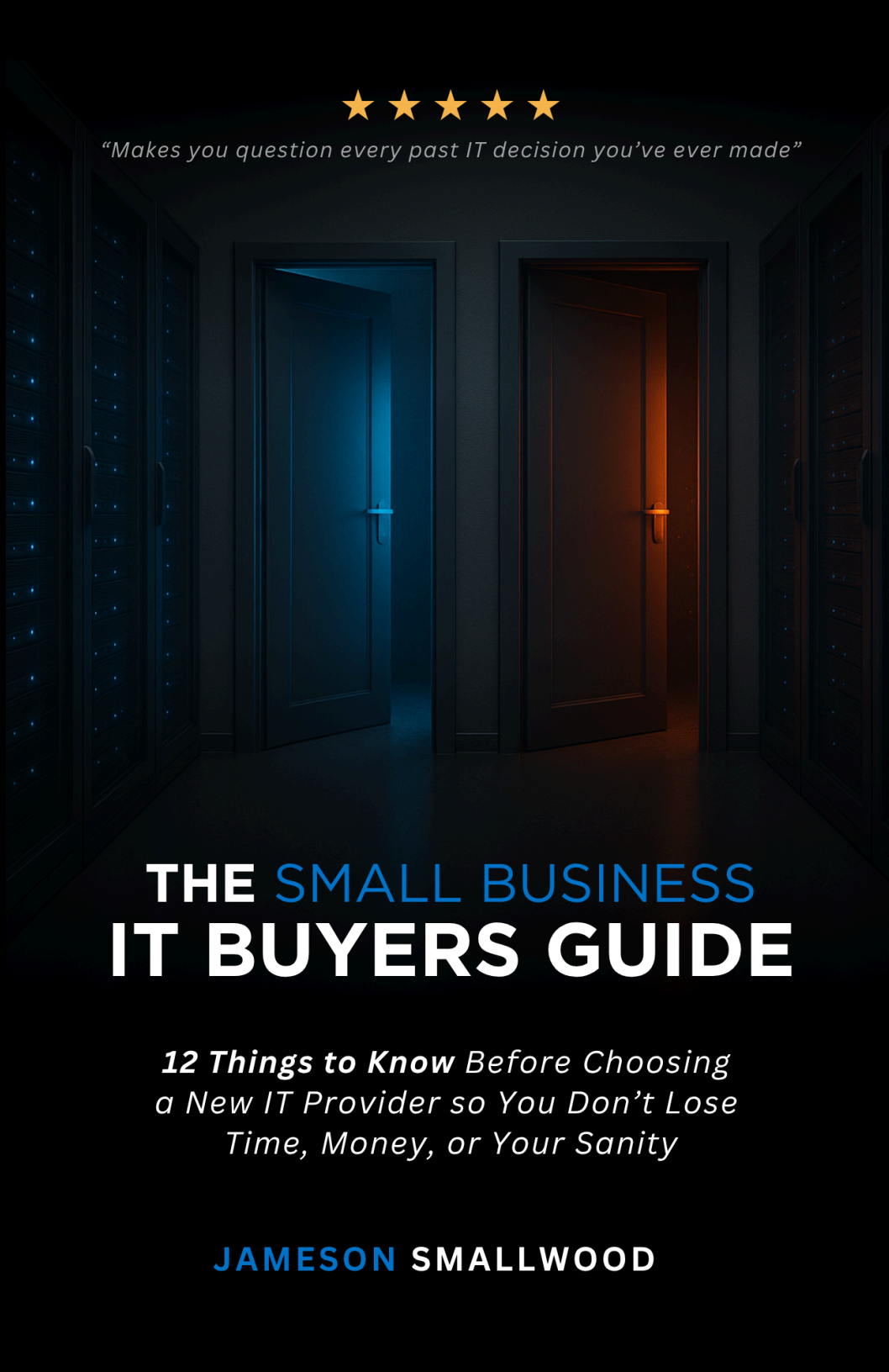

★★★★★
"Makes you question every past IT decision you've ever made"
THE SMALL BUSINESS
IT BUYERS GUIDE
12 Things to Know Before Choosing a New IT Provider so You Don't Lose Time, Money, or Your Sanity
JAMESON SMALLWOOD

THE SMALL BUSINESS IT BUYERS GUIDE

12 Things to Know Before Choosing a New IT Provider so You Don't Lose Time, Money, or Your Sanity

Copyright © 2025

All rights reserved. This publication is provided under a limited-use license for educational purposes only.

It may be shared, printed, or distributed freely, provided it remains complete and unaltered in its original digital or physical form.

No part of this publication may be modified, edited, repackaged, or claimed as your own. The copyright and all intellectual property rights remain with the original author and publisher.

The original author reserves the right to publish, bind, and commercially distribute this material in any format.

This publication is intended to provide accurate and helpful information regarding the subject matter covered. It is shared with the understanding that the author is not offering legal, financial, or professional advice. If such advice is needed, the services of a qualified professional should be sought.

Use of this material is at the reader's own discretion and responsibility.

Compliance with all applicable laws, regulations, and licensing requirements is solely the responsibility of the reader. The author assumes no liability for any actions taken based on the content of this publication.

TABLE OF CONTENTS

FROM ONE BUSINESS OWNER TO ANOTHER

Dear Fellow Business Owner,

If you're reading this, there's a good chance you're looking for an IT provider, or at the very least, wondering if your current one is still pulling their weight.

Either way, I'm glad you picked this book up.

I run an MSP myself. And over the years, I've had countless conversations with business owners who were burned by their last provider, overwhelmed by tech jargon, or just plain tired of guessing what "good IT" is supposed to look like.

This book is the outcome of those conversations.

That said, it's probably not what you'd call a "normal" book.

I don't expect you to read this cover to cover with a cup of tea and a highlighter. (Unless that's your thing, in which case, carry on.)

Think of it more like a toolbox than a novel.

You don't start at wrench and work your way to screwdriver. You grab what you need when you need it.

Flip to the chapter that fits what you're dealing with right now. Get your answer, find a good IT provider, and forget this book exists.

If you do that, my job is done.

And I say that because I'm not here to sell you anything.

I'm here to walk you through the 12 simple questions I believe everyone should ask before signing an IT contract.

These are the same questions I'd want my own friends or family to ask if they were picking someone to manage their systems, protect their data, and keep the business running.

By the time you're done with this book, you'll know:

- How to become immune to the shady "bait and switch" tactics of many IT providers
- What to look for in an IT contract before you sign it, so you don't get stuck with hidden fees, auto-renew traps, or missing services
- How to protect your business from downtime, data loss, and blame games when switching providers
- The most common red flags IT providers try to hide during sales calls, and how to spot them
- How to tell the difference between a provider who actually wants to help your business grow... and one who just wants your monthly payment
- The warning signs that your current provider might be coasting, even if things seem "fine" on the surface
- How to choose the best type of IT support for your business goals, needs, and budget.

And more!

Some of the pages will confirm what you already suspected. Others might make you look at your current setup a little differently.

Either way, the goal is to give you clarity without the usual tech nonsense.

So flip through, and feel free to take notes. Or just mentally tally up the red flags you've already spotted. That works too.

Regards,

Jameson Smallwood
Owner, Katalism Cybersecurity

"In the moment of decision, the best thing you can do is the right thing. The worst thing you can do is nothing."

— Theodore Roosevelt

BEFORE YOU DIVE IN

If you're like most business owners I talk to, you didn't wake up excited to choose an IT provider.

The goal of this guide is to make the whole process easier and a lot less frustrating. These 12 questions are here to help you figure out if someone's actually going to have your back, or offer poor service.

What you'll find inside:

- 12 straight-to-the-point questions
- What good answers sound like
- Red flags to watch for
- A few things you might not have thought to ask

You'll also find a handful of extra tools to help you compare providers and make smarter decisions without spending hours Googling things.

Bonuses Included:

Quick-Compare Worksheet
A checklist you can use to vet your top 3 IT Providers side-by-side.

Plain-English Tech Jargon Decoder
A glossary of the 50 most common terms an IT provider might use.

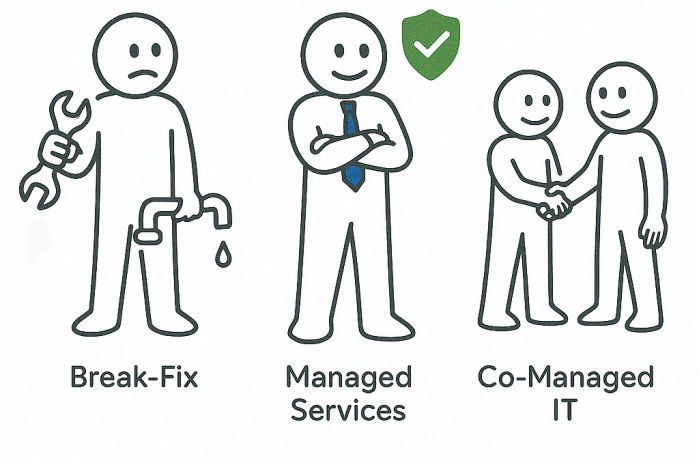
IT Setup Breakdown
A guide to help you determine what level of tech support you need.

Sales Call Detective
A list of key questions to ask IT Providers during sales calls.

How to Read a Service Agreement Without Falling Asleep
A guide to help you never fall prey to a bad Service Agreement.

CHAPTER 1

The 3 Types of IT Support You Should Know



NOT ALL IT IS BUILT THE SAME

Most people lump “IT support” into one big, blurry category.

Something breaks, you call the IT guy, and he does... something with a keyboard. Maybe the problem disappears. Maybe it doesn’t. Either way, you pay the invoice and move on.

But in reality, IT support comes in three distinct models, each with its own structure, strengths, and trade-offs.

If you don’t know which one you’re using (or what you’re actually paying for), it’s easy to end up with mismatched expectations.

You’ll think you hired someone to “manage everything,” but what you really got was someone who shows up once a quarter and resets a password.

