**2026 SURETY BONDING
& CONSTRUCTION RISK
MANAGEMENT CONFERENCE**

Hosted by:

AGC
THE CONSTRUCTION
ASSOCIATION

Insurance Issues in Constructing Data Centers — A GC's Perspective

By: Regina Adler, Aon; Amy Iannone, DPR Construction; Alicia Pavelko, Zurich, Tracy A. Saxe, Saxe, Doernberger & Vita, P.C.; Ted Wickenhauser, McCarthy Building Companies, Inc.

Insurance Issues in Constructing Data Centers – A GC's Perspective

AGC 2026 Surety Bonding & Construction Risk Management Conference
Regina Adler (Aon)
Amy Iannone (DPR Construction)
Alicia Pavelko (Zurich)
Tracy A. Saxe (Saxe, Doernberger & Vita, P.C.)
Ted Wickenhauser (McCarthy Building Companies, Inc.)[1]

---

[1] Paper written by Kiley Stackpole (Saxe, Doernberger & Vita P.C.)

## I.	Introduction

Data centers are physical facilities that house computer servers and associated components of computing infrastructure.[2] Due to the rise in artificial intelligence, the demand for new data centers has surged.[3] The data center construction market is projected to grow from $17.01 billion in 2024 to $28.95 billion by 2033.[4]

This growth offers significant opportunities for general contractors ("GCs") but also introduces risks far more complex than typical commercial construction. Insurance markets have not fully developed products specifically tailored to these risks, leaving GCs to rely on traditional coverages to protect themselves such as Builder's Risk, Commercial General Liability, Professional Liability, Subcontractor Default Insurance and Controlled Insurance Programs. As a result, GCs may face substantial risks and may find themselves without coverage unless risks are proactively managed and coverage is carefully tailored to the project. This paper outlines key risks in data center construction and how insurance may respond.

## II.	Unique Risk Profile of Data Center Projects

### a.	Speed-to-Market Pressures

Owners often prioritize rapid project completion to capture revenue sooner, which can compromise quality. For instance, owners may look to cut corners in geotechnical work by skipping soil testing or rushing foundation pouring and waterproofing. This increases the risk of foundation failure and could create cracks or gaps that allow water intrusion—particularly critical in data centers, where sensitive electrical and server equipment is highly vulnerable. These speed-to-market pressures heighten the risk of construction defects and long-term exposure.

### b.	Powered Shells

To accelerate occupancy, owners may construct powered shells rather than fully built "turnkey" data centers. Powered shells include a completed exterior with basic internal systems, such as power and connectivity, while leaving the interior as raw space for tenants to install their own equipment or hire separate contractors to customize the space,

---

[2] *The Data Center Construction Risks,* ALLIANZ COMMERCIAL, at 9 (Nov. 2025).

[3] *US Data Center Construction Industry Report 2025: Market to Grow Rapidly Through 2030, Driven by Cloud Expansion, Digital Transformation, and Demand for Scalable, Energy-Efficient Infrastructure*, GLOBE NEWSWIRE (Nov. 26, 2025), https://www.globenewswire.com/news-release/2025/11/26/3194982/0/en/US-Data-Center-Construction-Industry-Report-2025-Market-to-Grow-Rapidly-Through-2030-Driven-by-Cloud-Expansion-Digital-Transformation-and-Demand-for-Scalable-Energy-Efficient-Infra.html.

