

Choosing a Secure & Strategic
IT Partner:

THE 2026 BUYER'S GUIDE FOR FINANCIAL SERVICES FIRMS



“

Most IT guides talk about features. We focus on risk, red flags, and finding a partner who protects your firm like it's their own.

<https://novixit.co.uk>







The 2026 IT SERVICES BUYER'S GUIDE

[Page 5 - Chapter 1:](#)

The 5 Technology Shifts Reshaping Risk in Financial Services

[Page 11 - Chapter 2:](#)

You've Grown. Your IT Strategy Hasn't. That's a Problem.

[Page 13 - Chapter 3:](#)

Why business owners & managers switch IT partners

[Page 20 - Chapter 4:](#)

The New Cyber Strategy: Secure. Agile. Blended.

[Page 22 - Chapter 5:](#)

Why You Should Be Highly Sceptical of Any IT Provider... Including Us

[Page 26 - Chapter 6:](#)

What Most Firms Misunderstand About IT Support, Until It's Too Late

[Page 29 - Chapter 7:](#)

Strengthen Your Internal IT, Without Adding Headcount

[Page 31 - Chapter 8:](#)

We told you what best looks like; here's what it feels like

[Page 32 - Chapter 9:](#)

Why We Exist (And Why That Matters When You're Under Pressure)

[Page 35 - Chapter 10:](#)

What will happen during your first 90 days

[Page 36 - Chapter 11:](#)

What to do next



Chapter 1:

The 5 Technology Shifts Reshaping Risk in Financial Services

The past five years have fundamentally changed how firms operate, store data, serve clients, and stay compliant.

In regulated, high-trust environments such as accountancy, asset management, and financial advisory, these shifts create new risks, demand new protections, and necessitate strategic alignment between IT and business goals.

The five shifts we'll outline aren't trends; they're tectonic movements reshaping how your firm is measured by clients, regulators, and the market.

On the following pages, we'll break them down:

- What's changing
- Why it matters
- What forward-thinking firms are doing in response
- How to align IT with compliance, continuity, and client trust

This isn't about chasing the latest tools; it's about building a strategic, secure, and scalable foundation.

It's about defending your data, protecting your reputation, and gaining a competitive edge through resilient, compliant infrastructure.



"In financial services, technology isn't just a tool; it's a potential liability. And the firms that treat IT as infrastructure, not insurance, will outpace those still relying on reactive support."

- Ricci van Eeden, Founder & Strategic Advisor



Shift 1: AI Is Now Both a Cybersecurity Asset and an Attack Surface

The rise of AI tools like Copilot and ChatGPT has permanently changed the threat landscape.

They boost productivity, but they also help cybercriminals scale faster, craft more convincing attacks, and exploit blind spots most firms haven't prepared for.

THE RISKS

1 - AI-Powered Phishing

Attackers now use AI to:

- Clone writing styles
- Create fake emails that bypass detection
- Mimic internal messages with shocking accuracy

Your staff won't be fooled by typos anymore; they'll be tricked by AI-crafted authenticity.

2 - Data Leakage from AI Tools

Using tools like Copilot to draft reports or analyse data can feed sensitive client info into AI models, **violating GDPR and FCA expectations** if controls aren't in place.

3 - Autonomous Threat Actors

AI systems acting independently (agentic AI) are already in use by nation-state attackers. This isn't future tech; it's real, live, and aimed at SMEs.

Smart firms:

- Audit internal AI usage across teams
- Train staff to recognise AI-powered attacks
- Partner with IT providers who understand AI risk, not just AI tools

Innovative firms use AI to defend. Vulnerable firms ignore how it's being used against them.



Shift 2: Hybrid Working Creates New Risk Surfaces

When staff work from home, cafés, or client sites, your firm's network perimeter disappears.

Unsecured Wi-Fi, personal device use, and weak MFA create invisible entry points. Often, without the user knowing. For regulated firms, this isn't just an IT inconvenience; it's a compliance exposure.

