LoadSpring™

GUIDE

How to Choose Managed Cloud Hosting for P6

By Jim Smith, Co-Founder & Chief Operating Officer

Jim Smith, Co-Founder and COO of LoadSpring Solutions, has spent more than 25 years helping organizations manage the applications and technology that support complex project delivery.

Choosing a **managed hosting** provider for Primavera P6 starts with your project requirements, not a provider's feature list. Look for demonstrated expertise in managing P6 applications and databases, reliable performance for your users and project workloads, strong security and recovery capabilities, support for essential integrations, and clearly defined application-level support.

This guide gives IT and project controls leaders a practical framework for comparing providers using documented evidence, performance testing, service commitments, and total cost of ownership rather than advertised capabilities alone.

Key Takeaways

- **Clarify what's included.** Determine whether the provider manages infrastructure alone or also handles P6 application administration, databases, and technical support.
- **Verify security and compliance.** Confirm that security controls, data residency, access management, and recovery arrangements meet your organization's requirements.
- **Test application performance.** Evaluate P6 performance under realistic workloads, not just infrastructure uptime guarantees.
- **Validate integrations and flexibility.** Confirm that essential applications can exchange data and that you can retain control of your information.
- **Compare total cost of ownership.** Account for migration, licensing, support, ongoing administration, and potential exit costs—not just hosting fees.

LoadSpring™

What Is Managed Cloud Hosting for P6?

Managed cloud hosting for P6 places your Primavera P6 environment under a third-party provider's operational management. The service agreement defines the scope: infrastructure, database administration, application maintenance, security patching, backups, monitoring, and user support should each have a named owner.

Don't assume that "managed" includes every layer. One offer may cover servers and backups while another includes application administration. Your evaluation should make those boundaries explicit.

Why Application-Specific Experience Matters

Oracle Primavera P6 EPPM is a complex, data-intensive enterprise application. Large project portfolios, intricate schedules, thousands of activities, and multiple concurrent users place significant demands on application performance and database resources. When performance suffers, planners lose valuable time. And with sensitive project schedules, resource information, and potentially confidential contract data at stake, inadequate security and access controls can expose organizations to significant operational, contractual, and compliance risks.

Hosting P6 effectively requires expertise beyond cloud infrastructure. Look for a provider that understands the relationship between application performance, database configuration, security, and infrastructure, and knows how to manage risks and resolve issues across all four. Ask how they handle performance tuning, access controls, upgrades, and troubleshooting, and where their responsibilities end.

When Should You Consider Managed Cloud Hosting?

Managed hosting is worth considering when maintaining performance, security, and availability begins to strain internal IT resources or requires specialized expertise.

Start with the operational problem you need to solve. Moving infrastructure is not, by itself, a measure of success.

Common reasons to evaluate managed hosting include:

- Reduce the time internal teams spend maintaining infrastructure, applications, and support.
- Improve access and alignment for distributed project teams.
- Receive specialized support and reduce reliance on limited internal experts.
- Meet project-specific security and compliance requirements.

- Strengthen backup, recovery, and continuity arrangements.
- Standardize hosting across project applications.

Compare managed hosting with your current environment using the same requirements. Include transition effort, retained internal responsibilities, and contractual constraints rather than assuming that a change of hosting model will automatically improve cost or performance.

How to Evaluate Managed Cloud Hosting Providers for Primavera P6

Choosing the right provider requires looking beyond infrastructure and pricing to understand how well the hosting environment will support your P6 applications, project teams, and operational requirements. Use the following eight questions to compare managed cloud hosting providers, identify potential risks, and determine which services best meet your organization's needs.

1. What Security and Compliance Requirements Should a P6 Hosting Provider Meet?

Your P6 environment may contain sensitive project schedules, cost information, resource allocations, and contractor details. Your hosting evaluation should reflect the sensitivity of that information, along with security, regulatory, and contractual obligations. Define those requirements before reviewing a provider's security materials.

Review Security Evidence and Its Scope

Ask for documentation your security team can assess, including relevant **SOC 2 Type II** reporting and evidence supporting any ISO 27001 claims. Have reviewers distinguish documented alignment from certification rather than treating the terms as interchangeable.