Here’s the big picture:

- **Break-Fix** is like calling a plumber when the pipe bursts. You only pay when something goes wrong.
- **Managed Services (MSP)** is like hiring a property manager. They handle upkeep, monitoring, and emergencies on your behalf.
- **Co-Managed IT** is a team effort: your in-house staff runs the day-to-day, while an MSP supports the backend and handles specialized tasks.

You don’t need to be a techie to understand these. But you do need to know what you’re signing up for, so you can match the model to your actual needs, not just your budget.

Let’s break them down one by one, starting with the most common starting point: Break-Fix.

BREAK-FIX IT

This is the most basic form of IT support, and for a while, it seems like the most logical one.

Break-Fix is exactly what it sounds like: Something breaks, and you call someone to fix it.

There's no monitoring, no monthly fee, no proactive maintenance or regular check-ins.

You get a technician who responds when there's a problem, charges you an hourly rate, and moves on once the issue is resolved.

It's a lot like calling a plumber when a pipe bursts. You don't pay to keep them around, you just pay when something goes wrong.

For very small businesses — solo operators, small shops, or startups with a shoestring budget — Break-Fix might be perfectly fine.

Especially if you only use a couple of computers, don't store sensitive data, and can afford a bit of downtime here and there.

But once your business starts to grow, this model starts to crack.

Here's why:

- The technician often has no real context on your setup. They're walking into the problem cold, without documentation or history.
- They may not be available right away, which means downtime drags on longer than you'd like.

- Because there's no ongoing relationship, there's no incentive to help you prevent future issues.
- Every fix is reactive. By the time they arrive, the damage is already done.

And let's not forget: since there's no monitoring or behind-the-scenes visibility, issues that are bubbling under the surface (like failed backups or an expired antivirus) go unnoticed until they become real problems.

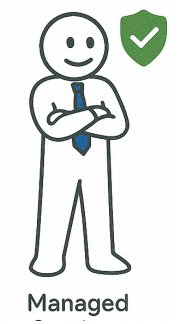
It's not a bad model. It's just a risky one to rely on if tech plays a critical role in your operations.

If you only need help once in a blue moon?

Break-Fix might work just fine.

But if you've ever said, "We can't afford to be down for a day," it's probably good to start thinking beyond it.

MANAGED SERVICES



If Break-Fix is calling the plumber only when a pipe bursts, Managed Services is having a licensed pro regularly checking the valves, tightening the seals, and making sure nothing leaks in the first place, even when you're not looking.

With Managed Services, you don't wait for things to go wrong. Instead, you pay a monthly fee for your IT provider to actively manage your systems.

That includes monitoring for issues, installing updates, patching security holes, handling backups, and offering day-to-day support when something's off.

But it's more than just "outsourced helpdesk."

A good MSP doesn't just respond to problems, they prevent them.

They'll document your entire environment. They'll know your people, your devices, and the systems you rely on. And over time, they should guide your IT strategy, not just fix your tickets.

That said, not all MSPs are created equal.

Some promise the moon but only offer surface-level support. Others bundle in everything except what you actually need, unless you ask. So while the model is proactive by design, its success still depends on choosing the right partner.

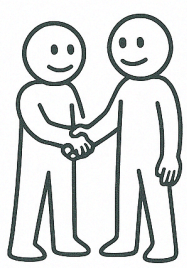
If you're running a business with shared devices, cloud apps, or even mild compliance needs — and you hate surprises — this model is often the most cost-effective in the long run.

You'll know this model might be right for you when:

- You want predictable costs and fewer tech emergencies.
- You're past the point of "just calling someone" when things break.
- Downtime equals lost revenue, productivity, or customer trust.
- You want strategic input, not just tech support, from your provider.
- You're looking for a long-term relationship, not just a quick fix.

This is what it means to have your IT actually managed.

CO-MANAGED IT



Co-Managed

In a co-managed setup, your internal IT team and an external MSP work together.

Think of it like having an in-house plumber who knows every pipe in the building — and bringing in a professional plumbing company to handle the city hookups, the flood prevention system, and the pressure testing.

Your internal team handles the everyday IT needs: user setups, password resets, printer issues, and questions from Janet about her email not syncing.

Meanwhile, the MSP steps in for infrastructure audits, system backups, patching, security updates, and planning for growth or compliance.

You give your Internal IT team breathing room while gaining access to deeper expertise, enterprise tools, and backup when someone's out sick, overloaded, or simply stumped.

But that only works if the boundaries are clear. Without defined roles, shared documentation, and mutual trust, things can unravel fast. Tickets get lost, wires get crossed, and "us vs. them" creeps in... which helps no one.

You'll know co-managed might be right when:

- Your Internal IT team is strong — but stretched thin
- You're preparing for compliance, growth, or audits
- There are gaps in monitoring, cybersecurity, or documentation
- You want a safety net if your key tech person leaves

WHICH ONE'S RIGHT FOR YOU?

Now that you've seen the options laid out, let's talk about which one actually fits your needs.

There's no universal "best" model. Just the one that works best for your size, systems, budget, and tolerance for tech headaches.

So how do you decide?

Start with where you are, and where you're heading.

- **Size matters.** If you're a solo operator or a team of two, Break-Fix might work (for now). But as soon as tech becomes essential to daily operations, you'll want something more stable.
- **Think about complexity.** Are you just checking email and using spreadsheets? Or are you juggling cloud platforms, remote access, file servers, and compliance rules? The more moving parts, the more value you'll get from Managed or Co-Managed services.
- **Downtime tolerance.** How much time, and money, do you lose when systems go down? If an outage means customer complaints, lost sales, or missed deadlines, Break-Fix starts to feel like playing with fire.
- **Do you already have internal IT?** If yes, do they look tired? If they're always stuck fixing "mundane" issues instead of focusing on security or planning, Co-Managed IT gives them breathing room and backup.
- **What about growth?** Are you hiring? Expanding? Entering new markets? A proactive IT partner can help you scale without tripping over your own infrastructure.
- And lastly, **are you sleeping well?** If tech stress is waking you up, or slowing your team down, you'll need more than just Break-Fix.

You don't need to become an IT expert to make a smart choice. You just need to know your business, your risks, and your goals.

CHAPTER 2

Why Businesses Switch IT Providers, and How to Know if You Need to Switch Right Now

6 SIGNS TO PAY ATTENTION TO

Switching IT providers isn't something most businesses do lightly. It usually comes after a pattern of frustrations, the kind that build slowly, then explode all at once.

When things stop working the way they should, or when trust erodes past the point of repair, that's when businesses decide they've had enough.

And while every situation is unique, the reasons most companies switch fall into a few very familiar buckets.

1. Operational Failures

These are the moments when things break and the provider just… isn't there. A ransomware attack is mishandled, a critical outage drags on for days, or backups that were "definitely working" turn out to be empty folders.

When these failures happen, they damage the business. Revenue halts. Reputation takes a hit. Compliance may be at risk.

And worst of all, trust in your IT provider erodes.

The real damage isn't always in the failure itself, it's in how the provider responds (or doesn't).

Are they calm, clear, and in control? Or scrambling with no plan, no updates, and no accountability?

These breakdowns usually aren't one-offs. They're signs of weak systems and poor planning, and they often become the final straw.

2. Recurring Technical Issues

A good IT provider doesn't just fix the problem once. They diagnose, document, and make sure it doesn't come back. But when that doesn't happen, your team adapts… the wrong way.

They stop contacting support. They find their own workarounds.
And slowly, you're paying for support that you're not really using.

3. Lack of Proactivity

Some providers are great at reacting. But only reacting.

They wait until something breaks, then jump in. But outside of emergencies, you rarely hear from them. No strategy. No upgrades. No forward planning.

There's no technology roadmap, no check-ins, no suggestions to keep your systems sharp. You feel like you're the one bringing up problems, not them.

4. Poor Communication and Support

It's one thing for systems to glitch. It's another for support to do the same. When tickets sit unanswered, updates never come, or your team has to re-explain problems over and over, that's bad service.

Or if every new issue gets handled by a stranger with zero context, your business becomes just another number in the queue.

And that's when employees stop bothering. "Don't even contact them. It'll take a week." they say.

That kind of internal culture is hard to undo.

5. Mismatched Relationship

Sometimes, it's not about the tech at all.

The provider might be competent. But if they don't understand your business, if they don't ask about your goals, or if every conversation feels transactional, it's hard to build trust.

Some providers never make the leap from vendor to partner. They fix computers, sure. But they don't think strategically, offer guidance, or show curiosity about how your business actually runs.

6. Price vs. Value Misalignment

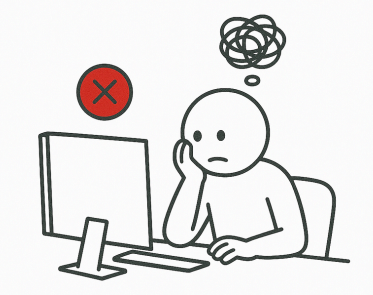
IT is an investment. But when the cost keeps climbing and the experience stays the same (or worse), people notice.

Maybe you're being nickel-and-dimed, charged for every little thing. Maybe your invoices feel like a surprise party every month. Or maybe you're paying more for "upgrades" that don't seem to do anything.

And the most frustrating part?

You're never quite sure what's included, what's extra, or whether the price reflects the value.

QUESTIONS TO ASK YOURSELF (BEFORE YOU MAKE THE SWITCH)



If your provider disappeared tomorrow, how hard would it be to recover?

Would you be able to hand over a list of systems, logins, software, and processes to someone new? Or would you be digging through old emails and hoping for the best?

If everything lives in your provider's head (or their accounts), you're dependent.

What's actually improved in the last 12 months?

Has support gotten faster? Are problems happening less and less? Have they helped you upgrade systems, improve security, or streamline something?

If the answer is "not really" or "I guess it's the same," that's worth noting.

IT should never feel like it's just treading water. A good provider pushes things forward, even if just a little, quarter by quarter.

Would you proudly recommend them to another business owner?

Forget politeness. Would you tell a friend, "You should definitely talk to our IT provider"?

If your instinct is to say "they're okay," or "they're decent for the price" — that tells you everything you need to know.