[4] *Id.*

including installing cooling systems, server racks, backup generators, and IT equipment, to meet their specific needs.[5] Below are examples of how powered shells are configured.[6]
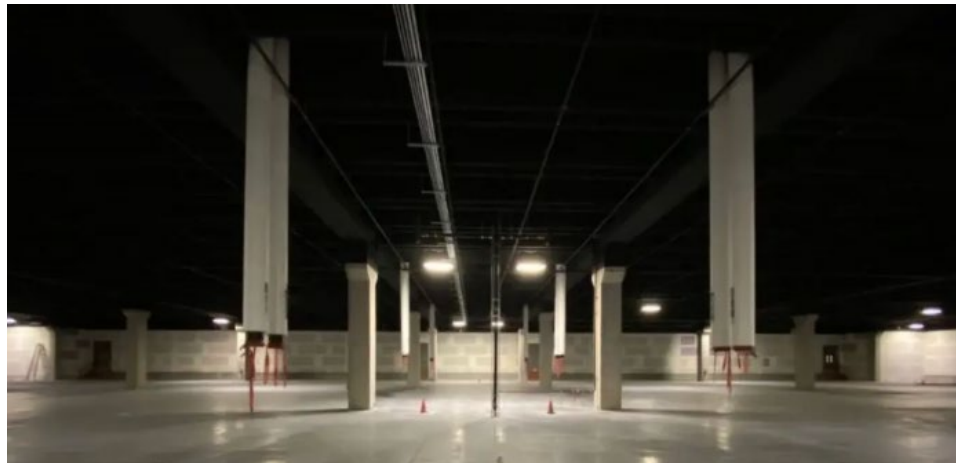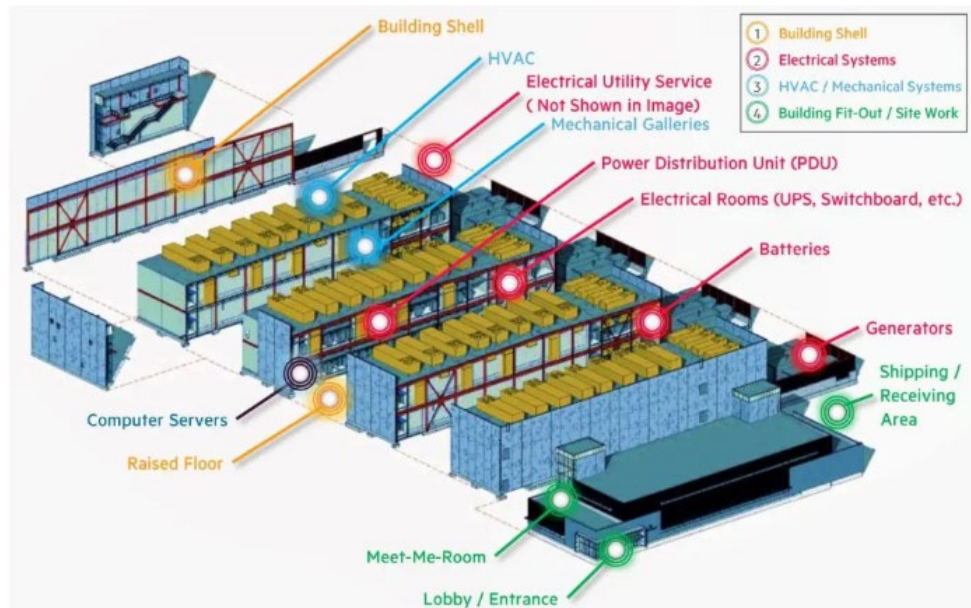
While this model increases the owner's time-to-value because leases can commence earlier,[7] it presents heightened risks. First, because tenants control the interior build-out, tenants contract with their own vendors, and GCs do not have the ability to vet the tenant hired contractors. Second, powered shells are phased build-outs based on demand.[8] The owner will complete the construction of the building shell but only gradually finish the data halls according to demands.[9] This means tenants may be operating servers in one area while construction continues in another, increasing the likelihood of performance issues,

---

[5] Rick Waddle, *How speed-to-market is transforming data center design and construction*, STACK INFRA, https://www.stackinfra.com/resources/thought-leadership/how-speed-to-market-is-transforming-data-center-design-and construction/#:~:text= Pre%2Dfabrication%20is%20fabulous,%2C%20in%20some%20cases%2C%20months.
[6] Mary Shang, *Powered Shell Data Centers: A Comprehensive Guide* (Feb. 13, 2024), https://dgtlinfra.com/powered-shell-data-centers/.
[7] *Id.*
[8] *Id.*
[9] *Id.*

equipment contamination, and potential liability for the project's general contractors.[10] Particularly, data center equipment cannot be exposed to dust, vibration, temperature fluctuations, or other environmental conditions.[11] If dust accumulates on circuit boards, sensors, or fans it can cause overheating, short circuits, or permanent failure.[12] Even minor vibrations can disrupt servers or storage devices, resulting in data errors or physical damage.[13] Temperature fluctuations are especially dangerous because they can push equipment outside safe operating ranges, triggering overheating, shutdowns, or long-term wear.[14] Because even small disturbances can take systems offline, environmental conditions must be tightly controlled at all times.

c. Supply Chain Constraints

Due to the specialized equipment and labor required, data center construction faces increased risks from supply chain delays and skilled labor shortages.[15] GPUs—silicon-based microprocessors that handle data—can take months or even years to procure.[16] Additionally, the increased and increasing demand for these projects creates competition for skilled labor and specialized contractors, often resulting in project backlogs.[17] These factors increase the risk of default and delays for project completion leading to greater liability for the GCs.[18] On some data center projects, equipment is procured early to avoid supply chain delays and price fluctuations, but this practice also poses risks as the early-procured equipment is susceptible to moisture and condensation exposures which may affect equipment performance and void warranties.

d. Contract-Imposed Performance Standards

Contracts for data centers specify performance criteria, unlike the typical commercial contract.[19] These metrics may include continuous data processing and storage capacities, internet connection speeds, power consumption, IT equipment cooling, and ambient temperature and humidity levels.[20] The contract provides for performance liquidated damages should the GC fail to meet the performance levels.[21] As a result, a GC's risk is significantly heightened: even if the building is structurally sound, failure to achieve the required performance standards can trigger substantial liability.

e. Increased Workforce Density and Site Congestion

Data center construction sites typically involve far more personnel than standard commercial building projects. For example, the scale of a $20 billion+ facility can involve

