

Thinking of Leaving Your IT Provider?

Read This First

A straight-talking guide for practice managers and operations leads at architecture and design firms.

INTRODUCTION

This guide was written by an IT provider. You should know that upfront.

We could have written it as a sales document. We chose not to. Because the truth is, switching IT providers is not always the right call — and if that is where you end up after reading this, we would rather you knew it before you wasted everyone's time, including ours.

What this guide will do is help you think clearly. It will tell you what switching actually involves, what it costs, what to watch out for, and how to evaluate whether a new provider is genuinely better or just new. It will also give you the tools to have a more honest conversation with your current provider, if that turns out to be the right path.

Either way, you will come out of this better informed than most people who make this decision.

SECTION 1

Is It Actually Time to Leave?

The frustration that brings someone to Google "how to switch IT provider" is usually real. But frustration alone is not a good enough reason to switch. Switching has a cost — in time, disruption, and risk — and it only makes sense if what you are moving to is genuinely better than what you have.

Before you do anything else, be honest about what is actually going on.

Signs that switching is probably the right call:

- Your team has stopped raising tickets because they have given up expecting things to be fixed properly. Silence is not satisfaction.
- Problems recur. The same issues come back week after week with no permanent resolution.
- Your provider reacts to problems but never gets ahead of them. You are always the first to notice something is wrong.
- You have no idea what your IT roadmap looks like for the next twelve months. Neither does your provider.
- Costs are unpredictable. Invoices arrive with items you did not expect and cannot easily query.
- When things go wrong, your provider goes quiet rather than taking ownership.
- They have no meaningful understanding of how an architecture practice actually works — your project workflows, your software dependencies, the pressure of deadlines.

Signs that switching might not be the answer:

- Your frustration is mostly with one or two specific incidents, not a pattern.
- Your provider is responsive when you push them, but you rarely push.
- The service has been fine but you have had a change in internal expectations — perhaps a new MD or a period of growth.
- You have not actually told your provider clearly what is not working.

That last point matters more than people admit. A difficult conversation with your current provider costs nothing and occasionally fixes everything. If you have not had it, have it first.

Not sure which camp you are in?

Our IT Service Partnership Scorecard takes less than three minutes and gives you an objective view of how your current setup compares to what good looks like. No email required to see your results.

[Take the Service Self-Assessment at ingenious.co.uk/assessments/service-self-assessment]

SECTION 2

What Switching Actually Involves

The fear around switching is almost always bigger than the reality. Here is an honest walkthrough of what the process actually looks like.

Your contract

Start here. Find your current agreement and look for three things: the notice period, any minimum term remaining, and what the exit provisions say about data and system access. Notice periods of thirty to ninety days are standard. If you are inside a minimum term, you may face an early termination charge — this is negotiable more often than providers let on, particularly if you have a legitimate grievance about service quality.

Your data

This is the question that worries people most and is usually the least problematic in practice. Your data lives in your systems — Microsoft 365, your project management platform, your design software, your file server or cloud storage. None of that moves when you change IT provider. What your provider manages is access to those systems, not the data itself.

The main data consideration is documentation. A good outgoing provider will hand over a full asset register, network documentation, licence details, and account credentials. A poor one will drag their feet or be vague. Ask for this documentation before you serve notice — a provider who refuses or delays is telling you something useful.

The transition timeline

A well-managed transition for a firm of ten to fifty people typically runs over four to eight weeks. The phases look like this:

Weeks one and two: discovery. Your new provider audits your existing setup — hardware, software licences, network configuration, security posture, user accounts. No changes yet.

Weeks three and four: preparation. Your new provider sets up their monitoring tools, establishes their remote management capability, and prepares the onboarding documentation. Parallel running where possible.

Weeks five and six: cutover. Support tickets start routing to the new provider. Your previous provider's remote tools are removed. User introductions happen.

Weeks seven and eight: bedding in. New provider resolves anything that emerged during cutover, completes any outstanding configuration, and conducts an initial review.

