CSC

# How To Choose An IT Support Provider (UK)

*Reducing risk, avoiding lock-in, and choosing IT support with confidence*

**Prepared by**

**Computer Support Centre**

https://computersupportcentre.com

# How to choose an IT support provider (UK)

## Executive Summary

- IT support is a business decision, not a technical one.
- UK SMEs are often confused about their IT support needs and therefore pay too much or specify their IT support incorrectly.
- There are many different types of IT support models, and each will work differently for each organisation.
- Security, documentation and exit plans are just as important as the response time of your IT support provider.
- A quality IT support provider will reduce risk and friction in your business, they will not create dependency.
- Contractual agreements and pricing models are extremely diverse, and you must understand them before entering into an agreement.
- The quality of the onboarding process is a good predictor of the future quality of IT support.
- You should know how to exit your IT support provider safely.
- This guide gives you a neutral framework, it is not a sales pitch.

How to Find the Right IT Partner
Assess capabilities, support and fit to choose the best vendor for your business.
Security and credentials
Daily support and help desk
Business goals alignment
Align tech with business goals
Verify support, skills and service
Compare quotes and long-term fit

## This guide was developed specifically for:

- Small and medium-sized enterprises (SMEs) in the United Kingdom employing 5–250 personnel
- Owners/directors; Operations Managers; Practice Managers; non-technical decision-makers within an organisation

- Small/mid-size enterprises considering primarily managed IT support for the very first time, or those reviewing their current IT support
- Small/mid-size firms who employ cloud-based applications (e.g., Office 365; Google Workspace) and have mixed workforces with some employees working in a traditional office environment and others telecommuting

## This guide will NOT be relevant to:

- Large, multinational organisations with sophisticated, global IT infrastructures that are staffed by dedicated teams responsible for managing internal cybersecurity, and with dedicated legal support or resources to provide guidance on contract-related issues, and/or regulatory compliance obligations
- Highly specialised sectors (such as large-scale, 24/7 manufacturing operations; or oil and gas extraction) where organisations will require sector-specific technical consulting.

## Overview: what IT support covers

IT Support includes much more than simply "fixing computers". Typically for most small & medium-sized businesses (SMEs) in the United Kingdom, IT Support will generally cover 4 areas by a competent IT Service Provider:

1. **Reactive IT Support (Helpdesk Service):**

Fixing Issues e.g. Email Issues, Slow Computer Performance, Printer Problems, Account Access, Teams Issues, etc., as well as answers to Basic Queries "How Do I...?"

2. **Proactive IT Maintenance:**

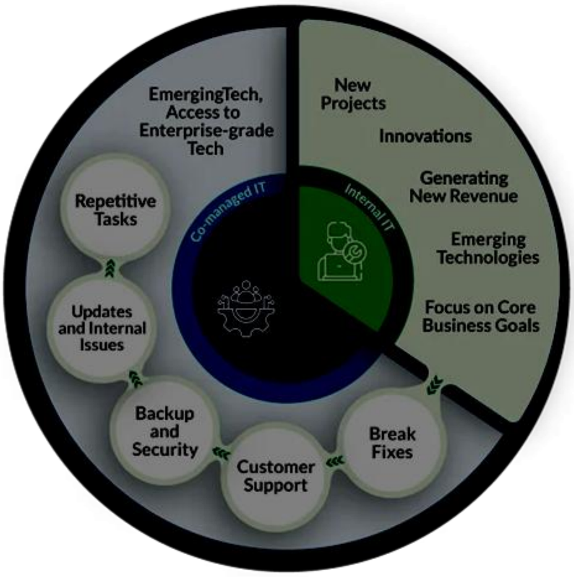
Keeping IT Healthy; e.g. Patching, Check Devices, Back Up, Monitor Alerts, Check Licences, Regular Admin.

3. **Preventative & Responsive IT Security:**

Mitigating Risk; e.g. Multi-Factor Authentication (MFA), Endpoint Protection, Controls Against Phishing, Vulnerability Management, Basic Steps To Handle An Incident.

4. **Strategic IT Planning & Governance:**

To help you avoid surprises; e.g. Lifecycle Planning, Budget Guidance, Risk Review, Vendor Management, Documentation.