---

[10] *Construction Best Practices for Critical Equipment in Data Centers*, CADENCE, https://cadencenow.com/construction-best-practices-for-critical-equipment-in-data-centers/.
[11] *Id.*
[12] *Id.*
[13] *Id.*
[14] *Id.*
[15] *The Data Center Construction Risks, supra* note 1, at 21.
[16] *Id.*
[17] *Id.*
[18] *Id.*
[19] *Construction, Permitting & Delivery,* UMBREX, https://umbrex.com/resources/data-center-primer/construction-permitting-delivery/.
[20] *Building Data Centers—Key Considerations,* KING & SPALDING (April 10, 2025), https://www.kslaw.com/news-and-insights/building-data-centers-key-considerations.
[21] *Id.*

tens of thousands of workers on site at peak times, along with substantial equipment and building supplies moving in and out.[22] This level of congestion significantly increases the risk of missteps or faulty workmanship.[23] High worker density also raises the likelihood of bodily injury claims. Thus, the sheer volume of personnel and equipment magnifies the risks of bodily injury, faulty workmanship, and design defects.[24]

f. Geographic and Environmental Vulnerabilities

The target location for data centers is remote areas with ample land but underdeveloped local infrastructure, including limited grid capacity and transportation.[25] According to a Business Insider study, many new data centers are being built in regions such as Texas, the Midwest, and Arizona, areas that are highly exposed to severe weather.[26] These locations increase the risk of natural catastrophes, including tornadoes, hurricanes, and wildfires, creating potential for property damage and business interruption claims.[27]

g. Fire and Water Risks

Data centers are more prone to fire than standard commercial buildings due to their high electricity consumption for servers and cooling systems. A key risk comes from the increasing use of lithium-ion (Li-ion) batteries, which are replacing lead-acid batteries.[28] Li-ion batteries offer higher energy density, faster charging, and longer service life (up to 20 years), but they also present a higher fire risk that is harder to control due to thermal runaway, increasing the overall risk profile for data centers.[29] The extreme heat generated by data centers drives substantial cooling and water demands.[30] This extensive use of water for cooling and fire protection increases the risk of leaks, exposing both equipment and the building itself to potential water damage.[31]

III. Coverage Challenges

As a result of the heightened risks associated with data center construction, GCs must ensure they are insured to the fullest extent possible against these exposures. However, because the insurance market for data center construction is still developing, traditional Builder's Risk, Commercial General Liability, Subcontractor Default and Professional Liability policies may contain coverage gaps or present challenges in fully addressing these risks.

---

[22] R&I Editorial Team, *Data Center Building Boom Creates Insurance and Risk Management Complexities,* RISK & INSURANCE (Nov. 6, 2025), https://riskandinsurance.com/data-center-building-boom-creates-insurance-and-risk-management-complexities/.
[23] *Id.*
[24] *Id.*
[25] *The Data Center Construction Risks, supra* note 1, at 22.
[26] Adam Rodgers et al., *Tallying the True Costs of AI* (Jun. 17, 2025), https://www.businessinsider.com/ai-data-center-cost-2025-6.
[27] *The Data Center Construction Risks, supra* note 1, at 22.
[28] *Id.* at 6.
[29] *Id.* at 9-10; 12.
[30] *Id.* at 23.
[31] *Id.* at 24.

a. Builder's Risk Coverage

i. Overview of Builder's Risk Coverage

Builder's risk is a form of commercial property policy that provides coverage for the risk of direct physical loss to the construction project while it is being built.[32] Builder's risk insurance is commonly referred to as "course of construction insurance" because it covers a project in construction, before it becomes insurable as a building, while its materials and components are being moved on-site, assembled, and put in place.[33] Builder's risk policies require there be a "direct physical" loss to the construction project that is not otherwise excluded in order to trigger coverage.[34]

A builder's risk policy should include all parties with an "insurable interest," meaning any party whose financial stake would be adversely affected by a loss.[35] Typically, the policy is purchased by the building owner or the general contractor.[36] The purchasing party is responsible for ensuring that all relevant parties are listed as insureds, which commonly includes the owner or GC, subcontractors of all tiers, and sometimes financial lenders.[37]

Builder's risk policies are highly manuscript and can vary significantly from one policy to another.[38] Generally, they protect against physical loss or damage to property during construction, including the building or structure itself as well as materials, equipment, and machinery used in the construction process.[39] They may also cover indirect financial impacts such as lost income and additional costs caused by construction delays.[40] There are two primary types of builder's risk insurance: "all-risk" and "named peril."[41] All-risk policies provide broad coverage for all risks of loss except those explicitly excluded.[42] Named peril policies, by contrast, cover only losses caused by specific, listed perils such as fire, vandalism, weather events, explosions, or theft.[43]

Because builder's risk insurance is intended to protect insureds during construction, it is inherently temporary. Coverage typically begins on the project's "start date" and ends either on a specified date in the policy or when the project is considered "completed."[44]

---

[32] Jeffrey J. Vita & Michael V. Pepe, *Identifying and Accessing Coverage in Complex Construction Claims*, SAXE DOERNBERGER & VITA, P.C. (Sept. 21, 2021), https://www.sdvlaw.com/insights/identifying-and-accessing-coverage-in-complex-construction-claims.

[33] Rodrigo Garcia, Jr. et al., *Issues in Builder's Risk and Commercial General Liability Insurance* (2024).