This is not complicated. It is a process. Done properly, your team barely notices.

What actually causes disruption

Transitions go wrong when one of three things happens. The outgoing provider is obstructive — slow to hand over documentation, slow to remove their tools, slow to transfer licences. The incoming provider has not done adequate discovery and is surprised by what they find. Or the client has not allocated any internal time to the process and expects it to happen entirely invisibly.

All three are avoidable with the right preparation and the right provider on both sides of the transaction.

SECTION 3

The Questions Most People Forget to Ask

When people evaluate a new IT provider, they tend to ask about price, response times, and whether they have worked with architecture firms before. Those are reasonable questions. They are also the ones every provider has polished answers for. Here are the questions that reveal more.

"Can you walk me through exactly what happens on day one of our contract?"

A provider who has a detailed, confident answer to this has done it before and thought about it properly. Vague reassurances about a smooth transition are a warning sign.

"What does your monitoring catch that our current provider is likely missing?"

This forces them to be specific about their capability rather than generic about their approach. If they cannot name concrete examples, push harder.

"How do you handle a situation where you make a mistake that affects our business?"

Every provider will make a mistake eventually. What matters is accountability. A good provider will answer this with a clear process: we own it, we communicate immediately, we fix it, we tell you what happened and what we changed. A poor provider will become evasive or pivot to reassurances about how rarely things go wrong.

"What does a quarterly business review with you actually cover?"

If the answer is mostly a report on ticket volume and resolution times, that is operational reporting, not a strategic partnership. A meaningful QBR covers your IT roadmap, upcoming business changes, security posture, licence optimisation, and forward risk. Ask to see an example.

"Who specifically will be working on our account, and what is their experience with architecture practices?"

Not "do you work with architecture firms" — that is too easy to answer yes to. You want to know whether the actual engineer who will be picking up your tickets understands Revit, knows why large file transfers matter, and has worked in a project-based environment before.

"What are you not good at?"

The answer to this question is more revealing than almost anything else. A provider who claims to be excellent at everything is either dishonest or has no self-awareness. A provider who says "we are not the right choice if you need X, because we do not specialise in it" is being straight with you. That is the kind of provider worth trusting.

Ask these questions of us too. We would rather you asked them and decided we were not the right fit than signed up without really knowing what you were getting.

SECTION 4

How to Evaluate a New Provider Without Buying on Price

Price comparison is the default because it is easy. It is also the worst way to choose an IT provider, and it almost always leads to regret.

Here is a more useful framework.

Evaluate on outcomes, not inputs

SLAs tell you how fast a provider will respond. They do not tell you how often you will need to call them, how proactive they will be, or whether they will actually solve your problems. Ask for client references specifically from architecture or design firms, and ask those references how often IT comes up as a concern at their end.

Check their security posture

An IT provider whose own internal systems are poorly secured is not in a position to protect yours. It is reasonable to ask what cyber certifications they hold — Cyber Essentials at minimum, ideally Cyber Essentials Plus. Ask whether they have achieved ISO 27001. Ask how they handle their own data.

Look at what they say publicly

Does their website explain what they actually do and how, or is it full of stock photography and vague promises about "alignment"? Do they publish useful content, case studies, or benchmarks? A provider who is willing to be transparent publicly is more likely to be transparent privately.

Assess sector knowledge honestly

Any provider can claim to work with architecture firms. Ask them to describe the specific technology challenges that practice managers in AEC face — BIM software, large file management, remote collaboration, project-based licensing, planning software. If the answer is generic, the knowledge is not real.

Use a scoring framework

Our Service Self-Assessment was built around the benchmarks we hold ourselves to. Use it to score your prospective new provider as well as your current one. The questions are the same. The comparison will tell you more than any sales conversation.

[ingenious.co.uk/assessments/service-self-assessment]

SECTION 5

Red Flags to Watch For in Any New Provider

Some of these are subtle. Some are not.

Vague SLAs

"We aim to respond within four hours" is not an SLA. An SLA specifies what happens if that target is not met. If there is no consequence, the target is a marketing claim, not a commitment.

