FLYGHT

MANAGED IT SERVICES | TOLEDO, OHIO

The 2025 MSP Buyer's Guide

What to Look For (and What to Run From) When Choosing a Managed IT Provider

A practical, no-BS guide for business owners who are tired of guessing whether their IT provider is actually doing their job.

flyght.support | (419) 670-7100 | support@flyght.support

What's Inside

This guide was written by Flyght, a managed IT and security provider based in Toledo, Ohio. We serve businesses across Ohio, Michigan, and Indiana. We wrote this because we're tired of watching businesses get burned by providers who overpromise and underdeliver. Use it to hold us — or anyone else — accountable.

01 WHAT MANAGED IT ACTUALLY INCLUDES

"Managed IT" gets thrown around a lot. But what does it actually mean? At its core, a managed IT provider (MSP) takes over the day-to-day responsibility of keeping your technology running, secure, and aligned with your business goals.

Here's what a legitimate MSP should be providing as part of their standard service. If your current provider isn't covering these basics, that's a problem.

Core Services You Should Expect

- 24/7 network monitoring and alerting — Not checking once a day. Continuous, automated monitoring that catches issues before you notice them.
- Patch management and updates — Regular, tested updates to your operating systems, firmware, and applications. Not "we'll get to it."
- Backup and disaster recovery — Daily backups with regular test restores. If they can't prove your backups work, they're worthless.
- Endpoint protection and security — Managed antivirus, EDR (endpoint detection and response), and DNS filtering across all company devices.
- Help desk and user support — A real person answering your calls within a reasonable timeframe. Urgent issues in 30 minutes. Non-urgent within a business day.
- Email security and spam filtering — Protection against phishing, spoofing, and business email compromise. This is the #1 attack vector for SMBs.
- Vendor management — Your MSP should handle coordination with your internet provider, phone system vendor, and software vendors. You shouldn't be the middleman.
- Strategic IT planning (vCIO) — Quarterly business reviews, technology roadmaps, and budgeting guidance. This is what separates a partner from a break-fix shop.
- Documentation — Complete, up-to-date records of your network, passwords, configurations, and procedures. If it's all in someone's head, you're stuck.
- Onboarding and offboarding — Secure setup of new employees and proper removal of access when someone leaves. This is a security essential, not an afterthought.

> *If an MSP can't clearly explain what's included in your monthly fee — and what isn't — that's your first red flag.*

02 15 QUESTIONS TO ASK EVERY MSP CANDIDATE

When you're evaluating MSPs, most of them will say all the right things. The trick is knowing which questions actually reveal the truth. Here are 15 that separate the real providers from the smooth talkers.

1. "What's your average response time for urgent issues?"

Why it matters: If they can't give you a specific number backed by data, that tells you everything. Look for 15-30 minutes.

2. "How do you handle after-hours emergencies?"

Why it matters: A real MSP has 24/7 coverage — not a voicemail box that gets checked in the morning.

3. "Can I see a sample monthly report?"

Why it matters: Good MSPs produce detailed reports showing work completed, issues resolved, and system health. If they don't report, they're not tracking.

4. "What does your onboarding process look like?"

Why it matters: A structured 30-60-90 day plan shows maturity. 'We'll figure it out as we go' is amateur hour.

5. "What's included in the monthly fee — and what costs extra?"

Why it matters: No surprises. You need a clear list. Watch for hidden per-incident or per-project charges.

6. "How do you handle cybersecurity?"

Why it matters: You want specifics: EDR, MFA enforcement, security awareness training, vulnerability scanning. Not just 'we have antivirus.'

7. "What happens if we want to leave?"

Why it matters: Ask about data portability, documentation handoff, and contract termination terms. A good MSP makes it easy to leave — because they know you won't want to.

8. "Do you have experience in our industry?"

Why it matters: Industry-specific compliance needs (HIPAA, CMMC, legal) require specialized knowledge.

9. "How often do you test our backups?"

Why it matters: Backups that aren't tested are just hope. You need proof of regular test restores.