Smart firms:

- Apply device-level security
- Run endpoint detection (EDR) on remote devices
- Train staff on hybrid-specific attack tactics



Shift 3: Cloud Flexibility = Compliance Complexity

Cloud makes data accessible, but also dangerously shareable.

Misconfigured permissions, old user accounts, and unsanctioned cloud tools ("shadow IT") are now the top causes of SME data breaches.

For firms governed by FCA and GDPR, these issues quickly become regulatory events, not just IT mishaps.

Smart firms:

- Audit cloud permissions quarterly
- Use tools to monitor unsanctioned file-sharing
- Align controls with compliance standards



Shift 4: Third-Party Tech & SaaS Are Now Your Biggest Blind Spot

Most financial firms rely on dozens of cloud apps: CRMs, client portals, e-sign tools, and file sharing, the systems that hold your client's most sensitive data.

But each of those tools is a risk surface. If just one is breached or misconfigured, your client data is exposed, and you're still responsible under FCA and GDPR rules.

Smart firms:

- Maintain a vendor risk register
- Limit app access to only what's necessary
- Audit connected tools and user permissions quarterly



Shift 5: Security Awareness Is Now a Business Culture Issue

Tech failures don't cause most breaches; people cause them.

Phishing emails, fake MFA prompts, social engineering, all now supercharged by AI. One employee click is all it takes.

If your team still sees security as "IT's problem," you're exposed.

Smart firms:

- Train staff with live, evolving threat examples
- Run internal phishing simulations monthly
- Make cybersecurity a standing board-level agenda item

“

Every week, we see firms lose client data, suffer reputational damage, or face regulatory fallout; not because of bad luck, but because they relied on the wrong IT partner.

Smart firms **defend and invest.**



Defend: Stop preventable breaches, phishing, and compliance slip-ups.



Invest: Build future-ready systems that support growth, not just maintenance.

Technology evolves fast. Threats evolve faster. If your provider isn't helping you defend your firm or build scalable infrastructure, you're exposed, and you'll fall behind.

Most providers fix. We fortify.

We don't just "fix IT." We:

- Help financial firms mitigate cyber risk
- Align IT with FCA and GDPR compliance
- Turn infrastructure into a competitive asset

This guide will show you how to assess whether your IT provider is protecting your firm or just reacting to it.

If you're already questioning whether your current support is fit-for-purpose, skip to **Chapter 11 and let's talk.**



Ricci vE

Ricci van Eeden
Founder & Operations Director
riccive@novixit.co.uk
+44 78 8772 0877



Scan to save my info



Chapter 2:

You've Grown. Your IT Strategy Hasn't. That's a Problem.

If your IT strategy hasn't changed since your business did, it's now your biggest blocker.

If your IT strategy hasn't been re-evaluated in the last 18 months, it's likely out of step with your business goals.

If your business runs on tech, even partially, your IT strategy can no longer be an afterthought.

The importance of a well-thought-out IT strategy for any successful business is critical.

Your IT strategy should be an extension of your business plan, driving progress, not reacting to problems. It should support long- and short-term goals, with built-in flexibility.

It should consider both long-term strategy and short-term tactical while leaving room for change where necessary.

Despite the name, it's not about the technology; it's about how the right tech strategy drives margins, momentum, and market share.

Start with your current IT foundation.

Consider:

- Is it helping you scale, or holding you back?
- Are the right tools aligned to the right goals?
- Will it still serve you at 2 times or 5 times your current headcount?



How we help our clients plan ahead:

We map out what's ahead and what it'll take to get there.

That means both of us know:

- What will be happening over the next 2 to 3 years
- What technology investments you need to make

Your IT strategy is stale. And it's quietly **sabotaging your growth.**

A good IT partner helps you:

- Identify smarter tools and infrastructure
- Align technology with your growth plan
- Stay compliant with FCA, GDPR, and security expectations

Most IT firms react. **Strategic partners prevent. The difference shows up in your margins.**

Smart firms:

- Hold regular strategic reviews (every 6 months is ideal)
- Track infrastructure performance against ROI, such as identifying which system costs you £10,000 per year in lost productivity.
- Involve their teams in identifying bottlenecks
- Plan tech investment like any other growth strategy

And there are no surprises. It's all planned with regular strategic reviews to help us both move in the right direction.