Great providers earn referrals. Mediocre ones rely on your inertia.

Do you feel more secure, productive, or in control than a year ago?

Have they flagged vulnerabilities or improved protections? Have systems gotten smoother and less disruptive? Do you feel informed, or still in the dark?

If your anxiety about tech hasn't gone down, or your workload around it hasn't eased, they're not doing their job well enough.

Are they helping you prevent problems?

Have they suggested improvements before things broke? Helped you budget ahead for upgrades? Notified you of a risky setup you didn't even know was a risk?

Or do you only hear from them when something fails, needs approval, or costs extra?

If they're not preventing problems, you might want to reconsider your collaboration with them.

WHY BUSINESSES DON'T SWITCH (EVEN WHEN THEY SHOULD)

Fear of Disruption

What if switching breaks more than it fixes?" It's a fair question. No one wants to make things worse in the name of improvement. You picture outages, access issues, forgotten passwords, confused staff, and fires everywhere.

Don't worry though. A good IT Provider creates a structured onboarding plan with overlap, documentation handoff, and risk control.

If your current provider is barely holding things together, the real risk is staying.

Loyalty and Familiarity

"We've worked with them for years. They're good people."

This might be the hardest one to confront. You like them. They helped you during that ransomware scare. You might've even had lunch together.

But sometimes, the person who used to be great isn't keeping up anymore. And when that happens, you need to act for the sake of your business.

Uncertainty About the Switching Process

"How do I even compare providers? What if I pick the wrong one again?"

It's the fear of the unknown. The belief that it's safer to deal with the devil you know than take another chance.

But that's why you're reading this guide. I'll walk you through what to look for. What to ask. What to expect.

CHAPTER 3

How to Prep for a Clean IT Handoff

WHY PREPARATION BEATS PANIC EVERY TIME

We've already clarified that the decision to switch IT providers usually comes after a slow boil of issues: repeated outages, ignored tickets, security scares, or a price hike that finally pushes you over the edge.

By the time you say, "We're done," you're likely frustrated. Maybe angry. Maybe even a little anxious about what comes next.

When you're upset, the natural urge is to move fast. Get out, rip the cord, move on. But speed without structure is how you end up locked out of your own email, scrambling to reset passwords, or stuck on the phone with your old provider begging for DNS access they forgot to transfer.

Panic leads to mistakes. And in IT, mistakes during a handoff are dangerous.

Here's what rushing the switch often leads to:

- Critical logins and admin access left behind
- Gaps in service no one anticipated
- Accidental breaches of contracts or licensing terms
- A burned bridge with your current provider (who still holds keys to your tech)

If you want to protect your business, you need to go into this thinking "How do I make sure this never happens again?"

Let's walk through how to do that, step-by-step.

TAKE INVENTORY

Before you can hand anything off, you have to know what you're actually handing over.

That sounds obvious until you realize how many businesses have no real idea what lives in their IT environment.

Things were added over the years. Some by the last provider. Some by a tech-savvy intern. Some... you're not even sure by whom.

Most small to midsize businesses don't have a clean, central map of their hardware, software, tools, and accounts. That's fine, until it's time to switch providers.

Now's the time to fix that.

What to Include in Your Inventory:

Devices & Hardware

- Servers, Workstations, laptops, and mobile devices (including those used by remote staff)
- Printers, scanners, and VoIP phones
- Network gear: firewalls, switches, routers, access points

Software & Platforms

- Line-of-business software (like your CRM or accounting system)
- Email (Microsoft 365, Google Workspace, etc.)
- Antivirus/EDR tools, cloud storage (Dropbox, OneDrive), remote access tools

Accounts & Infrastructure

- Domain registrar (like GoDaddy or Namecheap)
- DNS host (Cloudflare, Microsoft, etc.)
- Website host (WordPress, Squarespace)
- Internet provider details and static IPs, if applicable

Backups

- Where are they
- Who monitors them
- How often are they tested

The truth is, this process might feel overwhelming.

That's okay. You don't need a perfect list, you just need to get a handle on what you actually use and rely on.

GET YOUR LOGINS (ALL OF THEM)

Here's what happens more often than it should: a company parts ways with their provider, only to realize they don't have admin access to Microsoft 365.

Or their backups. Or their domain registrar.

Trust me, that's not something you want to go through.

So before you move forward, take time to confirm who holds the access, and make sure that person is you.

Start with Critical Admin Access

You (or someone internal) must have full admin rights to:

- Microsoft 365
- Your backup platform
- Firewalls, routers, and other networking gear
- Your antivirus or endpoint protection
- Website CMS (like WordPress)
- Domain registrar and DNS host

Check MFA and Recovery Setup

Two-factor authentication should always be configured individually.

Not a generic admin@yourcompany.com. Not your MSP. And definitely not an ex-employee's personal number.

While you're at it, review the account recovery emails tied to your critical platforms.

If they lead to someone who left years ago, that's a vulnerability waiting to be exploited.

Review Licensing and Billing Ownership

You should be listed as the billing contact on every system and software platform your business relies on.

Some providers set up licenses under their own master accounts. It's convenient at first, but a nightmare when it's time to switch.

Untangling that dependency can be time-consuming, expensive, and risky.

Make sure you own what you pay for.

Organize Password Management

If your team still relies on shared spreadsheets or browser autofill for logins, now's the time to upgrade.

Use a password manager and split it into two vaults. One for day-to-day team logins, and one private vault for ownership-level credentials.

This protects you from access gaps, while also giving you visibility and accountability across your systems.

REVIEW THE CONTRACT

Take a deep breath, open your contract, and look out for these clauses:

Termination Notice Window

Check the fine print: most MSP contracts require 30 to 90 days' written notice. Some auto-renew unless canceled before a specific date.

If you miss the window, you could be stuck paying for another full term.

Early Termination Fees

Some contracts include flat penalties for leaving early. Others charge for data export, "transition labor," or even license transfers.

It's not always labeled clearly. It may be buried under terms like "offboarding fee" or "administrative processing."

Who Owns What

Do you actually own your documentation, scripts, and configurations, or are they considered "proprietary tools" developed by the provider?

Watch for phrases like "remains the intellectual property of..."

If your provider owns key system knowledge, they may not be obligated to hand it over.

Offboarding Support Obligations

Some contracts explicitly say the provider must help with transition (e.g. sharing documentation, maintaining systems during the exit window). Others say nothing at all, which means you're at the mercy of their attitude.

Either way, knowing what they're contractually obligated to do gives you leverage.

Non-Disparagement or Gag Clauses

It's rare, but some MSPs bake in clauses that restrict you from speaking negatively about them in reviews, referrals, or competitor discussions.

Be aware before posting anything publicly. Even if they messed up, violating a clause could land you in hot water.

PLAN THE HANDOFF

Nail the Timeline First

Most chaotic transitions happen because people rush the process or leave things half-finished.

Here's the right order:

1. Choose your new provider
2. Schedule onboarding and documentation transfer
3. Only after that, give notice to your old provider
4. Set a clear transition window (usually 2–4 weeks)
5. Deactivate old accounts only after full testing is complete

Why this order matters: If you cancel too soon, you lose leverage — and potentially access.

What the New Provider Should Actually Do

A real provider won't just mirror what your old MSP did. They'll re-evaluate everything.

Expect them to:

- Audit and document your environment (devices, platforms, settings, etc.)
- Standardize passwords and reset permissions
- Remove unused accounts or tools
- Apply patches, activate MFA, and harden your systems
- Set up fresh backups, monitoring, and antivirus
- Clean up sloppy hand-me-downs from your old provider

Expect a Few "Wait… What?!" Moments

Most businesses don't realize how messy things are until someone starts inspecting their setup.

Common surprises include:

- Shared passwords used by entire teams
- Backups that haven't worked in months
- Expired antivirus or licensing
- Former staff still having access
- Domains on the brink of expiration
- Documentation that's missing or outdated

Budget for Cleanup

Don't assume this transition will save you money on Day 1.

A good provider will likely recommend some upgrades or cleanup labor.

That's a sign they're doing it right, without cutting corners.

CHAPTER 4

12 Things to Know Before Choosing a New IT Provider so You Don't Lose Time, Money, or Your Sanity

CHECKPOINT #1

DO THEY ASK SMART QUESTIONS ABOUT YOUR BUSINESS?

You can learn a lot about an IT provider (or anyone, really) in the first 10 minutes of a conversation.

And you can do that by paying attention to the questions they ask.

A good IT partner won't kick things off by talking about their packages, plans, or "fully managed blah blah blah."

They'll be genuinely curious about your business.

How your team works.

What tools you rely on.

Where things tend to break down, like that one weird workflow that only Lisa in accounting understands.

The stuff that actually matters.

Because the truth is, your business isn't "just like every other business."

And if an IT provider treats you like a template to drop into their cookie-cutter solution, you're going to feel it through slower workflows, low-performing systems, and a lot of, "Why is this still a problem?" moments.

Instead, you want someone who acts like a partner.

Someone who listens first, then maps out how technology can support your goals, whether that's growing your team, reducing risk, or just making things less annoying on a Tuesday morning.

That's the type of approach you should be looking for in a IT provider.

If someone is proactive in their first conversation with you, it's very likely they'll be proactive throughout the entire partnership.

And it's not hard to spot.

You'll know you've found someone worthwhile if they ask questions like:

- "What's slowing your team down right now?"
- "What software is mission-critical for you?"
- "Are there any recurring headaches you've just learned to live with?"
- "Where do you see the business 12 months from now?"

On the flip side, if their first move is to shove a standard plan in front of you and start talking pricing before they understand your business, that's a problem.