A common mistake some SMEs make when they purchase IT Support is that they only purchase IT Helpdesk Support (i.e. fixing Issues) or IT Maintenance & do not realise that they must also provide support for Security, Back Up, Project Management & Compliance in addition to purchasing a Helpdesk or IT Maintenance Support service.

## Types of IT support models

| Model | How it works | Best for | Watch-outs |
|---|---|---|---|
| Break/fix (ad-hoc) | You pay when something breaks (hourly/day rate) | Very small, low-risk, stable setups | Can become expensive and reactive; little prevention |
| Managed IT (outsourced MSP) | Fixed monthly fee (often per user) covering support + maintenance | Most SMEs who want predictable cost and proactive care | Must confirm what's included; avoid tool-heavy oversell |
| Co-managed IT | Shared responsibility between your team and provider | SMEs with internal IT who need extra capacity/expertise | Requires clear boundaries and good documentation |
| In-house vs outsourced | Internal IT staff, outsourced, or hybrid | Larger SMEs, compliance-heavy, multi-site | In-house still needs specialist partners for security/projects |

The percentage quotes for managed support are generally per user per month for typical managed support and depending on the scope of the business and risk profile you will find some managed support from approximately £30 to approximately £120+. Commonly, break fix rates are quoted in the range of approximately £45 to approximately £150 per hour, depending on urgency and skill level needed.

## Step-by-step provider selection framework

### Step One: Create Your "Must Haves" (Before Talking to Providers)

- How many users/devices do you need? Sites? Remote Workers?
- What are Your Critical Systems (M365, Finance, CRM, Line of Business Applications)?
- What is Your Risk Profile? (e.g. Client Data Sensitivity, Downtime Impact, Insurance Coverage)
- What are Your Desired Outcomes? (e.g. Less Interruptions, Faster Onboarding, Better Security, Predictable Expenses)

**Output**: A one-page requirement list.

## Step 2: Shortlist 3–5 providers (avoid endless shopping)

**To create your shortlist:**

- Ask for recommendations from local businesses and verify that the provider is a good fit for you.
- Look for providers who have experience in your specific field, such as professional services or retail.
- Review company's reviews to identify trends and make an informed decision.

**Rule:** shortlist providers who can clearly explain *how* they work, not just what they sell.

## Step 3: Use a consistent question set (same questions to all)

**Ask for:**

- A sample of their typical monthly report.
- An example of an onboarding plan they typically provide to their clients.
- A list of what is included and excluded in their current service offering.
- Steps for escalating an issue to higher management when necessary.
- The owner of the administrative access to your account should you choose to work with them.

**Output:** comparable answers.

## Step 4: Do a paid discovery (if your environment is complex)

If you have a multi-site or compliance-related environment (more than 25 users), doing a paid discovery can help ensure that you do not sign into a wrong-fit contract.

The **output** of this step should include: the scope is clear, known risks have been identified, and the plan for the migration/onboarding process is documented.

## Step 5: Pilot and check references (especially service experience)

It is recommended to contact 1–2 reference clients who are similar in size and type of business as you are; ask them questions such as: "What happens when things go wrong?" Look for a reference client's response time from your service desk and if they are clear on the steps needed to resolve issues.

## Step 6: Choose based on fit + transparency, not promises

Pick the provider who:

- Honest Information About Trade-offs
- Proper Documentation
- A Security Bench Mark
- Clear & Concise Reporting
- An Exit Strategy

## Full comparison checklist (6 required sections)

For each area you will find the following:

- Why is it important?
- What questions do you need answered?
- What does good imply; What constitutes a warning sign?
- -Mistakes commonly made by prospective buyers.

## 1) Understanding your business needs

### Why it is Important?

If you haven’t defined your needs, you are going to just buy whatever the Provider is good at selling, not what meets your true needs; therefore, a good Provider will help push you to clarify your Priorities.

**Questions to Ask:**

- What are the ideal Size/Scope of the Clients you support? 5-25 Clients, 25 -100 Clients, 100-250 Clients
- What types of industries do you typically support, and how have you seen things go wrong for them?
- How do you customise the Support for Remote and Hybrid Teams?
- How do you assess your Risks and order your Priorities for Improvements?

### What does Good Look Like Compared to Warning Signs?

**How to gauge GOOD:**

- A good provider asks you questions about your Business Goals, the impact of downtime, and sensitivity of your Data.
- A good provider will explain what the recommended Minimum Viable Configuration is and why.
- A good provider will offer you a realistic phased plan.

