Phantom Technology Solutions



BUYER'S GUIDE

# Choosing the Right IT Provider

The questions to ask, the red flags to watch, and how to evaluate an MSP with confidence.

## Who this guide is for

You have already decided that hiring a managed service provider is the right move. Now comes the harder part: figuring out which one to trust. This guide is for business owners and office managers in Indiana and Michigan who want a clear, practical framework for evaluating their options. It covers the questions that expose weak providers, the contract terms worth negotiating, the pricing models you will encounter, and the cultural signals that tell you whether a provider is genuinely a good fit.

**This guide does not cover**

The basics of what managed IT is, what a typical service package includes, or general cost ranges. If you are still at that stage, read our companion guide: "The Small Business Owner's Guide to Managed IT" first, then come back here.

## 1 Start with what you actually need

Before you contact a single provider, spend thirty minutes clarifying your own requirements. A provider who asks these questions in the first conversation is doing it right. One who jumps straight to a pitch without asking them is not.

**Questions to answer for yourself first**

**How many users and devices do you have?** This drives pricing and scoping. Include remote workers, shared workstations, and any on-site servers.

**Do you have internal IT staff?** If yes, you may need co-managed IT rather than fully managed. A good provider will accommodate your internal team rather than competing with them.

**What compliance obligations apply to your business?** Healthcare, finance, legal, and government contractors often face specific requirements around data handling, audit trails, and security controls. Not every MSP is equipped for regulated environments.

**What is your honest budget?** Managed IT typically runs $100 to $200 per user per month for a solid mid-range package. If your budget is well below that, be direct with providers so you can discuss what trade-offs that involves.

**What has gone wrong in the past?** Previous incidents, close calls, or known gaps are the most useful briefing you can give a prospective provider. They reveal the risk areas that matter most to your business.

**Match the model to the need**

**Break-fix:** Reactive, hourly, no ongoing relationship. Fine for minimal tech environments. Not appropriate if your business depends on technology running reliably. **Fully managed:** Flat monthly fee covers support, security, monitoring, and maintenance. Right for most businesses with 5 or more employees. **Co-managed:** Your internal IT staff handles day-to-day work; the provider adds security tooling, after-hours coverage, and specialized expertise. Right when you already have IT staff but want deeper security capabilities or a second layer of oversight.

## 2 The questions that separate good from bad

Use this checklist in every provider conversation. Strong providers answer these directly and without deflecting. Weak providers hedge, change the subject, or promise to follow up later and never do. Print this page and bring it to your first call.

| Question | What to listen for |
|---|---|
| **What is your committed response time for a critical, business-down issue?** | Get a specific number in hours, not a vague 'as fast as possible.' |
| **What is included in the monthly fee, and what triggers an extra charge?** | Ask for a written scope of what is in and what is explicitly out. |
| **Is cybersecurity built into your service or is it a separate upsell?** | Endpoint detection, email security, and backup should be core, not optional add-ons. |
| **How do you handle backups, and how often do you test that a restore actually works?** | Testing is the key word. Many providers back up data but never verify they can recover it. |
| **Who owns my data, my documentation, and my admin accounts if we stop working together?** | You should always own these outright. Any hesitation here is a serious warning sign. |
| **Can you provide references from businesses similar to mine in size and industry?** | Call those references. Ask if the provider is responsive and if there have been surprises. |
| **Do you carry cyber liability insurance and errors-and-omissions insurance?** | Both should be in place. Ask for a certificate of insurance. |
| **Where do your technicians actually sit?** | Local, regional, or overseas help desk? This affects response quality and communication. |
| **What does onboarding look like, and how long does it take?** | A clear, written onboarding plan is a sign of a mature operation. |
| **How do you handle after-hours and weekend emergencies?** | Is there an on-call rotation? A dedicated emergency line? Or does 'after-hours' mean email only? |
| **Do you provide regular business reviews, and what do they cover?** | Quarterly or semi-annual reviews that include security posture and forward planning are standard at a good provider. |
| **How do you keep my employees trained against phishing and social engineering?** | Security awareness training and simulated phishing tests should be included, not optional. |
| **What reporting do I receive and how often?** | Monthly reports on open tickets, patch status, backup results, and security alerts are a baseline expectation. |

**On contract and exit terms:** Two questions belong in every final conversation: What are the contract term and auto-renewal provisions? And what is the offboarding process if we part ways? A confident provider answers both directly. Section 3 of this guide covers what to look for in the answers.

## 3 Understanding contracts and SLAs

IT service contracts are not complicated once you know what to look for. Here are the terms you will encounter and what they actually mean in plain English.

**Master Services Agreement (MSA).** The main contract governing the overall relationship: liability, dispute resolution, payment terms, confidentiality, and the general rules. This is the document you sign once and that covers all work going forward.

**Statement of Work (SOW).** The specific list of services included in your engagement: what is covered, how many users or devices, and at what price. Each renewal or service change typically generates a new SOW under the same MSA.

**Service Level Agreement (SLA).** A section of the contract that defines response and resolution time targets by issue severity. Important: in most MSP contracts, SLA targets are objectives, not guarantees. Read carefully to see whether missing an SLA triggers any remedy, credit, or consequence, or whether it is simply a statement of intent.

**Term length and auto-renewal.** Most MSP agreements are one to three years with automatic renewal unless you provide written notice 30 to 90 days before the end of the term. Missing that window means you are locked in for another full term. Mark the date the moment you sign.

