

21 questions to ask before hiring an IT provider

A practical comparison guide for construction and engineering businesses

Protect the work. Protect your clients. Know what you are buying.

21 QUESTIONS / EVIDENCE TO REQUEST / PRINTABLE WORKSHEETS

Bring this guide to a provider meeting. Ask for clear answers, written responsibilities and evidence that fits your business.

BUYER DISCUSSION GUIDE

Before the next deadline tests your IT

Picture an ordinary project morning: a crew needs the current drawings, an estimator is preparing a bid and accounting is checking a supplier payment. If one system stops working, those people need more than a reassuring sales promise.

This guide helps you ask how support will work when it matters. It is for owners, operations leaders, office managers and IT leads choosing a provider or reviewing an existing relationship.

Do not stop at "yes."

Ask what is included, who is responsible, what evidence supports the answer and where the commitment appears in the agreement. A provider may reasonably need to assess your environment before making a commitment.

How to use the guide

1. Choose the questions most relevant to your work. Invite someone from operations, finance and IT to contribute.
2. Ask each provider the same questions. Request redacted examples or a demonstration without exposing another client's information.
3. Record gaps and follow-up actions. Compare the scope and evidence before deciding whether the proposal fits.

A simple discussion path

Ask	Verify	Agree
Describe a real workflow or concern.	Request documents, examples or test results.	Record scope, owner, date and next step.

Security is a shared, ongoing responsibility. No provider, score or combination of tools guarantees that a breach will never occur. Coordinated controls can reduce risk, limit damage and improve recovery for your business and the clients who depend on it.

QUESTIONS 1-3

Support when the work happens

01 Who helps when our people actually work?

A superintendent starting early and an estimator working late may need different support from the office team. A monitoring service is not the same as a staffed help desk.

Ask to see: Written support hours, time zone, holidays, contact routes and after-hours eligibility. Separate remote help, onsite visits, security monitoring and emergency escalation.

Bring it to life: If a jobsite cannot open drawings at 6 a.m., who responds, through which channel, and what charges or limits apply?

02 What does a response-time commitment mean?

An automated acknowledgment does not get a crew moving again. Response, active investigation, restoration and final resolution are different milestones.

Ask to see: The proposed agreement's priority definitions, response targets, escalation steps, exclusions and remedies. Ask how performance is measured and reported.

Bring it to life: Walk us through an urgent outage and a single-user issue. When does the clock start, and what happens if a target is missed?

03 Can you support the way our projects run?

Technology decisions must fit drawings, estimating, accounting, scheduling and field access. A fast laptop can still be the wrong laptop for its workload.

Ask to see: A discovery plan covering your actual applications, software requirements, internet links and field workflows. Identify the provider's role versus each software vendor's responsibilities.

Bring it to life: Show how you would investigate slow CAD work or a jobsite access problem, and explain when the application vendor becomes involved.

QUESTIONS 4-6

Scope, cost and control

04 What is included, and what needs a separate scope?

The phrase 'all-inclusive' is not a service specification. Two proposals can look similar while covering very different work.

Ask to see: A service schedule listing users, devices, sites, business-hours support, onsite allowances, travel, projects, onboarding, security services, backups and disaster recovery work.

Bring it to life: What would be included if we opened a new jobsite, added users, replaced a server or needed recovery after an incident?

05 Can we understand the complete cost before signing?

Surprise costs make planning harder. Compare the same environment and responsibilities across providers instead of comparing a headline monthly figure.

Ask to see: An itemized proposal showing recurring services, licenses, onboarding, hardware, separately billed work and the rules for increases or changing user counts.

Bring it to life: Which assumptions could change this quote? Who approves additional work, and will we see the scope and cost before it starts?

06 What happens when the agreement changes or ends?

You should know how to move your information and services before a relationship begins. An orderly exit protects continuity for your clients as well as your staff.

Ask to see: Written renewal and cancellation terms, transition assistance, data-export formats, ownership of subscriptions and any return, retention or deletion obligations.

Bring it to life: If we change providers, who transfers documentation, access and subscriptions, how long will it take, and what will it cost?

QUESTIONS 7-9

Know what you can recover

07 Do we know what we own and depend on?

An overlooked firewall, cloud subscription or administrator account can turn a routine change into an interruption. Documentation needs an owner and a review process.

Ask to see: A sample inventory and dependency map covering devices, software, cloud services, internet connections, vendors and authorized administrative access. Do not request another client's secrets.

Bring it to life: How will our authorized staff access current documentation if our usual technician is unavailable?

08 What is backed up, and how are backup copies protected?

Knowing that 'we have backup' does not tell you whether the files or cloud data you need are covered. A compromised administrator account should not be able to erase every recovery option.