No named account manager

If your point of contact is a shared inbox or a ticketing system, you do not have a partner. You have a helpdesk. Those are different things, and the difference matters when something goes wrong.

No sector knowledge beyond a logo on the website

There is a meaningful difference between an MSP that has one or two architecture clients and one that has built its practice around the sector. The former knows what Revit is. The latter knows how an architecture practice uses it, what breaks, and what the workarounds are.

Reluctance to let you speak to existing clients

A confident provider with happy clients will give you references without hesitation. Delays or deflections are a signal.

Contracts with aggressive auto-renewal clauses

Twelve-month auto-renewals with short notice windows are a retention mechanism, not a partnership structure. Read the small print before you sign.

Over-promising on the transition

"It will be completely seamless" is not a credible promise. A transition involves some degree of adjustment. A provider who acknowledges this and has a clear plan to manage it is more trustworthy than one who tells you there will be no disruption at all.

Security theatre

Mentioning cyber security in every sentence while being vague about what they actually do is common. Ask specifically: do you provide 24/7 SOC monitoring? Do you conduct phishing simulation testing? Do you independently backup Microsoft 365 data? Specific questions require specific answers.

SECTION 6

What a Good Transition Actually Looks Like

Week by week, here is what you should expect from a well-run transition.

Before day one

Your new provider has completed a full discovery of your existing environment. You know exactly which systems are in scope, who owns each licence, and what the cutover sequence will be. Your current provider has been notified formally and asked to prepare handover documentation.

Weeks one and two

Remote monitoring tools from your new provider are installed and running in parallel with your existing setup. No support tickets have moved yet. Your team has been introduced to the new provider and knows who to contact and how. Any security gaps identified during discovery have been flagged to you with a priority rating.

Weeks three and four

Support routing moves to your new provider. Your previous provider's tools are removed cleanly. Licence transfers and account migrations are completed. Any issues from the cutover are documented and resolved within forty-eight hours.

Weeks five to eight

A first review meeting covers what was found during discovery, what has been resolved, what is planned for the next ninety days, and what your IT roadmap looks like for the year ahead. You have a named account manager, a support contact, and a clear escalation path.

If a provider cannot describe this process in similar detail before you sign anything, ask why not.

SECTION 7

And If You Decide to Stay?

This is a valid outcome. Not every frustration requires a switch, and a well-managed conversation with your current provider can sometimes reset a relationship that has drifted.

If you decide to stay, do it on clearer terms.

Put your expectations in writing. What response times do you need? What proactive activities do you expect? What does a quarterly review look like? What happens if things go wrong?

Ask for a technology roadmap. If your provider cannot produce a documented view of your IT priorities for the next twelve to twenty-four months, that is a reasonable thing to ask for formally.

Request a security review. If you have not had an honest assessment of your cyber and continuity posture recently, ask for one. Our Cyber and Continuity Resilience Check is free and takes less than three minutes — use it to understand what questions to ask.

[ingenious.co.uk/assessments/cyber-continuity-resilience-check]

Set a review date. Give the relationship three to six months against the new expectations and evaluate it honestly. If it improves, you made the right call. If it does not, you now have a documented basis for moving on.

A FINAL WORD

We wrote this guide because we believe the MSP market would be better if clients were more informed and providers were more accountable. Both of those things are good for everyone — including us.

If you read this and concluded that switching is the right move, we would be glad to have a conversation. If you concluded that staying made more sense, we hope this helped you do it on better terms.

Either way, if you would like an objective view of where your current IT stands, our self-assessments are there when you are ready.

No sign-up. No sales call. Just a score.

[ingenious.co.uk/assessments]



You deserve a straight answer

Ingenious is an MSP based in South London, working with architecture, design and property management firms. We provide IT support, managed security, cloud computing and AI enablement.

If you would like to talk, you can reach us at

ingenious.co.uk

020 3745 6630

ingenious.co.uk/contact