ranix

2026

10 QUESTIONS TO ASK YOUR IT PROVIDER

& EVALUATE YOUR SERVICE



www.ranix.net



Introduction

Most business owners can't evaluate IT support on technical merit — and you shouldn't have to. But you can evaluate a provider by how it answers these 10 questions. A confident, specific answer is usually a good sign. A vague, defensive, or evasive one usually isn't.

Be sure to keep this guide close and ask these questions if you are interviewing a new IT service provider, or bring them up at your next review call if you are concerned about your current service.

At the end of this document, if you are not sure how to read their answers or want a neutral second opinion, you can book a free 15-minute review at:
www.ranix.net/second-opinion



QUESTION 1

What do you actively monitor?

Why it matters: Good IT support catches problems before they become outages. You don't want to be the one reporting issues first. If you already are, then they may not be actively monitoring anything.

✅ **Good Response:** Specific systems named with automated alerts and a described process for what happens when an alarm is triggered. Bonus points for mentioning response times.

❌ **Bad Response:** Vague reassurance with no explanation of tools, alerts, or process.

QUESTION 2

When did you last test our backups?

Why it matters: A backup that has never been restored is unverified. Many businesses discover this only after a real failure, when it's too late. All critical devices should be backed up, from servers to firewalls.

✅ **Good Response:** A specific, hopefully recent date and a description of what was restored and verified. Bonus points for honesty when restores have failed.

❌ **Bad Response:** Evading the question by responding with something along the lines of *"the backups run every night"* without acknowledging any restore testing.



QUESTION 3

How often do you patch and update systems?

Why it matters: Unpatched systems are one of the most common ways businesses get breached. This should be routine, not an afterthought.

✅ **Good Response:** A documented patching schedule (e.g., a monthly maintenance window) and a method of identifying what has been updated. This should include your systems and any of the provider's own customer premises equipment (CPE).

❌ **Bad Response:** A generic response such as *"regularly"* with no schedule, process, or visibility offered.