With a smart roadmap, you'll know what to delay, what's mission-critical, and where to double down if you're ahead.

It's this level of planning that helps you stay in control and ahead.

We get to know your business as if it's our own. We're constantly working with you on your business and learning about you and your team.

This commitment makes it easy for us to help you because we know (just as well as you do) where your business is going.

The right strategy isn't just tech. It's people, process, and path, and we help you build all three.

Chapter 3:

Why business owners & managers switch IT partners

I hear from many businesses that are frustrated with their current IT support provider.

They're not getting what they need. Worse, they've started to accept it.

We've taken over from dozens of IT providers; these are the patterns we see every time, and why those firms are now more secure, agile, and supported.

#1

Reason 1: You can't see the value

Return on investment is non-negotiable, especially in today's climate.

You should be able to see exactly what your IT partner is delivering: what problems they're solving, and how that translates into time, cost, or risk savings for your business.

Any IT partner worth working with should:

- Deliver a clear IT strategy
- Track progress against short- and long-term goals
- Provide simple, business-relevant reporting

And that reporting should mean something, not vague KPIs or jargon-laced metrics. If they can't explain the business benefit, why are you paying them?

#2

Reason 2: Communication is unreliable

From slow responses to silence after a ticket is raised, communication gaps are one of the most common complaints.

Technology issues are disruptive. But what's more disruptive? Not knowing what's happening or when help is coming.

A true IT support partner:

- Acknowledges issues promptly
- Keeps you in the loop
- Does what they say, when they say they'll do it

Good support is transparent and responsive. Missed deadlines. Project delays. Poor client experiences. Bad communication causes real damage.

If your provider keeps you in the dark, it's time to move on.

#3

Reason 3: They don't take security seriously

Yes, it happens, even with providers whose job it is to protect your data.

Some IT support companies fail to stay updated on threats, patch management, or security best practices. They'll assume your systems are fine, while leaving theirs vulnerable (and by extension, yours too).

Some even respond with:

"Don't worry about that. We've got it handled." That's not reassurance; at best, it's a risk, at worst, negligence.

That's a **red flag**. You should always know:

- What are your biggest risks
- What your IT partner is doing to mitigate them
- How to protect yourself (and your people) from scams and attacks

Security is too important to be outsourced without transparency.

#4

Reason 4: "We don't cover that."

If your provider says this about something clearly related to your tech setup, it shows a lack of ownership.

A partner doesn't hide behind contracts. They step up to solve problems and proactively look for ways to improve your environment.

If your IT firm isn't curious, flexible, or willing to go outside the script, they're not a partner. They're a service desk.

You need someone who understands your goals and works like part of your team, not just a vendor on retainer.

#5

Reason 5: Problems drag on for too long

Some issues are complex. We get that.

But that's no excuse for silence or slow action.

Good partners:

- Acknowledge the issue quickly
- Communicate clearly throughout
- Keep you updated while resolving the problem

You should never be left chasing updates three days later.

You're not a priority. That's all you need to know.

#6

Reason 6: No one takes responsibility

One of the most damaging signs is when no one takes ownership of the issue.

It's shocking how often we hear:

"That's not our fault; you'll need to talk to the software vendor."
"You did not follow our advice."

Passing the blame doesn't solve the problem, and it certainly doesn't foster trust.

The right IT partner will take ownership, coordinate with third parties if needed, and see the issue through to resolution. That's what partnership looks like.

#7

Reason 7: They weaponise jargon

You shouldn't need to speak fluent tech just to understand your own IT environment.

Confusing, jargon-heavy conversations do more harm than good.

A good partner will:

- Explain things clearly, without dumbing them down
- Help you understand just enough to make informed decisions
- Never leave you feeling out of your depth

If your provider makes you feel stupid or confused, that's not communication. It's control.

#8

Reason 8: You're not learning anything

You're not hiring an IT tutor, but there should be some learning along the way.

