The Most Essential Outsourced IT Support Checklist

18 Critical Things a Non-IT Manager or Director Should Expect from Their Outsourced IT Partner (MSP)

If you're not an IT professional but carry responsibility for your organisation's IT, it can still work well. You can successfully manage the function with the right information and support. Without it, you are undoubtedly carrying a risk. **See how your current IT provision stacks up.**

The questions below were compiled during 20 years of IT audits. Documenting the biggest issues other non-IT Managers experienced when their support partner was not delivering effective IT or they experienced a Cyber Security breach.

Use this checklist to rate your IT Support.

breathetechnology

support | cloud | security | infrastructure | comms

THE MOST ESSENTIAL OUTSOURCED IT SUPPORT CHECKLIST

For Non-IT Managers Responsible for Outsourced IT

PASSED ☐ FAILED ☐

1. Proactive IT Monitoring and Maintenance

What to Look For:

- ☐ 24/7 monitoring of systems for threats, performance issues, and downtime.
- ☐ Regular maintenance to prevent problems before they arise.
- ☐ The critical control here is that you should receive a regular monthly report, showing evidence and ensuring that there is structure and consistency.

Warning Signs:

- ☐ You only hear from your provider when something breaks.
- ☐ Unplanned downtime with no root cause analysis.
- ☐ You receive no report. This means you have no evidence the work is being done.
- ☐ You don't receive a report meaning there is no structure or consistency, putting you at risk.

PASSED ☐ FAILED ☐

2. Transparent and Predictable Billing

What to Look For:

- ☐ Clear, all-inclusive pricing with no hidden fees.
- ☐ Itemised, transparent pricing
- ☐ Detailed monthly reports showing where your budget is being used.
- ☐ You have a clear understanding of your annual and monthly renewable licensing.

Warning Signs:

- ☐ Surprise charges for "extra" services that were never discussed.
- ☐ A lack of visibility into what you're actually paying for.
- ☐ You get caught off-guard with expensive licensing for the following year that you weren't expecting.
- ☐ You're not sure if the licensing, such as Office 365, is the correct license type or if you're paying for unused licenses.

PASSED ☐ FAILED ☐

3. Cyber Security Expertise

(Not every IT provider is a Cyber Security Expert)

What to Look For:

- ☐ Cyber Security is your single biggest risk and we are all at high risk of an attack.
- ☐ Have you ever seen their credentials?
- ☐ Robust protection against ransomware, phishing, and data breaches.
- ☐ Regular security updates, patching, and vulnerability assessments.
- ☐ Are you Cyber Essentials certified? It's the government recommendation for SME Businesses and schools. It means that you are being externally vetted to have the right security policies in place.

Warning Signs:

- ☐ No documented security policy or response plan.
- ☐ You are not aware of what your security posture is.
- ☐ There is no documented and communicated Cyber Security Policy in place.
- ☐ Vague assurances like "you're protected" without clear evidence.
- ☐ You've never had a Cyber Security Audit or Pen Test.
- ☐ There is no evidence of a Cyber Security framework that has been implemented.

PASSED ☐ FAILED ☐

4. Strategic IT Advice and Planning

What to Look For:

- ☐ An IT roadmap, Strategy or Plan aligned with your business goals.
- ☐ Regular meetings to review IT performance and plan for future needs. With your Account Manager and Technical Lead.

Warning Signs:

- ☐ Your IT feels reactive, not strategic. If you haven't planned with them or seen a document, it's not strategic.
- ☐ No updates on how technology can reduce costs or improve efficiency.
- ☐ You have no plan.
- ☐ There have been no recent meetings where to discuss your personal and organisational goals

PASSED ☐ FAILED ☐

5. Fast and Reliable Support Response Times

What to Look For:

- ☐ Clear service level agreements (SLAs) with guaranteed response times.
- ☐ Rapid resolution for critical issues affecting your operations. Slow response to tickets logged or days waiting for something to be resolved.
- ☐ They are addressing the problem intermittently, rather than resolving it quickly and efficiently.
- ☐ The fixes are sticky plaster fixes, not real resolutions and often involve workarounds.

Warning Signs:

- ☐ Long waits for help-desk responses or issue resolution.
- ☐ Excuses for delays without accountability.
- ☐ Issues are not properly fixed.
- ☐ Often fixes or projects, seems like it's the first time they have done it and you're a guinea pig.