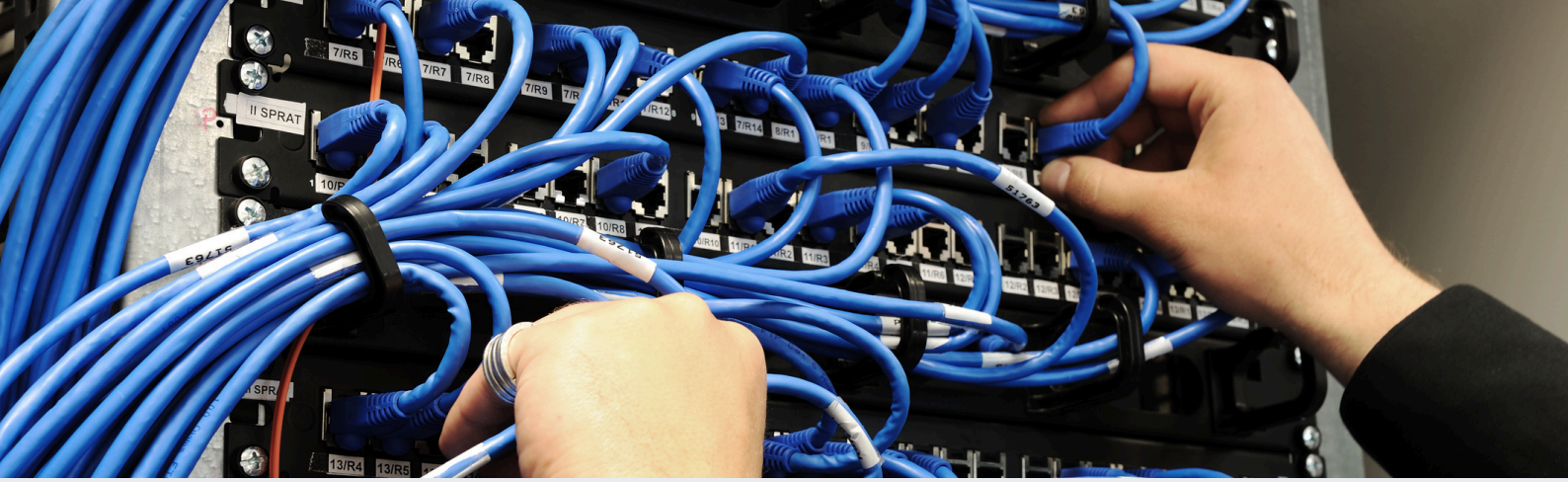
QUESTION 4

If we had a security incident tomorrow, what exactly would you do in the first hour?

Why it matters: If they can't answer this clearly, there isn't really a plan — and the first hour of an incident is often the most consequential.

✅ **Good Response:** A specific, ordered set of steps: isolate affected systems, assess scope, notify you, begin remediation.

❌ **Bad Response:** A generic response about their internal escalation procedure and nothing about how they investigate, troubleshoot and resolve issues.



QUESTION 5

Can you show me exactly what we're paying for, broken down by service?

Why it matters: Flat, unexplained monthly fees make it impossible to judge value or spot scope creep over time.

✅ **Good Response:** A clear breakdown by service (helpdesk, monitoring, backups, security, upgrades) that they can walk you through without hesitation.

❌ **Bad Response:** A single lump sum with reluctance or inability to itemise it.

QUESTION 6

What happens if I want to leave — specifically system access, data, licenses, and documentation?

Why it matters: Vendor lock-in is a red flag. You should always be able to leave cleanly, even if you never plan to.

✅ **Good Response:** A clear answer: you own your data, have admin access to your systems and licenses, and documentation would be handed over on request.

❌ **Bad Response:** Hesitation, passing the buck to another department, or systems/accounts accessible only through their logins.



QUESTION 7

Where is network and systems documentation stored and how often is it reviewed?

Why it matters: If documentation lives only in one person's head, you're a resignation away from losing institutional knowledge.

✅ **Good Response:** Maintained documentation should be shown or made available to you on the spot. Bonus points if the documentation has been reviewed or updated recently.

❌ **Bad Response:** Not being able or willing to show any proof of documentation. Or providing documentation that hasn't been reviewed for years or is out of date.

QUESTION 8

How do you report to me on what you've done, and how often?

Why it matters: Without regular reporting, you have no way of knowing what is being delivered and whether you're getting a proactive service or just paying for reactive firefighting.

✅ **Good Response:** A regular report or review call (monthly or quarterly) covering open and resolved issues, what changes occurred and what's planned over the next month/ quarter.

❌ **Bad Response:** No regular reporting — you only hear from them when something breaks.



QUESTION 9

What's your guaranteed response time, and what happens if you miss it?

Why it matters: A response promise with no defined time limit or consequence for missing this isn't a real commitment — it's a hope.

✅ **Good Response:** A written SLA with specific hours (e.g., "1 hour for critical issues") and a stated remedy such as credit, escalation, or penalty if it's missed.

❌ **Bad Response:** A non-specific response such as "*we usually get to things pretty quickly*" with no hard numbers and nothing in writing.

QUESTION 10

Are our systems compliant and when were they last reviewed?

Why it matters: Many businesses only discover a compliance gap after an audit fails. Your provider should know this before you need to. Most providers are compliant internally, but they don't always pass that down to the client.

✅ **Good Response:** A specific answer referencing your requirements (e.g. PCI) and status.

❌ **Bad Response:** A list of compliances that they meet, but not specific to your business or a hesitation around your last review.



How did they do?

8-10 good responses: You're likely in good hands.
4-7 good responses: You probably have some gaps worth addressing.
0-3 good responses: Your business is carrying more risk than you probably realise.

Not sure how to read their answers, or want a neutral second opinion? Book a free 15-minute review at: **www.ranix.net/second-opinion**

www.ranix.net



ranix

01530 686664

info@ranix.net