[34] *Id.*

[35] *Id.*

[36] *Id.*

[37] *Id.*

[38] *Id.*

[39] *Id.*

[40] Garrett S. Nemeroff & Sergio F. Oehninger, *The AI Data Center Boom: Key Insurance Coverage Considerations for Complex Risks*, MORGAN LEWIS, https://www.morganlewis.com/pubs/2025/08/the-ai-data-center-boom-key-insurance-coverage-considerations-for-complex-risks?utm_source=.

[41] Vita & Pepe, *supra* note 31.

[42] *Id.*

[43] *Id.*

[44] Edmund M. Kneisel, *Builders' Risk and Other "First Party" Coverage for Construction-Related Property Damage* KILPATRICK, at 4-5.

Disputes often arise over what constitutes "completion."[45] Insurers frequently argue that work is "substantially complete" to limit coverage. Courts have taken varying approaches: for example, an Arkansas court enforced policy termination when a partially completed fertilizer plant was more than 40% occupied, reasoning that coverage ended once the owner made "substantial use" of the building.[46] In contrast, a Michigan court held that partial occupancy of a few apartments did not trigger completion for a larger project still under construction.[47]

This issue is particularly critical for data centers, especially powered shell projects. Since powered shells are built and occupied in phases, tenants may move in before the entire project is finished. This raises a key question: when is the project considered "complete" for Builder's Risk purposes? The answer is not yet settled. Coverage could terminate upon substantial completion of the first occupied phase, or it might continue until the final phase is finished, depending on the policy language and judicial interpretation. Some insurers may offer endorsements or coverage extensions to maintain protection during phased occupancy. Until courts or policies provide greater clarity, owners and contractors face significant uncertainty about the duration of Builder's Risk coverage for multi-phase data center projects.

ii.   Builder's Risk Coverage Exclusions

Builder's risk policies include several exclusions that can create significant challenges for data center construction. The most notable is the defective workmanship exclusion, which bars coverage for the cost of correcting faulty or inadequate work, including work performed by subcontractors.[48] Courts also treat negligent or poor-judgment work the same as defective work.[49] Data centers are particularly vulnerable because much of their value depends on highly technical installations—such as cooling systems, UPS units, generators, lithium-ion batteries, switchgear, and structured cabling. If these systems are installed incorrectly, builder's risk policies will not cover the defective work.

While builder's risk policies typically exclude losses caused by defective workmanship, most include an "ensuing loss" provision, which restores coverage if the defective work causes a separate, covered peril. For example, a defective electrical installation that causes a fire may trigger coverage for the resulting fire damage, though not for the cost to correct the faulty wiring itself.[50] Courts have often interpreted such provisions broadly, permitting coverage for losses to property that occur as a consequence of an excluded

---

[45] *Id.* at 6.
[46] *McCarty v. Maryland Cas. Co.,* 429 F. Supp. 112 (W.D. Ark. 1976).
[47] *American & Foreign Ins. Co. v. Allied Plumbing & Heating Co.,* 194 N.W.2d 158 (Mich. Ct. App. 1971).
[48] Michael A. Stover, *A Guide to Builder's Risk Insurance*, 53 Tort Tr. & Ins. Prac. L.J. 819, 833-84 (2018).
[49] *Id.* at 834.
[50] *See Vision One, LLC v. Philadelphia Indem. Ins. Co.*, 276 P.3d 300, 308-09 (2012) (finding that the ensuing loss clause restored coverage to collapse damages because collapse is covered under the policy, despite the cause of the collapse being attributable to the faulty workmanship of the insured); *Sel. Way Ins. Co. v. Natl. Fire Ins. Co. of Hartford*, 988 F. Supp. 2d 530 (D. Md. 2013) (concluding that while the cost of replacing the faulty installation of the water line fitting was excluded under the workmanship exclusion, the ensuing damage to the building from the flow of water was an ensuing loss covered under the policy).

event, as long as the ensuing loss is otherwise covered by the policy.[51] Applied to data centers, this supports a strong policyholder argument. For instance, if a misinstalled cooling system causes operational failures such as server overheating or system shutdowns, these failures could qualify as an ensuing loss. While the cost to repair or replace the defective cooling system would remain excluded, the resulting equipment damage, downtime, and related losses would be covered under the ensuing loss provision. Conversely, some courts take a narrower view, holding that ensuing loss coverage does not apply when the resulting damage flows directly and proximately from the excluded peril, requiring a separate and independent cause for coverage.[52] Under this interpretation, equipment damage and operational disruption caused by defective installation could be deemed part of the excluded work and therefore not covered.

Builder's risk policies typically contain exclusions related to moisture in the atmosphere and corrosion. These exclusions may preclude recovery under a builder's risk policy that results from dampness and improper temperatures related to equipment that is stored temporarily until it can be installed. Further, sometimes manufacturers will void their warranties if equipment is not stored properly. Many builder's risk policies do not consider a voided warranty to be "direct physical damage" under the policy, and thus, there may be no coverage in these circumstances.

Builder's risk policies also commonly exclude owner-supplied or contractor-supplied machinery used in the construction process.[53] In data centers, this means that while permanent systems—such as elevators, electrical equipment, HVAC units, and water pumps—are typically covered, expensive construction tools, temporary cooling units, or other specialized equipment used to install servers, racks, or cooling systems are not. [54] This creates potential coverage gaps for GCs.