### How to gauge WARNING SIGNS:

- A warning sign is when a provider is offering a service to you but hasn't first asked you any questions to understand your needs.
- A warning sign is that the provider avoids talking about what they do with Risks, Backups and how they handle Incidents.
- A warning sign is when a provider Cannot explain to you what they mean by Typical Onboarding.

### Common Mistakes Buyers Make:

1. Purchasing the lowest quote without first defining the scope of the Work.
2. Assuming that all MSPs will produce the same results.
3. Not including Operations and Finance until later in the Vendor Selection process. (After then wouldn't feel the effects of Downtime).

## 2) Scope of services & exclusions

### Why it is Important?

A primary cause of disappointment among clients is the incorrect assumption that everything discussed in a given project will be included in the total amount (see also misunderstandings between Client and Supplier).

Managed Security Services
Allows You to Focus on Your Business
Superior Protection
Advanced Technology
Rapid Response
Manage Risk and Compliance
Reduces Your Costs

### Questions to Ask:

- What is included in my monthly fee (e.g., monitoring, support, backed up data, security tools)?
- What is not included in my monthly fee (e.g., on-site visits, add new users, vendor liaison work)?
- Do you support third-party applications (line-of-business) and printers?
- What are your standard limits on service (fair use)?

## What does Good Look Like Compared to Warning Signs?

**How to gauge GOOD:**

- Written communications clearly outlining what is/what is not included
- Full transparency on pricing for work that falls outside the scope
- A well-defined project process includes estimates

## How to gauge WARNING SIGNS:

- Vague statements of "everything's included"
- There are no exclusions written into the document
- Unexpected/frequently occurring fees associated with routine services

## Common Mistakes Buyers Make:

- Buyer not reading through the schedule of services
- Buyer failing to ask what costs will be incurred for getting started and completing a project
- Buyer assumes that Cybersecurity was automatically included

# 3) Security & compliance approach

## Why it is Important?

Cyber incidents can halt trading, even if you are not regulated. Security should be the standard baseline, rather than an 'up sell' following the incident.

## Questions to Ask:

- What is the default security baseline of your Company for any SME (MFA, Patching, Endpoint protection & Backup)?
- How do you monitor for suspicious logins or malware?
- What is your incident response procedure (1st hour, communication, evidence)?
- Do you meet the Cyber Essentials standard for alignment (if applicable)?
- How do you manage administrative access and privilege?

## What does Good Look Like Compared to Warning Signs?

**Good Signs:**

- Default MFA, Least Privilege, Patching Cadence, Monitored Alert Notifications.
- Defined Incident Response Steps and Communication Plans.
- Periodic Security Reporting (even light).

## How to gauge WARNING SIGNS:

- Antivirus is 'good enough' Mindset.

- No Defined Incident Response Plan.
- Security is an Optional Addition with no Standard Baseline.

### Common Mistakes Buyers Make:

- Assuming Microsoft 365 Provides Security and Backup. (It Doesn't)
- Not Asking Who Monitors Alerts and How Fast They React.
- Not Verifying How Backup Is Tested.

## 4) Support responsiveness & SLAs

### Why it is Important?

Support response time can negatively affect downtime within a company and create frustration for employees, negatively impacting your customers as well.

SLAs are only as useful as the realism of the goals stated within them and whether those goals can be measured.

### Questions to Ask:

- What hours do you provide support? Do you have support during UK business hours or do you have a 24/7 option?
- What do you target for your response times broken down by Priorities 1, 2, and 3?
- How do you escalate an issue that is stalled?
- What percentage of issues are resolved on the first contact with support?
- Who is the Service Manager / Escalation Point of Contact?

### What does Good Look Like Compared to Warning Signs?

Good Looks Like:

- Well defined priority categories including what is P1 (Priority 1).
- Performance is measured and there is a clear method for reporting those measurements.
- Escalation options do not require excessive effort by the user.

### How to gauge WARNING SIGNS:

- SLAs that are vague and only say “quick response.”
- No clearly defined escalation structure.
- Over-promised SLA numbers.

### Common Mistakes Buyers Make:

- Buyers rely solely on SLA number comparisons without assessing the scope of services included or number of support staff available.
- Buyers fail to determine what Urgency means to their organisation internally.

