NetMonkeys

WHITEPAPER · 2027 EDITION

BUYERS GUIDE · 2027 EDITION

The Accountant's IT Services Buyers Guide

How to evaluate, procure, and get the most from managed IT in modern accountancy practice

Cloud transformation, cyber compliance, AI tools, and hybrid working have fundamentally changed what accountancy firms need from their IT provider. This guide is written for finance, operations, and IT decision-makers at UK accountancy firms — whether you're reviewing your current setup or buying IT services for the first time.

PUBLISHER	NetMonkeys — Managed IT & Cybersecurity
AUDIENCE	Accountancy Practice Owners, Partners, Operations & IT Leads
EDITION	2027 — Updated for ISAE 3402, MTD Phase 3, Cyber Essentials Plus

CONTENTS

What's inside this guide

Eight chapters covering everything a UK accountancy firm needs to know before purchasing or renewing IT services — from evaluating proposals to understanding cyber compliance obligations.

"

73% of UK accountancy firms say technology decisions are now made at partner level — yet fewer than 1 in 3 have a formal IT procurement process.

— ICAEW Technology in Practice Survey, 2026

The IT requirements of an accountancy firm in 2027 look almost nothing like they did in 2019. Regulation, remote working, cloud adoption, and a new generation of AI-assisted tools have collectively transformed what "good IT" means for a practice of any size.

For decades, the IT needs of accountancy firms were relatively predictable — a server, desktop software licences, and a local support contract. That model has broken down entirely. The firms that are thriving in 2027 are those that treat technology as a strategic resource, not an administrative overhead.

89%
of UK accountancy firms now rely primarily on cloud-based software for client work

67%
have experienced at least one cyber incident or attempted breach in the past 24 months

3.2×
more likely to lose a client to a competitor following a data breach or system outage

The five forces reshaping IT in accountancy

Making Tax Digital Phase 3

The final phase of HMRC's MTD mandate extends to all remaining VAT-registered businesses and self-assessment filers. Firms unprepared with compliant software integrations and reliable data pipelines face significant client-retention risk.

Cyber compliance obligations

Regulators, PI insurers, and larger clients increasingly require Cyber Essentials or Cyber Essentials Plus certification. Without these, firms face higher premiums, lost tender opportunities, and exposure to regulatory scrutiny.

Hybrid and remote working

Staff across modern practices split their time across office, home, and client sites. IT that doesn't support secure, seamless access from any location is now an active barrier to talent retention and operational efficiency.

AI-assisted workflows

From Microsoft Copilot drafting engagement letters to AI-assisted bookkeeping review tools, the practices adopting these capabilities are realising measurable productivity gains. IT infrastructure must support — not obstruct — adoption.

Not all IT providers are the same. For accountancy firms, the stakes are higher than most — you hold sensitive client financial data, operate under regulatory obligations, and can't afford extended downtime.

The market is crowded with IT providers offering broadly similar-sounding services. The questions below are designed to help you cut through the noise and find out what's genuinely behind the proposal.

🏛️

Sector experience

Does the provider have demonstrable experience with accountancy or professional services firms? Can they reference Xero, Sage, CCH, or IRIS integrations? Do they understand Practice Management systems?

ASK FOR REFERENCES FROM SIMILAR-SIZED FIRMS

🔒

Security credentials

Are they Cyber Essentials certified themselves? Do they have experience helping clients achieve Cyber Essentials Plus? Can they demonstrate a documented security posture?

VERIFY CERTIFICATIONS — DON'T JUST TAKE THEIR WORD FOR IT

⏱️

Response commitments

What are their contractual SLAs? What counts as Priority 1? How is out-of-hours support handled? During your busiest periods — year-end, self-assessment — are response times guaranteed?

GET SLA RESPONSE TIMES IN WRITING

📍

UK-based support

Is the support desk UK-based? Are engineers who visit your offices directly employed or subcontracted? When you call, who answers — and do they understand your environment?

ASK SPECIFICALLY ABOUT HELPDESK LOCATION

RED FLAG

Any provider who can't clearly explain how they handle client data under UK GDPR and ICO guidelines — or who can't name the contractual mechanisms in place — is not a safe choice for an accountancy firm.

Accountancy firms are among the most attractive targets for cybercriminals in the UK. Client financial records, banking mandates, payroll data, and tax information represent a highly valuable and often under-protected data asset.

Basic antivirus and a firewall are no longer sufficient. In 2027, any IT provider serving an accountancy firm should be delivering — as a baseline — the following security capabilities.

Managed Endpoint Detection & Response (EDR)

24/7 monitoring of all devices, with behavioural threat detection that catches attacks traditional antivirus misses. Look for providers using Huntress, SentinelOne, or equivalent.

Multi-Factor Authentication everywhere

MFA must be enforced across Microsoft 365, remote access, banking portals, and all business applications. Any provider who doesn't make this mandatory is not taking security seriously.