Another common exclusion is for damage to existing buildings or structures caused by ongoing construction.[55] In phased data center projects, portions of the facility may already be operational while new sections are under construction. Work on unfinished areas could inadvertently damage completed areas, leaving owners and contractors exposed to costly repairs. Even if the parties negotiate waivers of subrogation related to permanent property coverage of the buildings turned over, the party procuring the permanent property insurance is often not a party to the prime contract. As such, these waivers can be meaningless when a claim occurs.

---

[51] *See e.g. Bartram, LLC v. Landmark Am. Ins. Co.,* 864 F.Supp.2d 1229 (N.D. Fla. 2012); *Vision One, LLC v. Philadelphia Indem. Ins. Co.*, 174 Wash.2d 501, 276 P.3d 300 (2012); *Arnold v. Cincinnati Ins. Co.,* 276 Wis.2d 762, 688 N.W.2d 708 (2004); *Selective Way Ins. Co. v. Nat'l Fire Ins. Co. of Hartford,* 988 F.Supp.2d 530 (2013); *Eckstein v. Cincinnati Ins. Co.,* 469 F.Supp.2d 444 (W.D. Ky. 2007).
[52] *See e.g., TMW Enterprises, Inc. v. Federal Ins. Co.,* 619 F.3d 574 (6th Cir. 2010); *Friedberg v. Chubb & Son, Inc.,* 691 F.3d 948 (8th Cir. 2012); Sapiro v. Encompass Ins., 221 F.R.D. 513 (N.D. Cal. 2004); *Acme Galvanizing Co. v. Fireman's Fund Ins. Co.,* 221 Cal.App.3d 170, 270 Cal.Rptr. 405 (1990).
[53] Stover, *supra* note 47, at 831.
[54] *Id.* at 831-31.
[55] *Id.* at 838.

Finally, builder's risk policies generally exclude contractual liquidated damages or penalties.[56] For example, if the owner-general contractor agreement requires the contractor to pay a penalty for project delays, the builder's risk policy will not cover that payment, even if the delay results from a covered event. As a result, the contractor's financial risk is increased.

b. General Liability Coverage

i. Overview of CGL Coverage

Commercial General Liability (CGL) policies are typically standardized forms—commonly ISO CG 00 01 01 96—providing coverage for "those sums that the insured becomes legally obligated to pay as damages" due to "bodily injury" or "property damage" caused by an "occurrence," or due to "personal and advertising injury," provided the injury occurs within the coverage territory during the policy period.[57] Most construction contracts include warranty and indemnity obligations for ongoing and completed work.[58] Project-specific CGL policies include a policy period which is typically several years designed to encompass the period of construction, followed by an extension of coverage for completed work.[59] During the policy period, the insured's have coverage for both ongoing and completed operations.[60] The extension then provides certain coverage for a period of time after the policy period.[61] Notably, these extensions are manuscripts and vary significantly from insurer to insurer.[62] For data center construction, the insured's primary concern should be ensuring that the completed operations extension fully addresses their CGL exposure for the entire statute of repose. Damage from defective work may not manifest until the facility is operational, as critical systems—such as cooling, electrical infrastructure, and other technical installations—may only be fully tested and stressed once the data center goes live.

ii. CGL Coverage Exclusions

The contractual liability exclusion (commonly Exclusion b) bars coverage for losses the insured is obligated to pay solely because of assuming liability under a contract or for claims arising from a breach of contract.[63] Notably, it excludes claims stemming from contractual warranties requiring the insured to repair or replace its own defective work.[64] For example, in a data center project, a contractor's agreement may include a warranty to fix any defective work, such as improperly installed cooling systems. If a contractor improperly installs a cooling system that malfunctions and must be fixed, the CGL policy

---

[56] Kneisel, *supra* note 43, at 10.
[57] Vita & Pepe, *supra* note 31.
[58] Jeremiah M. Welch (Saxe Doernberger & Vita, P.C.) & Chad Hall, *Project-Specific Policies and Products-Completed Operations Hazard Extension*.
[59] *Id.*
[60] *Id.*
[61] *Id.*
[62] *Id.*
[63] Adam P. Handfinger et al., *Managing Construction Risk Through Commercial General Liability Insurance*, Thomson Reuters, at 6.
[64] *Id.*

generally will not cover the cost, because this is a contractual obligation rather than a covered "occurrence."

Exclusion j(4) removes coverage for damage to "personal property that is in the care, custody, or control of the insured."[65] This exclusion applies only to personal property, not to real property such as buildings or permanently attached fixtures.[66] In data-center claims involving j(4), a critical question becomes whether the electronic equipment inside the data hall—servers, racks, cooling system, and other IT components—are personal property or fixtures. Property law recognizes two categories of fixtures: permanent fixtures and trade fixtures.[67] A permanent fixture is former personal property that has been "permanently attached to real estate with the intention that it shall become part of the freehold title thereto passes to the owner of the freehold."[68] To qualify, the equipment must be intended to become part of the building.[69] Conversely, a "trade fixture"—although physically attached—is the tenant's personal property, installed for the purpose of conducting the tenant's business, and is presumed to remain personal property."[70] Data center equipment most appropriately fits the definition of trade fixtures. Server racks, IT hardware, and similar components are installed for the tenant's operations, are not intended to become part of the building, and can typically be removed without damage to the structure. Accordingly, this equipment is best characterized as personal property— which means that j(4) is implicated and insurers may attempt to invoke it to deny coverage.