For each document, confirm:

- Which services and environments are covered.
- Whether the proposed hosting service falls within that scope.
- Which customer responsibilities remain outside the provider’s controls.
- Whether the documentation is current and available for review.
- How findings and exceptions are addressed.

Treat security credentials as inputs to due diligence, not a blanket guarantee that every contractual or regulatory obligation is satisfied.

Understand Data Residency and Governance

Ask where production data and backups will reside, who can access them, and how those arrangements are reflected in the agreement. Location choices should meet your requirements for the proposed environment, not simply appear on a provider's global footprint map.

Review identity management and operational controls alongside location:

- Single sign-on integration with your identity provider.
- Role-based access and privileged-account management.
- User provisioning and access removal.
- Audit logging and access to relevant records.
- Backup access, retention, and recovery responsibilities.

Document who approves access changes and how your team will verify that the agreed controls remain in place.

2. How Do You Evaluate P6 Performance and Global Accessibility?

A performance comparison needs a defined workload and a clear baseline. Ask providers to demonstrate the proposed environment using conditions relevant to your organization.

Assess P6-Specific Performance

Your evaluation should account for project count, schedule complexity, database configuration, network latency, and concurrent usage. Ask how the provider would size and tune the environment for those conditions.

Request a test plan that identifies:

- The workflows to be measured.
- The environment and configuration used.
- The number and location of concurrent users.
- The baseline against which results are compared.
- The criteria your team will use to accept the results.

Do not accept a percentage improvement without the underlying test conditions and a comparison relevant to your own deployment.

Assess Global Accessibility

Major capital projects often involve planners, engineers, contractors, and project leaders working across multiple offices, job sites, and time zones. Use the locations and working patterns of your actual users to evaluate access. Ask providers to demonstrate the proposed access method rather than assuming every hosted deployment is browser-only or eliminates desktop clients and VPN connections.

Your assessment should cover:

- Supported access methods for your P6 deployment.
- Sign-in and identity-provider requirements.
- Performance from project offices, remote locations, and field sites.
- User experience during peak working hours.
- Responsibilities for resolving local connectivity problems.

3. What Uptime and Recovery Commitments Should You Require?

Set availability requirements around the operational consequences of interrupted access to P6. A platform uptime SLA is useful only when you understand what it measures, what it excludes, and how it relates to the application your teams use.

Read Beyond the Uptime Percentage

Apply the same questions to every proposed SLA:

1. **What is measured?** Establish whether availability refers to infrastructure, the platform, or the P6 application.
2. **How is it measured?** Identify the measurement period and the monitoring method.
3. **What is excluded?** Review planned maintenance and other exceptions.
4. **How are incidents communicated?** Confirm notification responsibilities and update expectations.
5. **What happens if the commitment is missed?** Review remedies and the process for requesting them.

Compare historical service reports with contractual commitments. Do not treat an advertised percentage as evidence of past application performance.

Review Service History

Ask for historical availability reports and examples of incident handling. Review how the provider communicated, restored service, and followed up afterward.

Customer references can add context when they reflect similar application environments and operational requirements. Use them alongside test results and documentation, not as a substitute for either.

Verify Recovery Arrangements

Multiple data centers do not, on their own, establish how your P6 environment will recover from an incident. Request the recovery plan for the service you would purchase.

Ask providers to document their Recovery Time Objective (RTO) and Recovery Point Objective (RPO). These define how quickly service should be restored and how much data loss is acceptable, respectively. Also review backup arrangements, restoration testing, and responsibilities during an incident.

For additional guidance on disaster recovery planning, see **NIST's Contingency Planning Guide for Federal Information Systems**.

Assess Proactive Monitoring

Ask what the provider monitors across infrastructure, databases, and applications. Establish who investigates alerts and when your team receives an update.

Request examples of how the provider handles performance degradation, storage concerns, and service interruptions. Focus on the process and supporting records rather than broad promises that monitoring prevents outages.