From basic cybersecurity practices to understanding your network setup, a good partner helps you become more confident, not more reliant.

If you're kept in the dark or discouraged from asking questions, you're ***not being empowered, you're being sidelined.***

Knowledge builds resilience. Choose a partner who helps you grow.

#9

Reason 9: They're more interested in sales than support

If you feel like your IT partner is more interested in selling you gear than solving problems, you're not alone.

While occasional upgrades are necessary, constant pressure to buy new hardware is a red flag. Especially if you already have what you need.

A partner should:

- Focus first on stability, security, and usability
- Recommend upgrades when they support a business outcome
- Help you budget in advance with a roadmap, not spring surprises

If it doesn't support a strategic outcome, it's not an upgrade. It's upselling.

#10

Reason 10: You've outgrown them

This isn't a bad thing; it's just reality.

Your business has outpaced your provider. And now you're carrying the risk. Maybe you need faster response times, more expertise, or better infrastructure planning.

Sometimes, the right move is simply to level up.

And if you're working with a smaller provider you genuinely like, this can feel tough. But the risk of staying too long with an underpowered partner is far worse.

When to make the switch

Ask yourself:

- Are your support requests taking too long, or going unanswered?
- Have the strategic recommendations stopped coming?
- Do you now need a higher level of support than they can provide?

If you're nodding yes, it might be time to start exploring other options. Chances are, your provider knows it too.

It doesn't need to be awkward. But it can't be avoided.

You deserve a real partner

Switching IT partners can feel risky, but staying with the wrong one is riskier.

When your provider works like an extension of your team, communicates clearly, owns issues, and plans with you... Everything changes.

You don't need another vendor.

You need a partner who protects like a CISO, plans like a CTO, and acts like part of your team.

That's what we're built for.







Chapter 4:

The New Cyber Strategy: Secure. Agile. Blended.

A strategic approach to keeping your firm protected, without slowing it down.

Today, your team doesn't work in one place. They're in the office. At home. On client sites. Sometimes all in the same week.

That flexibility is a strength and an expectation. But it also introduces new risks that most IT setups aren't built to handle. Every unsecured login, every shared file, every personal device used to check a client email adds to your attack surface. And if your systems aren't designed to support this reality, you're exposed, whether you know it or not.

The real threat isn't someone trying to brute-force your firewall. It's the moment someone on your team clicks the wrong link. Approves the incorrect transfer. Or responds to a request that wasn't real.

Cybersecurity has changed. It's no longer just about prevention; it's about resilience. And it's no longer just about protecting data; it's about protecting your ability to operate.

For most firms we meet, the gap isn't in technology. It's in strategy.

The issue isn't that they don't care about security. It's that their systems were never designed to support how their team actually works.

Either they're under-protected, or locked down so tightly their staff end up working around the controls. Both lead to risk. Just in different ways.



And when something does go wrong? It's not just IT, it's operations, reputation, and regulatory exposure. That's especially true in sectors like accounting, investment, and legal, where client confidentiality is a non-negotiable part of doing business.

That's why we don't take a "set and forget" approach to protection. We design blended security, the kind that protects your business without getting in the way of it.

It's a balance. Go too far, and your own team will bypass the systems, not out of malice, but to get their job done.

The smartest firms aren't locking down their teams; they're enabling them. They're asking better questions. Designing smarter systems. And building security into the way they work.

The answer isn't more software. It's a smarter design.

Secure remote access. Role-based permissions. Response plans that aren't theoretical. Cyber awareness that's part of onboarding, not a tick-box exercise. All built around how your business actually functions.

When you get that right, you don't just reduce risk. You reduce friction.

And suddenly, security isn't a blocker, it's an enabler.

You don't need to decode every threat report or keep up with every exploit. You need a partner who does and builds your systems to stay ahead of them.

If your current provider isn't thinking this way, you've already outgrown them.

And if you're thinking your firm deserves more than tick-box IT, you're starting to ask the right questions.



Every firm will face a breach. What separates the ones that survive from the ones that suffer is whether they've built security around how they actually operate.



