areas introduce systemic risk and ongoing operational uncertainty.
- **Non-Scalable Design Approaches.** Tenant-specific solutions are sometimes prioritized over standardized architectures, limiting flexibility and complicating future expansion. For example, there is the custom containment solution shown here.
- **Insufficient Redundancy and Diversity.** Gaps in system redundancy and path diversity reduce fault tolerance and increase service disruption likel.
- **Single Points of Failure.** Critical dependencies remain unmitigated, creating scenarios where local failures can cascade into site-wide outages.
- **Outdated or Inaccurate Documentation.** Discrepancies between design documentation and actual conditions hinder effective operations and incident response.
- **Ad Hoc Containment Solutions.** Temporary airflow measures—such as improvised plastic containment—signal breakdowns in planning discipline and introduce both safety and performance risks.

B. Physical Security and Access Control

Physical security controls are, at times, inconsistent with industry expectations, exposing facilities to avoidable vulnerabilities.

- **Perimeter Control Gaps.** Insufficient barriers and access controls can allow unauthorized approach to critical infrastructure.
- **Surveillance Coverage Limitations.** Blind spots in camera coverage reduce situational awareness and impair incident response capabilities.

- **Inconsistent Authentication Standards.** Variability in access control protocols—particularly around two-factor authentication—can weaken overall security posture where stronger controls (e.g., badge + biometric) are warranted.

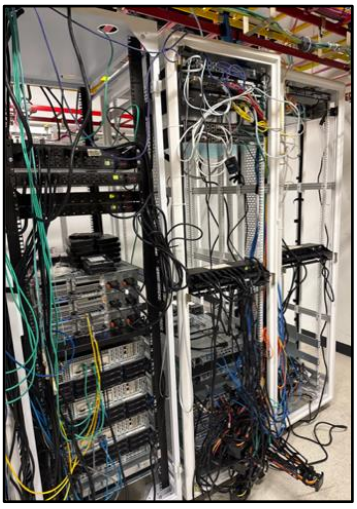
C. Facility, Power, and Cooling Infrastructure

In certain environments, infrastructure degradation or underinvestment has elevated operational risk. The following summarizes representative findings:

Component	Observed Condition	Operational Implication
Raised Flooring	Physical damage and compromised tile integrity	Reduced structural reliability and airflow control
Exterior Equipment	Exposure to environmental elements and tampering	Accelerated wear, corrosion, and performance degradation
Power	Constrained capacity	Limited growth potential and reduced redundancy under load
Cooling	Equipment beyond service life	Increased failure rates and inability to support high-density deployments
Fire Suppression	Incomplete inspection/ charge records	Uncertainty in system readiness and potential compliance exposure
Fuel Management	Lack of fuel quality and supply planning	Elevated risk during extended outages or regional disruptions

D. Structured Cabling and Equipment Management

The physical connectivity layer is often an overlooked source of both operational inefficiency and risk.



- **MMR Disorganization.** Poorly managed meet-me-rooms result in unclear connectivity paths and outdated records, complicating troubleshooting and provisioning.
- **Labeling and Documentation Gaps.** Inconsistent labeling and misaligned documentation increase dependency on institutional knowledge rather than repeatable processes.
- **Cable Management Issues.** Overfilled trays and improper separation of power and data cabling create both safety concerns and potential interference.
- **Fiber Exposure.** Unprotected fiber runs are vulnerable to physical damage, leading to avoidable service degradation or outages.
- **Lifecycle Management Deficiencies.** Continued reliance on end-of-life components, combined with weak preventive maintenance practices, shifts operations into a reactive posture.

- **Thermal Management Inefficiencies.** Improper cabinet layouts and airflow obstructions undermine cooling effectiveness and reduce overall system stability.

E. Technical Services and NOC Operations

Operational oversight functions are sometimes constrained by limited visibility, insufficient controls, and resource misalignment. One concern is the use of shared credentials for critical systems such as the Building Management System (BMS), which undermines auditability and incident traceability. Additionally, some environments lack robust remote monitoring capabilities or reliable access to key performance data. At the organizational level, technical staff are often tasked too broadly, limiting the depth of expertise applied to complex systems and increasing operational risk over time.

F. Remediation and Path to Readiness

Transitioning from elevated risk to operational resilience requires a structured, disciplined approach. BSP Technical Advisors recommends the following actions:

- **Comprehensive Assessment.** Conduct a full review of design documentation alongside a detailed, component-level onsite inspection.
- **Independent Verification.** Validate all systems directly—do not rely solely on reported status or historical assumptions.
- **Action-Oriented Remediation Planning:** Pair each identified issue with a defined scope, timeline, and accountable owner.
- **Specialized Resource Deployment.** Engage appropriately qualified experts for remediation efforts rather than relying on generalist staffing models.

Closing Perspective

Closing the gap between "what we've seen—and wished we hadn't" and "what best-in-class facilities demonstrate" requires more than incremental fixes. It demands disciplined execution, rigorous validation, and a commitment to operational standards that align with long-term performance expectations. BSP approaches this process with a singular goal: ensuring that infrastructure not only meets today's requirements but can support tomorrow's demands.

About BSP

BSP Technical Advisors is the leading digital infrastructure M&A technical advisor and due diligence specialist - completing over 140 evaluations of data centers and networks for over 80 clients such as Ares, Brookfield, Carlyle, DIF, Macquarie, Novacap, OMERS, Palistar and Sixth Street. The team consists of former operator technical executives who have designed, built and operated, data centers and networks. To learn more, please visit www.bspdd.com.