4. What P6 Expertise and Technical Support Should a Provider Offer?

When schedulers encounter P6 performance or application issues, they need support from people who understand the software, not just the underlying infrastructure. Infrastructure troubleshooting, database administration, application configuration, and project controls guidance are different services. Confirm which are included in the hosting agreement and which remain your team's responsibility.

Test P6 Expertise

Use representative issues from your own environment when assessing a provider’s support capability. Examples from this guide’s scope include schedule calculations, database performance, baseline comparisons, and resource leveling.

Ask who would investigate each issue, what information your team would need to supply, and when the provider would involve another party. Do not assume that hosting support includes every application or scheduling question.

> ***Real-world example: When MWH Constructors needed to establish an independent P6 environment following a corporate divestiture, the company required specialized expertise in Oracle Primavera P6 EPPM Web Services configuration. Working with LoadSpring, MWH migrated P6 and other critical project controls applications to a managed cloud environment, reducing the burden on its internal IT team. Read the MWH Constructors case study.***

Compare Support Commitments

Use a consistent checklist:

- **Coverage:** Does support availability match your operating hours and project locations?
- **Response:** What is the contractual response commitment for each severity level?
- **Resolution:** How does the provider distinguish an initial response from restoration or resolution?
- **Escalation:** Who takes ownership when an issue cannot be resolved at the first level?
- **Communication:** How often will your team receive incident updates?
- **Scope:** Which support activities are included, optional, or handled by another supplier?

Review these commitments with the people who will use the service, not only the procurement team.

5. How Well Does the Provider Support P6 Integrations?

P6 often sits alongside cost management, risk analysis, reporting, and ERP systems. Your hosting evaluation should account for those connections, not treat P6 as an isolated application.

For example, schedule data from P6 may feed cost management systems such as **Sequence Enterprise (formerly EcoSys)** or risk analysis tools such as **Acumen**, making reliable data exchange important for reporting and project decisions.

Map Required Connections

Start with the workflows your organization already relies on. Ask providers to demonstrate the integrations you require rather than accepting general compatibility claims.

For each connection, record:

- The source and destination systems.
- The information that must move between them.
- The required synchronization frequency.
- The owner of configuration and ongoing maintenance.

- The process for detecting and resolving failed transfers.
- The effect of upgrades or environment changes.

Set Appropriate Data-Movement Requirements

Do not make “real time” a universal requirement without a business reason. Define how current each downstream dataset needs to be and test whether the proposed approach meets that requirement. Ask providers to demonstrate a representative end-to-end workflow. Confirm that transferred information remains usable in the receiving system and that your team can identify when synchronization has failed.

Separate Hosting from Data and Analytics Scope

Hosting an application, connecting its data, and delivering analytics are distinct evaluation areas. Ask which capabilities are included in the proposed service and which require separate implementation or ongoing management.

If reporting or AI readiness is part of your business case, assess the data foundation as well as the hosting environment. Establish who is responsible for transformation, consistency, governance, and access before evaluating downstream analytics.

6. How Do You Evaluate Vendor Independence and Data Portability?

Assess flexibility through the agreement and the proposed architecture, not the provider’s category. Neither an independent hosting model nor a vendor-managed service establishes, by itself, how much control you retain.

Examine Operational Flexibility

Ask every candidate:

- Can you retain the application versions and configurations your organization needs?
- Which third-party applications and integrations are supported?
- Who controls administrative access and approves changes?
- Are there restrictions on accessing or exporting your information?
- What happens when your application portfolio changes?

Compare the answers with your likely future requirements. Distinguish requirements you need now from capabilities you may never use.

Document an Exit Plan

Before signing, establish how you would retrieve and transfer your P6 data and configurations if you needed to move to another hosting environment. Include data export formats, transition assistance, responsibilities, contractual conditions, and associated costs.

Request evidence that exported data and backups can support the transition you would need. An exit provision is useful only if your team understands how it would work in practice.

For more questions to consider when evaluating cloud provider restrictions, see **Five Questions to Ask About Data, Access, and Control in Vendor Clouds**.