Ask to see: A workload-by-workload backup scope, retention rules, monitoring responsibilities and protections for backup access and copies. Identify cloud data or devices outside the scope.

Bring it to life: Which information could we still lose? How would we recover if production systems and normal administrator accounts were unavailable?

09 Have recovery expectations been tested?

A backup job completing is not proof that the business can resume work. Recovery targets must reflect the applications, people and dependencies your company needs.

Ask to see: Agreed tolerable data loss and recovery time, a test schedule, recent test results and an action list for failures. Distinguish a file restore from a full business recovery exercise.

Bring it to life: What did the last test actually restore, how long did it take, and which recovery assumptions remain untested?

QUESTIONS 10-12

Build a security stack that operates

10 How will access to our accounts be controlled?

One stolen account can expose information beyond the person who owns it. Access should follow the job and change promptly when someone's responsibilities change.

Ask to see: A plan for multifactor authentication, separate administrator access, account recovery, least privilege and employee or subcontractor departures. Discuss phishing-resistant sign-in methods and exceptions.

Bring it to life: Who approves privileged access, reviews it and removes it? How do you protect the emergency access needed during an outage?

11 How will we improve and measure Microsoft 365 security?

Secure Score makes recommended improvements visible, but the work behind the score matters. Its recommendations do not cover every threat or every part of your business.

Ask to see: A baseline, prioritized improvement plan, assigned owners, licensing requirements and documented exceptions. Review implemented controls alongside the score and other security evidence.

Bring it to life: Computerbilities encourages an above-80% Secure Score target where appropriate. How would you work toward it without weakening usability or ignoring higher-priority gaps? This is our planning target, not a Microsoft guarantee or certification.

12 Who acts when security tools raise an alert?

A dashboard cannot make every business decision. Protection depends on how preventive controls, monitoring, investigation and response work together.

Ask to see: The security services included in your agreement, monitored systems, coverage hours, escalation contacts and authority to contain threats. Clarify endpoint protection, EDR and any managed response service.

Bring it to life: Who may isolate an infected device or disable an account, how will we be notified, and what response work is outside the subscription?

QUESTIONS 13-15

Protect office and field workflows

13 How are updates and unsupported systems handled?

Installing updates without a plan can disrupt work; leaving important gaps unresolved can expose it. Someone must own both the change and the exception.

Ask to see: An inventory of supported systems, risk-based update priorities, testing and maintenance windows, rollback planning and a replacement plan for unsupported software or hardware.

Bring it to life: How will you handle an urgent update when a project-critical application has compatibility concerns? Who accepts and reviews any temporary risk?

14 Will our payment-verification process stand up to pressure?

An urgent email can look convincing even when it is fraudulent. Protecting payments requires a business process as well as email security.

Ask to see: A trusted callback procedure, a second authorized review for bank-detail changes, clear approval responsibilities and a way to report a suspicious request. A signature alone is not independent verification.

Bring it to life: Where do we keep verified vendor contact details, and what happens if the caller cannot confirm the exact change?

15 How are field devices and remote connections managed?

Project information travels through tablets, home networks, temporary offices and job sites. The provider needs to understand where the work happens.

Ask to see: Device enrollment and protection rules, lost-device procedures, remote-access controls, personally owned device boundaries and the support scope for jobsite connectivity.

Bring it to life: If a tablet is lost or a jobsite connection fails, what can we do immediately, who authorizes it, and what remains available offline?

QUESTIONS 16-18

Protect clients and prepare to respond

16 How do we protect client information when sharing or using AI?

Your client's drawings, contracts and contact details deserve deliberate handling. Convenient collaboration can expose information when access rules are unclear.

Ask to see: Rules for external sharing, guest access, approved storage, retention and approved AI use. Confirm how the provider will review permissions and help staff recognize sensitive information.

Bring it to life: Who can approve sharing a project folder or entering client information into an AI tool, and how is access reviewed when the project ends?

17 Who leads the response if something goes wrong?

During an incident, uncertainty wastes time. The plan should connect technical containment with business decisions and communication.

Ask to see: Named internal and provider contacts, authority to act, an alternate communication method, exercise records and coordination with your insurer and qualified legal advisers where needed.

Bring it to life: Who coordinates the first hour, keeps a decision record and identifies separately scoped forensic or recovery services?

18 How does the provider protect its own access to us?

An IT provider's remote tools and privileged accounts can reach important systems. Ask how that access is protected, including access by subcontractors.

Ask to see: A plain-language description of access controls, staff training, logging, remote-tool safeguards and subcontractor responsibilities. Request relevant insurance evidence without assuming a policy guarantees recovery.

Bring it to life: How would you notify us if a provider account or remote management tool were compromised, and how could access be restricted?