Exclusion j(5) eliminates coverage for property damage to "that particular part of real property on which you or any contractors or subcontractors working directly or indirectly on your behalf are performing operations, if the 'property damage' arises out of those operations."[71] In practice, this bars coverage for faulty workmanship. For example, if an HVAC subcontractor installs a defective HVAC system causing data center batteries to overheat and explode, destroying racks of servers, j(5) would exclude coverage for the costs to repair the HVAC system itself, as that is "that particular part" worked on, however, coverage may exist for damage to the servers, which were not the part being worked on. Some jurisdictions, however, interpret "that particular part" broadly, treating it as the full area—or even the entire project—within the contractor's scope.[72] Applied to a data center build, this approach would significantly limit coverage for general contractors: because a GC's scope typically encompasses the entire facility, any damage anywhere in the building could be treated as occurring to "that particular part," effectively eliminating

---

[65] CG 00 01 01 96.
[66] Craig Stanovich, *Care, Custody, or Control Exclusion in the CGL (*Oct. 1, 2008),
https://www.irmi.com/articles/expert-commentary/care-custody-or-control-exclusion-in-the-cgl.
[67] *Mogilevsky v. Rubicon Tech., Inc.,* 2014 IL App (1st) 132702-U, ¶ 19.
[68] *Id.*
[69] *Id.* at ¶ 20-21.
[70] *Id.* at ¶ 21.
[71] CG 00 01 01 96.
[72] *See e.g., Bituminous Cas. Corp. v. N. Ins. Co. of N.Y.*, 548 S.E.2d 495 (Ga. App. 2001) (follows minority rule that "particular part" is entire house because general contractor was responsible for entire project); *E.H. Spencer & Co., LLC v. Essex Ins. Co.,* 944 N.E.2d 1094 (Mass. App. 2011) (same).

coverage for almost any property damage claim arising from the GC's or its subcontractors' operations.

The "impaired property" exclusion (usually Exclusion M) bars coverage for losses involving property that hasn't been physically damaged but is impaired due to: (1) a defect or deficiency in the insured's work or product, or (2) the insured's failure to perform a contract.[73] Essentially, it excludes coverage for economic losses arising from defective work itself.[74] However, the exclusion does not apply if there is damage to property other than the insured's work or if the insured's work cannot be repaired or replaced without causing physical injury to other property.[75] The key distinction is whether there is physical injury to property beyond the insured's work, which may trigger coverage despite the exclusion.[76]

A common issue in data centers is whether damage to data or data systems constitutes "property damage" sufficient to trigger CGL coverage.[77] Property damage is generally defined as "physical injury to tangible property" or "loss of use of tangible property that is not physically injured."[78] While the servers themselves are tangible property and physical damage to them is typically covered, electronic data stored on the servers is generally not considered tangible property under most traditional policy terms and therefore is not covered.[79] Even in jurisdictions where damage to data might be recognized as property damage,"[80] most CGL policies include an exclusion titled "Access or Disclosure of Confidential or Personal Information and Data-Related Liability," which bars coverage for damages arising from "[t]he loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data."[81] The exclusion defines "electronic data" to include "information, facts or programs stored as or on, created or used on, or transmitted to or from computer software, including systems and applications software . . . which are used with electronically controlled equipment."[82] To address these gaps in CGL coverage for cyber-related losses, data center owners and contractors should obtain dedicated cyber or network security insurance.[83]

---

[73] CG 00 01 01 96; Tracy Alan Saxe & Maria Pepe VanDerLaan, Sᴀxᴇ Dᴏᴇʀɴʙᴇʀɢᴇʀ & Vɪᴛᴀ, P.C., *Construction Defects and Additional Insured Coverage in Mediation*.
[74] Saxe & VanDerLaan*, supra* note 72.
[75] *Id.* (citing *Stand. Fire Ins. Co. v. Chester O'Donley & Associates, Inc.,* 972 S.W.2d 1, 10 (Tenn. App. 1998)).
[76] *Id.*
[77] *Data Centers: Emerging Risks and Insurance Coverage Considerations* (Oct. 21, 2025), https://www.cov.com/en/news-and-insights/insights/2025/10/data-centers-emerging-risks-and-insurance-coverage-considerations.
[78] CG 00 01 01 96.
[79] Larry P. Schiffer et al., *CGL Exclusions for Cyberattacks and Loss Of Electronic Data*, https://www.squirepattonboggs.com/-/media/files/insights/publications/2020/08/cgl-exclusions-for-cyberattacks-and-loss-of-electronic-data-is-there-a-gap-in-your-coverage/cgl-exclusions-for-cyberattacks-and-loss-of-electronic-data-is-there-a-gap-in-your-coverage.pdf.
[80] *See Am. Guarantee & Liab. Ins. Co. v. Ingram Micro, Inc.,* No. CIV. 99-185 TUC ACM, 2000 WL 726789, at *1 (D. Ariz. Apr. 18, 2000) (holding that computers suffered "physical damage," as required by the CGL policy, where information stored in the computers' memory was destroyed).
[81] Schiffer, *supra* note 78.
[82] *Id.*
[83] *Id.*

c. *Professional Liability*

Professional liability insurance covers claims arising from the rendering—or failure to render—professional services, which are typically excluded under standard CGL policies.[84] In construction, professional liability insurance—also called errors and omissions (E&O) insurance—is essential not only for architects, engineers, and other design professionals, but also is essential for construction contractors building data centers.[85]

