DartPoints
DATA CENTERS

MANUFACTURING INFRASTRUCTURE PROVIDER VALIDATION CHECKLIST

Most infrastructure providers can answer yes to the basics: 24x7 support, redundancy, recovery, compliance, and capacity. The harder question is what that “yes” actually covers in your environment.

For every major provider claim, verify five things:

1. What does it cover?
2. When was it last tested or reviewed?
3. Who owns it?
4. What is excluded?
5. Where is it documented?

1 Validate fit against your environment

1. Define ownership

Validation Area	What To Verify?
Infrastructure	What does the provider own and operate directly?
Network	Which connectivity, carrier, and routing responsibilities sit with the provider versus your team?
Security	Which controls does the provider manage, and which remain the customer's responsibility?
Monitoring	What does the provider monitor, how are alerts handled, and where does visibility stop?
Backup	Who owns backup configuration, testing, retention, and remediation when backups fail?
Recovery	Who initiates recovery, who executes it, and which recovery activities remain with your internal team or another vendor?

2. Test a plant scenario

During a connectivity failure affecting production systems:

- What can the provider diagnose and fix directly?
- Where does its responsibility end?

3. Verify local support

- Which support team would actually cover your environment?
- What happens after hours when hands-on help is needed?
- What response or dispatch times apply to your location, and where are they documented?

4. Uncover unsupported dependencies

- Which legacy systems, specialized hardware, network architectures, or on-premises dependencies could fall outside the provider’s standard operating model?

Ask for:
Architecture and dependency maps, service boundaries, escalation ownership, and a relevant customer reference.

2 Define migration and transition risk

Request the transition plan you would expect to use in production, not a description of the provider's migration methodology.

- How do they approach discovery, sizing, dependency mapping, migration waves, rollback criteria, and cutover requirements?
- What have test migrations revealed, and how have those findings shaped the production migration plan?
- What must be true before production cutover is approved, and who makes that call?
- How do they define RPO, RTO, maintenance windows, and acceptable production disruption for a specific environment?

Ask for:
A migration plan, test results, a rollback procedure, and named owners.

3 Confirm support and operating model

- When the provider says "24x7 support," what does that actually include: ticket intake, investigation, hands-on remediation, engineering support, or vendor coordination?
- Who owns escalation and recovery when multiple parties are involved?
- What response and restoration commitments apply to your environment, and where are they written down?

Ask for:
Support scope, escalation matrix, response and restoration commitments, and the SLA or service schedule where they are documented.

What to verify

Apply the same standard to us. Review the published SLA for the specific availability, response, restoration, exclusions, and service-credit terms that apply to the services and location you are considering.

4 Resilience and recovery

- When was the relevant recovery scenario last tested and what did the test reveal?
- Which systems, facilities, connectivity paths, and dependencies were included?
- What operating state did the test achieve, and how does it compare with your recovery requirements?

NIST recommends realistic recovery scenarios, testing, lessons learned, and continual improvement.

Ask for:
Recent test evidence, scenario scope, results, corrective actions, and recovery assumptions.

5 Compliance and audit readiness

- Which framework and version apply to your environment?
- What locations, services, systems, reporting periods, and exceptions are covered?
- What responsibilities remain with your organization?
- What evidence can the provider show for an auditor to review?

For CMMC, CUI handling requirements, ISO 22301, SOC reporting, or customer-specific audits, validate the exact scope and currency of the evidence. A broad compliance claim does not establish that the infrastructure supporting your environment falls within that scope.

Ask for:
The current report or certification, scope statement, reporting period, documented exceptions, and bridge documentation where applicable.

6 Capacity and future readiness

- What capacity is available now in the markets you need?
- How does the facility support your power density, cooling, connectivity, and high-density workload requirements?
- What capacity can actually be delivered by your required date, and what depends on utility delivery, construction, or future expansion?

What to verify

Apply the same test to our capacity claims. Ask what is available now at the specific site you are considering, what can be delivered by your required date, and what depends on construction, utility delivery, or planned expansion.

Ask for:
Current available capacity, the provisioning timeline for your specific requirement, power and cooling assumptions, and anything the delivery date depends on.

THE DECISION STANDARD

The right provider should demonstrate current, scoped evidence for your requirements.

Before committing, ask:

- What is covered?
- When was it tested?
- Who owns it?
- What is excluded?
- Where is it documented?

Compare the proof behind each answer, not just the answer itself.