7. What Should You Look for in a P6 Migration Plan?

Moving P6 to a new hosting environment requires careful planning to minimize disruption to active projects and the teams relying on their schedules. Ask for a migration plan based on your applications, data, customizations, integrations, and testing requirements rather than a generic completion estimate.

Use a Staged Migration Checklist

1. **Assess the current environment.** Identify application versions, databases, integrations, users, and dependencies.
2. **Prepare the target environment.** Agree on configuration, access, security, and responsibilities.
3. **Transfer and validate data.** Confirm that required information is present and usable.
4. **Test integrations and user workflows.** Include the project controls teams who depend on them.
5. **Approve cutover arrangements.** Define acceptance criteria, communications, responsibilities, and a fallback approach.
6. **Support the transition.** Establish go-live coverage and a process for resolving remaining issues.

Agree on milestones and ownership before committing to a cutover date.

> ***Real-world example: Chemours needed to migrate Primavera P6 from an on-premises environment to the cloud before scheduled manufacturing facility turnarounds. Working with LoadSpring, the company coordinated a staggered rollout across its sites, completing the transition with just one afternoon of downtime for users. Read the Chemours case study.***

Prepare Users for Access Changes

Training should reflect the changes users will actually experience. These may involve login procedures, access methods, or support processes rather than changes to P6 itself.

Ask what administrator guidance, end-user materials, and go-live support are included. Keep your internal team responsible for confirming that the transition works for the people delivering projects.

8. How Do You Compare Total Cost of Ownership (TCO) for P6 Hosting?

Compare hosting providers over the same period, such as three or five years, and against the same service scope. As **IBM explains in its overview of total cost of ownership (TCO)**, costs extend beyond the initial purchase price to include ongoing operational expenses. A monthly hosting fee therefore does not capture the full cost of operating a P6 environment.

Include These Cost Categories:

- **Implementation:** Environment setup, migration, configuration, testing, and training.
- **Licensing:** Relevant application and supporting software obligations.
- **Recurring operations:** Hosting, support, monitoring, backups, and agreed maintenance.
- **Integration:** Initial configuration and ongoing changes or troubleshooting.
- **Growth:** Additional users, storage, and workload requirements.
- **Internal effort:** Vendor management, access administration, reviews, and retained support tasks.
- **Exit:** Data export, transition assistance, and other contractual obligations.

Ask what changes the quoted amount and which activities require a separate agreement. Evaluate fixed and variable pricing against your expected usage rather than assuming either model is always preferable.

For an example of how hosting costs can vary across deployment models, see **LoadSpring's Total Cost of Ownership Comparison**, which compares estimated costs for on-premises hosting, commodity clouds, and managed hosting.

Consider Continuity Alongside Cost

Interrupted access to P6 can delay schedule updates, progress reporting, and decisions affecting active capital projects. Consider these potential consequences alongside recovery requirements when comparing hosting costs, using your organization's own assumptions to assess the financial impact.

Keep the financial comparison separate from unsupported claims that a particular provider will eliminate downtime or deliver a specific saving. The decision should rest on service scope, evidence, and your risk tolerance.

LoadSpring™

How to Build a Provider Evaluation Framework

Start with Non-Negotiable Requirements

Document requirements that a provider must meet to remain under consideration. These might include contractual data residency, supported P6 versions, critical application integrations, security evidence, recovery objectives, or support coverage during your operating hours.

Have IT, security, project controls, procurement, and other relevant stakeholders agree on these requirements before scoring proposals.

Compare Providers in Six Areas

1. **Security and governance:** Evidence of the controls and access arrangements your organization requires.
2. **Availability and recovery:** Defined service measurements, incident procedures, and tested recovery arrangements.
3. **Application performance:** Results from workloads representative of your P6 environment.
4. **Support:** Clear ownership, relevant expertise, coverage, and escalation commitments.
5. **Integration and portability:** Demonstrated workflows, accessible information, and a workable exit plan.
6. **Total cost:** A complete view of implementation, operation, retained internal work, and transition costs.

