

The SME IT Service Health Checklist

25 questions every growing business should ask

Use this checklist to spot hidden risk, unclear ownership, supplier gaps, and operational friction in your IT setup. It is designed for growing SMEs that already have IT systems and support in place but want a clearer view of whether those arrangements are reliable, accountable, and fit for growth.

How to use it

Mark each question as Yes, No, or Review. Any No or Review answer is a useful prompt for a focused conversation, supplier review, or 90-day improvement plan.

Systems and critical services

No.	Question	Yes	No	Review
1	Have you identified the IT systems and services that are genuinely critical to daily operations?			
2	Do you know which business processes would stop or slow down if each critical system failed?			
3	Is there a named business owner for each key system, application, or service?			

Supplier accountability

No.	Question	Yes	No	Review
4	Do you have a clear list of all IT suppliers, what they support, and how to escalate issues?			
5	Are service levels, response expectations, responsibilities, and exclusions documented for each supplier?			
6	Do you review supplier performance regularly using evidence, not just anecdotal feedback?			

Cyber and access control

No.	Question	Yes	No	Review
7	Is multi-factor authentication enabled for email, Microsoft 365, remote access, and other critical systems?			
8	Are admin accounts limited, monitored, and separated from everyday user accounts?			
9	Do you have a clear process for approving, changing, and removing user access?			

Backup and recovery

No.	Question	Yes	No	Review
10	Do you know exactly what data and systems are backed up, how often, and by whom?			
11	Have you tested a restore recently, rather than only assuming backups are working?			
12	Are recovery priorities agreed for the systems the business would need first after an outage?			

Joiners and leavers

No.	Question	Yes	No	Review
13	Is there a repeatable process for setting up new starters with the right equipment, access, and guidance?			
14	Are leavers removed from all systems, shared mailboxes, devices, and third-party platforms promptly?			
15	Do movers and role changes trigger an access review, rather than simply adding more permissions?			

Documentation

No.	Question	Yes	No	Review
16	Do you have a current record of core systems, suppliers, contracts, renewals, admin access, and support routes?			
17	Are key IT procedures documented well enough for someone else to follow during absence or crisis?			
18	Is IT knowledge held centrally, rather than depending on one person or one supplier relationship?			

Service performance

No.	Question	Yes	No	Review
19	Do you track recurring incidents, delays, service requests, and common user frustrations?			
20	Are IT priorities agreed with the business, rather than driven only by whoever shouts loudest?			
21	Do leadership teams receive simple reporting on service quality, risks, trends, and improvement actions?			

Business continuity

No.	Question	Yes	No	Review
22	Do you have a practical plan for operating if email, internet, phones, cloud systems, or key suppliers are unavailable?			
23	Have you agreed who makes decisions, communicates updates, and coordinates suppliers during a major IT incident?			

Improvement priorities

No.	Question	Yes	No	Review
24	Is there a realistic 90-day improvement plan for reducing IT risk, friction, cost, or uncertainty?			
25	Are improvement actions owned, prioritised, reviewed, and linked to business outcomes?			

Need a clearer view of your IT setup?

Use your answers to start a practical IT Service Health Check and build a focused 90-day improvement plan for your business.