Red Flags:

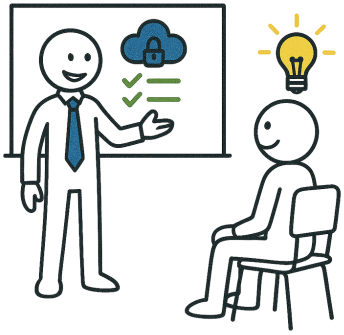
- ✗ "Our standard plan fits all."
- ✗ Rushes straight to pricing
- ✗ Talks only about tech specs
- ✗ Little interest in unique processes
- ✗ No detailed workflow questions
- ✗ Pushes quick commitment

Green Flags:

- ✓ Asks about team workflows
- ✓ Probes your staff frustrations
- ✓ Asks future-focused questions
- ✓ Curious about critical software
- ✓ Uncovers recurring headaches
- ✓ Asks questions that make you think

CHECKPOINT #2

CAN THEY EXPLAIN WHAT THEY DO IN PLAIN ENGLISH?



You shouldn't need a computer science degree to understand what your IT provider is talking about.

Nobody's got the time (or the willpower) to decode tech jargon. Even I roll my eyes when I see it.

A good provider should know this.

They'll use everyday language, not rattle off buzzwords to sound smart.

If you leave a meeting feeling confused, overwhelmed, or like you've just been nodding along to avoid looking out of your depth...

You're definitely talking to the wrong person.

Clarity is not optional in IT.

Decisions involve your data, your money, and your team's ability to do their job well.

Those decisions needs to be easy to understand, otherwise your business is at risk, which is the exact opposite of what should happen when you bring in someone to help.

The goal isn't to impress you with technical vocabulary. It's to make sure you understand what's being done, why it matters, and how it affects your business.

That's why you should pay attention to how they speak from the very first meeting.

More often than not, how they engage with you early on will set the tone for the partnership. (This is a recurring theme throughout the book).

Some will talk circles around you to sound impressive.

Others will make the complex feel simple without making you feel small.

You'll know you've found a good IT provider when:

- They simplify complicated ideas.
- You never feel talked down to.
- They use relatable examples.
- Visual aids clarify, not confuse.
- You understand exactly what's next.

If that doesn't happen, move on. And don't look back, because it's not worth the trouble.

Red Flags:

- ✗ Heavy jargon
- ✗ Talks down or patronizes
- ✗ "It's complicated—trust us."
- ✗ Leaves you feeling lost
- ✗ Overwhelming technical detail
- ✗ Confusion after meetings

Green Flags:

- ➤ Simple, clear explanations
- ➤ Makes you feel comfortable
- ➤ Relatable, everyday language
- ➤ Uses visuals to simplify concepts
- ➤ Checks your understanding
- ➤ Patient with your questions

CHECKPOINT #3

WILL THEY SHOW YOU A SAMPLE AGREEMENT BEFORE YOU COMMIT?

Surprises are fine at birthday parties. Not in contracts.

Especially not the kind that show up after you've said yes, hidden in ten pages of fine print and vague legal fluff.

A good IT provider won't play games with the paperwork.

In fact, they'll offer to walk you through the agreement before anything's official. Not just email it over and hope you don't ask questions, but actually sit down and go through the key points together.

What's included. What's not. How long it lasts. How you get out if you part ways down the road.

You should know exactly what to expect before you sign. That means no fuzzy terms, no "gotchas," and no magical disappearing services that were only mentioned during the sales pitch.

Reviewing the agreement together also gives you a chance to see how they handle the unglamorous stuff.

What's their response time?

Do they charge extra for onsite visits? Is support available on weekends?

Can you cancel easily if you're not happy, or are you locked in until the heat death of the universe?

If they delay sending the agreement until after you've given a verbal yes, or brush off your questions with something like, "Don't worry, it's all standard," that's a sign they'd rather not be held to specifics.

And you don't want to do business with someone like that. It all goes downhill from there.

Those types of IT providers have a tendency to delay responses, dodge accountability, and in some cases... disappear into thin air.

That's why it helps to know what the right approach actually looks like.

You'll know you've found a trustworthy IT provider when...

- They insist on reviewing contracts together.
- Terms are crystal clear—no hidden surprises.
- They proactively highlight critical clauses.
- There's transparency around costs and timelines.
- Exiting the agreement is straightforward and fair.

Red Flags:

- ✗ Contract shown last-minute
- ✗ Says "It's all standard"
- ✗ Hidden clauses or tricky terms
- ✗ No clear exit strategy
- ✗ Dodges specific questions
- ✗ Pushes for quick signing

Green Flags:

- ✓ Upfront agreement review
- ✓ Clearly outlines what's included
- ✓ Transparent pricing and timelines
- ✓ Simple cancellation terms
- ✓ Proactive with contract discussions
- ✓ Invites your questions openly

CHECKPOINT #4

CAN THEY PROVIDE RECENT, RELEVANT REFERENCES?

Any provider can talk a big game. The real question is: can they back it up with someone who's not being paid to say nice things?

You should be able to talk to a real client. Not just read a cherry-picked testimonial from five years ago, and not just skim through a bunch of five-star reviews that could've been written by their cousin.

An actual business owner or manager who worked with them recently.

Ideally, someone running a business about the same size as yours, dealing with similar problems.

When a provider says, "We don't really do references," or offers vague excuses about privacy, that's usually a sign they don't have anyone willing to vouch for them.

And that matters, because you're not buying a product off a shelf.

You're choosing someone who'll be inside your systems, touching your data, and helping your business stay operational if things go wrong.

That's why a good provider won't flinch when you ask for references. They'll either have a list of clients who've already agreed to share their experience, or they'll go out of their way to put one together.

Some might even offer to set up a quick call so you can hear directly what it's like to work with them.

If someone else like you had a good experience, that's worth more than any sales pitch.

You can ask about things no website will tell you.

What the onboarding was like.

How the provider handled issues that came up. Whether promises were actually kept once the contract was signed.

You'll know you've found a reliable IT provider when...

- They offer references without hesitation.
- You can speak directly to recent clients.
- Their references match your business profile.
- Clients openly discuss both strengths and challenges.
- Conversations with references leave you confident.

Red Flags:

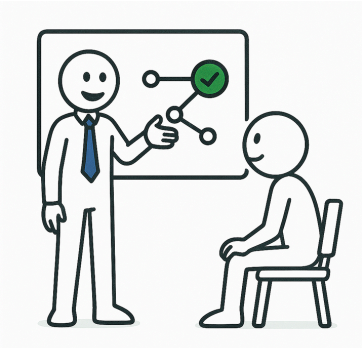
- ✗ Vague privacy excuses
- ✗ Only outdated testimonials
- ✗ Reviews sound too generic
- ✗ No direct client contact
- ✗ Avoids discussing past issues
- ✗ References sound rehearsed

Green Flags:

- ▶ Readily provides relevant contacts
- ▶ Recent client conversations
- ▶ Similar-sized client experiences
- ▶ Clients discuss problem-solving
- ▶ Open about past challenges
- ▶ Authentic, balanced feedback

CHECKPOINT #5

DO THEY WALK YOU THROUGH A CLEAR ONBOARDING PLAN?



The last thing you want is to sign a contract and be left hanging for weeks — or even months — without proper IT support.

That's why you should never agree to anything until you know exactly what's going to happen once the contract is signed.

A good IT provider should be able to clearly explain the onboarding process, step by step.

How they'll take over support, and what systems they'll audit.

Who on their team talks to whom on yours.

What to expect in week one, week two, and beyond.

The more clarity they give you upfront, the more likely it is that they've done this before, and done it well.

They'll have a checklist, and ideally a timeline, so you know exactly when things will be reviewed, installed, improved, or cleaned up.

If, on the other hand, they wave off your questions with "We'll figure that out once the paperwork's in," that's usually a problem.

It could mean they're winging it, and if they're improvising the start of the partnership, it certainly doesn't inspire much confidence in how they'll handle the rest.

Pay close attention to this, especially if you're planning a handoff from your previous IT provider.

You don't want someone more focused on closing the deal than on what happens after.

The handoff is where most problems start, and it can quickly snowball into a mess that's hard to escape.

You'll know you've found a prepared IT provider when...

- They provide a clear onboarding timeline.
- You know exactly who's involved, and when.
- Each onboarding step is mapped out clearly.
- There's no guesswork about early expectations.
- You feel confident from day one.

Red Flags:

- ✗ "We'll figure it out later."
- ✗ Unclear first-week expectations
- ✗ Avoidance of timeline specifics
- ✗ Vague about systems audits
- ✗ Appears unprepared or improvising
- ✗ Hesitates with your questions

Green Flags:

- ➤ Step-by-step onboarding plan
- ➤ Clear team roles & responsibilities
- ➤ Defined schedule of events
- ➤ Clearly identifies initial actions
- ➤ Proven onboarding checklist
- ➤ Proactive, confident communication

CHECKPOINT #6

DO THEY AUDIT YOUR IT AND SECURITY BEFORE QUOTING YOU?

Imagine walking into a doctor's office and being handed a prescription before you've said a word.

That's what it's like when an IT provider sends over a quote without first reviewing how your business actually runs.

If they don't take the time to audit your systems, ask questions about your setup, or assess your security risks, they're making a guess.

And in IT, guessing usually leads to problems later.

Every business has its quirks. Maybe you've got aging hardware that's barely holding on.

Maybe your Wi-Fi is rock solid, but your backup system hasn't been tested in years.

Maybe your staff is clicking on phishing emails like it's a sport.

There are so many scenarios, it would take another book to go through all of them.

A one-size-fits-all plan isn't going to cut it. That's why a proper provider starts with discovery.

They'll ask for access to your systems, run scans, talk to your team, and dig into what's working, what's not, and what's putting you at risk.

This kind of audit is the only way to know what support you actually need.

It also tells you something important about how they operate.

Are they taking your business seriously, or just trying to push a pre-packaged plan?

The goal should be to get an accurate picture of where you are now, so they can help you get where you want to go.

You'll know you've found a thorough IT provider when...

- They perform a proper system audit upfront.
- Security risks are identified clearly.
- Their recommendations match your actual setup.
- They understand your team's unique habits.
- They investigate instead of guessing.