**Termination and exit terms.** Look for what happens to your data, your documentation, and your admin credentials when you leave. A good contract specifies a transition period, defines what the provider will hand over, and does not hold your own accounts hostage.

**Price-adjustment clauses.** Many contracts allow the provider to increase pricing annually, often tied to a percentage or an index. Know the cap and whether you have the right to exit if the increase exceeds it.

**Liability caps.** Providers typically cap their liability at the amount you paid in the prior month or prior year. This is standard in the industry but worth understanding, particularly if you are in a regulated industry with significant exposure.

**Out-of-scope work.** Anything not listed in the SOW is billable separately. Common examples include major infrastructure projects, emergency after-hours work beyond a defined threshold, and support for personal devices. Ask the provider to give you examples of what would be billed outside the monthly fee.

**Read the exit terms before you sign anything:** The most important clause in any IT services contract is not the SLA, it is the exit. Before you sign, confirm in writing: you own your data and all admin credentials, there is a defined transition period, and the provider cannot hold your accounts or documentation as leverage. If those terms are not clear, negotiate them before signing.

# 4 Pricing models explained

MSPs use several different pricing structures. Each has real trade-offs. Understanding the model helps you compare quotes that otherwise look identical on the surface.

| Model | How it works | Best for | Watch out for |
|---|---|---|---|
| **Per-user / month** | A flat fee for each user in your organization, regardless of how many devices that user has. | Businesses where employees use multiple devices (laptop, desktop, phone). | Make sure the user count definition is clear. Some providers count contractors or shared accounts. |
| **Per-device / month** | A flat fee for each managed device: servers, desktops, laptops, and sometimes network equipment. | Businesses where device count is stable and users have exactly one device each. | Can get expensive as you add devices. Servers often carry a higher per-device rate. |
| **Tiered / bundled** | Defined service tiers (basic, standard, advanced) at different price points with increasing inclusions at each level. | Businesses that want a clear packaged option without custom scoping. | Read what each tier actually includes. Security and backup are often reserved for higher tiers. |
| **A-la-carte / break-fix** | Services billed as used, often hourly. No ongoing relationship or monitoring. | Very small environments with minimal technology dependency. | Costs are unpredictable, nothing is monitored proactively, and security is typically excluded. |
| **All-you-can-eat vs. metered** | All-you-can-eat means unlimited support hours within the agreement scope. Metered means a block of hours per month with overages billed at an hourly rate. | All-you-can-eat is better for businesses with frequent support needs. Metered works if usage is genuinely low and predictable. | With metered models, providers may deprioritize small tickets to conserve your hours. Ask how usage is tracked and reported. |

### Why the cheapest quote often costs the most

A low headline price frequently excludes the services that matter most: managed backup, endpoint detection and response, email security filtering, and security awareness training. When you add those back in as line items, the 'affordable' provider often lands at the same cost as a provider who included them from the start, except now you are managing multiple vendor relationships instead of one. Always ask for a fully-loaded apples-to-apples comparison before making a price-based decision.

## 5 Red flags and cultural fit

Technical capability is necessary but not sufficient. The provider you choose will have access to your most sensitive systems, and the relationship typically runs for years. These signals, both negative and positive, matter.

### Red flags to take seriously

- **No written response-time commitment.** If they will not put specific response targets in the contract, those targets do not exist.
- **Security is an upsell, not a core service.** In 2026, endpoint protection, email security, and backup are the floor, not premium add-ons.
- **They cannot explain their backup process in plain English.** If a technician cannot describe how your backups work and when they last tested a restore, that backup is not reliable.
- **Long lock-in contracts with no exit path.** Reasonable agreements protect both parties. Contracts designed to trap you protect only the provider.
- **Fear-based selling.** Providers who lead with catastrophe scenarios and pressure rather than facts and a clear plan are selling anxiety, not service.
- **No references from businesses similar to yours.** A provider with real clients in your size range and region should be able to connect you with them.
- **Slow or inconsistent communication during the sales process.** How a provider treats a prospective client is how they will treat you as a client. Slow responses and missed follow-ups before the contract is signed reliably predict the same after.
- **Vague scope of work.** If the proposal does not clearly list what is included and what is not, expect billing disputes later.

### Cultural fit: the signals that matter

Beyond the checklist, pay attention to how a provider communicates. The right fit usually shows itself in the first two conversations.

**They explain things without condescension.** Good technical partners translate clearly without making you feel foolish for asking. If a provider makes you feel like you should already know something, keep looking.

**They ask about your business before pitching their services.** A provider genuinely interested in fit asks about your operations, your team, your risks, and your goals before they quote you anything.

**They understand your industry.** Healthcare, legal, financial services, and manufacturing each have distinct compliance and operational requirements. A provider with real experience in your industry is a meaningfully different partner than one who treats all clients identically.

**They have a local presence.** For Indiana and Michigan businesses, a provider that can physically show up when a situation requires it, and that understands the regional business environment, offers something a national help desk cannot match.

**They are honest about what they cannot do.** No provider does everything well. A good partner will refer you to a specialist for work outside their expertise rather than overpromising and underdelivering.

## Evaluating providers right now?

We are happy to answer every question in this guide honestly, compare our own contract terms against these standards with you, and give you a no-obligation assessment of where you stand. No pressure, no jargon.

### Talk to PTS

hello@phantomts.com
phantomts.com
Indiana & Michigan, since 2010