Email filtering and phishing protection

Business Email Compromise (BEC) attacks are the number one financial threat facing accountancy firms. Microsoft Defender for Office 365 with Safe Links, Safe Attachments, and anti-impersonation rules should be standard.

Backup and ransomware recovery

Immutable, off-site backups with a tested recovery process are non-negotiable. Ask providers for their RTO (Recovery Time Objective) and RTO test results — not just their backup frequency.

£8,460

Average cost of a cyber breach for a small UK professional services firm

93%

of accountancy firm breaches begin with a phishing or impersonation email

21 days

Average recovery time for a firm without tested backups following a ransomware attack

Microsoft 365 is now the default platform for most UK accountancy firms. But buying the licence is only the beginning — the value lies in how well it's configured, governed, and managed.

Many firms pay for Microsoft 365 Business Premium — the highest-value, most security-rich licence tier — but receive only a fraction of its capability because their IT provider has never configured the security features, governance settings, or collaboration tools it includes.

The Microsoft 365 capability gap

Typical under-configured M365	Well-managed M365
✗ No Conditional Access — any device, any location can sign in	✓ Conditional Access enforces MFA and device compliance on every sign-in
✗ Defender features unused — licence paid, protection absent	✓ Defender for Office 365 fully configured — email is actively protected
✗ SharePoint ungoverned — documents everywhere, no structure	✓ SharePoint structured by client/matter — searchable, auditable, governed
✗ Guest access unchecked — ex-staff or clients still have visibility	✓ Guest access reviewed quarterly — only active collaborators have access
✗ No audit logging — no visibility of who accessed what	✓ Audit logs retained and reviewed — visibility across all activity

BUYER'S TIP

Ask any prospective IT provider what your current Microsoft Secure Score is — and what their target score would be at 90 days. If they can't answer either question, they're not actively managing your Microsoft 365 environment.

AI has arrived in accountancy practice — but the way it's discussed often obscures what actually matters: which specific tools deliver measurable time savings, and what does your IT infrastructure need to support them safely?

The risk for accountancy firms isn't that AI will replace staff — it's that practices without AI-enabled workflows will be less efficient, less competitive, and less attractive to the next generation of talent. Here's what matters in 2027.

🤖

Microsoft Copilot

Copilot for Microsoft 365 assists with drafting client correspondence, summarising meetings, analysing spreadsheets, and building reports. Requires Microsoft 365 Business Premium or E3/E5 licence plus Copilot add-on.

⚡

Power Automate

Already included in most M365 licences. Automate client onboarding workflows, approval chains, document filing, and routine reporting — without bespoke development.

📊

AI in practice software

Xero, Sage, CCH, and IRIS all have AI-assisted features for bank reconciliation, anomaly detection, and client queries. Your IT infrastructure needs reliable, low-latency connectivity to support these effectively.

What your IT provider should be doing

- Assessing which AI tools are appropriate for your licence tier
- Ensuring Microsoft 365 is configured to support Copilot deployment securely
- Reviewing data governance before Copilot is switched on
- Identifying Power Automate opportunities in your practice workflows
- Training staff on responsible AI use and data handling
- Advising on AI-related cyber risks (prompt injection, data leakage)
- Monitoring AI tool usage and access controls
- Connecting practice software integrations for seamless data flow

IMPORTANT

Before enabling Microsoft Copilot, your SharePoint and file structure must be correctly governed — Copilot surfaces data based on what users have access to. A poorly configured environment can expose sensitive client files to unintended users.

IT service contracts can be genuinely complicated. Understanding what you're actually buying — and what isn't included — is one of the most important skills a practice partner or operations manager can develop.

Common pricing models explained

Per-seat managed service

A fixed monthly fee per user, covering support, monitoring, and security tools. The most common model. Predictable and easy to budget — but check exactly which tools are included and at what level of service.

Break-fix (pay as you go)

You pay only when something goes wrong or you need help. Appears cost-effective but incentivises slow resolution and creates an adversarial support relationship. Not recommended for any regulated firm.

Block hours / retainer

A bank of hours purchased monthly or annually. Can work for consultancy-heavy engagements but often leads to hour-burning behaviour and gaps in proactive monitoring.

Tiered bundles

Essential/Standard/Premium packages. Common and often well-structured — but interrogate what "Essential" actually excludes. Many security-critical features are often only in the top tier.

Questions that reveal hidden costs

- **Is onboarding included, or is it a separate project fee?** Initial setup, data migration, and configuration work can add thousands to the first-year cost.
- **What's excluded from the SLA?** "Best endeavours" clauses, exclusions for third-party software, and limits on onsite visits are common contract surprises.
- **Who pays for Microsoft licences?** Some providers bundle licences; others charge separately. Clarify whether you're buying licences through them (with a margin) or directly from Microsoft.
- **Are project or consultancy days charged separately?** IT strategy work, migrations, and major changes often fall outside the managed service and are billed at a day rate.