Weight these areas according to your organization's priorities and score each provider against the same criteria. Record the evidence supporting each assessment, and flag unverified claims or unanswered questions rather than treating them as confirmed capabilities.

Conclusion: Choose a P6 Managed Hosting Provider Based on Evidence and Operational Fit

The right managed hosting arrangement is the one that meets your P6 requirements with documented responsibilities, measurable service commitments, and costs your team understands.

Before selecting a provider, confirm that you can:

- Explain who manages each layer of the environment.
- Validate security and governance arrangements.

- Assess application performance under representative conditions.
- Rely on defined support and recovery procedures.
- Maintain required integrations and retrieve your information.
- Account for implementation, operation, and exit costs.

Use the same evidence requirements for every candidate. Resolve unanswered questions and confirm responsibilities in the service agreement before signing.

Considering Managed Hosting for Primavera P6?

LoadSpring brings decades of experience hosting and managing complex project applications, including Primavera P6, for organizations around the world. Our team can help you evaluate your current environment, identify opportunities to improve performance and support, and determine the right hosting approach for your needs. Talk to a P6 Hosting Expert

FAQs About How to Choose Managed Cloud Hosting for P6

What is the difference between managed hosting and SaaS for P6?

Managed hosting typically provides a dedicated or separately managed environment for your P6 applications, with responsibilities defined by the hosting agreement. SaaS generally delivers software as a provider-managed service, with less customer control over the underlying environment. The distinction depends on the offering, so confirm who controls application versions, configuration, upgrades, licensing, administrative access, and integrations.

How long does a P6 migration take?

A P6 migration timeline depends on the complexity of your environment, including data volume, customizations, integrations, validation, and more. Timelines can also vary by provider, depending on their P6 expertise and migration processes. Request an estimate based on your environment and agree on milestones and acceptance criteria before committing to a cutover date.

What security certifications should a P6 hosting provider have?

Look for providers with recognized security credentials relevant to your requirements, such as SOC 2 Type II and ISO 27001. Confirm that these credentials cover the hosting services you're considering and that the provider's security practices meet your organization's requirements for data protection, access controls, and disaster recovery.

Can managed hosting integrate P6 with other project applications?

Yes. Managed hosting can support P6 integrations with cost management, risk analysis, reporting, and ERP systems. Integration capabilities vary by provider and configuration. Confirm that the provider supports your required applications, data flows, and synchronization needs, and clarify who manages and troubleshoots those connections.

What support should I expect from a P6 managed hosting provider?

A P6 managed hosting provider should offer technical support with clearly defined coverage hours, response times, severity levels, and escalation procedures. Confirm which infrastructure, database, and P6 application issues the provider handles, which remain your responsibility, and how issues involving other suppliers are escalated. Providers differ in their application-specific expertise and support availability, so confirm whether coverage meets your team's operating requirements.

How do I avoid vendor lock-in with managed cloud hosting?

You can reduce vendor lock-in by choosing a hosting provider that allows you to retain control of your application data, configurations, and integrations. Before signing, confirm your rights to access and export data, the formats available, any restrictions on moving to another environment, and the provider's obligations and fees for transition assistance.

ABOUT LOADSPRING

For over 25 years, LoadSpring Solutions has been at the forefront of transforming capital-intensive projects worldwide, supporting over $1 trillion in project value and serving more than 100,000 users across 5,000 organizations. As the industry's most trusted digital transformation partner, LoadSpring leverages its deep expertise in cloud technology, data modernization, and AI-powered analytics to deliver customized solutions, drive measurable results, and maximize ROI for the world's most complex capital projects.

ABOUT THE AUTHOR

Jim Smith, Co-Founder and COO of LoadSpring Solutions, has spent more than 25 years helping organizations manage the applications and technology that support complex project delivery.

Contact us

info@loadspring.com

Website

www.loadspring.com

Phone

U.S. +1 877-562-3777

U.K. +44 800 088 5889

Address

170 Commerce Way, Suite 200
Portsmouth, NH 03801
United States

© Copyright 2026 LoadSpring Solutions, Inc. All rights reserved.