- Euan Stewart, Founder & Strategic Advisor



Chapter 5:

Why You Should Be Highly Sceptical of Any IT Provider... Including Us

IT is an unregulated industry. And that's a problem.

There's no licensing. No compliance body. No entry bar.

Anyone can set up shop as an "IT support" company, even if they've never managed a network, implemented security controls, or supported regulated firms.

That leaves business owners like you in a dangerous spot: you're forced to trust providers in areas where you lack visibility or control. You assume it's handled, until it isn't. And by the time you find out, the damage is done.

This isn't sales talk. It's operational risk management. It's about protecting you from a decision that could cost far more than money.

And just to be clear where we stand:

One of our founders, Ricci van Eeden, serves as Vice Chair of the IT Managed Service Provider Best Practice Charter, the same body that helps define what "great" actually looks like across the industry.

We don't just follow the standard. We help write it.

Here's how to separate the professionals from the pretenders.

Below are questions every firm should ask a potential IT partner.

Not just to get answers, but to see how clearly, confidently, and operationally they can respond.



Ask them: “How fast do you respond, and what’s your worst-case delay?”

Don’t settle for “quickly.” Ask for timeframes by severity:

- What’s your SLA for critical issues?
- How are tickets triaged?
- What happens after hours?

You’re not just checking response times, you’re testing their process under pressure.

Ask them: “What proactive work do you do?”

Strong providers fix issues. Great ones prevent them.

Ask what they do weekly, monthly, and quarterly to keep your systems running. Then ask when it happens. If it's during working hours, that's a red flag.

Ask them: “Who owns the relationship?”

Do you get a named contact who knows your business? Or a rotating helpdesk of strangers?

The right partner doesn’t wait for problems; they engineer stability. That starts with accountability.

Ask them: *“How do you document and track changes to our systems?”*

If they can't show you an audit trail, they can't prove what they've touched. That's a risk to your uptime, your compliance position, and your ability to switch providers without disruption.

Ask them: *“What happens in the event of a breach?”*

Not just what tools they use. What's the actual response plan?

Who gets notified? What gets isolated? What can you expect hour-by-hour? If they can't articulate this clearly, they won't lead confidently in a crisis.

Ask them: *“How do you help us meet our industry's regulatory expectations?”*

Whether you're FCA-regulated, working in professional services, or handling sensitive data, the rules matter.

If they can't demonstrate how their stack and support model aligns with your compliance obligations, they're not qualified to protect your firm.

Ask them: *“What's your onboarding process, and what happens in the first 90 days?”*

You don't want a lift-and-shift. You want a structured handover with documentation, risk reviews, and clean ownership.

*Weak answers aren't just a red flag;
they're a liability.*

IT support is a business-critical partnership.

Poor visibility, unclear processes, and vague answers aren't minor oversights; they're signs of a provider who may be making it up as they go.

You deserve better.

If this sounds blunt, it's because it needs to be.

When one of your founders helps define the standards for the entire MSP sector, you don't tolerate vague answers or half-baked setups, and neither should you.



Most firms don't realise just how unregulated this industry is. That's exactly why the Best Practice Charter exists: to raise the bar and hold providers to a standard.

If your IT partner can't clearly explain how they keep you protected, they probably aren't.



- Ricci van Eeden

Founder & Strategic Advisor
Vice Chair, IT MSP Best Practice Charter

Chapter 6:

What Most Firms Misunderstand About IT Support, Until It's Too Late

#1

Good IT Support Looks Boring When It's Working

When everything runs smoothly, it's easy to assume your IT provider isn't doing much.

That's exactly how it should feel.

The real work happens behind the scenes, monitoring endpoints, patching systems, reviewing logs, and hardening infrastructure. No tickets? No chaos? That's not luck. That's design.

If your provider is constantly reacting, it's because they didn't plan well enough in the first place.

Strong IT support is invisible, until it isn't.

#2

Faster Isn't Always Better. Reliable Is.

Speed matters, but predictability matters more.

In regulated sectors, it's not just about fixing problems quickly; it's about ensuring they don't happen often, and when they do, that your provider has the discipline and documentation to act methodically, not just quickly.