The single most common reason accountancy firms stay with a poor IT provider is fear of what switching involves. In practice, a well-run transition is far less disruptive than most firms expect — and the payoff is immediate.

The fear of switching is understandable. IT systems touch everything in a practice — client data, billing systems, email, remote access. But that same interconnectedness means that poor IT support has an outsized negative impact on productivity and security. Staying out of inertia is a decision with real costs.

A typical well-run transition — six weeks

Week 1–2
Discovery & documentation

New provider documents your full environment — hardware, software, accounts, licences. Dual-running begins where possible.

Week 3–4
Platform deployment

RMM, security tools, backup platforms, and monitoring deployed across devices. Staff communicate via agreed channels — typically Microsoft Teams.

Week 5–6
Go-live & handover

Support desk formally transferred. Staff introductions completed. Previous provider access removed. First security sweep completed.

Your rights when switching

- **Domain and DNS records** are yours — your provider cannot legally withhold them. Request the transfer process in writing before giving notice.
- **Email and data** held in Microsoft 365 or Google Workspace remains your property. Your new provider can assist with migration — ensure your existing provider grants access.
- **Contract notice periods** vary — typically 30 to 90 days. Check whether there are auto-renewal clauses that require notice before a specific date.
- **Documentation** about your own environment — passwords, configurations, network diagrams — belongs to you. Request full handover documentation as part of your exit.

KEY PRINCIPLE

The best time to plan a transition is before your contract renews. Most providers require 30–90 days' notice — and many auto-renew if that window is missed. Set a calendar reminder three months before your renewal date.

Use this checklist when evaluating any IT provider proposal. Each item represents a minimum standard for an accountancy firm in 2027. If a prospective provider can't confirm any of these, ask why.

Security Fundamentals

- [ ] Managed EDR on all devices (not just antivirus)
- [ ] MFA enforced across all Microsoft 365 accounts
- [ ] Email filtering and anti-phishing configured
- [ ] Immutable, tested off-site backups
- [ ] Patch management automated
- [ ] Cyber Essentials pathway confirmed

Microsoft 365 Management

- [ ] Microsoft Secure Score actively managed
- [ ] Conditional Access policies configured
- [ ] Defender for Office 365 fully activated
- [ ] SharePoint governed and structured
- [ ] Guest access reviewed regularly

Support & Response

- [ ] Defined P1/P2/P3 SLA commitments in writing
- [ ] UK-based support desk confirmed
- [ ] Out-of-hours cover for critical incidents
- [ ] Named account or customer success manager

Commercial & Contract

- [ ] Onboarding cost clarified (included or separate)
- [ ] Licence costs itemised separately
- [ ] Contract exit and notice period confirmed
- [ ] Auto-renewal terms understood
- [ ] Project/consultancy day rate confirmed

Sector & Compliance

- [ ] GDPR/ICO data processing agreement available
- [ ] Experience with Xero, Sage, CCH, or IRIS
- [ ] MTD compliance support confirmed
- [ ] References from similar-sized accountancy firms

Strategic & Forward-Looking

- [ ] Regular IT strategy or roadmap reviews offered
- [ ] Phishing simulation and staff training available
- [ ] AI / Copilot readiness assessment offered
- [ ] Virtual IT Director / CISO option available

ABOUT NETMONKEYS

IT that works as hard as your practice does

NetMonkeys is a UK-based managed IT and cybersecurity provider with over 15 years of experience helping SMEs and professional services firms operate securely and efficiently.

What we do for accountancy firms

Managed IT Support · Cybersecurity & EDR · Microsoft 365 management and governance · Cloud migration · Phishing simulation and security training · Virtual IT Director · AI & automation planning · Cyber Essentials Plus readiness

Why firms choose us

UK-based engineers. Named account managers. Sector-relevant experience. Commercial honesty. We'll tell you what you need and — importantly — what you don't. No upselling. No long-winded onboarding.

15+
Years delivering IT services to UK businesses

12
UK cities with active clients and on-site cover

95%
Client retention rate over the past three years

24/7
SOC monitoring and security operations

MICROSOFT SOLUTIONS PARTNER

NetMonkeys holds Microsoft Solutions Partner status — recognised across Modern Work, Security, and Infrastructure. This means our team is independently certified to the highest standards in Microsoft 365 deployment, security configuration, and Azure infrastructure management.

Ready to talk to someone who actually understands accountancy practice IT?

Whether you're reviewing your current setup, preparing to switch, or simply want an independent view of where your IT stands — a 30-minute conversation with our team costs nothing and comes without obligation.

0161 834 9345 · 0115 822 1860 · contact@netmonkeys.co.uk · netmonkeys.co.uk