Red Flags:

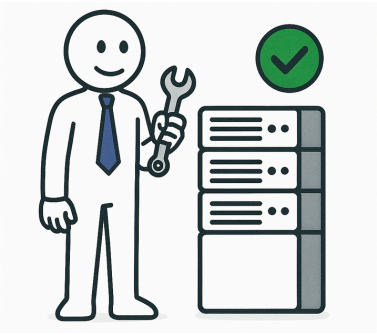
- ✗ Quotes without auditing first
- ✗ Assumes all clients are the same
- ✗ Ignores your current setup
- ✗ Generalized, generic advice
- ✗ Seems rushed to sell quickly
- ✗ Relies heavily on guesswork

Green Flags:

- ➤ Conducts initial discovery sessions
- ➤ Provides security assessments
- ➤ Bases quotes on actual data
- ➤ Understands unique business quirks
- ➤ Highlights risks & improvements
- ➤ Tailors recommendations carefully

CHECKPOINT #7

DO THEY PRIORITIZE PREVENTING PROBLEMS, OR JUST FIXING THEM?



Some IT providers love playing the hero when things break. They swoop in, save the day, and collect the praise.

But if you're always waiting for something to go wrong before anyone takes action, you're only paying for damage control.

Good IT is never just about putting out fires. It's about making sure fewer fires start in the first place.

The right provider will focus on prevention when setting up your tech.

That means monitoring your systems 24/7, applying security patches, keeping software up to date, and spotting issues before they turn into real problems.

Most of it happens behind the scenes, and if they're doing their job well., you won't even notice it's happening... which is kind of the point.

When you're evaluating providers, ask them how they minimize disruptions.

Do they track recurring issues and look for patterns?

Do they send regular reports that show what they've been doing to keep things running smoothly?

Or do they mostly sit back and wait for the next outage to hit?

You shouldn't hire someone for the sole purpose of dealing with crises.

If their approach to support feels reactive, it probably is.

Fixing things after they break might look helpful in the moment, but it's not a smart long-term strategy.

And cleanup gets expensive fast, especially when downtime starts affecting your clients or your team's ability to work.

You'll know you've found a proactive IT provider when...

- They actively monitor systems 24/7.
- Problems are stopped before you notice.
- Regular reports show preventive actions clearly.
- They identify patterns to prevent repeat issues.
- Their strategy is prevention, not reaction.

Red Flags:

- ✗ Waits for problems to happen
- ✗ Celebrates fixing frequent issues
- ✗ Ignores issue patterns
- ✗ Only reactive communication
- ✗ No clear plan for prevention
- ✗ Talks mainly about emergencies

Green Flags:

- ✓ 24/7 active monitoring
- ✓ Regular preventive maintenance
- ✓ Proactive updates and patching
- ✓ Transparent reporting on prevention
- ✓ Identifies trends to avoid repeats
- ✓ Focuses consistently on uptime

CHECKPOINT #8

CAN THEY CLEARLY EXPLAIN WHAT'S INCLUDED, AND WHAT'S NOT?

A good IT provider will make it crystal clear what you're paying for each month and, just as important, what's not included.

That means having a one-pager or clear breakdown of services, so there's no confusion when something needs fixing, upgrading, or replacing.

If a project comes up, you should know in advance whether it's part of your plan or considered extra.

Same goes for on-site visits, after-hours support, and hardware installs.

Even things like helping Dave from sales recover that file he deleted three weeks ago but suddenly needs right now.

Watch out for terms like "unlimited support" if they come with a long list of footnotes and fine print.

Unlimited rarely means what you think it means, and if the boundaries aren't clear, the invoices can pile up fast.

A transparent provider won't dodge these conversations.

They'll walk you through what's included, where the line is for extra work, and how they handle anything outside the plan.

That way, there are no awkward surprises later.

The point isn't to nickel-and-dime every detail. It's to avoid confusion when something needs doing and you're not sure if it's covered.

When expectations are clear on both sides, decisions get easier and trust builds faster.

And a long-term trust-based partnership is probably what you're looking for.

You'll know you've found a transparent IT provider when...

- Service inclusions are spelled out clearly.
- Extra costs are never a surprise.
- They proactively clarify "unlimited" services.
- Boundaries for projects and after-hours work are clear.
- You're never left guessing about your bill.

Red Flags:

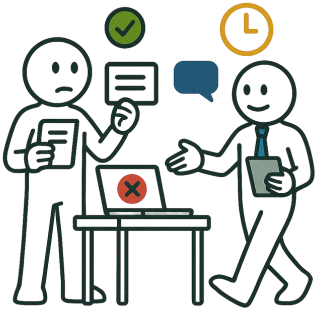
- ✗ "Unlimited" loaded with exceptions
- ✗ Frequent surprise charges
- ✗ Dodges specifics on what's included
- ✗ Vague about on-site visit fees
- ✗ Avoids talking billing details upfront
- ✗ Footnotes hiding exclusions

Green Flags:

- ➤ Crystal-clear service breakdown
- ➤ Transparent about extra costs
- ➤ Clarifies what's considered extra
- ➤ Clearly defined billing structure
- ➤ Straightforward documentation
- ➤ Welcomes billing questions openly

CHECKPOINT #9

HOW DO THEY HANDLE COMMUNICATION AND SUPPORT REQUESTS?



Benjamin Franklin famously said: “In this world, nothing is certain except death and taxes.”

I’d personally say that “In this world, nothing is certain except death, taxes, and tech breaking down.”

It’s common in IT for things to go sideways at the worst possible moment.

In fact, things tend to break exactly when you need them most.

And when that happens, how quickly you get help makes all the difference.

Before you sign with any IT provider, ask what support looks like on a normal day.

How do you submit a request? Is there a ticketing system?

Do you call, email, or chat with someone? Who actually responds? And how fast?

You’re paying for tech support, but you're also paying for responsiveness, structure, and peace of mind.

If something critical stops working, you need to know exactly who to reach and what kind of response you can expect.

The best providers have a clear process for this.

They'll make it clear where to go when you need help, who's responsible for resolving the issue, and how long it usually takes.

IT providers that go the extra mile will even share reports showing average response and resolution times. It's their way of proving they take accountability seriously.

If, on the other hand, the answer is something like "Just shoot us an email and we'll get to it," that's a warning sign. It sounds casual, but it usually means there's no real system behind the scenes.

You'll know you've found a responsive IT provider when...

- There's a clear, structured support process.
- You know exactly how to reach them, and who responds.
- Response times are tracked and shared.
- Urgent issues get urgent attention.
- You feel confident they'll have your back when it counts.

Red Flags:

- ✗ "Just email us and wait"
- ✗ No clarity on who responds
- ✗ No mention of response times
- ✗ Casual or vague about process
- ✗ Hard to reach during emergencies
- ✗ Inconsistent communication

Green Flags:

- ▶ Defined ticketing/support system
- ▶ Named human point of contact
- ▶ Tracks and shares support metrics
- ▶ Step-by-step support workflow
- ▶ Prioritized help for urgent issues
- ▶ Fast, reliable response channels

CHECKPOINT #10

DO THEY WORK WITH YOUR TOOLS OR FORCE YOU TO SWITCH?

Some IT providers walk in, take one look at your setup, and immediately start planning how to replace it.

New software, new systems, new platforms — all chosen based on what they prefer using, not what's actually right for your business.

Now, sometimes switching tools does make sense, if your current systems are outdated, unsupported, or constantly breaking.

A good provider will point that out and explain the risks clearly.

But if their only reason for replacing something is "this is what we use with all our clients," you should start asking questions.

Your business already runs on certain tools. Maybe your team knows them inside and out. Maybe your workflows are built around them.

A provider that respects that will at least try to work with what you have first.

If they do suggest a switch, they'll walk you through the pros, the cons, and the plan for making that transition as smooth as possible.

The goal should always be to support your way of working more effectively.

So if the conversation starts with "We'll need you to move everything," and ends without a solid reason why, it might be time to move on... without them.

It's easy for a provider to push what's familiar to them.

However, if they're not asking how your team actually works day to day, they're not designing a personalized solution for your business.

That's why you want someone who's curious before they're opinionated.

Someone who asks questions, maps your workflows, and looks for ways to improve starting from your current setup.

You'll know you've found a good IT provider when...

- They take time to understand your current tools.
- Upgrades come with clear, strategic reasoning.
- Your workflows are respected, not bulldozed.
- They support smooth transitions, not forced ones.
- The tech fits your business, not the other way around.

Red Flags:

- ✗ "We'll move you to our stack"
- ✗ One-size-fits-all software approach
- ✗ Pushes changes without explanation
- ✗ Ignores team familiarity with setups
- ✗ Switches tools for their convenience
- ✗ No input on changes

Green Flags:

- ✓ Open to working with your tools
- ✓ Recommends based on your setup
- ✓ Explains pros, cons, transition plans
- ✓ Respects existing workflows
- ✓ Prioritizes business continuity
- ✓ Collaborative, consultative upgrades

CHECKPOINT #11

DO THEY HAVE A PROCESS (OR ARE THEY JUST WINGING IT)?

There's almost nothing worse than an IT provider who operates more on gut feeling than on systems.

They can turn your tech infrastructure into a bowl of spaghetti.

These are people who react to whatever breaks and cross their fingers the issue doesn't happen again.

They have no checklist, no routine, and no way to track their progress.

You'll never see that from a good IT provider. Whether it's a one-person show or a team of fifty, they should have clearly documented processes for how they work.

And they should be able to explain how their processes work, even if it's just a high-level overview.

You don't need to know all the details, but you need to see they have a system for handling tickets, updates, maintenance, and security checks.

So make sure to ask about their routines.

Do they run regular maintenance?

How are support requests handled?

Do they schedule reviews or check-ins?

Even a solo consultant can run a tight ship if they've built proper systems.

And on the flip side, if every answer starts with "It depends" or "I just go with the flow," you've got a problem.

Because without structure, things go wrong more often than you'd like.

And if they're always in reaction mode, your business is the one taking the hit.

You'll know you've found a process-driven IT provider when...

- They explain how they handle tickets, updates, and maintenance.
- You understand how support requests are tracked and resolved.
- Regular maintenance is scheduled, not reactive.
- Processes are 'documented', not just in someone's head.
- They can explain how their systems work.