Contractor professional liability insurance protects a contractor or subcontractor against errors or omissions in the provision of professional services (which can be defined to include Construction Management Services) in connection with a construction project.[86] It is particularly valuable for contractors who provide in-house design services or retain third-party design professionals, such as architects, engineers, technical or specialty subcontractors (with a scope of delegated design duties), surveyors, and other specialists, as it covers mistakes made by these parties.[87] It is a common misconception that general liability policies cover professional liability risks; they do not.[88] Professional liability insurance covers economic losses resulting from professional errors, and unlike general liability insurance, property damage or bodily injury is not required to trigger coverage.[89]

Contractor E&O policies may cover the following types of claims:

- In-house building design service errors or omissions, such as architectural and engineering services offered by the general contractor;
- Specialty contractors or subcontractors with delegated design duties;
- Design and building service mistakes made by third-parties, such as architects, engineers, and other building professionals hired by the general contractor; and
- Construction management errors.[90']

Standard Contractor Professional Liability policies generally do not cover:

- Mistakes made during the bidding process, either overbidding or underbidding;
- Time management issues;
- Construction Errors/Damage from Faulty Workmanship;
- Means and Methods Errors;
- Operation and maintenance errors to the equipment made by the contractor or subcontractor; and
- Bodily Injury.[91]

---

[84] Vita & Pepe, supra note 31.
[85] *What is Contractor Professional Liability*, Saxe Doernberger & Vita, P.C.
[86] *Id.*
[87] *Id.*
[88] *Id.*
[89] *Id.*
[90] *Id.*
[91] *Id.*

GCs face significant financial exposure when contracting to meet specific performance criteria, such as temperature stability, humidity control, and uptime requirements. For example, if a GC delegates the design of a data center's cooling system to a mechanical engineer who lacks professional liability coverage, and the engineer miscalculates the heat load, the HVAC system may fail to maintain required tolerances.[92] If the data center cannot meet contractual temperature specifications, the owner could demand millions from the GC to replace or reconfigure the system.[93] Because these losses are purely economic, neither CGL nor Builder's Risk policies would respond—only a professional liability policy could provide coverage. Thus, it is critical for GCs to obtain professional liability policies but must ensure that the definition of "professional services" in the policy aligns with the contractor's actual roles. If the definition is too narrow, the insurer may deny coverage, leaving the contractor exposed to substantial financial risk. It is also critical for the GCs to ensure that the subcontractors with delegated design duties also procure appropriate professional liability insurance.

d. Wrap-Up Insurance Policies

It has become increasingly common for owners and contractors to purchase consolidated or "wrap-up" insurance programs that cover the entire project and most, if not all, on-site participants.[94] These programs replace what would otherwise be separate policies held by the owner, general contractor/construction manager, and subcontractors with a single, unified insurance structure.[95] Most wrap-ups include CGL and excess/umbrella coverage, and some also incorporate workers' compensation insurance.[96] A wrap-up is usually procured by either the owner (an "Owner Controlled Insurance Program" or "OCIP") or the general contractor (a "Contractor Controlled Insurance Program" or "CCIP").[97] All project participants performing on site work, with a few notable exceptions[98], are typically included as insureds on the wrap-up policies and have equal rights to coverage thereunder.[99]

Given the size and scope of data center construction projects, wrap-up policies are often at play. This offers advantages to both the entity procuring the coverage and the other project participants.[100] Given the economies of scale involved, the procuring party typically has greater bargaining power with potential insurers.[101] As a result, it can often secure better coverage terms than any one party could obtain on its own.[102] The party sponsoring the wrap-up controls the coverage it procures. However, these programs often

---

[92] Fred Muse, *Professional Liability: Are Contractors Adequately Protected* (Dec. 1, 2000), https://www.irmi.com/articles/expert-commentary/professional-liability-are-contractors-adequately-protected.
[93] *Id.*
[94] Vita & Pepe, supra note 31.
[95] *Id.*
[96] *Id.*
[97] *Id.*
[98] Most wrap-up policies will exclude coverage for certain "high risk" insureds, such as hazardous materials remediation contractors or transport companies, as well as those project participants who do not perform any actual work or labor at the project site (e.g., suppliers, truckers, etc.). Design professionals are also usually excluded from participation in wrap-up programs.
[99] Vita & Pepe, supra note 31.
[100] *Id.*
[101] *Id.*
[102] *Id.*

include excess limits that are too low for the scale and risk profile of data center projects. They also often contain unusual manuscript exclusions (e.g., course of construction property damage exclusions) that can negatively impact coverage that enrolled parties typically can count on under their own corporate programs. However, when participating in a wrap up, most enrolled parties cannot rely on coverage from their own corporate programs due to "wrap-up exclusions" that their own carriers include in the corporate policy. As such, it is important for GCs and other enrolled parties to review and negotiate insurance provided under a data center wrap-up carefully.