- Buyers ignore support response time expectations for multi-site installations.

## 5) Tools & technology stack

### Why it is Important?

Many tools provide businesses proactive user support, visibility and documentation, however many companies and/or businesses acquire too many tools. Thus tool overload makes it difficult to manage.

### Questions to Ask:

- What types of remote support and monitoring tools are used by the business (or partner)?
- Does the partner provide visibility through customer portals, reporting, Asset Lists, etc.?
- How does the partner provide documentation (i.e., password management vaults, architecture diagrams, run books, etc.)?
- Does the partner have standardised Microsoft 365 Security Settings?
- Will the business's support or service be impacted by the partner changing tools?

### What Is A Good Technology Tool/Technology Platform?

- A good technology tool will be a standard stack (and supported by a clear reason/use case).
- A good technology tool will provide access to product/service documentation as part of their support service.
- A good technology tool will ensure you have access to all of your critical information needed to perform your job/

### How to gauge WARNING SIGNS:

- Too many tools with no clear value proposition or benefit to you as a customer.
- You do not have access to product/service documentation or products/assets.
- You will only be granted administrative access/passwords by the providing company/partner.

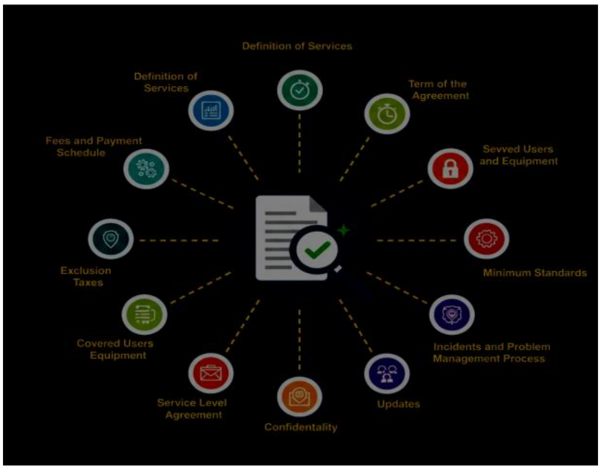
### Common Mistakes Buyers Make:

- Selected a technology tools because of the quantity of tools being used.
- Did not ask about the location of documentation.
- Did not ask for shared admin access/credentials.

## 6) Pricing models & contracts

### Why it is Important?

The way you operate should dictate your approach to pricing. Consider how the way you run your business impacts the headcount of users, the mix of devices and risk levels you are managing. The contract should protect both parties from unexpected events and not create a situation where either party has no way to exit the agreement.



## Questions to Ask:

- What is the pricing structure (per user, per device or hybrid)?
- What does the fee include (tools, licenses, backup services) and
- What is the minimum contract term and is there an exit clause?
- How does the annual increase work?
- What is the procedure if we wish to add or remove users while under contract?

## What does good look like vs. what are the warning signs?

**Good**: A clear explanation of pricing; a separation of the support fee from the third-party license fees; a reasonable term with a reasonable exit process.

**Warning Signs:** Long-term commitments without justification; Unclear response to annual increases; Bundles that do not disclose true costs.

## Common Mistakes Buyers Make:

To compare quotes without fully understanding what is included in each quote; not separating the cost of 'support.' (Support includes service level agreements, help desk support etc.) and 'license/security tools', and not allowing a long enough period of time to assess the quality of service before committing to a contract.

# Red flags & warning signs (quick list)

- Scope Synecdoche (i.e., “All Things”) – Failure to document what is excluded from the contract.

- Onboarding / Documentation Deliverables are non-existent.
- Provider wants to be only Super User/Admin for your systems.
- Security is optional with no minimum requirements.
- No Reporting, Reviewing or Transparency.
- Lengthy Contracts lack proper Break Clause, unclear Uplift.
- Excessive Jargon & Lack of capability of providing non-technical Leaders with simple explanations.
- Lack of an escalation chain – service owner not defined.
- Engineer/account Manager frequently changing.
- Follows a “one-size-fits-all” mentality with no consideration for the risk profile of your business.