PASSED ☐ FAILED ☐

6. Backup and Disaster Recovery Plans

What to Look For:

- ☐ Regularly tested backups and a documented disaster recovery plan.
- ☐ Guaranteed recovery times (RTO/RPO) in case of system failures.

Warning Signs:

- ☐ Uncertainty about when or how quickly your data can be restored.
- ☐ You've never seen a backup test report.

PASSED ☐ FAILED ☐

7. Third-Party Review and Certification

What to Look For:

- ☐ Systems aligned with government advice, such as NCSC (National Cyber Security Centre) guidance.
- ☐ External certifications like Cyber Essentials or ISO27001.
- ☐ Regular external audits to validate your IT security.

Warning Signs:

- ☐ No certifications or external security reviews.
- ☐ Lack of documentation or policies for security and compliance.

PASSED ☐ FAILED ☐

8. Scalability and Support for Growth

What to Look For:

- ☐ Systems and services that can grow with your organisation's needs.
- ☐ Advice on cloud solutions, automation, and process improvements.
- ☐ Getting the most out of platforms such as Office 365.
- ☐ Regular account reviews where we discuss your goals for the business. It then becomes a supporting function and enabler.

Warning Signs:

- ☐ Your IT feels "stretched" as your organisation grows.
- ☐ No discussion of future-proofing your systems.

PASSED ☐ FAILED ☐

9. User Training and Awareness Programs

What to Look For:

- ☐ Regular training sessions for staff on Cyber Security and software use.
- ☐ Tools to help employees be more productive and secure.

Warning Signs:

- ☐ Frequent user errors causing IT issues.
- ☐ Employees are unaware of phishing risks or best practices.

PASSED ☐ FAILED ☐

10. Vendor Management

What to Look For:

- ☐ Management of third-party vendors to ensure software and hardware reliability.
- ☐ Handling of vendor support tickets and negotiations on your behalf.

Warning Signs:

- ☐ You're left managing IT vendors on your own, or going between them to co-ordinate.
- ☐ Confusion about who to contact when things go wrong.
- ☐ They don't take responsibility and blame each other.

PASSED ☐ FAILED ☐

11. IT Management Reporting

What to Look For:

- ☐ A monthly management report covering key system maintenance, security updates, and issues resolved. Providing evidence that the work is being done and giving you peace of mind.
- ☐ Clear evidence that critical maintenance tasks are being completed.

Warning Signs:

- ☐ Reports are vague or non-existent.
- ☐ You have to "assume" maintenance is being done without proof. This is incredibly risky.

PASSED ☐ FAILED ☐

12. IT License Management

What to Look For:

- ☐ Regular reviews of licensing to ensure compliance and cost-effectiveness.
- ☐ Optimisation of licensing models to avoid over or under-licensing.
- ☐ Tracking of licensing included as part of the monthly IT Management Report.

Warning Signs:

- ☐ Unexpected license costs or fines.
- ☐ Features or functionality missing due to poor licensing decisions.
- ☐ You've never checked or spoken about licensing.

PASSED ☐ FAILED ☐

13. Service Review Meetings

What to Look For:

- ☐ Monthly or quarterly meetings with an account manager and technical lead.
- ☐ Updates on support tickets, project progress, and your business needs.
- ☐ Both the commercial and technical contact must be present.

Warning Signs:

- ☐ No structured updates or meetings.
- ☐ A lack of understanding of your business goals.
- ☐ You get no real update and/or higher-level overview.

PASSED ☐ FAILED ☐

14. Dedicated Team

What to Look For:

- ☐ A lead engineer, service desk, and account manager assigned to your business.
- ☐ A team that knows you, your team and your setup and works proactively, not just reactively.

Warning Signs:

- ☐ A ticket-based system with no personal accountability.
- ☐ No proactive management or regular contact.

PASSED ☐ FAILED ☐

15. Strategic Alliance

What to Look For:

- ☐ An IT provider that understands your business goals and challenges.
- ☐ Proactive support to align IT strategy with company objectives.

Warning Signs:

- ☐ No conversations about your business vision or goals.
- ☐ IT feels disconnected from your business strategy.