Red Flags:

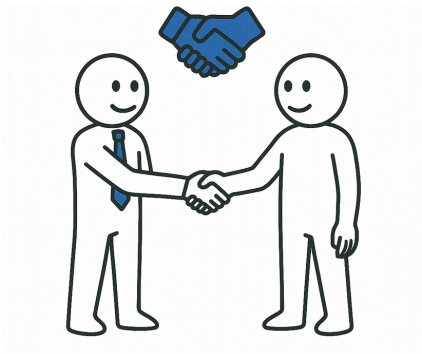
- ✗ "I just fix things as they come up"
- ✗ No defined process for tickets
- ✗ No schedule for reviews or udates
- ✗ No documentation of their systems
- ✗ Unclear roles/responsibilities
- ✗ Can't explain prevention

Green Flags:

- ▶ Documented support process
- ▶ Uses a system for managing tickets
- ▶ Proactively schedules reviews
- ▶ Shares onboarding steps
- ▶ Clear roles and responsibilities
- ▶ Tracks recurring problems

CHECKPOINT #12

DO THEY FEEL LIKE A PARTNER, NOT JUST A PROVIDER?



By the time you're having sales conversations, you've probably seen the website, read the materials, and maybe even skimmed a proposal.

But none of that tells you what it's actually like to work with them.

The real clues come from how they handle the early interactions. The tone of the emails, the questions they ask, the way they respond when you raise an issue.

If they don't follow up, or they're quick to gloss over your concerns now, don't expect that to magically improve after you sign.

This is your chance to pay attention to how they treat you.

Do they actually listen when you talk about your business?

Do they ask thoughtful questions?

Are their answers tailored to your situation, or do they feel copy-pasted from someone else's pitch?

A true partner shows you they want to build something long-term. That means being responsive, transparent, and saying "I don't know" when they don't know, and following up when they say they will.

If they seem rushed, pushy, or too eager to close the deal, that's a bad sign, and you should probably reconsider.

In short, trust your gut.

It's one of the most underrated decision-making tools you've got.

If you listen to it, it'll be pretty clear who's a good partner, and who's not.

You'll know you've found a real partner when...

- They take time to understand your business, not just your tech.
- Their responses feel thoughtful, not templated.
- They follow through on what they say.
- You feel respected, heard, and valued.
- The relationship feels collaborative from day one.

Red Flags:

- ✗ Pushy or rushed sales process
- ✗ Overpromises without real answers
- ✗ Vague or evasive responses
- ✗ Doesn't listen or ask about your goals
- ✗ "Just sign and we'll handle it"
- ✗ Ignores concerns during the sales process

Green Flags:

- ➤ Consultative, low-pressure conversations
- ➤ Honest tailored recommendations
- ➤ Clear direct communication
- ➤ Asks thoughtful questions
- ➤ Willing to earn your trust
- ➤ Responsive and respectful

CHAPTER 5

What Kind of IT Setup Do You Actually Need?

BASIC NEEDS / LOW RISK

You're here if:

- You have 1–5 employees
- Everyone mostly uses basic tools (email, office docs, browser)
- You don't store sensitive data (health, finance, legal, etc.)
- Your business can survive a tech issue for a few hours or even a day

Common signs:

- "We only call someone when something breaks"
- "Our guy is cheap and gets the job done, eventually"
- "We don't really think about IT unless something goes wrong"

What you need:

- Ad-Hoc / Break-Fix Support
- A better go-to expert for emergencies
- At minimum: documented passwords, verified backups, and antivirus

GROWING BUSINESS / MODERATE RISK

You're here if:

- You have 5–250 employees
- You use industry-specific tools or cloud platforms
- You can't afford downtime longer than an hour or two
- You've grown past "we'll deal with it later" mode

Common signs:

- "We've had the same issue three times this month"
- "I think we're paying for 3 different Cloud Storage vendors"
- "We have a backup system, but I'm not 100% sure it's working"

What you need:

- Managed IT Services (MSP)
- 24/7 monitoring
- Fast helpdesk support
- Management of updates, security, backups, vendors

MISSION-CRITICAL / HIGH RISK

You're here if:

- You have 50+ employees OR you have an Internal IT Team
- Your business stops if IT stops
- You're handling sensitive data with compliance (HIPAA, GDPR, etc.)
- You want to plan for growth, M&A, or digital transformation

Common signs:

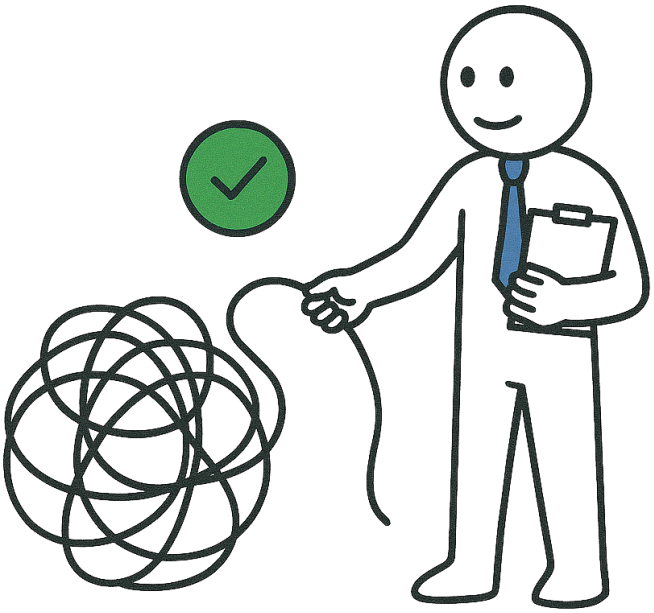
- "Our internal IT team is overwhelmed"
- "We need to standardize and document everything"
- "We've had an audit or insurance scare"

What you need:

- Co-Managed IT
- In-house IT team + MSP backup/support
- Documentation & planning
- Budget forecasting & risk mitigation

CHAPTER 6

IT Terms Explained in Plain English



PLAIN-ENGLISH TECH JARGON DECODER

Active Directory / Entra ID

Where all your user logins and access rules live.

Admin Rights

Accounts with full access to your systems. Everyday Users should never have Admin Rights as it leads to too many open doors for mistakes or malware.

Antivirus

Basic software that blocks known threats. Must-have for anyone operating a computer, but not bulletproof.

Backup

Copies of your important files. Crucial for recovery after deletion.

Bandwidth

How much data your internet can handle at once. The more data it can handle, the faster it will be.

Business Continuity

A mix of backups, plans, and systems that keep you online.

BYOD (Bring Your Own Device)

When staff use personal phones/laptops for work. Handy sometimes, but can be risky if not managed properly.

Cloud

Your stuff (emails, files, systems) stored securely online.

Cloud-to-Cloud Backup

Backups of your cloud data (like emails or Drive)

Compliance

Following rules like GDPR or HIPAA so you don't get fined (or hacked).

PLAIN-ENGLISH TECH JARGON DECODER

Disaster Recovery

The plan for "What happens if everything goes boom?" Think backups, spare hardware, cloud failovers.

DNS (Domain Name System)

The internet's address book. If it breaks, websites stop loading, even if your internet works.

Downtime

When your systems stop working and business hits the brakes.

Email Filtering

Blocks malicious and nasty emails before they hit your inbox.

Encryption

A method of locking your data so only authorised people can read it, even if someone steals it.

Encryption at Rest

Your data is scrambled even when stored, so it's safe if someone steals it.

Endpoint

Any device connected to your network: laptops, desktops, tablets, phones.

Endpoint Detection & Response (EDR)

Smart antivirus that looks for unusual behavior, not just known viruses.

Firewall

A "security guard" that keeps unwanted traffic from hitting your network.

Firewall Rules

Settings that decide what traffic gets in or out of your network.

PLAIN-ENGLISH TECH JARGON DECODER

Helpdesk SLAs
Response time promises from your IT provider.

Helpdesk Ticket
A formal way to log an IT issue.

IT Audit
A full review of your systems, risks, licences, and weak spots

Lifecycle Management
Tracking tech so it's replaced before it becomes slow, risky, or breaks.

Log File
A behind-the-scenes diary of what your system's been doing.

MFA Fatigue Attack
Hackers spam you with login requests hoping you click "Approve" to make it stop.

Mobile Device Management (MDM)
Keeps work phones and tablets secure. Can wipe data if an employee has lost their device to protect against leaks.

Multi-Factor Authentication (MFA)
Extra security steps to log in, like getting an SMS after typing your password.

Onboarding / Offboarding
Getting new staff set up with logins and devices (onboarding) or removing access when they leave (offboarding).

Patch / Patching
Software updates that fix bugs (issues) or security holes.

PLAIN-ENGLISH TECH JARGON DECODER

Patch Management
The system that makes sure your devices stay updated and secure.

Password Manager
An app that remembers your passwords so you don't have to use "123456."

Penetration Testing (Pen Test)
Hired hackers (the good kind) try to break into your system to find weaknesses before the bad guys do.

Phishing
Trick emails that try to steal your login or bank info.

Phishing Simulation
Safe 'fake' scam emails sent to your staff, to test how well prepared they are for a potential phishing attack.

Ransomware
Malware that locks your files and demands payment to unlock them.

Remote Desktop
Accessing your work computer from a remote location, like you're sitting at it.

RMM (Remote Monitoring & Management)
Software that lets your IT provider watch your systems 24/7 and fix problems without coming onsite.

Root Cause Analysis
Figuring out why something broke, to make sure it doesn't keep breaking.

SaaS (Software as a Service)
Subscription-based apps you access online, like Xero, Quickbooks or Canva.

PLAIN-ENGLISH TECH JARGON DECODER

Sandboxing
Testing suspicious files in a safe, sealed-off digital bubble.

Shadow IT
When your staff install their own apps/tools without telling anyone.

SLAs (Service Level Agreements)
Promises your provider makes about response time, support hours, etc.

SSO (Single Sign-On)
One login to access everything. Convenient, but must be secured properly.

Uptime
The percentage of time your systems are working.

User Permissions
What each person is allowed to access, edit, or delete. Set wisely.