You don't want the fastest fix. You want the right one, done once, done properly, with no surprises three months later.

Ask yourself: Is your provider preventing chaos or just cleaning it up?

#3

You Always Pay, One Way or Another

Every firm wants the best IT support at the lowest cost. But when the numbers don't add up, it's because something is being skipped: documentation, monitoring, patching, risk planning.

You don't save money by underinvesting in security or support. You just move the cost downstream, into outages, breaches, regulatory exposure, or lost time.

You're already paying for IT. The only question is whether it's preventing risk or cleaning up damage.

#4

Long-Term IT Partnerships Are a Business Advantage

The longer your IT partner works with you, the more context they build about your team, systems, risks, and goals.

That's not just convenient, it's strategic.

Firms with long-term IT partners have:

- Fewer failures
- Stronger compliance posture
- More stable roadmaps

You don't need a vendor. You need a partner who can think beyond tickets and tools, and act like an extension of your business.

Continuity isn't optional; it's your firm's IT resilience strategy.

#5

In-House IT Isn't Always Cheaper... or Safer

An internal IT person may understand your business, but they can't scale, monitor 24/7, or stay current with a constantly evolving threat landscape.

A mature IT partner brings:

- Depth of experience across multiple sectors
- A team with redundancy (so your support doesn't vanish during leave)
- Specialised roles for cyber, compliance, recovery, and strategy

The result? **Broad capability. Zero single point of failure.**

In-house might know your systems. A true partner knows how to protect them.

In a high-risk, high-expectation environment, IT support isn't just service, it's strategy. Choose like your reputation depends on it. Because it does.



Chapter 7:

Strengthen Your Internal IT, Without Adding Headcount

If your business has an internal IT manager or team, you're already ahead of the curve. You've invested in people who know your infrastructure, understand your workflows, and can handle the day-to-day.

But here's what we see, over and over again, even in highly regulated industries:

- Your IT person is spread too thin.
- There's no redundancy.
- Critical tasks get postponed because "they know we're short this quarter."
- Cyber security? It's on their list, but so is setting up printers.
- And if they leave? The entire firm is exposed.

This isn't a knock on your internal team. It's a reflection of reality: **the job has outgrown the job title.**

You Don't Need to Replace Them. You Need to Reinforce Them.

Co-managed IT isn't about taking over. It's about building around the team you already trust.

When we work alongside in-house IT, here's what firms gain:

- 24/7 monitoring and threat detection
- Backups tested regularly, not assumed
- Extra hands for projects, migrations, and compliance work
- A second set of eyes on infrastructure and cloud security
- A long-term strategy aligned to business risk, not ticket volume

And your internal team? They get to breathe. To think. To lead.

They stay in control. We remove the pressure.