## 90-day onboarding expectations (what “good” looks like)

### Discovery and Stabilisation (Days 1-15)

- Inventory of all assets (users, devices, major systems and applications).
- Review of access (Admin accounts, Multi-Factor Authentication, risks from 'leavers').
- Quick-fix activity to put in place (MFA, critical patches, identified security vulnerabilities).
- Confirmation of backup coverage and proof of ability to perform basic restoration.
- Alignment on priorities and communication methods.

### Baseline and Documentation (Days 16-45)

- Use of Standard Configuration Baseline for devices where possible.
- Visibility of endpoint protection and monitoring of endpoints.
- Documentation created/updated to reflect network diagrams, tenant notes and password vaults.
- Review of ticket trends and fixing recurring issues at their source.
- Alignment on service delivery cadence (monthly reporting and quarterly reviews).

### Optimisation and Planning (Days 46-90)

- Establishing a Patch Compliance and Backup Testing Rhythm.
- Prioritisation of Security Improvements (email security, conditional access where needed).
- Aligning on Business Continuity basics (what is most important first).
- Development of Budget and Lifecycle Plan (12 month view).
- Exit Readiness, confirm you have access and documentation.

## FAQs

- **Do we want managed IT or ad-hoc support?**

If downtime or security incidents would hurt trading, managed IT is usually the most predictable and preventative route. Conversely, break/fix is often better suited to smaller, lower-risk organisations.

- **How long should an IT contract last?**

Most SMEs will choose an IT contract lasting from between 12 and 36 months. Contracts longer than this can work if the scope is clear, service has been proven to be effective, and exit terms are reasonable.

- **If we want to switch IT providers, what is the process?**

A solid provider will have an exit process, which includes: documentation handover, credentials transfer, and transition support. We should continue to have access to administrative rights for our systems and data.

- **Will IT support include Cybersecurity?**

In 2026, it is reasonable to expect an established baseline which includes: Multi-Factor Authentication (MFA), Patching, Endpoint Protection, Backups, and a Basic Incident Process. However, the inclusion of deeper level Cybersecurity will likely be at an additional cost.

- **What is the difference between per user pricing or per device pricing?**

Per user pricing mirrors how people consume IT Services, whereas, per device pricing accommodates for device-heavy environments. Hybrid pricing models are now prevalent.

- **Is it appropriate to include the cost of Microsoft 365 licences in the overall cost of support services?**

Occasionally it is, but it is important to understand what the difference is between the cost of support versus the cost of third-party licensing. Transparency is more important than bundling.

- **What arethe components of an SLA?**

An SLA typically defines the support hours, response time targets by priority levels, the escalation path, and how performance will be measured and reported.

- **Can we keep some IT in-house?**
  Yes…...co-managed IT works well when roles are clear and documentation is shared.

## Final soft CTA (not a hard sell)

If you're looking for a neutral IT support "fit check" before selecting an IT provider, a sensible assessment would typically include:

- Your current risk exposure (access controls, patching, backups and email security).
- An outline of what you should include in scope versus what should be kept as a project.
- A shortlist of potential providers with a scorecard to compare the providers against one another.
- Key contract clauses to clarify (ownership and access rights, and exit processes).

- A 90-day onboarding outline so you know what a reputable provider will do for you.

No pressure, just a clearer decision with fewer surprises later on.

## About this guide

This guide has been produced by **Computer Support Centre**. We are an IT Consultancy based in the UK and focus on small to medium sized businesses and helping them with improving their IT system reliability, security and overall day to day operations using Technology more effectively.

The purpose of this guide is to support non-technical business owners and managers to understand what is considered as good IT Support, the various different types of IT Support options available, and how to select an IT Support provider that is a true match for their business's needs.

The aim of this guide is not to promote a specific provider or service but rather to provide a UK SME's with a clear set of tools to assess their business's needs and requirements, formulate more relevant questions regarding IT Support options, avoid common pitfalls or mistakes when selecting an IT Support provider and feel more comfortable making IT related decisions.

If you learn more about **Computer Support Centre**, our services, and our approach, please visit our official website:
□ **https://computersupportcentre.com**

## Conclusion

Selecting your IT support provider, while perceived frequently as a technical decision, is in fact, a business decision.

The ideal IT support partner will help you mitigate risk, develop your business and provide clarity instead of complexity to your operations and processes.

A proper review of your current objectives; and comparing these with many available Providers, will enable a small-medium business (SME) within the UK to create a sustainable and secure IT environment and avoid future unnecessary expenses.