Version Control
Tracks changes to documents or code, so nothing important gets lost.

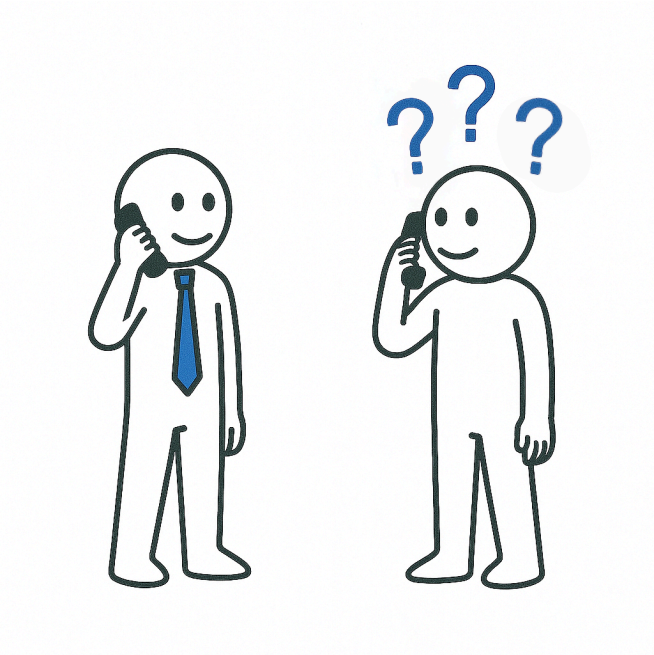
VPN (Virtual Private Network)
A secure tunnel for your internet traffic, handy for remote teams.

Whitelist / Blacklist
What's allowed in (whitelist) and what's blocked (blacklist), like emails or apps.

Zero-Day Vulnerability
A new security hole hackers already know about, but no one's patched yet.

CHAPTER 7

Smart Questions to Ask During the Sales Call



WHAT TO EXPECT

Most small business owners don't know what to ask on a sales call with an IT provider.

So they nod along.

They hear big words like "cyber resilience," "next-gen endpoint protection," and "zero trust architecture."

The delivery is slick. The deck looks polished. The pricing sounds reasonable.

But beneath the buzzwords… is there real substance?

This chapter gives you the exact questions that high-performing business owners ask. The type of questions that make IT providers sit up a little straighter in their chairs.

They make it obvious who's prepared to support your business, and who's just reading from a script.

You'll notice something as you go through them: good providers don't get defensive when you ask.

They welcome it, because they've done the work. They know their stuff. And they want to work with clients who ask smart, strategic questions.

Use this as your call companion. Print it out, keep it on your second monitor, turn it into a checklist, whatever helps you stay in control of the conversation.

You don't need to ask every question word-for-word. But you do need to come into the call with intention.

Ask with confidence.

Listen closely to how they respond.

And remember: you're not there to be sold to.

QUESTIONS

ABOUT THEIR BUSINESS

1 Who will actually be supporting us day-to-day?

You're checking to see if they are a proper business.


Green flag: "We have a dedicated helpdesk team, and your main contact will be Sarah. You'll meet her during onboarding."


Red flag: "That would be me, and I'll get back to you when I can."

2 How many clients do you support, and how many are similar to us?

You're checking for experience and capacity.


Green flag: "We support 42 businesses, mostly in the 5–50 employee range. About 6 of them are in your industry."


Red flag: "We've worked with all kinds of businesses… in the past."

3 Can I speak to a client who's been with you for over a year?

You're checking for actual partnership quality and long-term trust.


Green flag: They offer a reference happily.


Red flag: "Our clients prefer to stay anonymous."

QUESTIONS

ABOUT THEIR SERVICE MODEL

1 What's included in the monthly fee, and what's not?

You're checking for sneaky exclusions or gotchas.

 Green flag: Clear, written breakdown with no ambiguity

 Red flag: "It's all unlimited" (but can't show you what that includes)

2 How do you handle after-hours emergencies?

You're checking for true 24/7 support.

 Green flag: "We have an on-call rotation and guaranteed response times".

 Red flag: "We'll get back to you the next day".

3 Do you take care of vendor management too, like dealing with our internet provider or line-of-business apps?

You're checking to see if they help when the finger-pointing starts.

 Green flag: "Yes, we'll handle it end-to-end so you're not caught in the middle."

 Red flag: "That's outside our scope".

QUESTIONS

ABOUT YOUR BUSINESS

1 What would your onboarding plan look like for us?

You're checking for structure and thoughtfulness.


Green flag: "We'd start with a full audit, document your environment, meet your staff, and lay out a 30–60–90 day roadmap."


Red flag: "Once you sign, we'll figure it out"

2 Do you do a tech or security audit before giving us a quote?

You're checking for due diligence and whether their offer is based on facts.


Green flag: "Absolutely. We do a risk assessment and discovery session before anything else."


Red flag: "All our clients are on the same plan, so no need".

3 How often do you review our IT strategy with us?

You're checking for proactive partnership, not reactive break-fix.


Green flag: "We'll set a cadence with you to regularly review issues, risk, improvements, and align your tech with your business goals."


Red flag: "We're available if you need us."

QUESTIONS

ABOUT RESULTS & REPORTING

1 What kind of reports will we get, and how often?

You're checking for transparency, trends, and accountability.


Green flag: "Monthly reports covering tickets, response times, updates, and potential risks."


Red flag: "We don't do reports unless you ask."

2 How do you measure your own performance internally?

You're checking whether they hold themselves to real metrics.


Green flag: "We track SLA adherence, customer satisfaction scores, and ticket resolution times."


Red flag: "We just make sure things get done."

3 Can you show me a sample report from another (anonymized) client?

You're checking whether the reports are actually useful.


Green flag: "Sure, here's a real one, names removed, of course. It shows exactly what we track."


Red flag: "We don't really have a standard format, it depends..."

QUESTIONS

ABOUT SECURITY & COMPLIANCE

1 What's your process for handling a security incident, and how do you notify us?

You're checking for a clear incident response plan and transparency.


Green flag: "We follow a formal incident response process, notify you immediately, document everything, and debrief after."


Red flag: "We'll fix it and let you know if it's serious."

2 How do you help us stay compliant with data protection laws or insurance requirements?

You're checking whether they understand your industry's obligations.


Green flag: "We'll align your setup with requirements like GDPR, HIPAA, or insurance policies and provide documentation".


Red flag: "That's on your legal team, not us."

3 What tools or practices do you use to proactively reduce security risk?

You're checking if they go beyond the basics.


Green flag: "We use vulnerability scans, MFA, patching, and phishing simulations to stay ahead of threats."


Red flag: "We've got antivirus and a firewall, so you're covered."

QUESTIONS

ABOUT THEIR THINKING & STRATEGY

1 What trends or threats are you keeping an eye on for your clients right now?

You're checking if they're proactive, informed, and strategic.


Green flag: "We're watching AI-driven phishing attacks, Microsoft licensing changes, and upcoming compliance shifts."


Red flag: "We deal with issues as they come up."

2 What's a recent example where you helped a client grow, scale, or improve productivity through better tech?

You're checking whether they can create business impact.


Green flag: "We helped a logistics firm automate 4 hours of manual work per day by restructuring their SharePoint system."


Red flag: "We mostly just keep systems running."

3 How do you decide when it's time to upgrade or change something in our environment?

You're checking if they plan ahead or just react when stuff breaks.


Green flag: "We assess based on lifecycle, support status, performance, and business goals."


Red flag: "We replace it when it stops working."

QUESTIONS

ABOUT FIT & HONESTY

1 When would you not be the right fit for a client?

You're checking if they're self-aware, and clear on who they work best with.


Green flag: "We're not ideal for companies that just want occasional help or don't value long-term strategy."


Red flag: "We work with anyone."

2 What would make you fire a client?

You're checking their values and boundaries.


Green flag: "If a client ignores security best practices, treats our team poorly, or won't invest in the basics."


Red flag: "We'd never do that." (Translation: no boundaries)

3 What does a great client relationship look like to you?

You're checking whether they've thought about partnership.


Green flag: "Ongoing communication, shared accountability, openness to feedback, and clear business goals."


Red flag: "One where we don't hear from you much."

QUESTIONS

ABOUT THE AGREEMENT

1 Can you walk me through the key parts of your service agreement right now, and not just send it after?

You're checking for transparency and willingness to explain.


Green flag: "Of course. I'll highlight response times, cancellation terms, and scope of work."


Red flag: "You'll see all that in the contract once you're ready."

2 What's one clause in your contract most clients don't notice, but should?

You're checking whether they understand their own fine print.


Green flag: "The out-of-scope work section, it's where surprise fees often hide."


Red flag: "Nothing really. It's all pretty standard."

3 If we ever want to leave, how do you handle offboarding and handover?

You're checking how they treat clients at the end.


Green flag: "We provide documentation, transfer access, and assist your next provider to ensure a clean exit."


Red flag: "We'll figure that out if it comes up."

CHAPTER 8

How to Read a Service Agreement Without Falling Asleep

WHAT TO EXPECT

Most people sign IT service agreements without actually reading them.

And honestly? I can't blame them.

I've read plenty. They're long, boring, and packed with vague legal fluff and terms like "reasonable effort" or "industry standard response times."

You make it three lines in, your eyes glaze over, and the next thing you know... you're scrolling to the signature.

A lot of business owners do this, but it's risky.

Because when you sign blind, you're tying yourself to responsibilities you might regret later.

And these contracts are usually needed when things are not going well.

When something breaks or there's an issue with your IT provider.

When you're locked out, billed for something you thought was included. Or stuck with an auto-renew you didn't see coming.

That's when you dig out the agreement, and realize you should've paid closer attention.

So let's make sure that never happens to you.

This chapter will show you what parts you should pay attention to, the red flags most people miss, and how to read an IT contract without needing a translator or a law degree.