Most Firms Wait Too Long to Reinforce

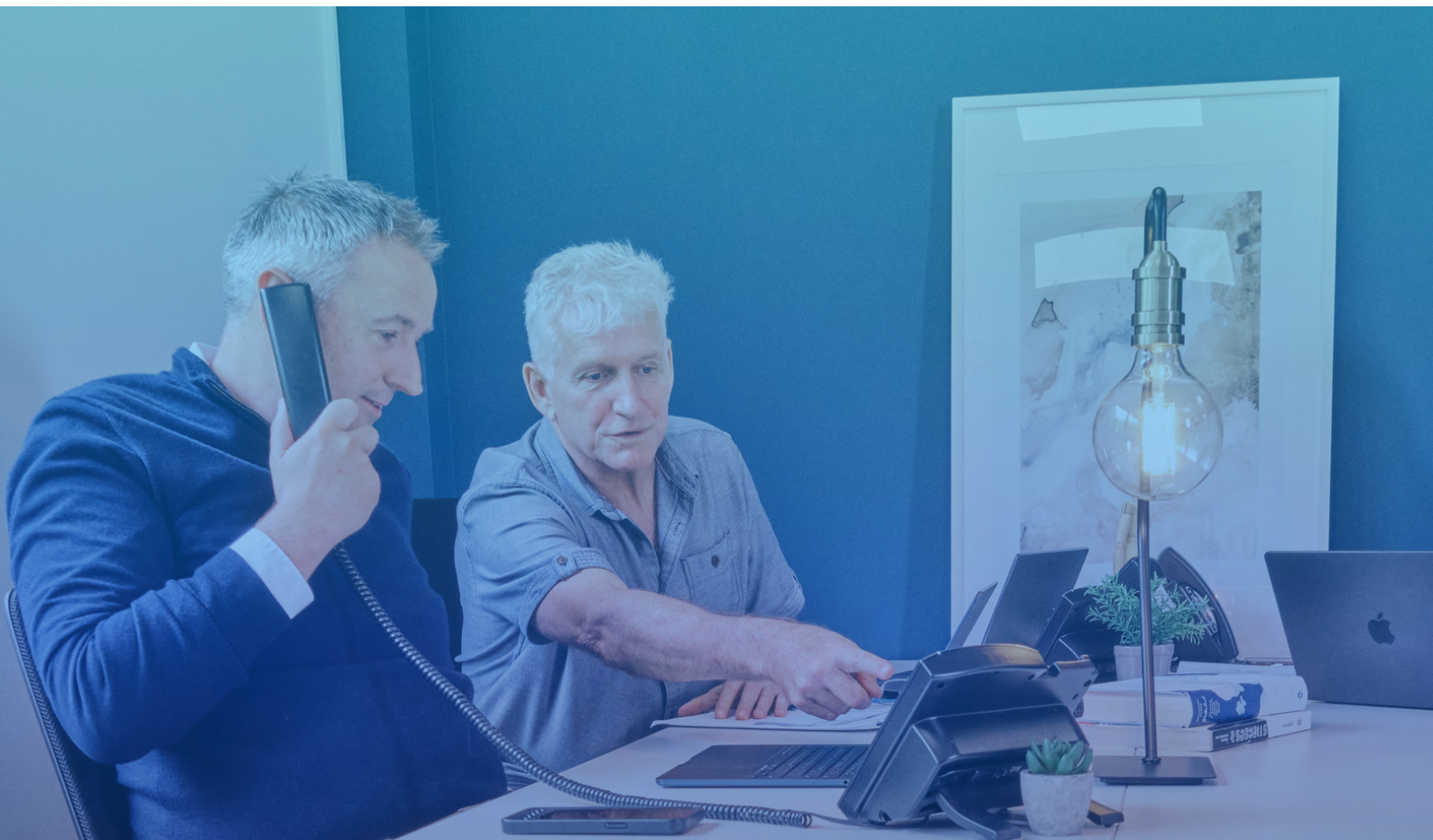
Here's when clients usually come to us for co-managed support:

- Their IT manager just handed in their notice
- Their insurer is asking about MFA, SIEM, and recovery times
- A regulator or auditor flagged major gaps
- Or something breaks... and no one has the keys

The more brilliant move is to strengthen your posture before the risk materialises. Co-managed gives you scale, strategy, and resilience, without adding headcount.

If your internal IT team is critical to your business, they shouldn't be left unsupported.

Let's build a safety net beneath them, and a strategy around them.



Chapter 8:

We told you what best looks like, here's what it feels like.

You've seen how to assess risk, spot red flags, and choose an IT partner who protects your business like it's their own. But what does that actually feel like in practice?

Here's what our clients say about working with Novix, whether we're protecting sensitive data or just getting people back online fast.

"Professional, diligent, and genuinely effective."

"The Novix team are attentive, professional, and thorough. Their IT support is both efficient and highly effective, you immediately know your systems are being taken seriously."

- feedback from clients in regulated industries

"They've future-proofed our IT and transformed our security."

"Novix IT have been instrumental in preparing our company for the future, from security enhancements to staff training. Their personal, proactive support makes them a partner we'd confidently recommend to any business."

- strategic feedback from a compliance-driven firm

Everyday feedback, same-day impact.

"The team always responds fast. Doesn't matter how big or small the issue is."