10. "Who will be our main point of contact?"

Why it matters: You should have a dedicated account manager or vCIO, not a rotating cast of random techs.

11. "What certifications does your team hold?"

Why it matters: Look for Microsoft, Cisco, CompTIA Security+, and vendor-specific certs. These show investment in their team's skills.

12. "Can I talk to three current clients in a similar industry?"

Why it matters: Any MSP worth hiring will happily provide references. Refusal is a dealbreaker.

13. "How do you handle projects vs. day-to-day support?"

Why it matters: Make sure project work (migrations, new deployments) doesn't get mixed into your support queue and cause delays.

14. "What's your employee turnover rate?"

Why it matters: High turnover at an MSP means your dedicated team keeps changing. That kills institutional knowledge and service quality.

15. "What makes you different from every other MSP?"

Why it matters: Skip the generic answers. Look for specifics: unique processes, specializations, tools, or service guarantees that matter.

03 RED FLAGS THAT SHOULD MAKE YOU WALK AWAY

Some problems only become obvious after you've signed a contract. But many red flags are visible during the sales process — if you know what to look for. Here are the warning signs that should give you serious pause.

They can't explain their pricing clearly

If the proposal is vague, confusing, or full of caveats, imagine what your invoices will look like. Transparency isn't optional.

No documented onboarding process

An MSP that wings your transition is going to wing your ongoing support too. Onboarding should be structured and timeline-driven.

They don't ask about your business goals

An MSP that only asks about your servers and not your growth plans is just a break-fix shop with a monthly invoice.

Long-term contracts with no exit clause

3-year lock-ins with steep termination fees are a trap. Good MSPs earn your business every month. 1-year terms with reasonable exit options are standard.

No proactive security strategy

If they don't mention MFA, security training, EDR, or vulnerability scanning unprompted, security isn't a priority for them.

They badmouth every other MSP

Some competitive awareness is fine. But an MSP that builds their pitch entirely around trashing competitors usually has little of substance to offer.

They guarantee zero downtime

That's either a lie or a sign they don't understand IT. Honest MSPs talk about minimizing downtime and having fast recovery plans.

No references or case studies

If they can't point to happy clients doing similar work, you're their guinea pig.

The salesperson disappears after signing

If your main contact during the sales process has no role in your ongoing service, expect a significant drop in attention.

They use fear to sell

Scare tactics about imminent hacks and compliance fines are a manipulation strategy, not a service differentiator. Good MSPs educate; they don't terrorize.

04 GOOD IT SUPPORT VS. BAD IT SUPPORT

Most business owners don't know what good IT support looks like because they've never experienced it. Here's a side-by-side comparison so you can see the difference clearly.

BAD IT SUPPORT	GOOD IT SUPPORT
You call and leave a voicemail. Maybe someone calls back today, maybe tomorrow.	You call and reach a real person. Urgent issues get a response in under 30 minutes.
You only hear from them when something breaks.	They proactively notify you about potential issues before they become problems.
Updates and patches happen sporadically — or not at all.	Patches are scheduled, tested, and applied regularly with documentation.
Your 'backups' haven't been tested since they were set up.	Backups run daily with regular test restores, and you receive verification reports.
Security is an antivirus subscription and nothing else.	Multi-layered security: EDR, MFA, email filtering, DNS protection, and security training.
No one can explain your IT spending or where it's going.	Quarterly business reviews with clear budget tracking, forecasts, and strategic recommendations.
When a tech leaves the MSP, so does all the knowledge about your network.	Everything is documented: network diagrams, credentials, procedures, vendor contacts.
Projects take forever and always seem to cost more than quoted.	Projects have defined scopes, timelines, and fixed pricing with clear change-order processes.

Here's the uncomfortable truth: if most of the left column sounds familiar, you're not getting managed IT — you're getting expensive neglect.

05 MSP PRICING MODELS EXPLAINED

MSP pricing isn't standardized, which makes it confusing to compare proposals. Here are the most common models, what they mean, and what to watch out for.