CLAUSE #1

SCOPE OF SERVICES

Look for:

- A detailed list of services (e.g. helpdesk, monitoring, backup)
- Specific technologies or systems they're managing
- What's covered under "maintenance" or "support"
- Any limitations (e.g. no mobile devices)

Watch out for:

- Vague phrases like "general IT support" or "standard maintenance"
- Exclusions buried elsewhere in the doc (e.g. projects, security work, cloud apps)

Ask them to walk you through a real-life example. "If my laptop dies, what exactly happens under this agreement?"

CLAUSE #2

SERVICE LEVEL AGREEMENTS (SLAS)

Look for:

- Defined response and resolution times (e.g. 1 hour response for high-priority issues)
- Priority levels clearly explained (P1 = outage, P2 = slow email, etc.)
- Business hours vs. after-hours SLAs

Watch out for:

- “Best effort” language
- SLAs that apply only to certain services
- No financial penalties for SLA breaches (they need skin in the game)

Make sure there’s a financial penalty if they breach the SLA. E.g. For any SLA breaches they will refund part of the monthly agreement.

CLAUSE #3

TERM & TERMINATION

Look for:

- Clear term length (e.g. 12-month agreement)
- Termination notice period (e.g. 30 days)
- Exit procedures — how do they offboard

Watch out for:

- Auto-renewals buried in the fine print
- Long lock-ins with no early exit option
- Cancellation fees that aren't clearly stated

Ask for a summary of the offboarding process before you sign. If they squirm, that's a red flag.

CLAUSE #4

BILLING & PAYMENT TERMS

Look for:

- Monthly fee spelled out clearly
- What's included in the monthly vs. billed separately (e.g. projects, after-hours work, hardware)
- Payment due dates, late fees, overage charges

Watch out for:

- Charges like "out of scope hourly support" without a definition
- "Unlimited support" language with fine print that contradicts it
- Vague terms like "miscellaneous fees" or "service adjustments" with no explanation

Ask for a one-pager that outlines what's included in plain language. If it's not in writing, assume it's not included.

CLAUSE #5

OUT-OF-SCOPE WORK

Look for:

- Clear hourly/project rates for any extras
- Examples of typical out-of-scope scenarios
- A process for getting approval before starting out-of-scope work

Watch out for:

- “To be determined” pricing
- Anything that gives them discretion to charge at-will
- Language like “as needed” or “if required” without cost specifics

This section often reveals more about the true cost than the pricing page.

CLAUSE #6

LIABILITY & INSURANCE

Look for:

- Clear language about liability limits
- A statement about their insurance (e.g. professional indemnity, cyber insurance)
- Whether their liability caps match the potential risk to your business

Watch out for:

- No mention of insurance
- Clauses that exclude “indirect” or “consequential” damages without clarification

Ask for proof of insurance. A legit MSP will have no issue sharing it.

CLAUSE #7

DATA OWNERSHIP & ACCESS

Look for:

- Clear statement that you own all your data
- Rights to retrieve data on request, in readable formats
- Policies on data deletion upon termination

Watch out for:

- “Data stored in our systems remains our property”
- Any clause that limits your access during disputes
- No timeline for how quickly they’ll return your data after termination

Ask how they handle client offboarding and what you get at the end.

CLAUSE #8

CONFIDENTIALITY & PRIVACY

Look for:

- NDA or confidentiality clause covering your data, credentials, communications
- Who has access to what (e.g. subcontractors, offshore staff)
- Agreement to follow applicable privacy laws (e.g. GDPR)

Watch out for:

- Loopholes that let them share your data with “affiliates”
- No mention of subcontractor controls
- Overly broad language like “may use data to improve our services”

Ask if they’ve signed NDAs with their staff. Many haven’t.

CLAUSE #9

SCOPE CHANGES & PROJECT WORK

Look for:

- A clear process for quoting and approving out-of-scope work
- What's considered day-to-day support vs. a paid project
- Details on hourly/project rates for extra work

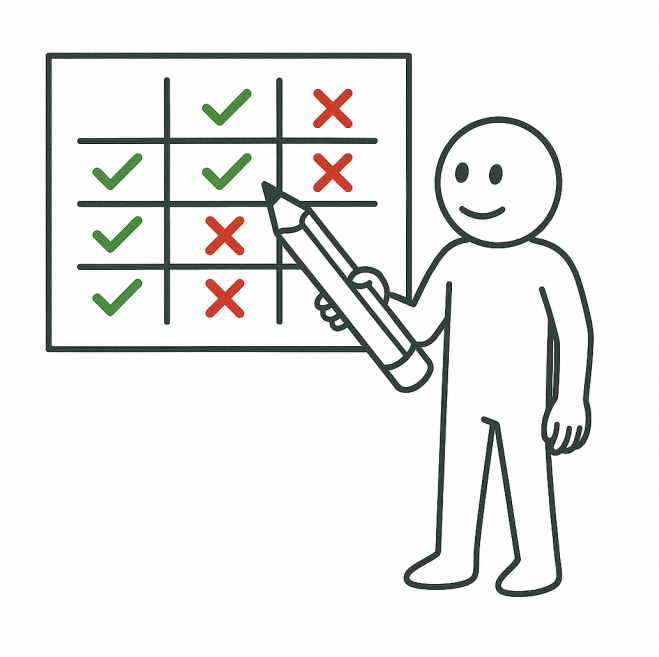
Watch out for:

- "Any task not listed is billable at provider's discretion"
- No approvals needed before extra charges
- Fine print that turns simple requests into pricey projects

Ask for examples of what wouldn't be covered in your plan.

CHAPTER 9

BONUS: Quick-Compare Worksheet



RESOURCE

🗂️ QUICK-COMPARE WORKSHEET

Use this worksheet to compare up to three IT providers before making a decision.

Tick the boxes where they meet the criteria. The more ✅s, the better your odds of a smooth, secure, and sanity-saving partnership.

Criteria	Provider 1	Provider 2	Us
1. Asked smart questions about your business	☐	☐	✅
2. Explained services in plain English	☐	☐	✅
3. Provided a sample agreement early	☐	☐	✅
4. Gave recent, relevant references	☐	☐	✅
5. Walked you through a clear onboarding plan	☐	☐	✅
6. Did a proper audit/discovery before quoting	☐	☐	✅
7. Prioritized prevention, not just break-fix	☐	☐	✅
8. Clearly outlined what's included/excluded	☐	☐	✅
9. Had a clear, professional support process	☐	☐	✅
10. Worked with (or explained) your tools	☐	☐	✅
11. Had real processes for their IT support	☐	☐	✅
12. Felt like a partner, not just a vendor	☐	☐	✅

ONE LAST THING BEFORE YOU GO

If you've made it this far, nicely done.

Most people never take the time to really think through how they choose an IT provider. They sign the first contract that sounds decent, cross their fingers, and hope for the best.

But you've now got a clear picture of what to look for and what to avoid, so you can hopefully choose an IT provider that checks all the right boxes🙂

And now that you're at the end of the book, you might be expecting to see some kind of sales pitch from me.

It would make sense, right? I'm an IT provider, so why not tell you all about the amazing experience you'd have working with me?

That's what most IT providers would do. But I made a promise at the beginning of the book that I'm not going to sell you anything.

And I'm the type of person who keeps their promises. So instead of putting my salesperson hat on, I'm putting my "advisor" hat on... and offering you a free advisory call where I'm going to HELP (not ~~SELL~~) with anything IT-related in your business.

I can give you a second opinion on a quote/proposal, take a look at your setup, or give you clarity on anything that's been keeping you up at night.

Send me an email at: jameson@katalism.tech

Or call me at: 469-583-2485

Thank you for reading!

Regards,

Signature

John Smith
Owner, MSP Royal

ENJOYED THE BOOK? CHECK THIS OUT...

I think it's fair to say technology is something you can't run a business without in today's world. No matter how you look at it, you need tech if you want to compete in the market.

The problem is... technology can be overwhelmingly confusing. And boring. And frustrating.

At least, that's what I hear from the business owners I talk to.

So, I put together a free newsletter called Tech for Humans to help fight the growing epidemic of tech overwhelm.

In this newsletter, I break down tech topics in a way that's easy to understand and even fun to read (that's the word on the street, anyway).

You'll learn practical stuff and stay on top of the latest tech news... without needing to Google every third word.

Things like:

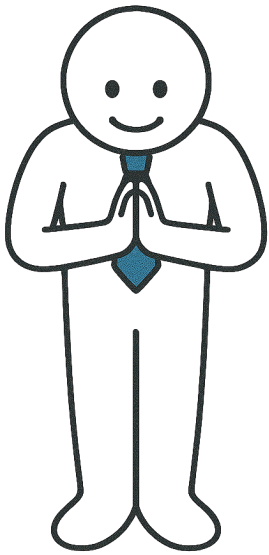
- How to spot fake emails and train your team against phishing attacks
- How to use Microsoft 365 more effectively to boost productivity
- How to leverage AI to drive growth in your business

I also share interesting stats, gadget recommendations, and fun facts.

So if you want to learn useful, non-geeky things — and pick up random trivia like the origin of the word "SPAM" — Tech for Humans is a quick, 5-minute read I think you'll enjoy.

You can subscribe for FREE here:
katalism.tech/tech-for-humans

THANK YOU!



THE SMALL BUSINESS IT BUYERS GUIDE

When you choose an IT provider, you're not just buying support. You're choosing who gets access to the inner workings of your business.

And yet, most business owners are left to make that decision with nothing more than a gut feeling and a vague proposal.

This book aims to change that.

Written by an experienced MSP owner, **The Small Business IT Buyers Guide** gives you the essential questions, practical insights, and behind-the-scenes understanding you need to make a confident, informed decision about your technology partner.

Inside, you'll discover:

- What separates a true partner from a generic provider
- The hidden costs and red flags that rarely get discussed
- How to evaluate proposals, service agreements, and onboarding timelines without needing a translator

https://katalism.tech

ABOUT JAMESON SMALLWOOD

Jameson Smallwood is the founder of a managed IT services company that helps small and mid-sized businesses stay productive, protected, and one step ahead of the chaos. With years of hands-on experience, he's seen what happens when companies get IT right, and what happens when they don't.