DATA CENTER CHECKLIST

Procurement & Vendor Risk

AI-Enabled Infrastructure, Systems, and Services

HOW TO USE THIS CHECKLIST

This checklist is designed to help executive teams and in-house counsel identify and manage legal, operational, and regulatory risks associated with procuring hardware, software, and services for modern data center environments. It is not intended to be exhaustive or to provide legal advice but rather to highlight issues that can materially affect reliability, security, cost certainty, and compliance if not addressed early. The questions below are intended to support informed decision-making and coordinated planning across legal, procurement, infrastructure, and operational teams.

WHO THIS IS FOR

CFOs, COOs, CIOs, GCs, chief procurement officers, and infrastructure and operations leaders responsible for sourcing and managing data center vendors and technology providers.

01. Scope of Procurement & Embedded AI Capabilities

- ☐ Are all procured systems, equipment, software, and services clearly identified and scoped?
- ☐ Do semiconductor, equipment, and networking hardware specifications reflect intended operational use, performance requirements, and scalability needs?
- ☐ Have you identified the key vendors from which to procure these systems, tools, and services?

WHY IT MATTERS:

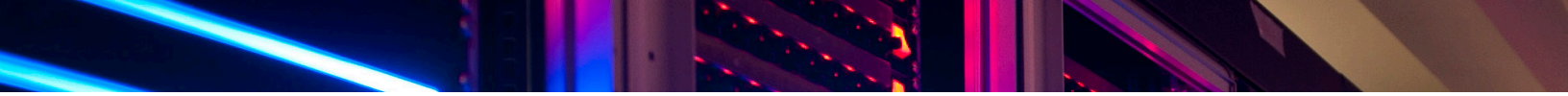
Different AI use cases can lead to varying operational requirements with unique and often complex hardware and services needs not always present in traditional procurement models.

02. Vendor Due Diligence & Risk Assessment

- ☐ Have vendors been assessed for technical capability, financial stability, and operational resilience?
- ☐ Have security posture, compliance maturity, and incident history been evaluated?
- ☐ Are vendors or critical suppliers subject to sanctions, export controls, or geopolitical risk?
- ☐ Are subcontractors, OEM dependencies, and upstream supply chains identified?

WHY IT MATTERS:

Vendor failures or disruptions can have cascading effects across data center operations, and continuity of supply is of paramount importance to satisfy downstream obligations to customers.



03. Contractual Risk Allocation & Performance Standards

- ☐ Are service levels, uptime commitments, and performance metrics clearly defined?
- ☐ Are remedies, credits, and termination rights aligned with actual operational impact, downtime risk, and customer-facing SLAs?
- ☐ Are warranties appropriate for the equipment or services being provided?
- ☐ Does the contract clearly allocate responsibility for regulatory compliance?

WHY IT MATTERS:

Contracts are the primary mechanism for allocating operational and regulatory risk. There may be customer reliability requirements that need to be reflected in agreements with your vendors to ensure your compliance.

04. Pricing, Cost Certainty & Change Control

- ☐ Are pricing structures transparent and tied to clearly defined deliverables?
- ☐ Are price escalation, indexing, and pass-through mechanisms subject to unambiguous parameters?
- ☐ Are change-order and scope-expansion controls clearly defined?
- ☐ Are long-term total cost assumptions tested against realistic scale scenarios?

WHY IT MATTERS:

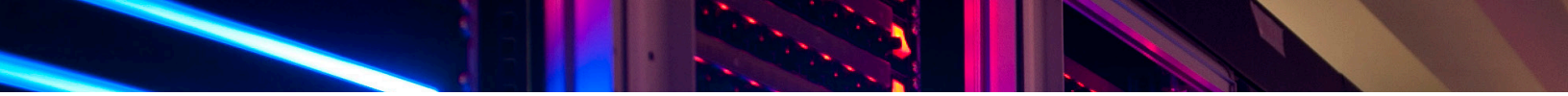
Cost volatility and uncontrolled scope creep undermine procurement strategy and forecasting.

05. Open-Source, IP & Licensing Considerations

- ☐ Are open-source components in firmware and software identified and evaluated for “copy-left” or other potential risks for the contemplated use case?
- ☐ Are IP ownership and usage rights clearly defined and fixed in the procurement agreement and not subject to change (e.g., by incorporating a hosted license agreement)?
- ☐ Are indemnities in place for claims that vendor’s IP infringes a third party’s rights?
- ☐ Does the agreement specify any restrictions on modification, integration, or resale?

WHY IT MATTERS:

IP and licensing risks can create long-term compliance and commercialization constraints and limit exit opportunities.



06. Supply Chain Resilience & Continuity

- ☐ Are critical components subject to long lead times or single-source dependency?
- ☐ Are contingency plans in place for supply disruptions or vendor disruptions?
- ☐ Are force majeure, allocation, and delay risks allocated appropriately?
- ☐ Are vendors required to provide advance notice of material supply chain changes?
- ☐ Are potential damages resulting from late delivery risk sufficient to cover construction or buildout downtime?

WHY IT MATTERS:

Supply chain fragility can undermine delivery timelines and operational stability.

07. Compliance, Audit & Regulatory Readiness

- ☐ Are audit rights sufficient to verify compliance, performance, and security controls?
- ☐ Are regulatory obligations and industry-standard obligations integrated into vendor obligations?
- ☐ Are reporting, recordkeeping, and documentation requirements clearly defined?
- ☐ Are regulatory developments monitored for impact on vendor arrangements?

WHY IT MATTERS:

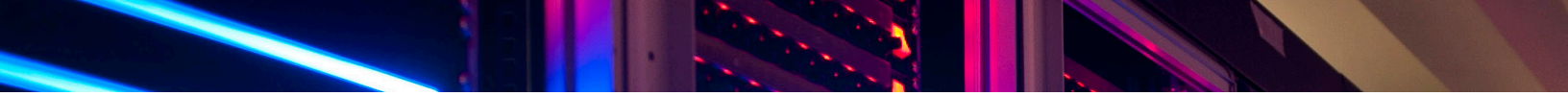
Regulatory scrutiny increasingly extends to vendor relationships and third-party risk management.

08. Exit, Transition & Substitution Planning

- ☐ Are termination rights feasible and enforceable in practice?
- ☐ Are transition assistance and cooperation obligations defined?
- ☐ Can vendors or systems be replaced or substituted without material disruption?
- ☐ Are exit scenarios aligned with long-term operational and scaling strategy?

WHY IT MATTERS:

Inflexible vendor relationships can lock in risk and limit future options.



When To Call Us

YOU SHOULD INVOLVE US EARLY IF:

- Hardware or services are critical to site operations or uptime
- Vendors retain operational control or access to systems
- Regulatory, export control, or national security issues affect sourcing
- Supply chain or geopolitical risk affects delivery or pricing
- Multivendor risk allocation requires coordination
- Long-term flexibility and substitution are core to the platform strategy

We help clients structure procurement and vendor relationships to manage risk, preserve flexibility, and support reliable, compliant data center operations at scale.

Authors:

Michael Herrera
Partner | San Diego
MichaelHerrera@perkinscoie.com

Christopher Wieman
Partner | Chicago
ChristopherWieman@perkinscoie.com

For additional resources, visit: perkinscoie.com/datacenterhub.

Perkins Coie