Per-User Pricing

Typical range: $100 - $250 per user/month

Pros:

+ Simple to understand and budget
+ Scales naturally with headcount
+ Usually includes all devices per user

Cons:

- Can get expensive with many part-time employees
- Definition of 'user' varies between MSPs
- Watch for exclusions (servers, network equipment)

Verdict: Best for most SMBs with 10-100 employees. Just make sure you know exactly what 'per user' includes.

Per-Device Pricing

Typical range: $30 - $100 per device/month

Pros:

+ Good for businesses with more devices than users
+ Easy to track and audit
+ Can be cheaper for companies with shared workstations

Cons:

- Mobile devices and tablets can inflate the count
- Servers and network gear are often priced separately
- Doesn't account for user complexity

Verdict: Less common now but can work for manufacturing, healthcare, or businesses with lots of shared equipment.

All-Inclusive (Flat Rate)

Typical range: $1,000 - $5,000+/month (varies by size)

Pros:

+ Completely predictable monthly cost
+ No surprise bills for extra support
+ Aligned incentives — the MSP benefits from preventing problems

Cons:

- Harder to compare across MSPs
- May include services you don't need
- Some MSPs pad flat rates with unnecessary line items

Verdict: The gold standard if you find an MSP that does it honestly. Predictable costs and aligned incentives are hard to beat.

Tiered Pricing

Bronze / Silver / Gold packages

Pros:

+ Lets you choose your level of service
+ Easy to compare tiers within the same MSP
+ Room to upgrade as you grow

Cons:

- The good stuff is always in the most expensive tier
- Lower tiers can feel like bait
- Creates a perverse incentive to upsell

Verdict: Fine as a starting framework, but ask specifically what each tier includes and what the upgrade triggers are.

> *The pricing model matters less than what's actually included. A $150/user MSP that covers everything is almost always a better deal than a $75/user MSP that bills extra for every project, after-hours call, and security add-on.*

06 MSP COMPARISON WORKSHEET

Use this worksheet to evaluate and compare MSP candidates side by side. Print it out, fill it in during your sales conversations, and use it to make an objective decision.

CRITERIA			
Monthly cost (total and per-user)			
Contract length and termination terms			
Response time SLA (urgent / non-urgent)			
24/7 support availability			
Dedicated account manager or vCIO			
Cybersecurity services included			
Backup and disaster recovery included			
Onboarding process and timeline			
Employee security training included			
Quarterly business reviews included			
Client references provided			
Industry-specific experience			
Documentation and knowledge transfer			
Project work pricing model			

How to Score Each MSP

Rate each criterion on a scale of 1 to 5 in the boxes above. Use this scale:

- **1** = Missing or unacceptable
- **2** = Below expectations
- **3** = Meets basic expectations
- **4** = Above average
- **5** = Excellent / best-in-class

TOTAL SCORE (out of 70)			

What Your Scores Mean

56 - 70 — STRONG CANDIDATE

This MSP checks the important boxes. Verify references and contract terms, then move forward with confidence.

42 - 55 — WORTH CONSIDERING

Decent foundation but gaps exist. Ask follow-up questions about weak areas before committing.

Below 42 — KEEP LOOKING

Too many gaps to overlook. Either this MSP isn't the right fit or they aren't ready to serve your business properly.

Notes:

Ready to Find the Right IT Partner?

Now that you know what to look for (and what to run from), let's have a conversation. We offer a free, no-pressure IT assessment where we take an honest look at your current setup and give you a clear picture of where things stand.

No sales pitch. No scare tactics. Just a straightforward conversation about whether your technology is helping your business — or holding it back.

We serve businesses across Ohio, Michigan, and Indiana

We specialize in managed IT, cybersecurity, and physical security

We don't do long-term contracts that trap you

We'll give you an honest assessment — even if we're not the right fit

GET YOUR FREE ASSESSMENT

flyght.support/contact

(419) 670-7100

support@flyght.support

7430 W Central Ave., Toledo, OH 43617