- Will,
Operations Manager

"The Team handled my request the same day. No Chasing, No Delay, just sorted."

- Kate,
General Manager

"Last-minute tech issue, no stress. Patient, helpful, and trusted our expertise too."

- Jim,
Managing Director

Chapter 9:

Why We Exist (And Why That Matters When You're Under Pressure)

Novix IT wasn't born to blend in; we built it to fix what was broken. We saw firms being overcharged to stay vulnerable. Where complexity was covered for poor design, and "best practice" meant cutting corners. That's not just broken, it's dangerous.

**We knew there was a better way...
So we started again, from the ground up.**





As Greg Lehmann, our Business Development Director, puts it:

“We’re not trying to be your vendor. We’re trying to be the last IT firm you ever need.”

It’s not a slogan. It’s how we treat every conversation.

So we built a model that prioritises three things:

Built on Security. Not Bolted On.

From architecture to onboarding, we bake resilience into every layer, not as an afterthought, but as a starting point. We don’t cut corners, and we don’t trade safety for speed or convenience.

One partner. Total coverage.

IT. Cybersecurity. Strategic input. From strategy to Service Desk, you get full accountability, no passing the blame. No dropped balls between vendors. Just one roadmap, and we own it.

Outcomes, Not Excuses.

We’re not here to hit sales targets. We’re here to protect your future. No upsells. No fluff. No excuses.

We’re in the business of real outcomes, not software sales. It’s about earning your trust, and keeping it.

Novix IT exists for firms that know they can’t afford to guess. Not with data. Not with downtime. Not with risk.

We cut through noise, skip the blame game, and get you protected, fast and right.

We don’t confuse complexity with competence.

We’re not a safer bet. We’re the end of the guessing game. **Let’s talk.**



Chapter 10:

This Isn't a Handover. It's a Hostile Takeover.

When your provider drops the ball, your business is exposed.

Switching isn't just about better service; it's about stopping risk fast. Smart firms don't ease in. They take back control.

#1

Expose Every Gap

We don't review the handover. We rip it apart.

- Every account, login, and device gets verified
- Every risk is documented, and the real story surfaces fast
- We make no assumptions and no compromises

You see the truth in Week 1.

#2

Eliminate Risk

We don't monitor risk. We remove it.

- Rogue access is revoked
- Shadow IT is cleaned up
- Unpatched software is replaced

Nothing is left to "transition." This is a clean break.

#3

Set the Strategy

Once the fires are out, we build forward.

- Your environment is stabilised
- We work with your leadership team
- You get a clear, actionable roadmap — not a deck, not a delay

By Day 90, the new standard is in place.



“

We don't do 'transition periods.' We do controlled takeovers that make you look good, fast.

**- Greg Lehmann,
Business Development Director**

Chapter 11:

What to do next (If you're serious about security, stability, and control.)

Let's be clear:

If your IT provider can't show you the risks or how they're removing them, they're not managing IT. They're managing your exposure.

Now it's time to stop tolerating less..

Here's the next move:

[Book a 15-minute call with our leadership team](#)

No sales scripts. No fluff.

We'll talk about your environment, your risks, and whether we're a fit.

If we are, we'll lay out your next step.

If we're not, we'll tell you, fast.

Why now?

You've just seen how we uncover risk, restore control, and rebuild IT that actually supports your business.

If your current provider was doing that, you wouldn't have made it this far.

This is the moment most firms realise:

It's time for a better standard.

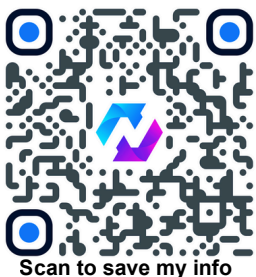


Euan Stewart

Founder & Technology Director

euans@novixit.co.uk

+44 33 33 580 560





This is how you can
get in touch with us:

CALL: [+44 33 33 580 560](tel:+443333580560)

EMAIL: hello@noxixit.co.uk

WEB: www.novixit.co.uk

LinkedIn: [linkedin.com/company/novixit](https://www.linkedin.com/company/novixit)