QUESTIONS 19-21

Evidence, continuity and fit

19 Will reviews show decisions and evidence, not just scores?

A green dashboard can hide an unresolved business risk. Useful reporting helps you decide what to fix, fund, accept or investigate.

Ask to see: An agreed review cadence and a sample report covering service performance, open risks, backup tests, security improvements, asset lifecycle and decisions with owners and dates.

Bring it to life: What would you bring to our next review if one issue kept recurring or a recommended improvement had stalled?

20 How will onboarding and technician handoffs work?

Changing providers should not leave staff guessing how to get help. Continuity also matters when your regular technician is away.

Ask to see: An onboarding plan, responsibilities for the outgoing provider and your staff, account and backup checks, communication dates, and a documented technician handoff process.

Bring it to life: How will you confirm that critical access and recovery information are available before old access is removed?

21 What experience can you substantiate?

Confidence is useful; relevant evidence is better. Look for experience with businesses whose work resembles yours and an honest explanation of limits.

Ask to see: Current relevant skills, permission-based references or documented client examples, and clear roles for specialist vendors. Respect confidentiality when requesting evidence.

Bring it to life: Describe a comparable problem, the work completed and the confirmed result. What would you need to learn about our environment before recommending a solution?

PRINTABLE WORKSHEET

Compare the proposal behind the price

Use one copy for each provider. Ask for clarification where the answer is missing, conditional or outside the proposed scope. A lower price can reflect a different service; a higher price alone does not establish quality.

Area	Included / excluded / limits	Evidence or follow-up
Users, devices, sites and applications		
Remote and onsite support; travel		
Coverage hours, targets and escalation		
Security, backup and recovery scope		
Licenses, onboarding and project work		
Renewal, changes and exit assistance		

Provider / proposal date:

Most important unresolved question:

A contract or insurance policy deserves review by the appropriate adviser. This worksheet helps organize the discussion; it does not determine legal obligations or coverage.

PRINTABLE WORKSHEET

Turn the discussion into a decision

Do not turn 21 questions into a pass/fail security score. First identify the gaps that could affect active projects, client information or your ability to recover. Then agree what needs evidence or a separate scope.

Status	What to record
Supported	The answer fits the need and evidence has been reviewed.
Needs clarification	An answer or document is incomplete, or responsibilities are unclear.
Gap / separate scope	Work is absent, excluded or needs a specific plan.
Not applicable	Record why this does not apply to your environment.

Question / concern	Next evidence or action	Owner / due date

Decision / next meeting:

Print these worksheets or use a separate action log. This PDF does not contain interactive form fields. Keep credentials, full banking details and sensitive client information in your approved secure systems.

BUYER DISCUSSION GUIDE

Bring your hardest questions to us

Computerbilities has served businesses since December 1995. We support construction and engineering teams whose work depends on reliable access, useful assistance and careful handling of client information.

Use these same questions when evaluating us. Ask which responsibilities belong in your proposed plan, which require separate work and what evidence we can provide. Support hours, response commitments and included services depend on the written agreement.

Free 15-minute IT Priorities Call

Discuss the IT concerns affecting your work. Receive a brief written follow-up with up to three priorities or questions and a recommended next step. No cost, no obligation to purchase and no system access required. Technical assessments are separately scoped.

[Book your IT Priorities Call](#)

Call 919-469-5060 | sales@computerbilities.com

Explore the work behind the conversation

[Construction IT plans and service scope](#)

[Iron Horse Contractors: office and field IT improvements](#)

[Allied Fire Protection: a more productive IT environment](#)

[Cimarron Homes: clearer calls and better support](#)

Review our published guarantee and its terms

[Computerbilities 100% Money-Back Guarantee](#)

The guarantee is described on that page. This guide does not create additional service, refund or recovery commitments.

REFERENCE LINKS

Keep learning, with sources you can check

The questions are practical discussion prompts prepared by Computerbilities. The references below support the security topics; they do not certify or endorse a provider, this guide or its planning targets.

[NIST Small Business Cybersecurity Corner](#)

Risk management, planning and guidance by topic.

[CISA small and medium business resources](#)

Account protection, software updates, incident planning and cloud security.

[CISA advisory for MSPs and their customers](#)

Provider access, remote management and shared security responsibilities.

[Microsoft Secure Score documentation](#)

How the score works and why a score does not cover every attack surface.

[FBI: Business Email Compromise](#)

Independent verification of payment changes and prompt reporting.

More Computerbilities resources

[The Easy Guide to Cybersecurity for Construction Companies](#)[Construction IT Checklist & Downtime Plan](#)[Construction Invoice-Fraud Prevention Kit](#)

Edition note: This 2026 revision replaces the earlier 21 Questions report. It removes outdated offers and blanket service claims and adds questions about cloud access, Microsoft 365, field workflows, payment verification and evidence. Sources checked October 5, 2026.