e. Subcontractor Default Insurance ("SDI")

Subcontractor Default Insurance ("SDI") is a first-party insurance product that reimburses an insured contractor for losses arising from a subcontractor's default. SDI typically covers the cost to complete the work, the cost to correct defective or non-conforming work, related legal and professional fees, and expenses incurred in investigating, adjusting, litigating, or defending disputes tied to the default.[103] SDI is often viewed as an alternative to performance bonds, but it differs in several key ways:

1. SDI is a two-party insurance agreement between Contractor and Insured as opposed to a three-party guarantee arrangement between bonding company, subcontractor, and contractor.

2. The Contractor prequalifies the subcontractors as opposed to the bonding company. Coverage extends to the policy limit, unlike a bond which is limited to the value of the contract.

3. The insurer responds quickly to the claim as opposed to the bonding company, which can take considerable time to investigate the claim.[104]

Given the complexity, pace, and subcontractor-heavy nature of data center construction, SDI can be critical to managing default risk. Yet many owners decline to have the GC procure SDI or subcontractor bonds, and the parties, instead, rely on weaker contractual indemnity provisions that offer far less protection than an insurance policy or surety product.

Also, the subcontractor volumes and bid package sizes for data center projects often far exceed those on a typical construction project and they do not fit nicely into a corporate rolling SDI program. Complicating matters, the SDI marketplace has limited capacity/appetite to provide high per loss and aggregate loss limits for these projects. To get enough capacity, it often takes more than one carrier to participate in the data center program. Coverage gaps can inadvertently occur when structuring these mega data center project programs since buildings are often phased and have different funding sources, and some carriers don't have the appetite to participate in every phase of the program and multiple excess carriers may need to be incorporated for various phases. This layering of coverage can inadvertently result in coverage gaps if the GC and its brokers do not carefully think through and negotiate how coverage layers will attach when

---

[103] *Id.*
[104] *Id.*

one subcontractor, involved in multiple subcontracts and phases of the project, defaults, and the multiple phases have different carriers participating.

IV. Practical Solutions

a. *Align contracts with insurance requirements*

GCs should ensure that their contractual obligations align with the scope of the insurance purchased. For data center projects, risk allocation must clearly identify which entity holds which insurance obligations and who bears liability for performance failures. Without this alignment, GCs may inadvertently assume obligations that their insurance programs do not cover. Also, it is important to understand the big picture when it comes to contracting. As a GC, you should be aware of who you are contracting with and how they fit into the big picture of the facility you are building. Are they the end user or are they a special purpose entity that is formed just to build the facility? Are they going to lease the facility to others who will ultimately be the end users of the facility? Do you understand the terms in the leases and do the contractual promises in the leases protect you (e.g., waivers of subrogation related to permanent property damage claims, or limitations of liability related to construction defects)? What other methods of risk management will you use to protect yourself from risks that are not effectively transferred under the contract documents?

b. *Engage brokers early for tailored endorsements and capacity solutions*

Data center risks require a range of insurance coverage and manuscript endorsements. Thus, GCs should engage with insurance brokers early who know the business in order to secure appropriate coverage, negotiate expanded definitions, and avoid capacity issues.

c. *Address phased completion explicitly in insurance and contract language*

Because data centers are typically built in phases based on demand, contracts and policies must define when Builder's Risk coverage and CGL "ongoing operations" terminate. This will help avoid gaps in coverage especially where policies contain "course of construction" exclusions or limit completed-operations coverage.

d. *Implement robust prequalification and risk mapping*

Data center construction requires high technical competency. GCs must prequalify subcontractors to avoid potential future risks. A risk map helps identify high-exposure systems where failures could result in costly delays or contractual penalties that traditional CGL or BR policies will not cover. Implementing robust prequalification processes, including implementing detailed risk mitigation planning is crucial to protecting against subcontractor and vendor default.

e. Educate teams on tenant equipment sensitivities and performance criteria

GCs should ensure their construction teams understand the performance requirements for the facility, such as temperature and humidity ranges, power tolerances, and uptime obligations that are built into contracts. Awareness of these tolerances reduces inadvertent system failures and helps avoid uninsured financial losses.

V.   Conclusion

Data center projects layer schedule-driven risk, tenant performance pressure, and performance lease obligations on top of already complex construction exposures. These facilities must not only be built correctly but also perform as promised long after construction ends, which expands GCs' risk far beyond traditional commercial construction. At the same time, insurance for data center work is highly manuscript and often fails to align naturally with the performance obligations imposed by contracts and leases. Accordingly, GCs must be proactive and formulate a tailored risk-transfer strategy to ensure they are adequately protected against the unique and evolving exposures presented by data center construction.