PASSED ☐ FAILED ☐

16. Flexibility in Contracts

What to Look For:

- ☐ Contracts that adapt to your changing business needs and remain relevant.
- ☐ Fair terms that avoid trapping you in a long-term dysfunctional relationship.

Warning Signs:

- ☐ Inflexible contracts that don't reflect current needs.
- ☐ Difficulty making changes to services or terms.

PASSED ☐ FAILED ☐

17. Annual Audit or System Review

What to Look For:

- ☐ Regular audits every 1–3 years to evaluate IT systems and recommend updates.
- ☐ Identification of risks, new technologies, and operational improvements.

Warning Signs:

- ☐ No proactive system reviews or updates.
- ☐ IT feels outdated or unaligned with your business operations.

PASSED ☐ FAILED ☐

18. True Partnership Approach

What to Look For:

- ☐ A team that works collaboratively with your staff, fostering a trusted partnership.
- ☐ Seamless integration of IT services into your company culture and operations.
- ☐ They behave and are seen as an extension of your team.

Warning Signs:

- ☐ An "us vs. them" dynamic with your IT provider.
- ☐ No relationship-building efforts from the provider.

Does Your IT Provider Measure Up?

If you're not receiving a good score on 18 critical services, it's time to re-evaluate your IT support.

Each of these components is critical and needs to be in place.

If you are concerned and would like to discuss these or perhaps consider an IT or Cyber Security Audit, please contact the friendly, knowledgeable team at Breathe today.

Score your Provider:

1 – 5: High Risk & Poor Services – The service is not fit for purpose, and your organisation is likely at risk from failing systems, unsupported staff, and inadequate Cyber Security. There is no plan or strategy in place to achieve operational goals. Real change is required!

6 – 10: Below Average – Significant improvement is required, likely alongside a shake-up of the support relationship to better align with your needs.

11 – 15: Average – Meets basic expectations, but there is still room for substantial improvement. The service is likely reactive, with a need for strategic support and enhanced Cyber Security.

16 – 18: Excellent – This appears to be a valuable, high-quality service that addresses both operational and strategic needs. At this level, IT functions as an enabler, helping you and your organisation achieve your goals.

How did you score?

1 – 5: Extremely Poor	6 – 10: Below Average	11 – 15: Average	16 – 18: Excellent

THE MOST ESSENTIAL OUTSOURCED IT SUPPORT CHECKLIST

For Non-IT Managers Responsible for Outsourced IT

"Our customers value their IT and Cyber Security more than ever. Our ideal customers are SME and mid-market businesses and the education sector.

Ten years ago, most of these organisations had relatively simple IT needs, with limited exposure to advanced technologies like cloud systems and lower risks of cyberattacks. Today, however, the world has changed, and almost every aspect of life has moved online – banking, booking holidays, attending training, shopping, dating, booking hair appointments, and more.

The need for robust IT and strong Cyber Security measures has become essential, regardless of an organisation's size. This also means our customers require excellent support from a trusted partner – someone who not only fixes technical issues but also provides expert advice, proactively manages IT, and helps leadership teams achieve their organisational goals.

Breathe is that partner, offering clearly defined service components to meet these demands and deliver premium IT solutions at the best value."

Craig van Aswegen
MD & Snr IT Management Consultant

Our Managed IT & Cyber Security Support Services

IT Support BASELINE PACKAGE

- Dedicated Technical Engineer
- Dedicated Account Manager
- Project Team
- Level 3 Service Desk
- **Software Tools**
  - Help Desk
  - Remote Support
  - Asset Management
  - Systems Monitoring
- **Consultancy Tools**
  - Network MOT (High Level Audit,
  - Security Review
  - Core Service Report

BOLT-ONS OPTIONS

- Bolt-on 1 – Pre-Scheduled Site Visits
- Bolt-on 2 – Proactive Maintenance Service & Maintenance Report
- Bolt-on 3 – Virtual IT Director / CISO (Chief Information Security Officer)
- Bolt-on 4 – Managed Cyber Security Services
- Bolt-on 5 – 24/7 SOC – Security Operations Centre
- Bolt-on 6 – DPO Services (GDPR)

www.breathetechnology.com
(live chat available)

London	020 3519 0124
Cambridge	01223 209920
Sheffield	0114 349 8054
Suffolk	0144 059 2163

lucy@breathetechnology.com

breathetechnology
support | cloud | security | infrastructure | comms